OO학 석사 학위논문

A Study about Complexities on Digital Currency Investigations

Case of Money laundering and Terrorism Financing (Zimbabwe)

디지털 통화 조사의 복잡성에 대한 연구
짐바브웨의 자금 세탁 및 테러 자금 조달 사례

Luckson Tafadzwa Zvirikuzhe

국제학과 Department in International Studies

법률 정보학 및 법의학 Major in Legal Informatics and Forensic Science

한림대학교 대학원

(Graduate School, Hallym University)

Table of Contents

List of Tables

List of Figures

CHAPTER 1: INTRODUCTION

1.0 Introduction

This research focused on the complexities digital currency has on financial investigations in relation to money laundering and terrorism financing. A case of Zimbabwe. Digital currency in this context is a form of currency that is available only in digital or electronic form, and not in physical form. It is also called digital money, electronic money, electronic currency, or cyber cash. (Adrian, 2018). The background of the study, the statement of the problem, the objectives of the study and the research questions are laid out in detail in this chapter to provide a conceptual foundation through which the research problem for this study can be understood. Study significance and assumptions are also presented and discussed together with the delimitations and limitations encountered during study.

1.1 Background of the study

Although global efforts are being made to standardize, control, and regulate digital currency use, structural issues in developing countries like Zimbabwe, more work is needed to be done especially in capacity building for investigators and provision of the necessary tools and software's introduced in developed countries that are being used for tracking transactions of digital currencies. There are numerous digital currencies in existence as of now but to best demonstrate the level of activity, our attention is on the gest and best-known digital currencies, crypto-currency, and Bitcoin. The non-regulation of digital currency in Zimbabwe gives rise to the use of crypto- currency like Bitcoin, of which trade has remained with peer-to-peer transactions taking place, as this offers users with storage of value, plug foreign currency and liquidity gaps in the financial system since the Zimbabwe dollar is overwhelmed by uncertainty. According to Chainalysis research, fraudulent digital currency platforms received just over $8 million from users in Africa in June 2020 alone and Bednar et al. (2008) nominates that when it comes to digital investigations, the cybercrime scene can exhibit a high amount of complexity and uncertainty and these characteristics add to the challenge’s investigators face for collaborating at an international level Financial Action Task Force (FATF) defines digital currency as a digital representation of either virtual currency or e-money worth to be digitally traded and can operate to store of value and as a unit of account.

In 2018 during launch of Cryptogem in Zimbabwe Capital City, where it offered Bitcoin trading despite the de facto cryptocurrencies ban by the Reserve Bank of Zimbabwe. Melissa Mwale, Cryptogem Global Chief Executive Officer and co-founder, told Bitcoin.com: “Cryptogem Global is a bitcoin trading platform where people around the globe can exchange their local currencies and e-money to bitcoin.” Tawanda Kembo, CEO and founder of Golix, a Zimbabwe-based crypto exchange, told Quartz Africa in 2019 that, “There is little supply compared to demand so all the activity in bitcoin which we are seeing is happening on dark markets instead of exchanges.”

Such use is not bound by any financial regulatory obligation which enforcement of traditional anti-money laundering and terrorism financing practices such as the suspicious transactions reporting and know your customer principles becoming an investigative nightmare. The cryptocurrency exchange Golix took the Reserve Bank of Zimbabwe to court after they tried to shut them down and won, legally declaring that Reserve Bank had no mandate over prohibiting cryptocurrency industry and trading, leaving the Reserve Bank with the only option of closing exchanges bank accounts. Firstly, the author notes that digital currency is the easiest, smartest, and most private way to launder money internationally, mainly sustained by anonymous Bitcoins. Secondly, there is no globally established standard for regulating digital currency exchanges, with many lacking risk, sanctions-screening and anti-money laundering protocols.

Reserve Bank of Zimbabwe (RBZ) deputy director of financial markets and national payment systems Josephat Mutepfa commented that, the bank is in the process of starting to come up with a fintech framework since proper structures in regulation are everything. “The framework, which is a regulatory sandbox, will be assessing the cryptocurrency companies as to how they are going to operate which would ensure that all cryptocurrency companies are properly vetted to meet regulatory requirements.” It is therefore aim of this study to do an analysis on how digital currencies continued use affect investigations modalities that should normally or systematically culminate from the formal requirements like customer due diligence for financial institutions to carry out as envisioned by Financial Action Task Force (FATF) recommendations for anti-money laundering and terrorism financing surveillance measures.

As underlined by Bo Mathiasen, the point person for (UNODC) United Nations Office on Drugs and Crime in Colombia, “the use of new technologies by organized criminal groups cannot be underestimated and has an impact on criminal activities across the spectrum of serious and organized crime. Technology has a fundamental and lasting impact on the nature of crime and development simultaneously". In 2014 ONODC presented a manual basically on detection and investigation of laundering crime proceeds using virtual currencies, to provide practical information for investigators and prosecutors on the detection, investigation, prosecution, and seizure of crime proceeds laundered using virtual currencies. This manual is paramount to be mentioned in this study as it complements the realization that digital currency investigation needs a formalized approach that has clear guidelines to be able to successfully fight money laundering and terrorism financing on these virtual platforms brought by technological advancements. In 2018, it was reported that Zimbabwe’s finance minister Mthuli Ncube said that” their country should treat bitcoin as Switzerland does”. A publication from IT Web Africa quoted him saying, “Zimbabwe should be investing in understanding innovations and often central banks are too slow in investing in these technologies.”

As digital currencies are unrestrained by terrestrial and political borders, a coalition of policy regulatory, law enforcement, banking, and academic collaborators must create global standards to tackle the escalating threat of digital money laundering. To effectively investigate digital currencies, it is paramount to provide the right set of tools and methods to investigators for countering this growing phenomenon because cryptocurrencies like Bitcoin with the use of blockchain technology have allegedly been accused of facilitating money laundering and promoting terrorist financing. Following articulated background, it is the wish of this study to gain deeper knowledge into the landscape of the complications digital currency platforms have on financial investigations in relation to money laundering and terrorism financing looking at a case of Zimbabwe.

1.2 Statement of the problem

Financial regulators are concerned that the nature of digital currency platforms complicates investigating cases of money laundering and terrorism financing. Companies like Golix, Cryptogem believe that digital currencies are a game changer that needs to be embraced in the era of digital society. However, from an investigative perspective it is therefore critical to look at the current notions that surround the resistance of digital currency platforms like virtual assets and how they affect investigations on money laundering and terrorism financing in Zimbabwe.

A case of note is that of Golix Crypto-exchange company whose operations were banned by central authorities in 2018 for allegations of violating financial regulations and further red-flagged all associated bank accounts in Zimbabwe, necessitated by the Financial Intelligence Unit (FIU) that is empowered by law to be responsible for investigating terrorism financing and money laundering cases and since digital currencies have allegedly been accused of playing a facilitation role for financial crimes as an advanced financial system fundamental questions arise, for example, does the current crop of investigators have the know-how in terms of technical expertise to investigate digital currency platforms? What does it mean for investigators that digital currency has capabilities of operating outside normal or traditional financial institutions practices? Is there cooperation when investigating digital currencies as its transactions sometimes cross-country boundaries? Absence of a centrally controlled system makes it easy to facilitate illegal transactions with digital currencies. These are some of the matters that this study seeks to address.

The reality of the problem can simply be exemplified by imagining a Sinaloa drug cartel in Mexico moving millions of moneys on a flash drive, as an alternative of smugglers carrying physical sacks full of dollar bills, which makes this study not a future-state scenario, but a present financial security threat. Digital currencies do not only facilitate money laundering and terrorism, financing but has also far-reaching consequences that allow criminals to buy and sell unlawful goods and services, ranging from weapons to human trafficking, illegal drugs, child pornography, organs, and mercenaries for hire, through darkweb which is a black-market platform of the internet. It is also against this backdrop that this study therefore seeks to have deeper visualization on the characteristics that digital currency has and the relationship with investigating money laundering and terrorism financing from an investigator's point of view making the study one of its kind to attempt on unveiling a subject whose knowledge is still in infancy.

1.3 Research objectives

The broad objective of this research is to analyze the nature of the complexities digital currency has on financial investigations in relation to money laundering and terrorism financing. A case of Zimbabwe. The specific objectives are.

i. To determine specific complexities encountered when investigating digital currencies from a sample of financial investigators.

ii. To investigate how other developing countries who have adopted digital currencies are coping.

iii. To assess any international standards set by developed nations in investigating digital currencies that can also be adopted by developing countries like Zimbabwe.

iv. To recommend action and guidelines to improve the current financial digital currency investigations eco-system.

To achieve these objectives, the study focused on the following questions.

1.4 Research questions

i. What is the nature of digital currencies that create challenges for investigators in Zimbabwe?

ii. Are the challenges the same with other countries? Knowledge about how others are coping prepares for strategy.

iii. Which international standards set can solve these problems? Standards can be away to ensure harmonization for cooperation.

iv. Can capacity building for regulators and investigators in developing countries yield results? Given UNODC program to increase investigators skills on how to trace transactions on digital currency platforms.

1.5 Hypothesis of the study

The hypotheses for the study are that criminal intentions to use digital currencies are based on:

H1: Its nature and expected performance.

H2: The effort put in investigating.

H3: Social influence on fintech developments.

H4: The facilitation conditions.

1.6 Conceptual Framework

Based on the hypotheses of the study, the conceptual framework for the complexities digital currency has on financial investigations in relation to money laundering and terrorism financing. A case of Zimbabwe is presented in **Figure 1.1** below.

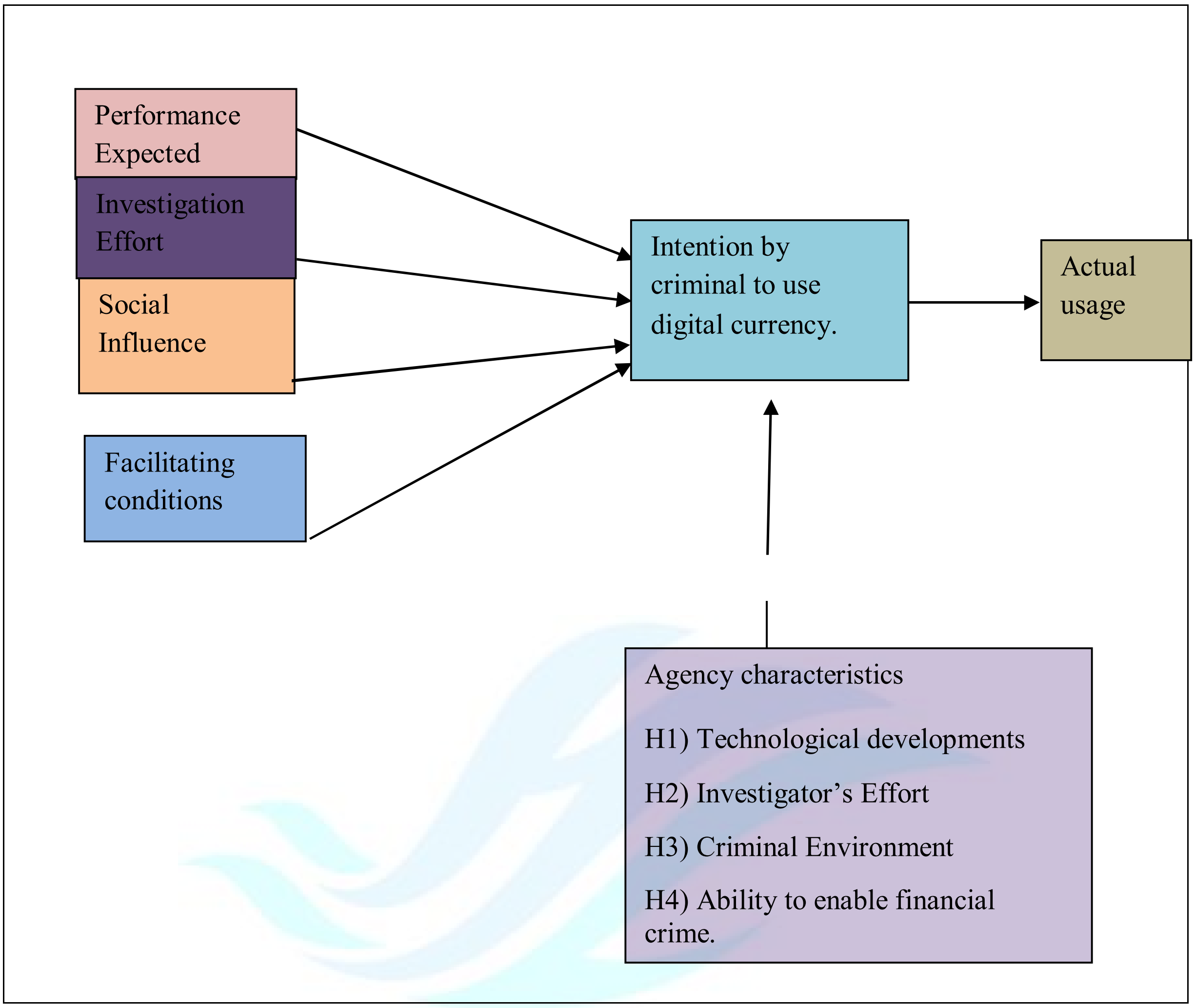

Performance Expected
Investigation Effort
Social Influence
Facilitating conditions
Intention by criminal to use digital currency.
Actual usage
Agency characteristics
H1) Technological developments
H2) Investigator's Effort
H3) Criminal Environment
H4) Ability to enable financial crime.

Figure 1.1: Conceptual framework

Source: Done for this research study

1.7 Significance of the Study

1.7.1 To the student

This research will aid in broadening the researcher's knowledge on the complexities digital currency has on financial investigations in relation to money laundering and terrorism financing. A case of Zimbabwe. Also, this research is in partial fulfillment of the master's degree and for the academic enhancement of the students' knowledge in the field of financial.

1.7.2 To the university

Hallym University being a center of excellence the study will allow the institute to refer to the area of study for future learning purposes. This research will be used by future researchers as reference material for their study. This research shall add on the already existing body of knowledge in academia and in particular, Legal Informatics and Forensic Science department shall be commended for molding such students.

1.7.3 To Institutions

The Reserve Bank of Zimbabwe, Financial Intelligence Unit, Zimbabwe Police and Currency Agencies like Golix Zimbabwe and Cryptogem Global can make use of this study to enhance and fully embrace digital currency through aiding in policy and regulations drafting so as to mold a sustainable financial ecosystem that embrace modern technology by modeling according to international prescribed standards for the adoption of digital currency. This will ultimately give value to Zimbabwe's financial sector considering that digital currency is financial technology advancement is the direction where the world is pointing to.

1.8 Research assumptions

This research on the complexities digital currency has on financial investigations in relation to money laundering and terrorism financing was guided by the following assumptions.

i. Financial investigations about money laundering and terrorism financing on digital currency platforms are complicated.

ii. Despite respondents being bound by confidentiality of information they shall give accurate and unbiased information without exposing their organisations, and all questionnaires will be answered and returned.

1.9 Study delimitation and limitations

The researcher is currently based in South Korea and upon vacation break visited Zimbabwe to carry out the study in Harare the capital city where Financial Intelligence Unit agents are headquartered and Commercial Crimes unit with the Zimbabwe Republic Police. Targeted population are financial investigation analysts and compliance officers within the financial intelligence community responsible for money laundering and terrorism financing cases, digital currency users and Serious Crimes investigators. The study confined itself to the period 2017 to date because this assisted in evaluating the trend of the digital currency opinions that has been given over the stated period and this is the period where organizations and individuals increased adopting digital currency. More so, the choice of this period was to assist in the use of recent data to confirm results of prior studies.

The limitations of the study which were grouped into methodological, financial, and theoretical limitations. Due to the sensitive and interesting nature of the topic, some respondents were at first reluctant to participate.

The researcher assured respondents of privacy of interviews, their responses were going to be regarded as not breaching secrecy act, and the researcher elaborated to the respondents that their responses were going to be used for academic purposes only. Lack of adequate knowledge about digital currency by some respondents to respond fully to questions affected this research study. Meanwhile the researcher explained the questions to respondents. There was lack of proper finance. The researcher also decided to plan his time well to complete the research at the required time. Then the researcher sacrificed his time to keep the research as the priority and finally he went well with the deadline, and he finally met the deadline. However, the researcher asked for financial assistance from his friends and workmates.

1.10 Structure of the study

Table 1.1 below presents the structure of this study on the complexities digital currency has on financial investigations in relation to money laundering and terrorism financing. A case of Zimbabwe

CHAPTER	DETAILS
1	BACKGROUND AND INTRODUCTION
2	LITERATURE REVIEW AND THEORETICAL FRAMEWORK
3	STUDY METHODOLOGY
4	RESULTS ANALYSIS AND PRESENATION
5	RECOMMENDATIONS AND CONCLUSIONS

Source: Prepared for this study

Chapter 1 is composed of study background, problem statement, objectives of research, questions to research, and study assumptions, its significance, limitations encountered, and definitions of key terms, scope of the study and structure of the study.

Chapter 2 will present the literature review of the study guided by objectives of the study such as to determine specific complexities encountered when investigating digital currencies from a sample of financial investigators, document how other developing countries who have adopted digital currencies are coping, assess any international standards set by developed nations in investigating digital currencies that can also be adopted by developing countries like Zimbabwe and recommend action and guidelines to improve the current financial digital currency investigations eco-system and will also present theoretical framework of the study.

Chapter 3 is on the methodology of the study. The research design is introduced in this chapter. More precisely, the processes of both data collection and the approach stand out clearly, as distinct phases of the research are described. The research philosophy, the research strategy, research design, targeted population, sample size, sampling method, research instrument, data collection procedure, data analysis and presentation methods, reliability and validity, ethical considerations will be laid out.

Chapter 4 will present and analyse data collected in relation to this research study on the vulnerabilities of digital currency on financial investigations relating to money laundering and terrorism financing. Presentation and analysis of the data collected is the most important aspect on this chapter.

Lastly, chapter 5 of this Thesis offer the conclusions and recommendations of the research study.

1.13 Chapter summary

This research is on the complexities digital currency has on financial investigations in relation to money laundering and terrorism financing. A case of Zimbabwe. This chapter discussed the background of the study, statement of the problem, conceptual framework, research objectives, and research questions, scope of the study, significance of the study and limitations of the study. The following chapter will present the literature review of the study which will be guided by research objectives of the study.

CHAPTER 2: LITERATURE REVIEW

2.0 Introduction

This chapter presents literature related to this study to fully comprehend the fundamental aspects which are digital currency platforms and investigations thereof, also guided by previous studies in line with objectives of the study which are to determine specific complexities encountered when investigating digital currencies from a sample of financial investigators, determine how other developing countries who have adopted digital currencies are coping, highlight some international standards set in investigating digital currencies that can also be adopted by developing countries like Zimbabwe and recommend action and guidelines to improve the current financial digital currency investigations eco-system. It also presents theoretical frameworks of the study specifically looking at criminology and technology adoption theories for the purposes of analyzing the crucial subject matter.

2.1 Crypto-Currencies

Crypto currency is a subgroup of digital currencies, is either controlled by centralized institutions or can operationalized through a decentralized network Trautman (2014). According to Karlstrom (2014) asserts that, decentralized currency schemes try to avoid central financial institutions as much as possible and are constructed on a network of transaction associates. If the transaction partners can see each other, they can form up trust grounded on their performances. However, according to Bryans (2014), a centralized currency system, one institution monitors the digital currency, which guarantees that the digital coins can be traced back to fiat currencies or rather used to buy and sell digital goods. For example, the Linden Dollar is a centralized digital currency, with Linden Lab being the issuer. It has some features of fiat currencies just like in the formal money system; a central bank serves as a source of trust for any transaction. Furthermore, Bryans (2014) explains that cryptographic algorithms produce cryptocurrency as a digital token. It is then carried on cyberspace using protocols like peer-to- peer networking. Its value is mainly determined by the demand and supply for the tokens and the significant part of their application exist within the system that is decentralized in which they belong. Harvey (2015) cited benefits that comprises of comparatively inexpensive cost of production, reduces inflation risks, bold security features, comfort of usage on mobile devices and broadcasting through the block chain transmission protocol. Its non- reliance on formal financial institutions that verify and guarantee a transaction, cryptocurrency transactions are confirmed by the user's computers registered on the currency's network. Since the currency is protected by encryption codes, it becomes highly unlikely to upsurge the money supply over a predetermined algorithmic frequency.

Cryptocurrency is basically a digital asset used as a medium of exchange (Chohan, 2017) that is equipped with a cryptographic algorithm to secure or control the flow of transactions in effort to prevent double-spending and the issuance of new units in effort to maintain its limited supply. The idea of cryptocurrency can be traced back to 1983 when David Chaum published a paper titled Blind Signatures for Untraceable Payments. In that paper, he raised a concern about the privacy issue of payment system where the identity of the payee and the information of the transaction can be obtained by a third party. Thus, he proposed an automated payment system with cryptography mechanism that prevents information theft by a third party while still allows the payee and payer to provide proof of payment or their identity "under exceptional circumstances" (Chaum, 2017). He called the mechanism as blind signature cryptosystems that was basically an extension of the RSA algorithm (Griffith, 2014).

Chaum then established a company called DigiCash in the Netherlands to develop and commercialize his idea in the form of eCash. However, the company went bankrupt in 1998 and eventually eCash and other idea of cryptocurrency "faded into the background" (Nian & Chuen, 2015.

2.2 Types of cryptocurrencies

2.2.1 Bitcoin

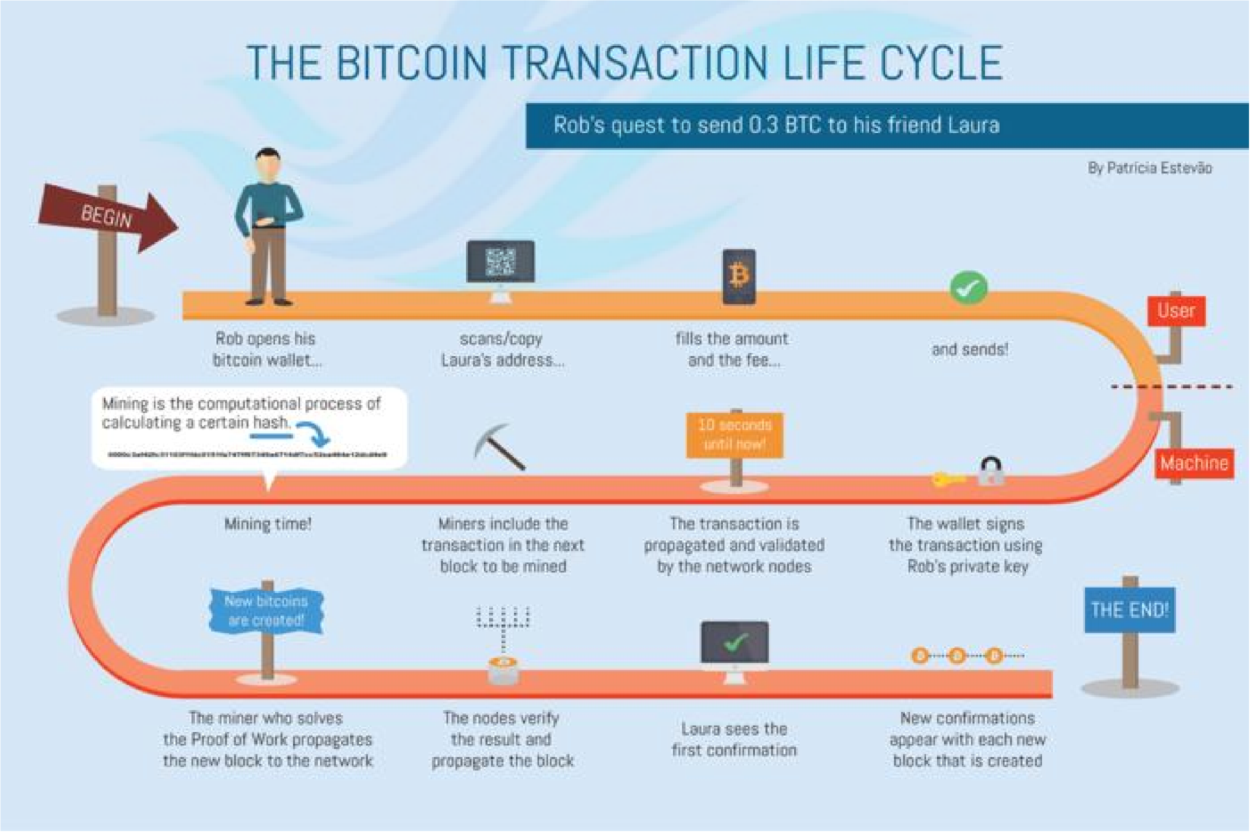
Bitcoin is a new currency that was operationalized in 2009 by a group of developers or an unknown person using the alias Satoshi Nakamoto. Transactions are made with no middlemen like financial institution. Böhme, Edelman, Christin and Moore (2015) state that, bitcoin is a communication peer-to-peer protocol that enables a payment system and use of virtual currency which (Kelly 2015) says that the concept of cryptocurrencies was described and suggested firstly in 1998, Bitcoin became the first practical proof of the theory. Weber (2015) states that in 2016 Bitcoin users were about 6.56 million and one year later increased to 11.05 million which shows a growing appetite amongst society for its usage. It uses blockchain technology based on encryption in form of a ledger that is updated constantly and run by computers of people in the network which by design eliminates the traditional regulatory institutions that facilitate transactions. Individuals own a copy of the ledger since accounts and transactions existing on blockchain get anonymized by computerized algorithms.

An approved transaction is added to the chain of blocks which is the blockchain and it goes through. Every transaction is public and in event someone tries to corrupt it, the algorithms behind it automatically red flags preventing a consensus among the ledgers. According to Swan (2015), the intermediaries, banks and financial institutions for example become obscured by cryptographic verification. Saure (2016) postulates that, bitcoin as a means of payment is the key function, with transacting costs being maintained low for Bitcoins, resulting in affordable and easy to move quantities of money around the world with fast speeds. However, nowadays it looks like bitcoins are being used for speculative purposes than its intended use which have created a lot of volatility.

Hay (2007) adds that the uncertainty about Bitcoin value makes it volatile, which results in it being a risky investment and even worse to be a formal currency substitute. According to Coin idol.com (2021) more Africans now have tools on their disposal to plug into the digital currency ecosystem but just like in Zimbabwe, countries like Uganda, Kenya, Tanzania, and Rwanda, digital currencies such as Bitcoin, Ethereum, XRP, are at this time not regulated nor backed by the state or the central banks in the East African region. Nevertheless, the current developments in the region seem to show that Bitcoin and other virtual assets could be treated as securities, but not as currencies which highlights those transactions that still go on despite the environment.

For an investigator to initiate digital investigations, it is necessary to have an appreciation of how the targeted digital currency platform works. Below is a diagram that depict Bit coin cycle or transaction:

Figure 2.1: Taken from https://changelly.com/blog/bitcoin-transaction-explained.


THE BITCOIN TRANSACTION LIFE CYCLE
Rob's quest to send 0.3 BTC to his friend Laura
By Patrícia Estevão
BEGIN
Rob opens his bitcoin wallet...
scans/copy Laura's address...
fills the amount and the fee...
and sends!
User
Machine
Mining is the computational process of calculating a certain hash.
10 seconds until now!
Mining time!
Miners include the transaction in the next block to be mined
The transaction is propagated and validated by the network nodes
The wallet signs the transaction using Rob's private key
New bitcoins are created!
THE END!
The miner who solves the Proof of Work propagates the new block to the network
The nodes verify the result and propagate the block
Laura sees the first confirmation
New confirmations appear with each new block that is created

Digital currency platforms as new technology are being closely scrutinised by law enforcement agencies because of their numerous abilities they possess which criminals favour especially to move and store financial economy with the use of pseudo names (anonymity) so investigations in this case will be aimed at tracing suspected transactions and possibly identify the origins and the destination for the purposes of exposing possible money laundering or terrorism financing cartels to either determine arrests or as evidence gathering for prosecutorial purposes.

According to Federal Bureau of Investigation Director Christopher Wray, cryptocurrency is a “significant issue” that is likely to become a “bigger and bigger” problem for the law enforcement agency. “We are looking at it from an investigative perspective, including tools that we have to follow the money even in this new world that we're living in.” Wray supported Romney's line of questioning concerning terrorist financing, saying that U.S. adversaries are becoming “more facile with technology and particular various types of technology that anonymize their efforts.” In June 2018, the Bureau said it had one hundred and thirty (130) active cryptocurrency investigations.

2.3 Cryptocurrency in the system of Money Laundering (Valeriia Dyntu 2019)

This study was aimed at studying the place of money laundering investigating the ways and means it is used. The paper also asserts that there is no unified legal status and definition of cryptocurrency which is another trigger for that complicates criminal investigations of money laundering facilitated by cryptocurrency thereby making law enforcement agencies face problems of identifying perpetrator and defining crime committed. There is further articulation of the main concepts of cryptocurrency complexities in terms of anonymity and decentralization, which engender the main antagonism in crime investigation. This clearly verifies the topical issue for the present study on complexities that exist in the investigation cycle of money laundering and terrorism financing on digital currency platforms.

The study also noted that transactions on cryptocurrency are chiefly not government monitored since when conducting any transactions, financial institutions are not involved to verify, and there is no limit to number of accounts one has, and transactions can be done in various spaces in one period.

2.4 Financial Action Task Force (FATF) Report on Virtual Currencies (2014)

This report emphasized on suggesting an understanding through addressing anti-money laundering and terrorism financing counter measures by adopting a working framework of risks that come along with virtual currencies as internet-based payment platforms. As decentralized, math-based virtual currencies particularly Bitcoin having garnered increasing attention, with two popular narratives emerging that the future lies in payment systems like virtual currencies and at the same time arming criminals with a lethal tool, for financiers of terror and sanctioned individuals to transfer and hide illegal funds from law enforcement and regulatory establishments. The popularity of Bitcoin and the understanding of the underlying technology of Bitcoin inspire other cryptocurrencies referred to as alternative coins or alt coins (Nian & Chuen, 2015), such as Ethereum, Dash, and Stellar, to appear.

2.5 Cryptocurrency Investigations Train-the-Trainer course UNODC April 2018

This course was aimed at increasing the capacity of law enforcement officers, analysts, prosecutors, and judges in order to understand the complexity of this new concept. Core aspects of the courses resided in analyzing transactions, inferring, identifying criminality and geo-locating criminals exploiting cryptocurrency.

The training concept used is expected to enable more efficient investigations against illicit of cryptocurrency for organize crime activities and allow further enforcement actions, seizure, confiscation including inter-agency coordination and information exchange. This kind of capacity building is what developing countries like Zimbabwe really need given the proliferation of digital currency use which will go a long way in increasing their capacity and honesty of criminal justice system to prevent, notice, order investigations and issue prosecutorial orders in money laundering and terrorism financing cases and other challenges that may seemingly be complex during investigations.

2.6 Hawks investigating multi-million Rand Bitcoin scam in South Africa: Business Tech Report (2018)

South Africa's elite policing unit, the Hawks, confirmed that they were looking into a serious scam of Bitcoins that could have negatively impacted a lot of South Africans which is suspected to have started with a firm namely BTC global with an estimated value of $50 million usd worth of stockholders all over the world. Hawks' spokesperson Captain Lloyd Ramovha said that there were more than 25,700 cases being probed for breaching the Financial Advisory and Intermediary Services Act with a substantial number out of South Africa.

2.7 Analysis of Illicit Flows into Digital Currency Services: Bitcoin Laundering (Yaya J Fanuise and Tom Robinson)

The unique characteristics of Bitcoin to evade law enforcement makes it quickly appreciated by criminals as they are often early adopters of technology. Users of Bitcoin employ pseudonyms rather than actual names and the ability to transact by without a middleman across borders just the way as e-mail is sent. Giving a mor thorough analysis of Bitcoin in facilitating illegal finance, an agenda situated at the Foundation for Defense of Democracies called Centre on Sanctions and Illicit Finance, grouped together with Elliptic, an analytics service for cryptocurrency, to examine blockchain information on Bitcoin and illegal income on digital currency platforms. This study is set to give vision for regulatory authorities, policy making, finance gurus interested in improving understanding the risks in finance resulting from adopting Bitcoin so as to prepare paths to increase combat against terrorism finance compliance and anti-money laundering crusade in cryptocurrency services.

2.8 Regulating crypto currencies in South Africa: The need for an effective legal framework to mitigate the associated risks (Karabo Mothokoa, 2017)

This study aimed to appreciate the concept of crypto currencies, their relevance in the financial sector and the risks associated with these virtual currencies. It also wanted to establish whether there is a convincing need for regulatory intervention in the operation of crypto currency. Mothokoa (2017) used a desktop-research methodology to carry out this study. The research combined analytical, explorative, and comparative strategies. Reasonable methods to compare were used for giving distinct regulatory and legal frameworks of America, European Union (EU) and Canada against that of South Africa's legal status for cryptocurrency and the multifaceted perceptions of crypto currency were analyzed and explored.

The study found that there are risks that arise from using crypto-currencies and some risks were found could be detrimental owing to the wide adoption of crypto-currencies. Factors like high volatility caused consumer protection, financial stability and money laundering was highlighted to be pertinent risks and with regards to laws governing cryptocurrency, it shows that EU, Canada and US have initiated laws that guard against the noted risks. In South Africa, it was established that there are no laws that governs cryptocurrencies, on another note South Africa Reserve Bank and National Treasury released position papers that cautioned people about the risks associated with these currencies. Therefore, the conclusion drawn was the undeniable necessity for South Africa to have an intervention of laws. In line with the necessity, author seeks to impose that it is critical institute interventions by integrating cryptocurrencies into relevant legislation that is Bank Use Promotion and Suppression of Money Laundering Act.

2.9 Advisory on Illicit Activity Involving Convertible Virtual Currency: The Financial Crimes Enforcement Network (FinCEN) Advisory (2019)

This advisory was to assist financial institutions in identifying and reporting suspicious activity concerning how criminals and other bad actors exploit convertible virtual currencies (CVCs) for money laundering, sanctions evasion, and other illicit financing purposes, particularly involving darknet marketplaces, peer-to peer exchangers, foreign-located Money Service Businesses, and Convertible Virtual Currency kiosks. It also highlights prominent typologies and red flags associated with such activities and identifies information that would be most valuable to law enforcement, regulators, and other national security agencies to initiate investigations.

2.10 Theoretical Framework

2.10.1 Theories for Adoption of Technology Developments

For this study, it is critical to be clear on how and why criminals, individuals or organisations adopt digital currency in their operations. There are available theories of technology adoption that have been developed that should help us in understanding. Technology adoption can be described as the decision to accept and use innovation as well as the effectiveness of adopted technologies based on acceptance or satisfaction (Chen et al., 2012; Hwang, 2010). In the literature for technology acceptance and adoption a significant number of models have been applied such as the Theory of Reasoned Action (TRA), Social Cognitive Theory, Technology Acceptance Model (TAM), Theory of Planned Behaviour (TPB), Model of PC Utilization, Motivation Model, Combined TAM-TPB, Innovation Diffusion, Extension of TAM2, Unified Theory of Acceptance and Use of Technology (UTAUT), TAM3, UTAUT2, Technology, Organization, Environment (TOE) to determine factors influencing adoption and use of technology (Tarhini, Elyas, Akour & Al-Salti, 2016).

2.10.2 Theory of Reasoned Action (TRA1975)

Theory of Reasoned Action was originally introduced by Fishbein (1967) and was extensively verified and built by Fishbein and Ajzen in (1975). Fishbein and Ajzen (1975) developed the TRA to identify components that predict behaviour. It was developed to explain behavioural factors that involve conscious decision making. Behaviours that are impulsive, habitual, or scripted were excluded in the model. The model predicts behaviour based on seven casual variables which are behavioural intention, attitude, subjective norm, belief strength evaluation, normative belief, and motivation to comply. Fishbein and Ajzen (1975) define behavioural intention as the person's plans, motivations, or desires. Intentions are not independent, but they result from underlying attitudes and subjective norms.

According to this theory, an individual behaviour manifests because of mindset pertaining that behaviour and also, recognised social influence from a fundamental person in one's life. An attitude is a general orientation toward a behaviour based on a variety of beliefs and evaluations. Subjective norm as the second variable is composed of normative belief which is the view of others regarding the behaviour and motivation to comply which is the pressure to please others regarding the behaviour. TRA has been used in technology adoption that utilise research for theoretical framework which is critical and has been combined with other theories and models. Despite the popularity of TRA a number of critiques have been proffered and this led to the development of Theory of Planned behaviour and Technology Acceptance Model. The TRA model is diagrammatically illustrated in **Figure 2.2** below.

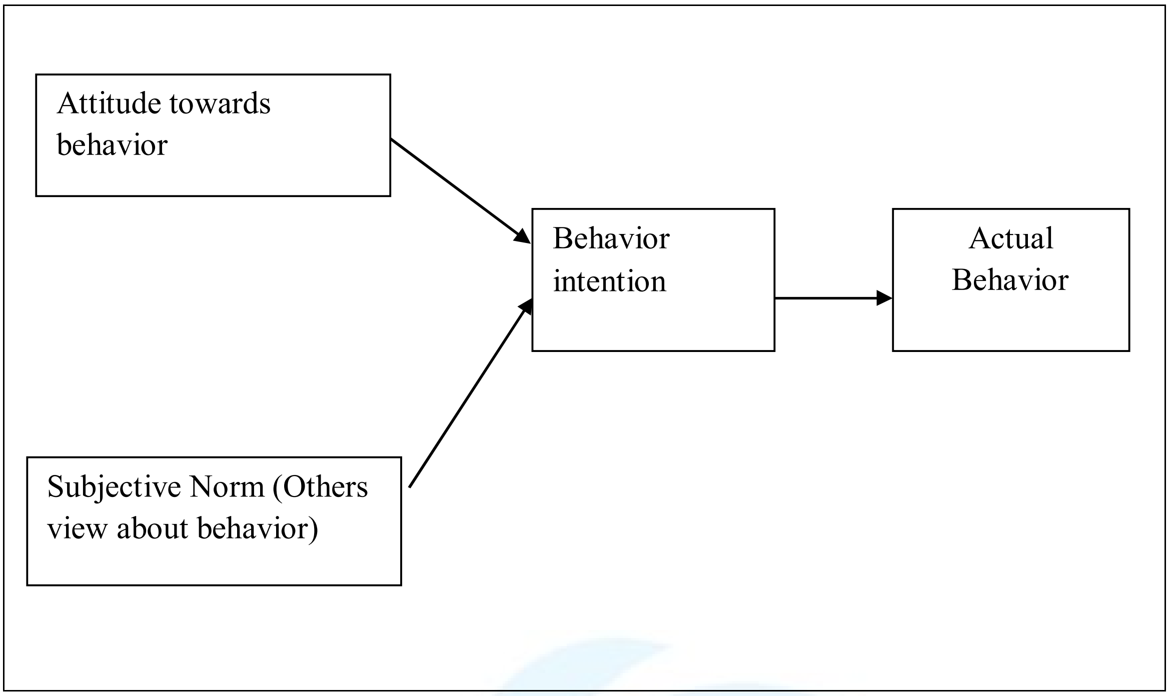

Attitude towards behavior
Behavior intention
Actual Behavior
Subjective Norm (Others view about behavior)

Figure 2.2: Theory of reasoned action

Source: Fishbein and Ajzen (1975)

2.10.3 Social Cognitive Theory 1986

This theory was developed by Albert Bandura in 1986 as a learning theory about the notion that watching others doing something makes people learn within the context of social interaction and experience. The theory is based on the fact that learning occurs in a social context with a dynamic and reciprocal interaction of the personal factors, environmental factors, and behaviors (Bandura, 1986). Bandura (1986) postulated that the person, the behaviour and the environment work hand in hand to create learning in an individual.

According to the SCT, people are either driven by inner forces or external stimuli. It shows that users acquire and maintain behaviour due to the social environment in which they develop their behaviour. Self-efficacy is the important factor in this model (Compeau et al., 1999). Self-efficacy refers to a personal belief in one's capabilities to learn or perform an action at designated levels (Schunk, 2000). It is about what one is capable of doing but it is not the same as knowing what to do (Bandura, 1997).

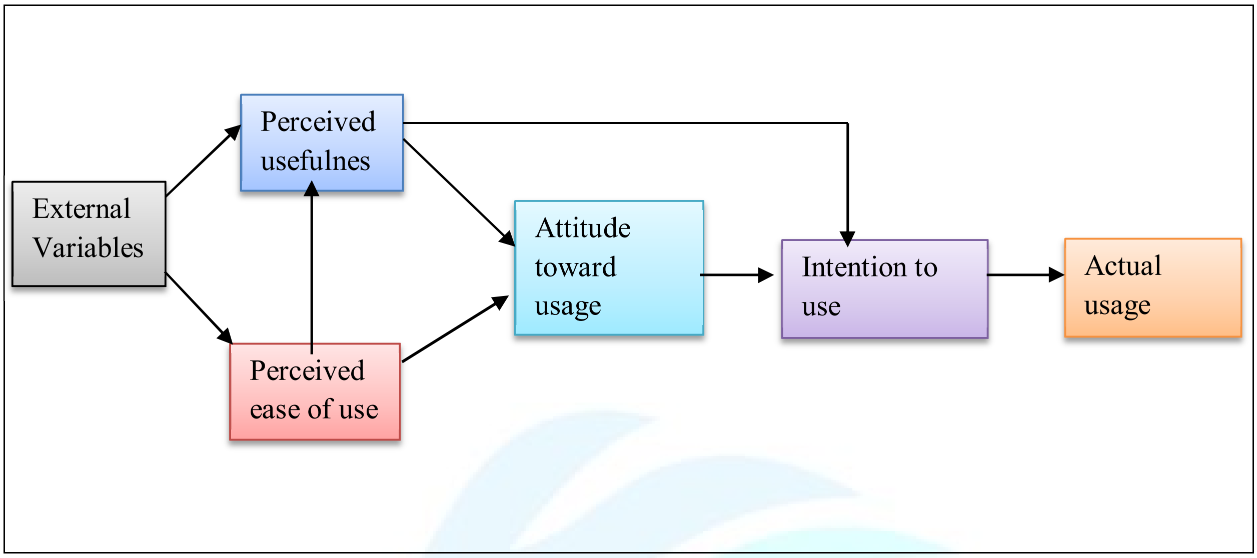
2.10.4 Technology Acceptance Model (TAM1986, 1989)

TAM is one of the extensions of Fishbein and Ajzen TRA. TAM was introduced by Davis in 1986 (Davis, 1989) to explain and predict users' adoption, acceptance or rejection of new technologies. The theoretical basis of TAM is built from a ground that a person considers three critical issues to determine when and how to use new technology when presented. The TAM consists of six related constructs namely external variable, perceived ease of use, perceived usefulness, attitude towards using, behavioural intention to use and actual use (Davis, Bagozzi & Warshaw, 1989; Ko et al., 2010). Perceived usefulness is defined as "the degree to which a person believes that using a particular system would enhance his or her job performance" (Davis, 1989, p.320). Perceived ease of use is defined as "the degree to which a person believes that using a particular system would be free of effort" (Davis, 1989, p. 320). According to TAM, perceived ease of use and perceived usefulness determine an individual's information system acceptance by determining their attitude toward using and subsequent behavioural intention to use, which has an effect on actual use (Erasmus, Rothmann & Van Eeden, 2015). Perceived usefulness is used as a dependent and independent variable since it is predicted by perceived ease of use and on the other hand predicts attitude towards using and behavioral intention to use simultaneously (Erasmus et al., 2015).

Perceived ease of use and perceived usefulness are indirectly influenced by external variables in reinforcing a user's belief of using a system (Erasmus et al., 2015). Attitude towards using in TAM involve judgment on whether the behaviour is good or bad (Erasmus et al., 2015). In TAM there is a direct effect on the intention to use a system. Attitude towards use is determined by perceived ease of use and perceived usefulness (Guritno & Siringoringo, 2013). Behavioural intention to use is influenced by an attitude towards using and perceived usefulness. The relationship between these variables can be illustrated by the model in Figure 2.3 as suggested by Davis.

Figure 2.3: Technology acceptance model

Source: Adopted from Davis et al. (1989)



2.10.5 Theory of Planned Behaviour 1991

The Theory of Planned Behaviour (TPB) is an extension of the Theory of Reasoned Action (TRA) that was established by (Ajzen, 1991). TPB was developed to overcome the limitation of TRA by Fishbein and Ajzen (1980). The TPB is similar to TRA with the addition of a component known as the perceived behavioural control to predict both behavioural intention and behaviours. PBC is defined as a person's approach on the difficulty to execute a particular behaviour. It is a function of one's belief about control and one's perceived power. Generally, the theory suggested subjective norms, perceived behavioural control and attitude toward behaviour as three concepts vital to predict intention to adopt innovation. In relation to TPB attitude, subjective norms and perceived behavioural control together leads to individual intention and behaviour (Mishra, 2014). **Figure 2.4** depicts the model of Theory of Planned Behaviour.

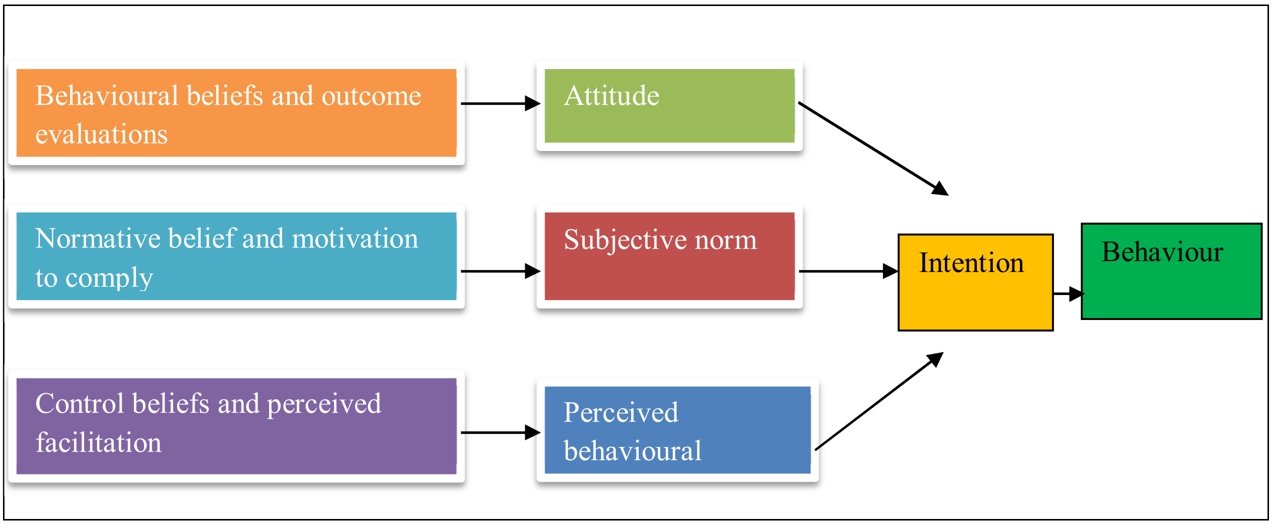

Behavioural beliefs and outcome evaluations
Attitude
Normative belief and motivation to comply
Subjective norm
Intention
Behaviour
Control beliefs and perceived facilitation
Perceived behavioural

Figure 2.4: Theory of planned behaviour

Source: Mathieson (1991)

2.11 Criminology Theories

2.11.1 Space Transition Theory

This theory explains the causation of crimes in the cyberspace. Jaishankar (2008) found out that general theoretical explanations were not enough to give a conclusion about cybercrime which led to the feeling to separate theory of cyber-crimes. Space Transition Theory is an explanation about the nature of the behaviour of the persons who bring out their conforming and non-conforming behaviour in the physical space and cyberspace (Jaishankar 2008). Space transition involves the movement of persons from physical space to cyberspace and vice versa.

This theory argues that there is a difference in behaviour when people shift from one space to a new one. Suggestions of the theory are that people's criminal behaviour can be suppressed while in the physical space though may have a tendency in cyberspace to perpetrate crime, because status and position physical space limits them. Decision to commit cybercrime comes from the fact that cyberspace gives anonymity, personality changes and general absence of prohibitive measures. Exporting unlawful conduct by criminals in cyberspace to real world is possible and vice versa, thus belonging to both space and time nature of cyberspace provide the chance to escape. Strangers are likely to unite in online to perpetrate illegal acts in real world. Colleagues are probable to connive in real world to commit crime in cyberspace. People in private society have higher chances of performing illegal acts online than people in accessible society.

Conflicting culture in real space against the online culture can result to cybercrime. Jaishankar (2008) further asserts that since online crime is now prevalent that scholars and professionals in the field of crime now view online platform as the new playground for illegal activities. The space transition theory presented above gives detailed analysis about illegal conduct in cyberspace.

2.11.2 Theory of Rational Choice

Rational Choice is a theory produced by Cornish and Clarke (1986) having three components. A person’s belief to commit acts of criminality is based on that they can derive a benefit from it and the determination required a basic decision-making process. Simon (1957) assets that even though arriving at a decision with incomplete information, rationality processing is made for criminal decision making through weighing the reward of act with injury in line with excitement, pleasure and thrill derived. Which means that performing the criminal act is purely based on the act giving more benefits than the cost.

Cornish and Clarke (1986) suggested second component in rational choice theory required crime-specific focus that was critical to obtain the characterists of distinct requirements connected to a criminal act. More-so, this focus brought attention to the scenarios of the illegal act rather than the person and permitted for understanding the uniqueness in information critical for various crimes.

The third component was a vital difference being made between criminal participation and the crime incident. Criminal scenes and criminal participation recognised decisions made by a person to be involved in crime. On another note, criminal participation is the method that a person utilised to become engaged in a specific crime in the first place, or to persist and to stop.

2.12 Chapter summary

This chapter presented literature related to this study. This chapter presented the literature review of the study guided by objectives of the study such as to determine specific complexities encountered when investigating digital currencies from a sample of financial investigators, investigate if other developing countries who have adopted digital currencies coping, assess any international standards set by developed nations in investigating digital currencies that can also be adopted by developing countries like Zimbabwe and recommend action and guidelines to improve the current financial digital currency investigations eco-system. The next chapter present the methodology of the study.

Chapter 3: Methodology for Research

3.0 Introduction

The chapter before focused on presenting literature on the complexities digital currency has on financial investigations in relation to money laundering and terrorism financing. A case of Zimbabwe. This chapter focuses on presenting the research methodology of this study. In this chapter research philosophy, research design, targeted population, sample size, sampling method, research instruments, data collection procedure, data analysis and presentation methods, reliability and validity and ethical considerations will be presented.

3.1 Research philosophy

According to Creswell (2010) prior to selecting the research method and commencing with the research design, a suitable research philosophy should be identified, as it establishes the foundation for what follows. According to Mingers (2011); Mingers (2013); Orlikowski and Barooudi (2011) there are three key research philosophical or epistemology approaches or assumptions: positivist, interpretive, and critical research. The two main approaches used in financial research which are positivism and interpretivism (Chen and Hirschheim, 2014; Gregor, 2016; Guba and Linclon, 2014; Orlikowski and Baroudi, 2011; Myers, 2017).

However, amongst the two research philosophies, positivism is considered as the most popular one in financial research as it has been used in many financial research (Mingers, 2013; Orlikowski and Baroudi, 2011; Straub et al., 2014; Yin, 2013). In this research study positivism was adopted because it is used to test theory for understanding a certain phenomenon that is in research question (Orlikowski and Baroudi, 2011). Moreover, positivism assumes that the research study is undertaken in a value-free way. In this research study positivism was also adopted to scrutinize facts such as they are with no room for bias from the researcher. Positivism was adopted because it uses better coordinated methodology for the purposes that enable reproduction.

3.2 Research design

According to Avison et al., (2018) and Bryman (2014) research design refers to a framework or systematic approach to be adopted to fulfill the aim and objectives of this research. Research design can be exploratory, descriptive, and explanatory (Robson, 2012; Sekaran, 2013). For this study, the researcher adopted an exploratory research which enabled him to gain new insights on the concept of digital currency. The researcher conducted exploratory research through the search of literature from the internet's publications about digital currency adoption through searching on websites, research papers on financial investigations and by reading e-books about theories on technology adoptions and risks associated written by various authors. Cross sectional research design was also used in this research study because data was collected over a short period of time.

According to Kothari and Garg (2014) a research design is a blueprint for data collection, measurement, and analysis. As such the design includes an outline of what the researcher will do from writing the hypothesis and its implications for the final analysis of data (Kothari and Garg, 2014). Due to the nature of this research study cross-sectional survey design was adopted to accomplish the research objectives. The researcher adopted cross-sectional survey since it gives an effective manner on the gathering of huge volumes of information from a significant populace. Moreover, cross-sectional survey provides a quick, often inexpensive, efficient and accurate means of assessing data about a population (Zikmund and Babin, 2017).

3.3 Targeted population

Walliman (2018) state that target population refer to the individuals in a group that are drawn from the general population and share a common characteristic of interest to the researcher, and it should be defined ahead of time, clearly specifying the inclusion of eligibility criteria. The study population comprised of financial intelligence analysts, financial crime compliance investigators, and employees of digital currency agents in Harare, Zimbabwe. This figure of 130 people was drawn from the vital targeted organizations in Harare shown in table 3.1 below. The size of targeted population of this study which explains the reasoning for that certain number constituting relevant agencies responsible for subject matter in Zimbabwe as they are shown below.

Table 3.1 Organisations of targeted population.

Organization	Estimates of population
FINANCIAL INTELLIGENCE UNIT	50
ZIMBABWE POLICE (COMMERCIAL CRIMES)	50
GOLIX CURRENCY	20
CRYPTOCEM	10
Total	130

3.4 Sample size

In this research about the complexities digital currency has on financial investigations in relation to money laundering and terrorism financing. A case of Zimbabwe. Raosoft online sample size calculator was adopted. Raosoft Tool is powerful collection of more than 15 utilities for database and file management of research survey data gathered with Raosoft online survey software (http://www.raosoft.com). The researcher typed the url http://www.raosoft.com and entered 130 as population size and automatically the site calculated a sample size of 98 which was adopted in this study.

3.5 Sampling method and techniques

Sampling method is the strategy used to select participants into a study. Makanyeza (2016) state that, it is possible to enlist everyone into the study if the population is small but in most cases the population is so large that few participants from the population can be chosen to represent the whole population. Basically, there are two techniques for sampling exist which are non-probability and probability. The researcher adopted both non-probability and probability sampling techniques. Probability sampling is when all participants in the study have an equal opportunity to be selected (Easterby-Smith, Thorpe and Lowe, 2012). Probability sampling will use mathematics methods. Whilst non-probability sampling participant in the population are selected based on their availability or on the judgment of the researcher that they are information rich (Walliman, 2018).

Zikmund and Babin (2010) defined sampling as any procedure that draws conclusions basing on measurements of a portion of the entire population. This research study adopted convenience sampling because there are no available statistics of digital currency investigations in Zimbabwe at the time study was carried out hence convenience sampling was adopted to draw the sample, because of willingly available subjects invited to be part of research. Convenience sampling allowed the researcher to obtain the necessary number of completed questionnaires as the most of participants represent a sensitive section of individuals because of nature of their jobs so prior arrangements and clearance had been made due to the nature of the research study.

3.6 Research instruments

The major research instrument adopted in this research study was a google generated structured questionnaire consisting of 8 typed questions in a definite order or set. The questionnaires were used to collect data by asking respondents to respond the same set of questions. The structured questionnaire was adopted because it is the best study strategy for gathering explanatory and descriptive data on individual views. The structured questionnaire was adopted because they are quick to gather data, easier to complete and more readily amenable to structuring responses and quantitative analysis.

3.6.1 Key informant interviews

Primary qualitative data were acquired from key informant interviews through google generated open ended interview questions form for filling up answers because of covid-19 regulations and lock-down rules, 1 on 1 sessions were not possible. Interviews were meant to empower a more profound comprehension of digital currency investigations from officers who are responsible for financial investigations in Zimbabwe. Key informants for in-depth interviews are usually selected based on their first-hand knowledge about the subject of interest (Choy, 2014). Data was automatically collected through the space filling on forms noted by respondent. Participants were required to consent to being interviewed for security reasons that their responses are for academic purposes and were able to send back their answers within the shortest period of time to better facilitate for the completion of study.

3.6.2 Survey Questionnaires

Primary quantitative data was acquired through a draft of a survey questionnaire. A questionnaire is a set of questions with a selection of answers which is designed for use in a survey (gam, 2018). It gathers standardised data in the same way from a number of respondents. Data acquired from questionnaires can be generalised if the sampling is appropriately done. A profound comprehension of the research problem was acquired from literature and questions developed on this basis which addressed the research objectives of this study. The designed questionnaires were pre-tested to determine their effectiveness.

Participating pre-tests were done where respondents were informed that it was a pre-test. Respondents provided their feedback on the questions, their order and wording as well as how understandable they were. Questionnaires were administered during the research by the researcher to enable probing and clarification of questions and responses. To ensure confidentiality no respondent-identifying information was gathered and all questionnaires were totally anonymous. Questionnaires were administered to identified participants in Zimbabwe over a two-week period.

3.7 Data collection procedure

Once the questionnaire was designed, pilot tested and amended, the sample selected, the questionnaire was used to collect data. The researcher seeks permission from organizations before collecting data. The researcher self-administered through sending links on WhatsApp and email of the questionnaire to the target population. The questionnaire heading highlighted an introductory statement that respondent's feedback is for educational purposes and a brief of subject matter and clear instructions preceded each question in order to facilitate its completion. The questionnaires were then sent back to the researcher within 1 month from sending date. When conducting interviews, the researcher started by developing "an interview guide" whose content was derived from the three objectives of this study (Bernard, 2016).

The interview guide was administered and tested on three research participants who were selected using the purposive sampling method (Sifile, Mazikana, Chavunduka and Bhebhe, 2018). The researcher ensured that all the necessary steps involved in conducting an interview were done (Easterby-Smith, Thorpe and Lowe, 2012). Consent was made through texts on mobile communication application like WhatsApp because of geographical location differences. The interviewees had the choice to either partake or excuse themselves from participating any time they felt like and were also notified of the unavailability of material benefits to be derived by those who participated in the study.

3.8 Data analysis and presentation methods

Data analysis is the application of reasoning to understand the data that have been gathered (Kothari and Garg, 2014). After the data collection the quantitative data from the respondents was edited, structured, and processed. Descriptive analyses were performed. Descriptive statistics consist of measures of central tendency, including means, medians, and standard deviations (Salkind, 2012). Multiple regression analysis was performed to strengthen and give direction of the hypothesized relationships. One-way ANOVA was also adopted.

3.9 Reliability and validity

According to Kothari and Garg (2014) reliability is about the correctness and exactness of procedure for measurement. Coherent outcomes gauge the reliability of measuring instrument. Testing internal uniformity of instrument for research alpha coefficients by Cronbach were utilized. Having a high alpha coefficient implies that the validity of scale. 0.70 value and upwards shows pleasing reliability levels than a value between 0.50 to indicate an acceptable level of reliability. The measurement scales were reliable since all the Cronbach’s alphas of the constructs were above 0.06 to ensure validity of the research instrument a thorough literature review was done.

3.10 Ethical considerations

Before data collection the researcher seek permission from the university to conduct a research study. During data collection the main objective of the study along with issues like privacy, discretion, consent that are ethical factors were highlighted in the introductory statement of the questionnaire. Voluntary participation and freedom to dropout from study any time was also indicated in the text’s messages during communications with possible participants. After data collection presented the data as it was, and the collected data was solely used for academic research purposes.

3.11 Chapter Summary

This research study is on the complexities of digital currency on investigations in relation to money laundering and terrorism financing with participating institutions being Headquartered in Harare, Zimbabwe. This chapter focused on presenting the research methodology of this study. In this chapter research philosophy, research design, targeted population, sample size, sampling method, research instruments, data collection procedure, data analysis and presentation methods, reliability and validity and ethical considerations were presented. Data presentation and analysis of this research study is the focus for the next chapter.

Chapter 4: Results Presentation and Analysis

4.0 Introduction

This research was focused on the complexities digital currency has on financial investigations in relation to money laundering and terrorism financing. A case of Zimbabwe. The data for analysis was collected using qualitative and quantitative analysis methods. Descriptive style presented qualitative data, and then the researcher has used graphs, tables, and pie-charts to present quantitative data. The use of graphs, tables and charts was chosen to enable easy interpretation of the data collected. Data collected was analyzed and interpreted to provide answers to the research objectives and questions.

4.1 Response rate analysis

A total of 130 respondents were considered for contribution in this study. The researcher personally engaged respondents at organisations namely, Financial Intelligence Unit, Zimbabwe Police, Golix, Cryptogem. Out of the targeted 130 participants, 98 valid answered questionnaires were returned, and the response rate was 87%, with a 13% consists of non-respondents making the questionnaires that were never returned. The response rate is considered excellent by Makanyeza (2018) who noted that a response rate of 50% or above is deemed adequate for analysis and reporting; a rate of 65% is very pleasing, making 70% and over excellent.

4.2 Responsibility of respondents in investigative cycle.

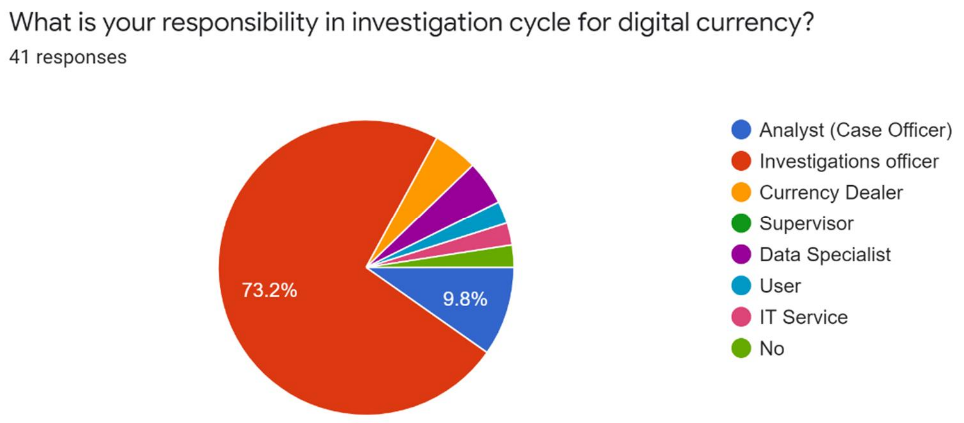
The **table 4.1** below shows Responsibility of respondents and the positions which they hold in the organization targeted.

Table 4.1: Responsibility of respondents and position held.

	Frequency	Percent %	Cumulative Percent %
Compliance Investigators	40	32	40
Intelligence Analysts	43	35	40
Digital Currency Traders’ Employees	15	20	20
Other	0	0	
Total	98	87	100

Table 4.1 above shows that 40 (32%) of the respondents were compliance investigators, 35 (35%) cited that they were intelligence analysts, 15 (20%) indicated they were employees of Digital Currency Agencies. The organization participants have much influence to make investigative decisions for their organizations pertaining to the use of digital currency and their contribution is fundamental to evidence gathering. Information displayed in **Table 4.1** above, it can infer that those are officers of organizations who are knowledgeable in digital currency issues.

Figure 4.1 Below also shows responsibility of respondents in targeted organizations.



Source: Study Questionnaire

Figure 4.1 displays that majority of respondents are from Financial Intelligence Unit (FIU) Investigations Analysts followed by Zimbabwe Police (Compliance Investigation), and Golix, Cryptogem (Currency Dealers) as the smaller number of respondents, who completed the questionnaire about the complexities of digital currency when investigating in the case of terrorism financing and money laundering in Zimbabwe indicating that they were participants. In a similar study conducted by Koreff (2018) on three studies examining auditors' use of digital currencies in Florida, United states of America, he noted that most employees in organizations constituted 80% of respondents of his study hence the results attained in this research were highly expected.

4.3 Level of understanding digital currency by organizations in Zimbabwe.

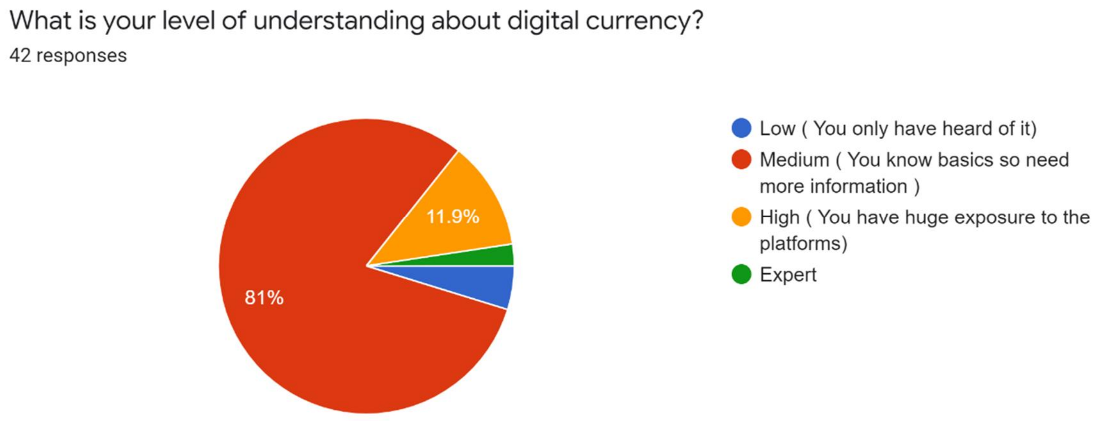


Figure 4.2: Source: Survey conducted for this study.

Respondents of this research on the complexities digital currency has on financial investigations in relation to money laundering and terrorism financing. A case of Zimbabwe asked about their level of understanding of digital currency and their responses were captured down in Pie Chart 4.3 above and it can be noted that majority of respondents (81%) indicated that they had a good understanding of digital currency. Idil, Halit & Koray (2018) conducted a study on digital currencies in Denmark. Idil, Halit & Koray (2018) noted that firms have a good understanding of digital currency. The research aimed to analyze the role and effects of digital currencies.

According to Idil, Halit & Koray (2018) the idea of using cryptographic technology to create digital currency can effectively transfer money without relying on any financial institution and intermediary agents. The ways of payment have transformed dramatically with the development of technology. Payment methods changed from cash payments to card payments, and then electronic payments appeared (Dennehy and Sammon, 2015). According to Idil, Halit & Koray (2018) the results were similar with the literature that firms have a good understanding of digital currencies and digital currencies had made payments easier. The responses show that according to our targeted participants understanding of digital currencies is very high which is important for the study as it requires articulation of the problem in the study.

In 2008, a paper written by Satoshi Nakamoto specifies the idea and underlying technology of a cryptocurrency called Bitcoin, including their solution to prevent double-spending using hash-based proof-of-work (Nakamoto, 2008). Bitcoin is implemented under open-source license and its network utilizes a form of distributed ledger technology called blockchain. Since its release, Bitcoin has been used for various transactions. As per 22 August 2018, Bitcoin network has processed on average 240,673 confirmed transactions per day.

4.4 Are the skills available to investigate digital currency platforms?

Research question two sought to find out if there are people skilled to investigates digital currency platforms operations.

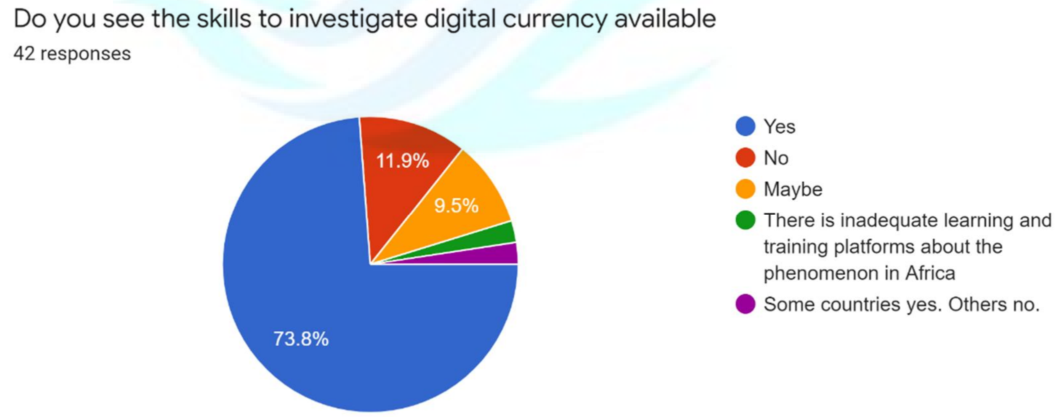


Figure 4.3 Source: Survey

It can be noted that 73.8% of the responses as shown above are confirming the availability of the skills base to investigate digital currency platform in Zimbabwe as the study wants to look at the vulnerabilities on digital currency platforms that make it difficult for investigations.11.9% view that there are no skills with 9,5% being not sure and the rest are of the opinion that there is inadequate learning and training platforms.

4.5 Is digital currency driven crime prevalent.

The question was aimed at understanding if the respondents were aware of criminal tendencies on digital currency platforms.

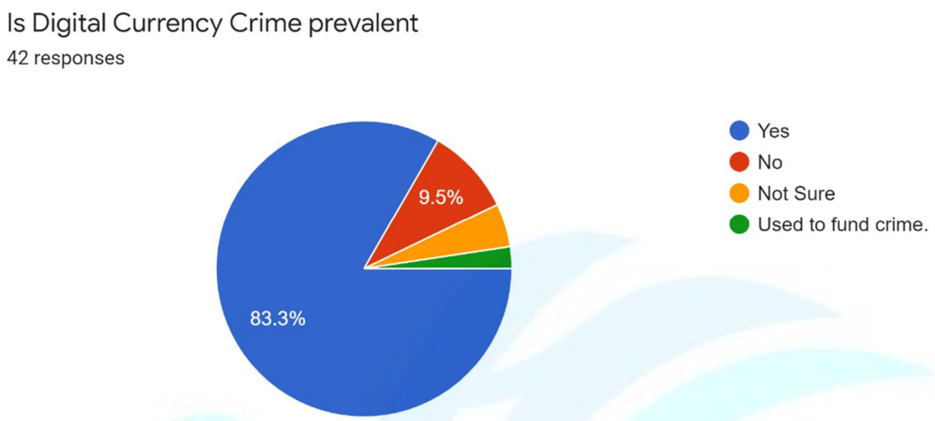


Figure 4.4 Source: Survey Pie chart

The above responses show data about the prevalence of criminality on digital currency platforms for the study on vulnerabilities of digital currency platforms which make investigations difficult. 83% admit that criminal activities are prevalent on digital currency platforms, with 9.5% saying prevalence is none and the rest not sure.

4.6 List of vulnerabilities digital currency platforms have

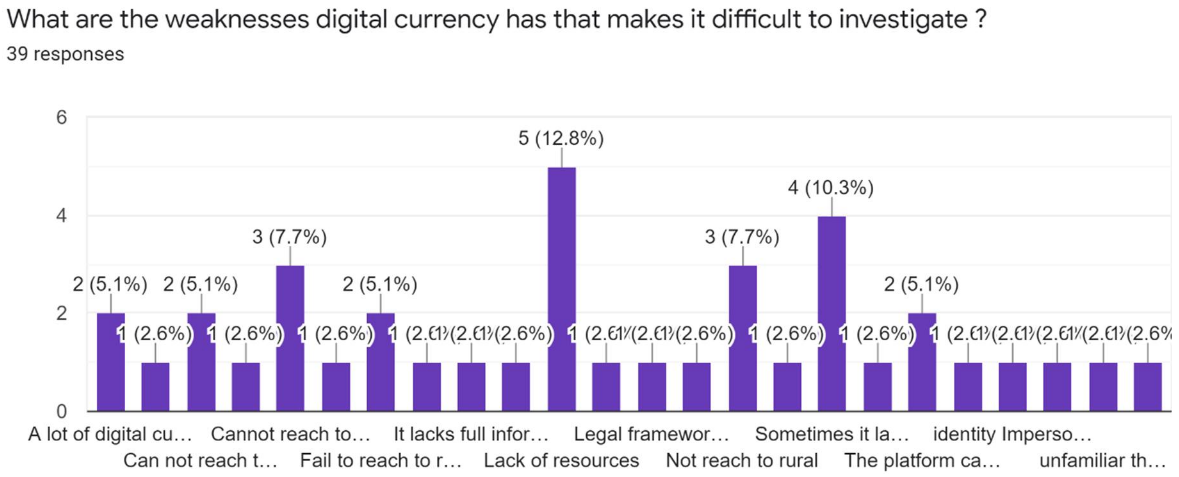


Figure 4.5 Source: Survey

Graph above shows that respondents who completed the questionnaire had various assertions about complexities digital currency has on financial investigations in relation to money laundering and terrorism financing. A case of Zimbabwe indicating that digital currency platforms can be difficult to investigate criminal activities facilitated by them. From the findings attained above 5(12.8%) cited lack of resources needed by investigators, 2(4.7%) cited lack of legal framework to regulate this kind of technology for the industry, 4 (10.3%) cited much about lack of enough information(actionable intelligence) critical to an investigation, 4 (10.3%) cited digital currency account holders use of anonymity through identity impersonation making traceability difficult (attribution) and 2 (4.7%) cited that it is a new phenomenon in academia in Zimbabwe which makes understanding of it by investigators difficult, 2(4.7%) citied that there are no main stream banks or institutions that deal with digital currency and that its unfamiliarity from fiat currency operations makes it difficult to investigate, 2(5.1%) cited remote access (transnational nature) of digital currency an investigative headache because of jurisdiction issues, 2(4.7%) cited the use of dark net(internet black-market) which further complicates nature of these transactions, 3(7.3%) cited encryption, lack of accountability and proneness to hacking as complexities that make it difficult for investigators and 11(35,4) cited issues that did not really reflect on the question asked with issues to do with reaching to rural areas, reach to different people.

According to Shi & Zhou (2020) inspired by the digital revolution to the financial industry, the discussion around central bank digital currency also attract attention from academics and central banks. According to Jad Mubaslat (2017), who was a Wright State University graduate student and creator of BitQuick.co, concurred with the outcome of this survey as he postulates that, other cryptocurrencies, such as Monero, are becoming popular for dark web uses including drug trafficking and human trafficking and also according to a 2015 Europol article, bitcoin had featured in high-profile investigations involving payments between criminals, and was used in over 40% of illicit transactions in the European Union.

It is therefore noticeable that when terrorists and money laundering criminals use digital currencies for their operations, it is difficult for investigators to trace and apportion responsibility for the illegal actions (attribution)given the absence of regulatory frameworks that gives motion to the wheels of criminal justice coupled mainly with the nature of digital currency transactions that offer use of pseudo identities raising anonymity levels, also necessitated with its access that can be done anywhere in the world remotely which criminals favour as they usually go to places called safe havens which have laxity in law enforcement and more-so internet platforms like darknet give investigations torrid time as criminals are always a step ahead of officers of law with the use of technology. It is also highly difficult to have reliable information that is actionable that an investigator can use because most of the communication used is facilitated by heavily encrypted messages which can take time for investigators to decode as information and timely reaction are fundamental aspects to all investigations. From the responses of this question, it shows that digital currency platforms are attracting a lot of scrutiny by law enforcement and financial policy regulators because of their potential to offer more to similar benefits of trust, reliability, and credibility as the traditionally used hawala financial system that money launders and terrorism operators had become accustomed to.

4.7 Interview Responses Outlook

4.7.1 Some argue that digital currency use needs financial authorities' involvement, how can this help investigators?

Responses

i) To get access to all the needed information which will be used as evidence.

ii) Maybe more visibility into transactions and an attempt to identify locations of transactions.

iii) In order to have rules and guidelines of operation.

iv) It is recognition by authorities means budgets are provided for training to combat it and there will be legislative progression to help in prosecution.

v) This will assist to know the people behind or proponents of the digital currency for easier follow up when customers are fleeced or in case of fraudulent transactions.

4.7.2 Given the crossing of borders of cyber space, how is the cooperation situation with other countries when investigating?

Responses

i) It is a complex situation as other countries are not cooperative.

ii) For individual cases, not great. For large scale operations that already have an international component then cooperation is better.

iii) It is a challenge because you do not know who exactly to contact for cooperation.

iv) Cooperation is important since cyber space is borderless and digital currency is used to fund international criminal activities and terrorism however due to fragmented policing and legislation particularly in Africa cooperation is minimal and difficult.

v) The use of Interpol and other organs such as SARPCCO assist so much in cross border investigations on these transnational incidences. However, there are some hiccups with some member states whose cooperation is not that pleasing as they take time to respond, or their statutes will be different from the requesting country hence that will pose as a challenge.

4.7.3 What are the consequences for investigators when digital currency use is banned though trade still goes on?

Responses

i) Their source of information and cooperation will be hindered.

ii) Investigators loose KYC data from local exchanges. They will have to rely on international cooperation.

iii) Work is very difficult for investigators because it is an unknown territory.

iv) The banning entails that the official system ignores it is existence and thus do not budget for it or legislate to combat it and yet it is a reality on the ground.

v) The investigators must stop the trade of the currency but in so doing there will be so much resistance from the transacting public who will be holding the digital currency.

4.8 Descriptive statistics

This section presents results on descriptive statistics (mean and standard deviation) of the study constructs). Five-point Likert scale was used on each of the four constructs that is to determine specific complexities encountered when investigating digital currencies from a sample of financial investigators, to investigate if other developing countries who have adopted digital currencies are coping, to assess any international standards set by developed nations in investigating digital currencies that can also be adopted by developing countries like Zimbabwe and to recommend action and guidelines to improve the current financial digital currency investigations eco-system. The response points being disagree firmly, disagree, impartial, agree, firmly agree.

4.8.1 To determine specific complexities encountered when investigating digital currencies from a sample of financial investigators.

Table 4.2: Mean and standard deviation for determining specific complexities encountered when investigating digital currencies from a sample of financial investigators.

Item	Mean	Std. Deviation	N
Unharmonized local regulations and international standards	4.13	.963	100
Criminal offences associated with virtual currencies	4.17	.933	100
Unavailability of tools and software's to trace transactions	4.03	.941	100
Privacy Rights (Apportioning responsibility of crime)	4.16	1.033	100

Overall mean =4.1225; Standard deviation= 0.9675

Results in Table 4.2 above shows the lowest mean rate that is 4.03 and standard deviation that is 0.941 as compared to the highest mean rating of 4.17 with a standard deviation 0.933. Descriptive statistics of determining specific complexities encountered when investigating digital currencies from a sample of financial investigators showed an average mean of 4.1225 with a standard deviation of 0.9675. On average, respondents were agreeing that there are some criminal offences associated with virtual currencies.

The results are similar to United Nations Office on Drugs and Crimes who noted that digital currencies by nature, may possibly be related to a variety of criminal crimes. Their focus was on money laundering offences involving virtual currency, they noted the vitality to quickly give a larger scope to which these offences could be looked at. This does not exclude worry on the relations that exist between digital currencies and cybercrime. Dyson & Bell (2020) conducted a study on the challenges of investigating cryptocurrencies and block chain related crime. They noted that we are incrementally living in a society seeking balancing need for consent and rights to privacy along with the obligation of the state to protect its citizens. Within this ever-evolving society, it is increasingly fundamental need to guard a person's financial trail of transactions which at the same time makes it problematic for financial crime agencies when investigating fraud or money laundering.

4.8.2 To investigate if other developing countries who have adopted digital currencies are coping.

Table 4.3 below shows descriptive statistics for investigating if other developing countries who have adopted digital currencies are coping.

Table 4.3: Mean and standard deviation for investigating in other developing countries who have adopted digital currencies are coping.

Item	**Mean**	**Std. Deviation**	**N**
Effective internet control	4.00	.878	100
Use of regulatory instruments	4.04	.893	100
Cryptocurrency regulatory institutions	3.92	.979	100
Financial Crimes agencies in place	3.99	.975	100

Overall mean =3.9875; Standard deviation= 0.93125

Results in Table 4.7 above shows the lowest mean rating of 3.92 with a standard deviation of 0.979 as compared to the highest mean rating of 4.04 with a standard deviation 0.893. Descriptive statistics of investigating if other developing countries who have adopted digital currencies are coping showed an average mean of 3.9875 with a standard deviation of 0.93125. On average, respondents were agreeing that other countries have adopted the use of regulatory instruments. The results were like Marian (2018) who presented a conceptual framework for the regulation of cryptocurrencies and noted that the write up proposed a conceptual framework for the regulation of transactions involving cryptocurrencies. Cryptocurrencies offer tremendous opportunities for innovation and development but are also uniquely suited to facilitate illicit behaviour (Marian, 2018). Marian (2018) proposed a monitoring legal concept which enforces costs on features of cryptocurrencies that define their facilitation for crime behaviour but leave out enforcing on key aspects that make it possible, especially transfer processes of value decentralisation. Using a basic utility model of criminal behaviour as a benchmark Marian (2018) clarifies on how the legal framework can be constructed. An example of a tax anonymity that is elective on transactions that makes one user not anonymous.

4.8.3 To assess any international standards set by developed nations in investigating digital currencies that can also be adopted by developing countries like Zimbabwe.

Table 4.4: Mean and standard deviation for assessing any international standards set by developed nations in investigating digital currencies that can also be adopted by developing countries like Zimbabwe.

Item	Mean	Std. Deviation	N
Rules for exchanges	3.83	.886	100

Taxation levels	3.76	1.068	100
Cohesive approaches on cryptocurrencies in form of policies guiding and regulating it.	3.92	.934	100
Approval of financial institutions that handle Bitcoin transactions	3.96	1.031	100

Overall mean =3.8675; Standard deviation= 0.97975

Results in Table 4.2 above shows the lowest mean rating of 3.76 with a standard deviation of 1.068 as compared to the highest mean rating of 3.96 with a standard deviation 1.031. Descriptive statistics for assessing any international standards set by developed nations in investigating digital currencies that can also be adopted by developing countries like Zimbabwe showed an average mean of 3.8675 with a standard deviation of 0.97975. On average, respondents were agreeing that there should be an approval of financial institutions who handles Bitcoin transactions as a standard that enhances digital currency investigations. According to Kyc (2021) major governments across the globe have taken very different approaches to the regulation of cryptocurrency. The landscape is still evolving, but given the bureaucratic tendencies of governments, much remains to be seen.

These examples of countries around the world on how they are regulating cryptocurrency. In United States, while cryptocurrencies are legal, there does not seem to be a consistent legal approach to them. Laws vary greatly state by state, and federal laws cannot seem to agree as to what cryptocurrency is. For example, the Financial Crimes Enforcement Network considers cryptocurrencies to be money transmitters, while the IRS regards them as property. Cryptocurrency exchanges also face much uncertainty when it comes to regulation. Several different regulators claim jurisdiction, and there has yet to be a cohesive approach. Policies vary greatly. The US though, is beginning to take steps to create overarching crypto regulation. The US Treasury has been outspoken regarding the regulation of cryptocurrencies to combat criminal activities, and change may be on the horizon.

According to Kyc (2021) in the European Union cryptocurrency is widely considered legal across the EU, but the rules for exchanges differ across member states. Taxation also varies, ranging anywhere from 0% to 50%, and crypto is subject to capital gains tax. To date, the EU Parliament has passed no specific legislation regarding cryptocurrencies. Exchanges are required to register with their local financial authority, and from there can operate across the entirety of the EU. The 5th AML Directive now requires that crypto exchanges follow the EU's anti-money laundering regulations. Luckily for some, exchanging FIAT currency to crypto is not subject to VAT.

While UK divorced itself from EU through Brexit, they have created their own regulations for cryptocurrencies. Currently, crypto is not considered to be legal tender, although cryptocurrency exchanges are legal. The potential taxability of cryptocurrency depends on the activities and parties involved, although gains or losses on cryptocurrency are subject to capital gains tax. Cryptocurrency exchanges will need to register with the Financial Conduct Authority (FCA, however, some exchanges may be able to apply for an e-license. As of January 2020, the FCA now has the power to supervise how cryptocurrency businesses deal with terrorism financing and money laundering associated risks. In the grand scheme of things, the UK is far from the target and post-Brexit it becomes interesting how the legal framework moves.

In Russia there has a complicated history regarding cryptocurrency, and now seems to be taking actions against its use. In Russia, crypto is considered to be a money substitute, and recent laws of 2019 have now made money substitutes illegal in the country. It is still unclear what crypto is defined as and can be used for. New proposals are being made that could allow crypto to be confiscated, and these proposals are rumored to soon be made into law. It is unclear as to how the

Russian government plans to confiscate crypto, especially Bitcoin which is anonymous and decentralized.

4.8.4 To recommend action and guidelines to improve the current financial digital currency investigations eco-system.

Table 4.5 below shows descriptive statistics for recommendations on action and guidelines to improve the current financial digital currency investigations eco-system.

Table 4.5: Mean and standard deviation for recommendations on action and guidelines to improve the current financial digital currency investigations eco-system.

Item	**Mean**	**Std. Deviation**	**N**
Improving mutual legal assistance approaches	3.48	1.175	100
Clear financial intelligence network in place	3.49	1.199	100
Capacity building through training investigators	3.74	.996	100
Setting up a regulatory authority	3.90	1.037	100

Overall mean =3.6275; Standard deviation= 1.101

Results in Table 4.9 above shows the lowest mean rating of 3.48 with a standard deviation of 1.175 as compared to the highest mean rating of 3.90 with a standard deviation 1.037. Descriptive statistics for recommendations on action and guidelines to improve the current financial digital currency investigations eco-system showed an average mean of 3.6275 with a standard deviation of 1.101. On average, respondents were agreeing on setting up a central regulatory authority. According to Mazikana (2018) a popular narrative noticed in his survey was the government giving warnings about dangers of relying on cryptocurrency investment which would be meant for educational purposes focusing on the non-government guarantee aspects of cryptocurrencies. These government notices tell people that most of the agencies facilitating cryptocurrency are unregistered and the unpredictability risks of cryptocurrency as such investing in at own risk with no legal action for restitution.

Table 4.6 Direction of the relationship between ways of adopting digital currency and investigations performance.

Chi-Square Tests	Value	Df	Asymp. Sig. (2-sided)
Pearson Chi-Square	78.079[a]	4	.000
N of Valid Cases	100		
a. 2 cells (20.0%) have expected count less than 5. The minimum expected count is 3.45.			

		Value	Approx. Sig.
Ordinal by Ordinal	Gamma	-.683	.000
N of Valid Cases		100	
a. Not assuming the null hypothesis.			
b. Using the asymptotic standard error assuming the null hypothesis.			

Tables 4.6 above shows there is an association between ways of adopting digital currency and investigations performance. Gamma -.683 displays a negative relationship that is strong. This means that as adopting digital currency in Zimbabwe become more and more formal, it would influence investigations outcomes. From the above statistical analysis conducted on the adoption of digital currency and its impact on investigations outcomes, conclusion can be drawn that there is association between adopting digital currency and

investigations performance as measured by prohibition orders per year.

4.9 Testing Research Hypotheses

This section presents results of research hypotheses.

4.9.1 Testing hypotheses (H1, H2, H3, H4)

The study seeks to test the following hypotheses.

H1: Expected performance possess a positive impact on the intention by criminals to use digital currency.

H2: The greater the effort expectancy in investigating the greater the intention by criminals to use digital currency.

H3: Influence of society has a positive impact on the intention by criminals to use digital currency.

H4: The greater the facilitating conditions digital currency has the higher the intention by criminals to use digital currency.

Multiple-regression analysis was used to test the hypotheses and results are shown in Table 4.7, Table 4.8 and Table 4.9 below

Table 4.7 Model summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.344[a]	.118	.091	1.67549
a. Predictors: (Constant), H1, H2, H3, H4 b. H1 Performance expected c. H2 Effort expected d. H3 Social influence e. H4 Facilitating conditions				

Results in Table 4.7 show that the four constructs explain about 12% of changes in behavioural intention. This is shown by the R square value of 0.118. This implies that there are other factors that influence the adoption of digital currency by individuals with criminal intentions. Table 4.8 below shows the ANOVA test results.

Table 4.8 ANOVA

ANOVA[a]						
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	48.189	4	12.047	4.291	.003[b]
	Residual	359.330	128	2.807		
	Total	407.519	132			
a. Dependent Variable: Behavioural Intention						
b. Predictors: (Constant)						

Results in Table 4.8 above show that the model is statistically significant (F= 4.219; p= 0.003). This implies that the regression model is relied upon. **Table 4.9 below** presents coefficients results for factors influencing behavioural intention.

Table 4.9 Coefficients

Coefficients[a]						
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	8.126	1.240		6.552	.000
	Performance Expected	.125	.065	.190	1.927	.056
	Effort Expected	.053	.062	.077	.841	.402
	Social Influence	.077	.068	.112	1.133	.259
	Facilitating Conditions	.055	.048	.099	1.146	.254
a. Dependent Variable: Behavioural Intention						

Results in Table 4.9 above show that performance expectancy has a partial effect on behavioural intention (Beta= 0.190, t= 1.927, p= 0.056). However, since the p-value of 0.056 is above the expected p-value of 0.050, H1 is not supported. This implies that performance expectancy does not influence behavioural intention to adopt digital currency among individuals with criminal intentions in Harare. These results contradict Venkatesh et al. (2003) who found a significant relationship between performance expectancy and behavioural intention. The reason could be that the study by Venkatesh et al. (2003) focused on the utilization of technology in general, while the current study focused only on a specific financial technology and criminality.

Results in Table 4.9 show that effort expectancy has an insignificant effect on behavioural intention (Beta= 0.077, t= 0.841, p= 0.402). Therefore, H2 is not supported. This implies that effort expectancy when investigations does not influence behavioural intention by criminals to adopt digital currency. This contradicts Venkateshet al. (2003) who claims that effort expectancy influences behavioural intention. The reason could be that the study by Venkatesh et al. (2003) focused on the adoption of technology such as machinery while the current study focused on digital financial application.

Results in Table 4.9 above indicate that social influence has an insignificant effect on behavioural intention (Beta= 0.112, t= 1.133, p= 0.259). Therefore, H3 is not supported. This implies that social influence does not influence behavioural intention by criminals to adopt digital currency. For this reason, one's environment do not have an impact on an individual to adopt digital currency use for criminality.

Results in Table 4.9 above show that facilitating conditions has an insignificant effect on behavioural intention (Beta=0.099, t= 1.146, p= 0,254). Therefore, H4 is not supported. This implies that facilitating conditions on digital currency does not influence behavioural intention by criminals to adopt digital currency. These findings differ from those of Venkatesh et al. (2003) showing that conditions for facilitating possess a positive impact on behavioural intention to adopt a technology. However, the findings are similar to those of Alshehri, Drew and Alghamdi (2012) which established no significant effect of facilitating conditions on behavioural intention to accept e-government services.

4.10 Chapter summary

In this chapter, quantitative data and qualitative data were presented. Pie Charts, Tables, Bar graphs were utilized to present data. The research adopted a mixed approach to collect quantitative and qualitative data. Quantitative data was presented by utilizing the sequence based on the research questions from questionnaire. The response rate which was recorded for this study was 87%, with a 13% non-response rate are questionnaires not returned.

Chapter 5: Recommendations and Conclusions

5.0 Introduction

This research focused on the complexities digital currency has on financial investigations in relation to money laundering and terrorism financing. A case of

Zimbabwe. The previous chapter looked at research results presentation, statistical analysis, and discussion. This final chapter of the study shall dwell on the recommendations by researcher and lastly offer conclusive statements based on the research questions and guided by the objectives of study.

5.1 Recommendations

The researcher makes the following recommendations as a direct outcome of this study.

5.1.1 Recommendation 1

Financial Investigations Agencies in Zimbabwe are encouraged to adopt a strategic approach to investigating digital currency platforms through the promotion of world best practices. It can be achieved by deliberate implementations of Financial Action Task-force (FATF) evaluation reports and United Nations Office on Drugs and Crime (UNODC) proposed virtual currency investigation manual and ask for assistance for capacity building initiatives as these international bodies have the funding and budgets aimed at helping developing countries like Zimbabwe be trained and be exposed to keeping abreast with emerging trends, tools and software's being used for investigative purposes.

5.1.2 Recommendation 2

Legislature and Judiciary should foster the creation and implementation of harmonisation of laws such as the Cyber Security, Crime and Data Protection Bill, Criminal Procedure and Evidence Act and Criminal Law Codification Act, for instance, to facilitate the plugging of legal impediments for investigators when seeking court orders to confiscate possible items or gadgets that may contain digital evidence and also to be able to effect arrests through clearly defined legal breaches when investigating digital currency platforms. This is possible when policy makers deliberately embrace these digital currency technology innovations and create a digital currency regulatory framework that encourage technology development.

5.1.3 Recommendation 3

Reserve Bank of Zimbabwe as the financial regulator through a piece of legislation formulated to promote bank use and suppression of money laundering should speedily formalise digital currency practices operations in order to adopt a professional stance which would make it easier to institute compliance and monitoring initiatives for basic anti-money laundering and terrorism financing modalities that would result in Financial Intelligence Unit (FIU) duties of supervision more effective as they would operate within the margins of regulatory guidelines. Formalisation of digital currency industry entails bringing more currency security and stability for the country.

5.1.4 Recommendation 4

Financial investigators in Zimbabwe should increase liaison with regional fundamental structures for cooperation such as Southern African Region Police Chiefs Coordination Organisation(SARPCCO), Southern Africa Organ on Politics, Security and Defence, Interpol Sadc Regional Headquarters, National Cyber Bureau (NCB) in Zimbabwe which should be utilised for digital currency investigations as they have an already existing cooperating network and infrastructure that can make facilitation of mutual legal assistance request be processed in time as a measure to curtail on bureaucratic tendencies involved when filing for cross border operations.

5.2 Conclusions of the Study

5.2.1 Conclusion: Research objective 1: To determine specific complexities encountered when investigating digital currencies from a sample of financial investigators.

This study did establish specific legal and technological issues surrounding digital currency platforms use which make investigations of money laundering and terrorism financing complicated to achieve arrests and prosecutions in developing countries like Zimbabwe chiefly being laxity in cyber regulatory framework and lack of tools and understanding on how to investigate new technology like blockchain. It was noted that criminals could be favouring the use of virtual currencies mainly because of their very nature which involve, increased ability to use pseudo-names which promote high chances of anonymity with platforms like darknets facilitating easy movement and illegal payments of services coupled with the transnational nature of digital technology facilitated by internet. Hence this objective was achieved.

5.2.2 Conclusion Research Objective 2: To investigate how other developing countries who have adopted digital currencies are coping.

The study established that other countries use regulatory instruments and are at an advanced stage to adopt centralised digital currency operations. It also established that there should be a framework to facilitate harmonisation of laws for better cooperation as the use of digital currencies by criminals has transnational characteristics that require use of existing bodies like INTERPOL, FATF and UNODC set standards. Cryptocurrencies give huge prospects for developments and inventions but at the same time are distinctively positioned to aid money laundering and terrorism financing as shown with cases in South Africa of illicit flows investigations increasing with identified individuals being on wanted lists. This objective was partially achieved as more work still needs to be from a developing countries perspective.

5.2.3 Conclusion Research objective 3: To assess any international standards set by developed nations in investigating digital currencies that can also be adopted by developing countries like Zimbabwe.

This study noted the Basic Manual on Detection and Investigation of Laundering of Crime Proceeds by Virtual Currencies UNODC and the Train the Trainers Course in 2018 by UNODC could be considered as best set practices for investigations of digital currency platforms so far. Another important set standard is the governing of financial institutions that handles digital currency transactions which would help investigators when tracking and monitoring operations. It was also noted that major governments across the globe have taken very different approaches to the regulation of cryptocurrency as the digital currency technology is still evolving so much remains to be seen but otherwise the objective was achieved.

5.2.4 Conclusion Research Objective 4: To recommend action and guidelines to improve the current financial digital currency investigations eco-system.

The study asserts that an effective digital currency investigation eco-system involves various stakeholders who are Policy makers, Regulators, Law enforcement, International Bodies, General Public and the Criminal Justice System as a whole. As a matter of priority there should be a setting up of a regulatory authority that result in central governing of digital currency operations than to have warnings issued by government on the disadvantages of cryptocurrency investments. Financial Intelligence Unit should be given arresting powers for financial breaches than investigative powers only as this would smoothen the chain of custody for digital currency evidence. Judiciary should also compliment investigators through being trained on how to recognize digital evidence of financial nature in court proceedings from arrest to trial and fundamentally the educating the citizenry is critical by emphasizing on reporting any suspicions transaction on any platform on time which influences investigations.

5.3 Further suggestions for future research

This research focused on the complexities digital currency has on financial investigations in relation to money laundering and terrorism financing. A case of Zimbabwe. The author for this study suggests that the following areas be examined to generate more knowledge on digital currency platforms investigations:

(a) The attitude of senior or older investigators who were used to traditional guidelines of fighting financial crime, as a barrier to adoption of digital currency technology investigations tools and software's.

(b) The contribution of capacity building programmes for digital currency investigation to the anti-money laundering and terrorism financing regime in Zimbabwe.

(c) The effect of formalising digital currency to financial investigations in Zimbabwe.

References

Adrian, A., (2018). Data Challenges. Database Systems Journal, 4(3), pp. 31-40.

Alles, M., (2015). Drivers of the Use and Facilitators and Obstacles of the Evolution of

Data by the Audit Profession. American Financial Association, 29(2), pp. 439-449.

Alves, M. D. C. G., Matos, S. I. A. (2010). Adoption of enterprise resource planning system – some preliminary results. Proceedings of the European Conference on Information Management & Evaluation

Brown-Liburd, H., Issa, H. & Lombardi, D., (2015). Behavioral Implications of Data's Impact on Audit Judgement and Decision Making and Future Research Directions. Financial Horizon's, 29(2), pp. 451-468.

Business.com, (2017). business.com. Available at: https://www.business.com/articles/-data--problem-coping-with-shortageof-talent-in-data-analysis/ Assessed 15 May 2017].

Byrnes, P., Criste, T., Stewart, T. & Vasarhelyi, M., (2016). Reimagining Technology in a Wired World. Available at: http://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/DownloadableDocuments/Whitepaper_Blue_Sky_Scenario-Pinkbook.pdf

Boerkamp, F., & Soerjoesing, S. (2010). Data-analyse als procesgericht controlemiddel. De IT-Auditor, 2, 29-34.

Byrnes, P., Ames, B., Vasarhelyi, M., & J.D. Warren, J. (2012). The Current State of Continuous Technology and Continuous Monitoring.

AICPA. Byrnes, P., Criste, T., Stewart, T., & Vasarhelyi, M. (2014). Re-imagining Technology in a Wired World. Chan, D., & Vasarhelyi, M. (2011). Innovation and practice of continuous technology.

International Journal of Financial Information Systems, 12, 152-160.

Cao, M., Chychyla, R. & Stewart, T., (2015). Digital currenciesin Financial Statement Audits. Financial Horizons, 29(2), pp. 423-429.

Coyne, E., Coyne, J. & Walker, K., (2017). Data Information Governance by Accountants. International Journal of Financial and Information Management (forthcoming), Volume Working paper, pp. 1-34.

Crawford, K. & Boyd, D., (2016). Six Provocations for Data. Oxford Internet Institute's, p. 17.

Cobbin, P. E. (2012). International Dimensions of the Audit Fee Determinants Literature. International Journal of Technology, 6, 53-77.

Coderre, D. (2015). Continuous Technology: Implactions for Assurance, Monitoring and Risk Assessment. IIA.

Craswell, A. T., Francis, J. R., & Taylor, S. L. (2015). Auditor brand name reputations and industry specilizations. Journal of Financial and Economics, 20, 297-322.

Culotta, Aron. (2010). "Towards Detecting Influenza Epidemics by Analyzing Twitter Messages." In Proceedings of the First Workshop on Social Media Analytics, 115–22. SOMA '10. New York, NY, USA: ACM. doi:10.1145/1964858.1964874.

Das, Sanjiv R., and Mike Y. Chen. (2017). "Yahoo! For Amazon: Sentiment Extraction from Small Talk on the Web." Manage. Sci. 53 (9). Institute for Operations Research; the Management Sciences (INFORMS), Linthicum, Maryland, USA: INFORMS: 1375–88. doi:10.1287/mnsc.1070.0704.

DeAngelo. (2011). Audit size and reducing liquidity crunch. Journal of Financial and Economics, 3, 183-199.

Zimbocash. (2010). Continuous monitoring and continuous technology: From idea to implementation. Zimbocash.

Dean, Jeffrey, and Sanjay Ghemawat. (2018). “MapReduce: Simplified Data Processing on Large Clusters.” Commun. ACM 51 (1): 107-13. doi:10.1145/1327452.1327492.

Domingos, Pedro. (2012). “A Few Useful Things to Know About Machine Learning.” Commun. ACM 55 (10). New York, NY, USA: ACM: 78-87. doi:10.1145/2347736.2347755

Earley, C. E., (2015). Digital currenciesin technology: Opportunities and Challenges. Business Horizons, Volume 58, pp. 493-500.

Gershkoff, A., (2015). techcrunch. [Online] Available at: https://techcrunch.com/2015/12/31/how-to-stem-the-global-shortage-of-datascientists

Ginsberg, Jeremy, Matthew Mohebbi, Rajan Patel, Lynnette Brammer, Mark Smolinski, and Larry Brilliant. (2019). “Detecting Influenza Epidemics Using Search Engine Query Data.” Nature 457: 1012-4. http://www.nature.com/nature/journal/v457/n7232/full/nature07634.html

Hay, D., Knechel, R. & Wong, N., (2016). Audit Fees: A Meta-analysis of the Effect of Supply and Demand Attributes. Contemporary Financial Research, 23(1), pp. 91-141.

Hayes, R., Gortemaker, H. & Wallage, P., (2017). Principles of Technology. 3e ed. Harlow: Pearson Education Limited.

Halevy, Alon Y., Peter Norvig, and Fernando Pereira. (2019). “The Unreasonable Effectiveness of Data.” IEEE Intelligent Systems 24 (2): 8-12. doi:10.1109/MIS.2009.36.

Kessel, P. v., (2017). Data: Changing the way business operate, United Kingdom: Ernst & Young.

Loukides, Michael. (2012). What Is Digital currency. Sebastopol, California:

O'Reilly.

Liddy, J., (2015). How Data and Analytics Are Enhancing Reducing liquidity crunch and Value. The CPA Journal, 85(5), p. 80.

Manson, S., McCartney, S. & Sherer, M., (2017). Audit automation: Improving quality or keeping up. In: M. Sherer & S. Turley, eds. Current Issues in Technology. Thousand Oaks,:Sage Publications.

Mayer-Schönberger, Viktor, and Kenneth Cukier. (2013). Data: A Revolution That Will Transform How We Live, Work, and Think. Second. New York, NY: Houghton Mifflin Harcourt.

Nasser, T. & Tariq, R., (2015). Data Challenges. Journal of Computer Engineering & Information Technology, 4(3), p. 10.

NBA, (2015). four investeren fors in data. Accountant, 13 11, p. 2.

Patil, Dhanurjay (2012). Data Jujitsu. Sebastopol, California: O'Reilly.

Patil, Dhanurjay (2011). Building Digital currency Teams. Sebastopol, California: O'Reilly.

Pepping W & Nooitgedagt (2014). Digital currenciesin financial statement audit: Does digital currenciesimprove the efficiency of an audit?

FINANCIAL INTELLIGENCE UNIT, (2015). Financial Intelligence Unit .com Available at: https://www.Financial Intelligence Unit .com/gx/en/audit-services/publications/assets/Financial Intelligence Unit -fact-sheet3-summary-of-eu-audit-reform-requirements relating-to-nas-feb-2015.pdf

Ramlukan, R., (2015). Available at: http://www.ey.com/gl/en/services/assurance/ey-reporting-issue-9-how--dataand-analytics-are-transforming-the-audit#item1

Ruhnke, K. & Schmidt, M., (2017). The audit expectation gap: existence, causes and the impact of changes. The audit expectation gap

Siegel, Eric. (2013). Predictive Analytics. New Jersey: John-Wiley; Sons.

Vasarhelyi, M. A., & Romero, S. (2014). Technology in audit engagements: a case study. Managerial Technology Journal, 29(4), 350-365.

Whitehouse, T., (2017). Technology in the Era of Data. Compliance Week, 29 April, p. 2.

Pîrjan, A., Petrosanu, D.-M., Huth, M., and Negoita, M. 2015. "Research Issues Regarding the Bitcoin and Alternative Coins Digital Currencies," Journal of Information Systems & Operations Management (9:1), pp. 1-14

Glaser, F., and Bezzenberger, L. 2015. "Beyond Cryptocurrencies-a Taxonomy of Decentralized Consensus Systems," 23rd European Conference on Information Systems (ECIS), J. Becker, J.V. Brocke and M. De Marco (eds.), Münster, Germany.

https://www.investvoyager.com/blog/peer-to-peer-transactions-spike-in-zimbabwe-following-foreign-currency-ban/

https://www.nasdaq.com/articles/the-future-of-digital-currency-2021-02-12

https://www.csis.org/analysis/train-leaving-station-digital-currency-sub-saharan-africa

https://www.unodc.org/unodc/en/drug-trafficking/crimjust/news/unodc-delivers-the-first-cryptocurrency-investigation-training-course-in-latin-america.html

https://bitcoinist.com/zimbabwe-finally-regulates-cryptocurrency/

https://www.imolin.org/pdf/UNODC_VirtualCurrencies_final_EN_Print.pdf

Frank Schmalleger & Michael Pittaro 2015, Crimes of the Internet, published by Prentice Hall (2008: 283-301).

Jaishankar, K. (2008). Space Transition Theory of cybercrimes. In Schmallager, F., & Pittaro, M. (Eds.), Crimes of the Internet. (pp.283-301) Upper Saddle River, NJ: Prentice Hall.

Cornish, D., & Clarke, R. V. (1986). The reasoning criminal: Rational choice perspectives in offending. Springer-Verlag: New York, NY.

http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf

https://thenextweb.com/hardfork/2019/12/26/bitcoin-cryptocurrency-criminals-law-enforcement/

https://www.reuters.com/article/bc-finreg-aml-cryptocurrency-idUSKCN1FX29I

https://coinidol.com/african-countries-cryptocurrency/

https://businesstech.co.za/news/technology/228769/hawks-investigating-multi-million-rand-bitcoin-scam-in-south-africa-report/

https://www.fincen.gov/sites/default/files/advisory/2019-05-10/FinCEN%20Advisory%20CVC%20FINAL%20508.pdf

Appendix 1

Questionnaire: Digital Currency Investigations Survey

Academic study by collection of financial investigators views about digital currency.

1.What is your level of understanding about digital currency?

Low (You only have heard of it)

Medium (You know basics so need more information)

High (You have huge exposure to the platforms)

Other

2.Which organization do you belong to?

Police

Financial Intelligence Unit

Bank Loss Control and Security

Anti-Corruption Unit

Currency Agent

Other

3.What is your responsibility in investigation cycle for digital currency?

Analyst (Case Officer)

Investigation's officer

Currency Dealer

Other

4.Is Digital Currency Crime prevalent?

Yes

No

Not Sure

5.What are the weaknesses digital currency has that makes it difficult to investigate?

…………………………………………………………………………………….

6.Do you see the skills to investigate digital currency available?

Yes

No

Maybe

7.How can authorities stop unregulated digital currency trade?

……………………………………………………………………………………

8.Do you believe in the regulatory framework available for digital currencies?

…………………………………………………………………………………….

Appendix 2

Interview guide for Digital Currency Investigation

1) Some argue that digital currency use needs financial authorities' involvement, how can this help investigators?...

2) Given the crossing of borders of cyber space, how is the cooperation situation with other countries when investigating?...

3) What are the consequences for investigators when digital currency use is banned though trade still goes on?..

디지털 화폐 플랫폼 수사의 복잡성에 관한 연구. 짐바브웨의 자금세탁 및 테러자금조달 사례.

2021년 6월 15일
정보법과학 석사학위 논문

럭슨 타파드와 즈비리쿠제
국제학과

지도교수: 장윤식

요약

주된 목적은 비트코인과 같은, 블록체인 기술을 활용해 금융 조사를 복잡하게 하고, 규제 기관과, 특히 자금 세탁과 전세계와 짐바브웨와 같은 개발도상국에 테러자금조달과 관련된 금융 시스템의 확산을 통찰하는 것이다.

본 논문은 짐바브웨에서 디지털 통화 플랫폼 내 거래가 실생활과 밀접함을 밝히며, 플랫폼

내에서 이뤄지는 자금 세탁과 테러 자금 조달의 범죄성을 보여주는 조사 통계가 아직 완전하지 않기 때문에, 조사 중에 금융 조사관에게 벽으로 다가오는 디지털 통화 플랫폼의 몇 가지 복잡성을 강조한다.

이 연구는 인터폴과 같은 기존 협력 기관과 디지털 화폐 거래 플랫폼 내의 모든 거래의 유동과 주소를 추적할 수 있는 소프트웨어 및 툴들을 이용한 법적 프레임워크로 도출되는 전략적 접근 방식을 채택할 필요성을 강조하고, UNODC 와 KOICA 와 같은 국제 기구가 디지털 화폐 거래 플랫폼 관련 수사관을 양성해야한다 조언하며, 질문과 인터뷰, 주제와 관련된 오픈 소스 자료를 통해 자금 세탁과 테러 자금 지원을 수사하는 금융 정보 조사관들의 관련 자료를 통해 금융 디지털 통화 조사의 생태계를 개선하기 위한 구체적인 실현 가능한 조치와 지침을 결정하기 위해 혼합 연구 전략을 이용했다.

. 키워드: 디지털 통화, 자금 세탁, 테러자금조달, 금융 수사, 복잡성

Study about Complexities on Digital Currency Platforms Investigations. Case of Money Laundering and Terrorism Financing in Zimbabwe.

2021 June 15, 2021
Master's Degree Legal Informatics and Forensic Science
Luckson Tafadzwa Zvirikuzhe
Department of International Studies
Advisor Prof Yunsik Jake Jang

Abstract

The main objective was to provide an insight on the proliferation of digital currency platforms like Bitcoin that uses blockchain technology that has brought with it some complications for financial investigations, regulatory authorities, and the financial system especially in relation to combating money laundering and terrorism financing the world over and developing countries like Zimbabwe have not been spared also. This paper highlighted some of the complexities about digital currency platforms that exist for financial investigators during investigations, undertaken because of the declarations that digital currency platforms for trade are a reality in Zimbabwe and investigations statistics on money laundering and terrorism financing that display criminality on these platforms are not yet fully available. A mixed research strategy was adopted for this study to determine specific possible recommendable actions and guidelines to improve the current financial digital currency investigations eco-system with relevant data drawn from mainly Financial Intelligence officers who are mandated to investigate money laundering and terrorism financing through questionnaires and interview forms and supported by open source material on the subject matter thereby necessitating to draw conclusions that there is need to adopt a strategic approach that is guided by legal frameworks, using existing cooperation bodies like Interpol, adoption of software's and tools that can be able to trace movements and addresses of transactions on any digital currency platform and the need to train investigators through capacity building programs by international bodies like UNODC and KOICA for skills development.

Keywords: digital currency, money laundering, terrorism financing, financial investigations, complexities

OO학 석사 학위논문

A Study about Complexities on Digital Currency Investigations

Case of Money laundering and Terrorism Financing (Zimbabwe)

디지털 통화 조사의 복잡성에 대한 연구
짐바브웨의 자금 세탁 및 테러 자금 조달 사례

Luckson Tafadzwa Zvirikuzhe

국제학과 Department in International Studies

법률 정보학 및 법의학 Major in Legal Informatics and Forensic Science

한림대학교 대학원

(Graduate School, Hallym University)

Table of Contents

List of Tables

List of Figures

CHAPTER 1: INTRODUCTION

1.0 Introduction

This research focused on the complexities digital currency has on financial investigations in relation to money laundering and terrorism financing. A case of Zimbabwe. Digital currency in this context is a form of currency that is available only in digital or electronic form, and not in physical form. It is also called digital money, electronic money, electronic currency, or cyber cash. (Adrian, 2018). The background of the study, the statement of the problem, the objectives of the study and the research questions are laid out in detail in this chapter to provide a conceptual foundation through which the research problem for this study can be understood. Study significance and assumptions are also presented and discussed together with the delimitations and limitations encountered during study.

1.1 Background of the study

Although global efforts are being made to standardize, control, and regulate digital currency use, structural issues in developing countries like Zimbabwe, more work is needed to be done especially in capacity building for investigators and provision of the necessary tools and software's introduced in developed countries that are being used for tracking transactions of digital currencies. There are numerous digital currencies in existence as of now but to best demonstrate the level of activity, our attention is on the gest and best-known digital currencies, crypto-currency, and Bitcoin. The non-regulation of digital currency in Zimbabwe gives rise to the use of crypto- currency like Bitcoin, of which trade has remained with peer-to-peer transactions taking place, as this offers users with storage of value, plug foreign currency and liquidity gaps in the financial system since the Zimbabwe dollar is overwhelmed by uncertainty. According to Chainalysis research, fraudulent digital currency platforms received just over $8 million from users in Africa in June 2020 alone and Bednar et al. (2008) nominates that when it comes to digital investigations, the cybercrime scene can exhibit a high amount of complexity and uncertainty and these characteristics add to the challenge's investigators face for collaborating at an international level Financial Action Task Force (FATF) defines digital currency as a digital representation of either virtual currency or e-money worth to be digitally traded and can operate to store of value and as a unit of account.

In 2018 during launch of Cryptogem in Zimbabwe Capital City, where it offered Bitcoin trading despite the de facto cryptocurrencies ban by the Reserve Bank of Zimbabwe. Melissa Mwale, Cryptogem Global Chief Executive Officer and co-founder, told Bitcoin.com: "Cryptogem Global is a bitcoin trading platform where people around the globe can exchange their local currencies and e-money to bitcoin." Tawanda Kembo, CEO and founder of Golix, a Zimbabwe-based crypto exchange, told Quartz Africa in 2019 that, "There is little supply compared to demand so all the activity in bitcoin which we are seeing is happening on dark markets instead of exchanges."

Such use is not bound by any financial regulatory obligation which enforcement of traditional anti-money laundering and terrorism financing practices such as the suspicious transactions reporting and know your customer principles becoming an investigative nightmare. The cryptocurrency exchange Golix took the Reserve Bank of Zimbabwe to court after they tried to shut them down and won, legally declaring that Reserve Bank had no mandate over prohibiting cryptocurrency industry and trading, leaving the Reserve Bank with the only option of closing exchanges bank accounts. Firstly, the author notes that digital currency is the easiest, smartest, and most private way to launder money internationally, mainly sustained by anonymous Bitcoins. Secondly, there is no globally established standard for regulating digital currency exchanges, with many lacking risk, sanctions-screening and anti-money laundering protocols.

Reserve Bank of Zimbabwe (RBZ) deputy director of financial markets and national payment systems Josephat Mutepfa commented that, the bank is in the process of starting to come up with a fintech framework since proper structures in regulation are everything. "The framework, which is a regulatory sandbox, will be assessing the cryptocurrency companies as to how they are going to operate which would ensure that all cryptocurrency companies are properly vetted to meet regulatory requirements." It is therefore aim of this study to do an analysis on how digital currencies continued use affect investigations modalities that should normally or systematically culminate from the formal requirements like customer due diligence for financial institutions to carry out as envisioned by Financial Action Task Force (FATF) recommendations for anti-money laundering and terrorism financing surveillance measures.

As underlined by Bo Mathiasen, the point person for (UNODC) United Nations Office on Drugs and Crime in Colombia, "the use of new technologies by organized criminal groups cannot be underestimated and has an impact on criminal activities across the spectrum of serious and organized crime. Technology has a fundamental and lasting impact on the nature of crime and development simultaneously". In 2014 ONODC presented a manual basically on detection and investigation of laundering crime proceeds using virtual currencies, to provide practical information for investigators and prosecutors on the detection, investigation, prosecution, and seizure of crime proceeds laundered using virtual currencies. This manual is paramount to be mentioned in this study as it complements the realization that digital currency investigation needs a formalized approach that has clear guidelines to be able to successfully fight money laundering and terrorism financing on these virtual platforms brought by technological advancements. In 2018, it was reported that Zimbabwe's finance minister Mthuli Ncube said that" their country should treat bitcoin as Switzerland does". A publication from IT Web Africa quoted him saying, "Zimbabwe should be investing in understanding innovations and often central banks are too slow in investing in these technologies."

As digital currencies are unrestrained by terrestrial and political borders, a coalition of policy regulatory, law enforcement, banking, and academic collaborators must create global standards to tackle the escalating threat of digital money laundering. To effectively investigate digital currencies, it is paramount to provide the right set of tools and methods to investigators for countering this growing phenomenon because cryptocurrencies like Bitcoin with the use of blockchain technology have allegedly been accused of facilitating money laundering and promoting terrorist financing. Following articulated background, it is the wish of this study to gain deeper knowledge into the landscape of the complications digital currency platforms have on financial investigations in relation to money laundering and terrorism financing looking at a case of Zimbabwe.

1.2 Statement of the problem

Financial regulators are concerned that the nature of digital currency platforms complicates investigating cases of money laundering and terrorism financing. Companies like Golix, Cryptogem believe that digital currencies are a game changer that needs to be embraced in the era of digital society. However, from an investigative perspective it is therefore critical to look at the current notions that surround the resistance of digital currency platforms like virtual assets and how they affect investigations on money laundering and terrorism financing in Zimbabwe.

A case of note is that of Golix Crypto-exchange company whose operations were banned by central authorities in 2018 for allegations of violating financial regulations and further red-flagged all associated bank accounts in Zimbabwe, necessitated by the Financial Intelligence Unit (FIU) that is empowered by law to be responsible for investigating terrorism financing and money laundering cases and since digital currencies have allegedly been accused of playing a facilitation role for financial crimes as an advanced financial system fundamental questions arise, for example, does the current crop of investigators have the know-how in terms of technical expertise to investigate digital currency platforms? What does it mean for investigators that digital currency has capabilities of operating outside normal or traditional financial institutions practices? Is there cooperation when investigating digital currencies as its transactions sometimes cross-country boundaries? Absence of a centrally controlled system makes it easy to facilitate illegal transactions with digital currencies. These are some of the matters that this study seeks to address.

The reality of the problem can simply be exemplified by imagining a Sinaloa drug cartel in Mexico moving millions of moneys on a flash drive, as an alternative of smugglers carrying physical sacks full of dollar bills, which makes this study not a future-state scenario, but a present financial security threat. Digital currencies do not only facilitate money laundering and terrorism, financing but has also far-reaching consequences that allow criminals to buy and sell unlawful goods and services, ranging from weapons to human trafficking, illegal drugs, child pornography, organs, and mercenaries for hire, through darkweb which is a black-market platform of the internet. It is also against this backdrop that this study therefore seeks to have deeper visualization on the characteristics that digital currency has and the relationship with investigating money laundering and terrorism financing from an investigator's point of view making the study one of its kind to attempt on unveiling a subject whose knowledge is still in infancy.

1.3 Research objectives

The broad objective of this research is to analyze the nature of the complexities digital currency has on financial investigations in relation to money laundering and terrorism financing. A case of Zimbabwe. The specific objectives are.

i. To determine specific complexities encountered when investigating digital currencies from a sample of financial investigators.

ii. To investigate how other developing countries who have adopted digital currencies are coping.

iii. To assess any international standards set by developed nations in investigating digital currencies that can also be adopted by developing countries like Zimbabwe.

iv. To recommend action and guidelines to improve the current financial digital currency investigations eco-system.

To achieve these objectives, the study focused on the following questions.

1.4 Research questions

i. What is the nature of digital currencies that create challenges for investigators in Zimbabwe?

ii. Are the challenges the same with other countries? Knowledge about how others are coping prepares for strategy.

iii. Which international standards set can solve these problems? Standards can be away to ensure harmonization for cooperation.

iv. Can capacity building for regulators and investigators in developing countries yield results? Given UNODC program to increase investigators skills on how to trace transactions on digital currency platforms.

1.5 Hypothesis of the study

The hypotheses for the study are that criminal intentions to use digital currencies are based on:

H1: Its nature and expected performance.

H2: The effort put in investigating.

H3: Social influence on fintech developments.

H4: The facilitation conditions.

1.6 Conceptual Framework

Based on the hypotheses of the study, the conceptual framework for the complexities digital currency has on financial investigations in relation to money laundering and terrorism financing. A case of Zimbabwe is presented in **Figure 1.1** below.

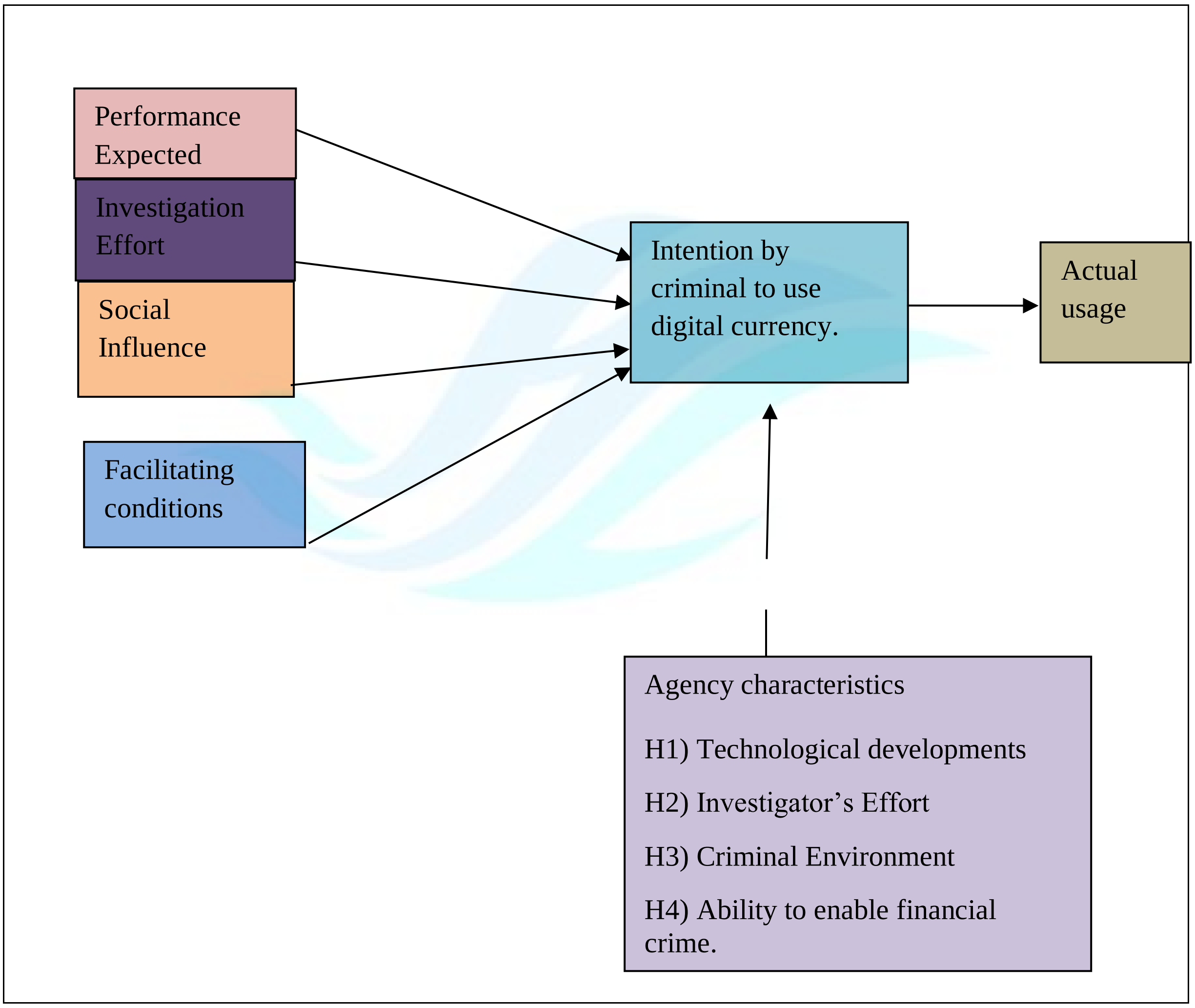

Performance Expected
Investigation Effort
Social Influence
Facilitating conditions
Intention by criminal to use digital currency.
Actual usage
Agency characteristics
H1) Technological developments
H2) Investigator's Effort
H3) Criminal Environment
H4) Ability to enable financial crime.

Figure 1.1: Conceptual framework

Source: Done for this research study

1.7 Significance of the Study

1.7.1 To the student

This research will aid in broadening the researcher’s knowledge on the complexities digital currency has on financial investigations in relation to money laundering and terrorism financing. A case of Zimbabwe. Also, this research is in partial fulfillment of the master’s degree and for the academic enhancement of the students’ knowledge in the field of financial.

1.7.2 To the university

Hallym University being a center of excellence the study will allow the institute to refer to the area of study for future learning purposes. This research will be used by future researchers as reference material for their study. This research shall add on the already existing body of knowledge in academia and in particular, Legal Informatics and Forensic Science department shall be commended for molding such students.

1.7.3 To Institutions

The Reserve Bank of Zimbabwe, Financial Intelligence Unit, Zimbabwe Police and Currency Agencies like Golix Zimbabwe and Cryptogem Global can make use of this study to enhance and fully embrace digital currency through aiding in policy and regulations drafting so as to mold a sustainable financial ecosystem that embrace modern technology by modeling according to international prescribed standards for the adoption of digital currency. This will ultimately give value to Zimbabwe’s financial sector considering that digital currency is financial technology advancement is the direction where the world is pointing to.

1.8 Research assumptions

This research on the complexities digital currency has on financial investigations in relation to money laundering and terrorism financing was guided by the following assumptions.

i. Financial investigations about money laundering and terrorism financing on digital currency platforms are complicated.

ii. Despite respondents being bound by confidentiality of information they shall give accurate and unbiased information without exposing their organisations, and all questionnaires will be answered and returned.

1.9 Study delimitation and limitations

The researcher is currently based in South Korea and upon vacation break visited Zimbabwe to carry out the study in Harare the capital city where Financial Intelligence Unit agents are headquartered and Commercial Crimes unit with the Zimbabwe Republic Police. Targeted population are financial investigation analysts and compliance officers within the financial intelligence community responsible for money laundering and terrorism financing cases, digital currency users and Serious Crimes investigators. The study confined itself to the period 2017 to date because this assisted in evaluating the trend of the digital currency opinions that has been given over the stated period and this is the period where organizations and individuals increased adopting digital currency. More so, the choice of this period was to assist in the use of recent data to confirm results of prior studies.

The limitations of the study which were grouped into methodological, financial, and theoretical limitations. Due to the sensitive and interesting nature of the topic, some respondents were at first reluctant to participate.

The researcher assured respondents of privacy of interviews, their responses were going to be regarded as not breaching secrecy act, and the researcher elaborated to the respondents that their responses were going to be used for academic purposes only. Lack of adequate knowledge about digital currency by some respondents to respond fully to questions affected this research study. Meanwhile the researcher explained the questions to respondents. There was lack of proper finance. The researcher also decided to plan his time well to complete the research at the required time. Then the researcher sacrificed his time to keep the research as the priority and finally he went well with the deadline, and he finally met the deadline. However, the researcher asked for financial assistance from his friends and workmates.

1.10 Structure of the study

Table 1.1 below presents the structure of this study on the complexities digital currency has on financial investigations in relation to money laundering and terrorism financing. A case of Zimbabwe

CHAPTER	DETAILS
1	BACKGROUND AND INTRODUCTION
2	LITERATURE REVIEW AND THEORETICAL FRAMEWORK
3	STUDY METHODOLOGY
4	RESULTS ANALYSIS AND PRESENATION
5	RECOMMENDATIONS AND CONCLUSIONS

Source: Prepared for this study

Chapter 1 is composed of study background, problem statement, objectives of research, questions to research, and study assumptions, its significance, limitations encountered, and definitions of key terms, scope of the study and structure of the study.

Chapter 2 will present the literature review of the study guided by objectives of the study such as to determine specific complexities encountered when investigating digital currencies from a sample of financial investigators, document how other developing countries who have adopted digital currencies are coping, assess any international standards set by developed nations in investigating digital currencies that can also be adopted by developing countries like Zimbabwe and recommend action and guidelines to improve the current financial digital currency investigations eco-system and will also present theoretical framework of the study.

Chapter 3 is on the methodology of the study. The research design is introduced in this chapter. More precisely, the processes of both data collection and the approach stand out clearly, as distinct phases of the research are described. The research philosophy, the research strategy, research design, targeted population, sample size, sampling method, research instrument, data collection procedure, data analysis and presentation methods, reliability and validity, ethical considerations will be laid out.

Chapter 4 will present and analyse data collected in relation to this research study on the vulnerabilities of digital currency on financial investigations relating to money laundering and terrorism financing. Presentation and analysis of the data collected is the most important aspect on this chapter.

Lastly, chapter 5 of this Thesis offer the conclusions and recommendations of the research study.

1.13 Chapter summary

This research is on the complexities digital currency has on financial investigations in relation to money laundering and terrorism financing. A case of Zimbabwe. This chapter discussed the background of the study, statement of the problem, conceptual framework, research objectives, and research questions, scope of the study, significance of the study and limitations of the study. The following chapter will present the literature review of the study which will be guided by research objectives of the study.

CHAPTER 2: LITERATURE REVIEW

2.0 Introduction

This chapter presents literature related to this study to fully comprehend the fundamental aspects which are digital currency platforms and investigations thereof, also guided by previous studies in line with objectives of the study which are to determine specific complexities encountered when investigating digital currencies from a sample of financial investigators, determine how other developing countries who have adopted digital currencies are coping, highlight some international standards set in investigating digital currencies that can also be adopted by developing countries like Zimbabwe and recommend action and guidelines to improve the current financial digital currency investigations eco-system. It also presents theoretical frameworks of the study specifically looking at criminology and technology adoption theories for the purposes of analyzing the crucial subject matter.

2.1 Crypto-Currencies

Crypto currency is a subgroup of digital currencies, is either controlled by centralized institutions or can operationalized through a decentralized network Trautman (2014). According to Karlstrom (2014) asserts that, decentralized currency schemes try to avoid central financial institutions as much as possible and are constructed on a network of transaction associates. If the transaction partners can see each other, they can form up trust grounded on their performances. However, according to Bryans (2014), a centralized currency system, one institution monitors the digital currency, which guarantees that the digital coins can be traced back to fiat currencies or rather used to buy and sell digital goods. For example, the Linden Dollar is a centralized digital currency, with Linden Lab being the issuer. It has some features of fiat currencies just like in the formal money system; a central bank serves as a source of trust for any transaction. Furthermore, Bryans (2014) explains that cryptographic algorithms produce cryptocurrency as a digital token. It is then carried on cyberspace using protocols like peer-to- peer networking. Its value is mainly determined by the demand and supply for the tokens and the significant part of their application exist within the system that is decentralized in which they belong. Harvey (2015) cited benefits that comprises of comparatively inexpensive cost of production, reduces inflation risks, bold security features, comfort of usage on mobile devices and broadcasting through the block chain transmission protocol. Its non- reliance on formal financial institutions that verify and guarantee a transaction, cryptocurrency transactions are confirmed by the user's computers registered on the currency's network. Since the currency is protected by encryption codes, it becomes highly unlikely to upsurge the money supply over a predetermined algorithmic frequency.

Cryptocurrency is basically a digital asset used as a medium of exchange (Chohan, 2017) that is equipped with a cryptographic algorithm to secure or control the flow of transactions in effort to prevent double-spending and the issuance of new units in effort to maintain its limited supply. The idea of cryptocurrency can be traced back to 1983 when David Chaum published a paper titled Blind Signatures for Untraceable Payments. In that paper, he raised a concern about the privacy issue of payment system where the identity of the payee and the information of the transaction can be obtained by a third party. Thus, he proposed an automated payment system with cryptography mechanism that prevents information theft by a third party while still allows the payee and payer to provide proof of payment or their identity “under exceptional circumstances” (Chaum, 2017). He called the mechanism as blind signature cryptosystems that was basically an extension of the RSA algorithm (Griffith, 2014).

Chaum then established a company called DigiCash in the Netherlands to develop and commercialize his idea in the form of eCash. However, the company went bankrupt in 1998 and eventually eCash and other idea of cryptocurrency “faded into the background” (Nian & Chuen, 2015.

2.2 Types of cryptocurrencies

2.2.1 Bitcoin

Bitcoin is a new currency that was operationalized in 2009 by a group of developers or an unknown person using the alias Satoshi Nakamoto. Transactions are made with no middlemen like financial institution. Böhme, Edelman, Christin and Moore (2015) state that, bitcoin is a communication peer-to-peer protocol that enables a payment system and use of virtual currency which (Kelly 2015) says that the concept of cryptocurrencies was described and suggested firstly in 1998, Bitcoin became the first practical proof of the theory. Weber (2015) states that in 2016 Bitcoin users were about 6.56 million and one year later increased to 11.05 million which shows a growing appetite amongst society for its usage. It uses blockchain technology based on encryption in form of a ledger that is updated constantly and run by computers of people in the network which by design eliminates the traditional regulatory institutions that facilitate transactions. Individuals own a copy of the ledger since accounts and transactions existing on blockchain get anonymized by computerized algorithms.

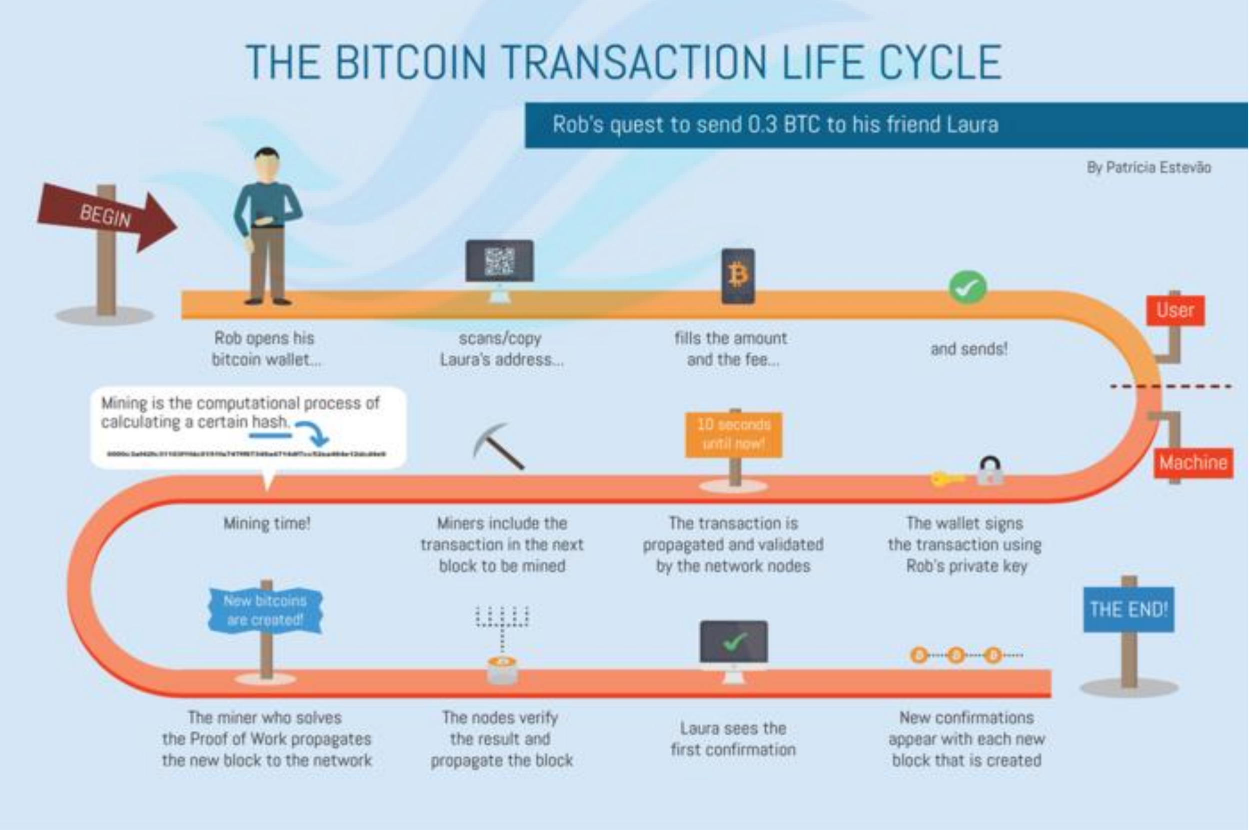
An approved transaction is added to the chain of blocks which is the blockchain and it goes through. Every transaction is public and in event someone tries to corrupt it, the algorithms behind it automatically red flags preventing a consensus among the ledgers. According to Swan (2015), the intermediaries, banks and financial institutions for example become obscured by cryptographic verification. Saure (2016) postulates that, bitcoin as a means of payment is the key function, with transacting costs being maintained low for Bitcoins, resulting in affordable and easy to move quantities of money around the world with fast speeds. However, nowadays it looks like bitcoins are being used for speculative purposes than its intended use which have created a lot of volatility.

Hay (2007) adds that the uncertainty about Bitcoin value makes it volatile, which results in it being a risky investment and even worse to be a formal currency substitute.

According to Coin idol.com (2021) more Africans now have tools on their disposal to plug into the digital currency ecosystem but just like in Zimbabwe, countries like Uganda, Kenya, Tanzania, and Rwanda, digital currencies such as Bitcoin, Ethereum, XRP, are at this time not regulated nor backed by the state or the central banks in the East African region. Nevertheless, the current developments in the region seem to show that Bitcoin and other virtual assets could be treated as securities, but not as currencies which highlights those transactions that still go on despite the environment.

For an investigator to initiate digital investigations, it is necessary to have an appreciation of how the targeted digital currency platform works. Below is a diagram that depict Bit coin cycle or transaction:

Figure 2.1: Taken from https://changelly.com/blog/bitcoin-transaction-explained.


THE BITCOIN TRANSACTION LIFE CYCLE
Rob's quest to send 0.3 BTC to his friend Laura
By Patrícia Estevão
BEGIN
Rob opens his bitcoin wallet...
scans/copy Laura's address...
fills the amount and the fee...
and sends!
User
Machine
Mining is the computational process of calculating a certain hash.
10 seconds until now!
Mining time!
Miners include the transaction in the next block to be mined
The transaction is propagated and validated by the network nodes
The wallet signs the transaction using Rob's private key
New bitcoins are created!
THE END!
The miner who solves the Proof of Work propagates the new block to the network
The nodes verify the result and propagate the block
Laura sees the first confirmation
New confirmations appear with each new block that is created

Digital currency platforms as new technology are being closely scrutinised by law enforcement agencies because of their numerous abilities they possess which criminals favour especially to move and store financial economy with the use of pseudo names (anonymity) so investigations in this case will be aimed at tracing suspected transactions and possibly identify the origins and the destination for the purposes of exposing possible money laundering or terrorism financing cartels to either determine arrests or as evidence gathering for prosecutorial purposes.

According to Federal Bureau of Investigation Director Christopher Wray, cryptocurrency is a "significant issue" that is likely to become a "bigger and bigger" problem for the law enforcement agency. "We are looking at it from an investigative perspective, including tools that we have to follow the money even in this new world that we're living in." Wray supported Romney's line of questioning concerning terrorist financing, saying that U.S. adversaries are becoming "more facile with technology and particular various types of technology that anonymize their efforts." In June 2018, the Bureau said it had one hundred and thirty (130) active cryptocurrency investigations.

2.3 Cryptocurrency in the system of Money Laundering (Valeriia Dyntu 2019)

This study was aimed at studying the place of money laundering investigating the ways and means it is used. The paper also asserts that there is no unified legal status and definition of cryptocurrency which is another trigger for that complicates criminal investigations of money laundering facilitated by cryptocurrency thereby making law enforcement agencies face problems of identifying perpetrator and defining crime committed. There is further articulation of the main concepts of cryptocurrency complexities in terms of anonymity and decentralization, which engender the main antagonism in crime investigation. This clearly verifies the topical issue for the present study on complexities that exist in the investigation cycle of money laundering and terrorism financing on digital currency platforms.

The study also noted that transactions on cryptocurrency are chiefly not government monitored since when conducting any transactions, financial institutions are not involved to verify, and there is no limit to number of accounts one has, and transactions can be done in various spaces in one period.

2.4 Financial Action Task Force (FATF) Report on Virtual Currencies (2014)

This report emphasized on suggesting an understanding through addressing anti-money laundering and terrorism financing counter measures by adopting a working framework of risks that come along with virtual currencies as internet-based payment platforms. As decentralized, math-based virtual currencies particularly Bitcoin having garnered increasing attention, with two popular narratives emerging that the future lies in payment systems like virtual currencies and at the same time arming criminals with a lethal tool, for financiers of terror and sanctioned individuals to transfer and hide illegal funds from law enforcement and regulatory establishments. The popularity of Bitcoin and the understanding of the underlying technology of Bitcoin inspire other cryptocurrencies referred to as alternative coins or alt coins (Nian & Chuen, 2015), such as Ethereum, Dash, and Stellar, to appear.

2.5 Cryptocurrency Investigations Train-the-Trainer course UNODC April 2018

This course was aimed at increasing the capacity of law enforcement officers, analysts, prosecutors, and judges in order to understand the complexity of this new concept. Core aspects of the courses resided in analyzing transactions, inferring, identifying criminality and geo-locating criminals exploiting cryptocurrency.

The training concept used is expected to enable more efficient investigations against illicit of cryptocurrency for organize crime activities and allow further enforcement actions, seizure, confiscation including inter-agency coordination and information exchange. This kind of capacity building is what developing countries like Zimbabwe really need given the proliferation of digital currency use which will go a long way in increasing their capacity and honesty of criminal justice system to prevent, notice, order investigations and issue prosecutorial orders in money laundering and terrorism financing cases and other challenges that may seemingly be complex during investigations.

2.6 Hawks investigating multi-million Rand Bitcoin scam in South Africa: Business Tech Report (2018)

South Africa's elite policing unit, the Hawks, confirmed that they were looking into a serious scam of Bitcoins that could have negatively impacted a lot of South Africans which is suspected to have started with a firm namely BTC global with an estimated value of $50 million usd worth of stockholders all over the world. Hawks' spokesperson Captain Lloyd Ramovha said that there were more than 25,700 cases being probed for breaching the Financial Advisory and Intermediary Services Act with a substantial number out of South Africa.

2.7 Analysis of Illicit Flows into Digital Currency Services: Bitcoin Laundering (Yaya J Fanuise and Tom Robinson)

The unique characteristics of Bitcoin to evade law enforcement makes it quickly appreciated by criminals as they are often early adopters of technology. Users of Bitcoin employ pseudonyms rather than actual names and the ability to transact by without a middleman across borders just the way as e-mail is sent. Giving a mor thorough analysis of Bitcoin in facilitating illegal finance, an agenda situated at the Foundation for Defense of Democracies called Centre on Sanctions and Illicit Finance, grouped together with Elliptic, an analytics service for cryptocurrency, to examine blockchain information on Bitcoin and illegal income on digital currency platforms. This study is set to give vision for regulatory authorities, policy making, finance gurus interested in improving understanding the risks in finance resulting from adopting Bitcoin so as to prepare paths to increase combat against terrorism finance compliance and anti-money laundering crusade in cryptocurrency services.

2.8 Regulating crypto currencies in South Africa: The need for an effective legal framework to mitigate the associated risks (Karabo Mothokoa, 2017)

This study aimed to appreciate the concept of crypto currencies, their relevance in the financial sector and the risks associated with these virtual currencies. It also wanted to establish whether there is a convincing need for regulatory intervention in the operation of crypto currency. Mothokoa (2017) used a desktop-research methodology to carry out this study. The research combined analytical, explorative, and comparative strategies. Reasonable methods to compare were used for giving distinct regulatory and legal frameworks of America, European Union (EU) and Canada against that of South Africa's legal status for cryptocurrency and the multifaceted perceptions of crypto currency were analyzed and explored.

The study found that there are risks that arise from using crypto-currencies and some risks were found could be detrimental owing to the wide adoption of crypto-currencies. Factors like high volatility caused consumer protection, financial stability and money laundering was highlighted to be pertinent risks and with regards to laws governing cryptocurrency, it shows that EU, Canada and US have initiated laws that guard against the noted risks. In South Africa, it was established that there are no laws that governs cryptocurrencies, on another note South Africa Reserve Bank and National Treasury released position papers that cautioned people about the risks associated with these currencies. Therefore, the conclusion drawn was the undeniable necessity for South Africa to have an intervention of laws. In line with the necessity, author seeks to impose that it is critical institute interventions by integrating cryptocurrencies into relevant legislation that is Bank Use Promotion and Suppression of Money Laundering Act.

2.9 Advisory on Illicit Activity Involving Convertible Virtual Currency: The Financial Crimes Enforcement Network (FinCEN) Advisory (2019)

This advisory was to assist financial institutions in identifying and reporting suspicious activity concerning how criminals and other bad actors exploit convertible virtual currencies (CVCs) for money laundering, sanctions evasion, and other illicit financing purposes, particularly involving darknet marketplaces, peer-to peer exchangers, foreign-located Money Service Businesses, and Convertible Virtual Currency kiosks. It also highlights prominent typologies and red flags associated with such activities and identifies information that would be most valuable to law enforcement, regulators, and other national security agencies to initiate investigations.

2.10 Theoretical Framework

2.10.1 Theories for Adoption of Technology Developments

For this study, it is critical to be clear on how and why criminals, individuals or organisations adopt digital currency in their operations. There are available theories of technology adoption that have been developed that should help us in understanding. Technology adoption can be described as the decision to accept and use innovation as well as the effectiveness of adopted technologies based on acceptance or satisfaction (Chen et al., 2012; Hwang, 2010). In the literature for technology acceptance and adoption a significant number of models have been applied such as the Theory of Reasoned Action (TRA), Social Cognitive Theory, Technology Acceptance Model (TAM), Theory of Planned Behaviour (TPB), Model of PC Utilization, Motivation Model, Combined TAM-TPB, Innovation Diffusion, Extension of TAM2, Unified Theory of Acceptance and Use of Technology (UTAUT), TAM3, UTAUT2, Technology, Organization, Environment (TOE) to determine factors influencing adoption and use of technology (Tarhini, Elyas, Akour & Al-Salti, 2016).

2.10.2 Theory of Reasoned Action (TRA1975)

Theory of Reasoned Action was originally introduced by Fishbein (1967) and was extensively verified and built by Fishbein and Ajzen in (1975). Fishbein and Ajzen (1975) developed the TRA to identify components that predict behaviour. It was developed to explain behavioural factors that involve conscious decision making. Behaviours that are impulsive, habitual, or scripted were excluded in the model. The model predicts behaviour based on seven casual variables which are behavioural intention, attitude, subjective norm, belief strength evaluation, normative belief, and motivation to comply. Fishbein and Ajzen (1975) define behavioural intention as the person's plans, motivations, or desires. Intentions are not independent, but they result from underlying attitudes and subjective norms.

According to this theory, an individual behaviour manifests because of mindset pertaining that behaviour and also, recognised social influence from a fundamental person in one's life. An attitude is a general orientation toward a behaviour based on a variety of beliefs and evaluations. Subjective norm as the second variable is composed of normative belief which is the view of others regarding the behaviour and motivation to comply which is the pressure to please others regarding the behaviour. TRA has been used in technology adoption that utilise research for theoretical framework which is critical and has been combined with other theories and models. Despite the popularity of TRA a number of critiques have been proffered and this led to the development of Theory of Planned behaviour and Technology Acceptance Model. The TRA model is diagrammatically illustrated in **Figure 2.2** below.

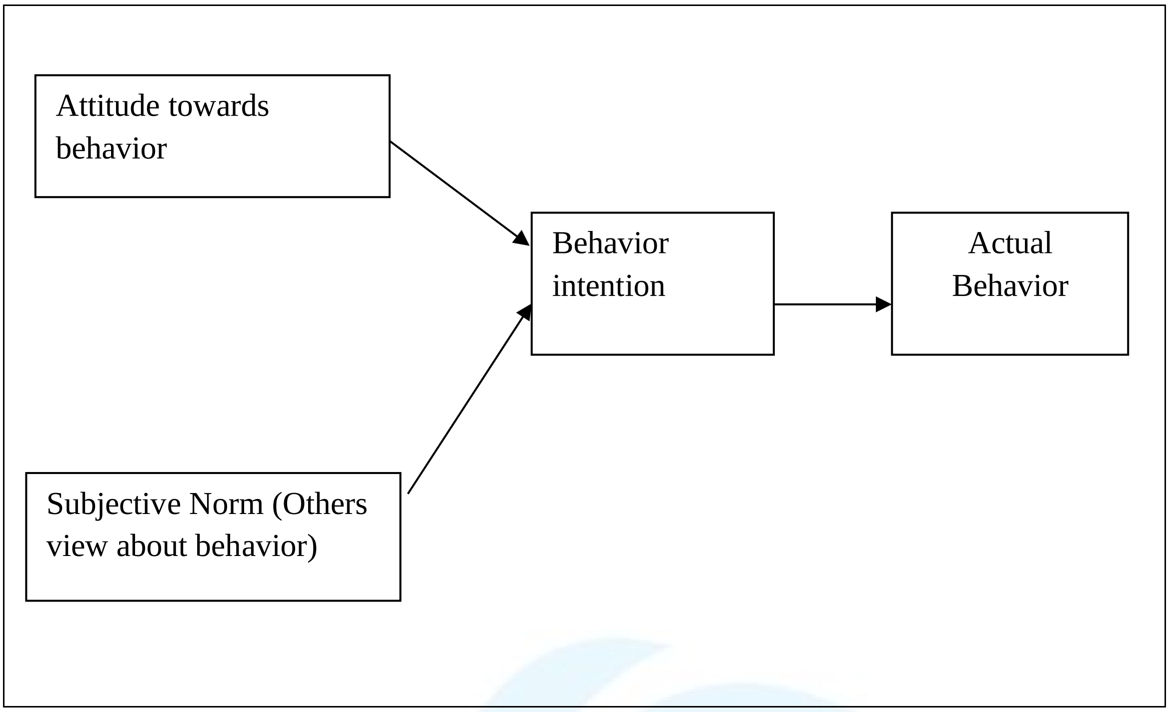

Attitude towards behavior
Behavior intention
Actual Behavior
Subjective Norm (Others view about behavior)

Figure 2.2: Theory of reasoned action

Source: Fishbein and Ajzen (1975)

2.10.3 Social Cognitive Theory 1986

This theory was developed by Albert Bandura in 1986 as a learning theory about the notion that watching others doing something makes people learn within the context of social interaction and experience. The theory is based on the fact that learning occurs in a social context with a dynamic and reciprocal interaction of the personal factors, environmental factors, and behaviors (Bandura, 1986). Bandura (1986) postulated that the person, the behaviour and the environment work hand in hand to create learning in an individual.

According to the SCT, people are either driven by inner forces or external stimuli. It shows that users acquire and maintain behaviour due to the social environment in which they develop their behaviour. Self-efficacy is the important factor in this model (Compeau et al., 1999). Self-efficacy refers to a personal belief in one's capabilities to learn or perform an action at designated levels (Schunk, 2000). It is about what one is capable of doing but it is not the same as knowing what to do (Bandura, 1997).

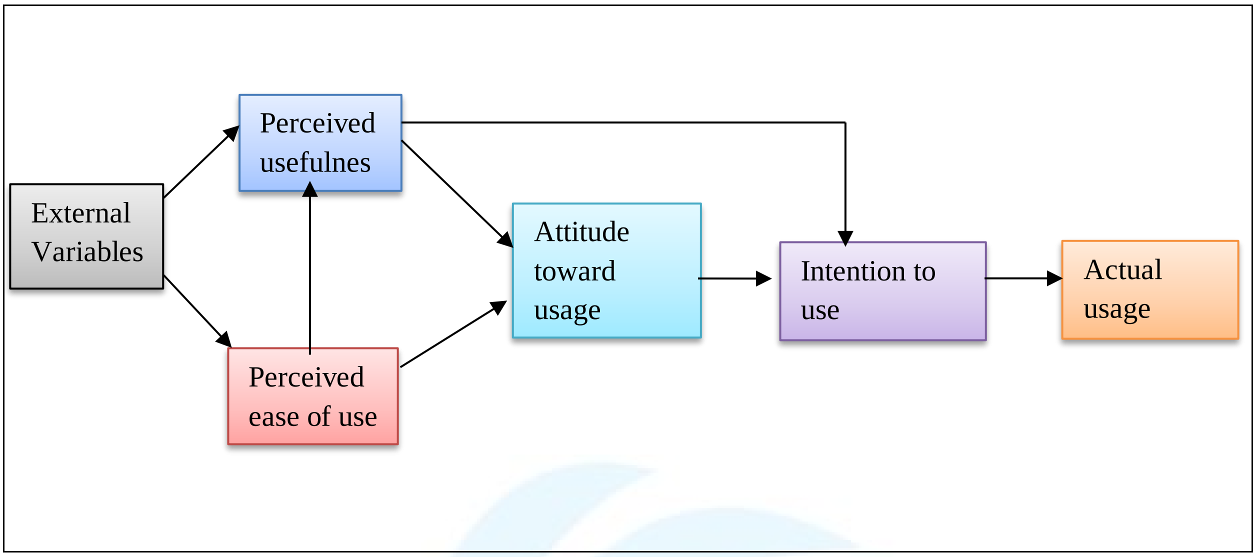
2.10.4 Technology Acceptance Model (TAM1986, 1989)

TAM is one of the extensions of Fishbein and Ajzen TRA. TAM was introduced by Davis in 1986 (Davis, 1989) to explain and predict users' adoption, acceptance or rejection of new technologies. The theoretical basis of TAM is built from a ground that a person considers three critical issues to determine when and how to use new technology when presented. The TAM consists of six related constructs namely external variable, perceived ease of use, perceived usefulness, attitude towards using, behavioural intention to use and actual use (Davis, Bagozzi & Warshaw, 1989; Ko et al., 2010). Perceived usefulness is defined as "the degree to which a person believes that using a particular system would enhance his or her job performance" (Davis, 1989, p.320). Perceived ease of use is defined as "the degree to which a person believes that using a particular system would be free of effort" (Davis, 1989, p. 320). According to TAM, perceived ease of use and perceived usefulness determine an individual's information system acceptance by determining their attitude toward using and subsequent behavioural intention to use, which has an effect on actual use (Erasmus, Rothmann & Van Eeden, 2015). Perceived usefulness is used as a dependent and independent variable since it is predicted by perceived ease of use and on the other hand predicts attitude towards using and behavioral intention to use simultaneously (Erasmus et al., 2015).

Perceived ease of use and perceived usefulness are indirectly influenced by external variables in reinforcing a user's belief of using a system (Erasmus et al., 2015). Attitude towards using in TAM involve judgment on whether the behaviour is good or bad (Erasmus et al., 2015). In TAM there is a direct effect on the intention to use a system. Attitude towards use is determined by perceived ease of use and perceived usefulness (Guritno & Siringoringo, 2013). Behavioural intention to use is influenced by an attitude towards using and perceived usefulness. The relationship between these variables can be illustrated by the model in Figure 2.3 as suggested by Davis.

Figure 2.3: Technology acceptance model

Source: Adopted from Davis et al. (1989)



2.10.5 Theory of Planned Behaviour 1991

The Theory of Planned Behaviour (TPB) is an extension of the Theory of Reasoned Action (TRA) that was established by (Ajzen, 1991). TPB was developed to overcome the limitation of TRA by Fishbein and Ajzen (1980). The TPB is similar to TRA with the addition of a component known as the perceived behavioural control to predict both behavioural intention and behaviours. PBC is defined as a person's approach on the difficulty to execute a particular behaviour. It is a function of one's belief about control and one's perceived power. Generally, the theory suggested subjective norms, perceived behavioural control and attitude toward behaviour as three concepts vital to predict intention to adopt innovation. In relation to TPB attitude, subjective norms and perceived behavioural control together leads to individual intention and behaviour (Mishra, 2014). **Figure 2.4** depicts the model of Theory of Planned Behaviour.

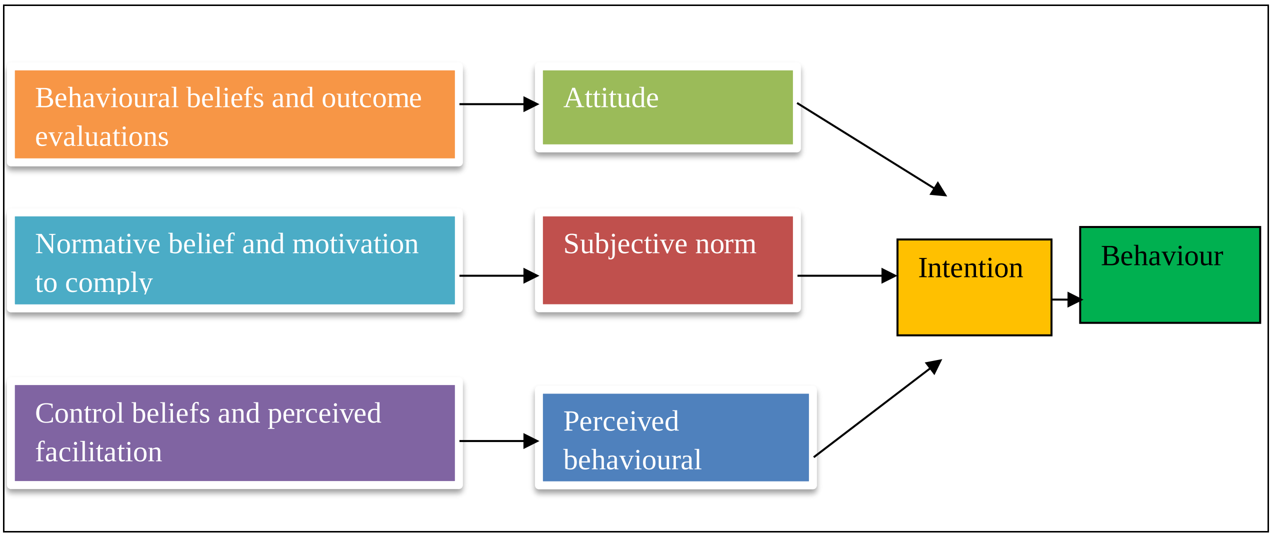

Behavioural beliefs and outcome evaluations
Attitude
Normative belief and motivation to comply
Subjective norm
Intention
Behaviour
Control beliefs and perceived facilitation
Perceived behavioural

Figure 2.4: Theory of planned behaviour

Source: Mathieson (1991)

2.11 Criminology Theories

2.11.1 Space Transition Theory

This theory explains the causation of crimes in the cyberspace. Jaishankar (2008) found out that general theoretical explanations were not enough to give a conclusion about cybercrime which led to the feeling to separate theory of cyber-crimes. Space Transition Theory is an explanation about the nature of the behaviour of the persons who bring out their conforming and non-conforming behaviour in the physical space and cyberspace (Jaishankar 2008). Space transition involves the movement of persons from physical space to cyberspace and vice versa.

This theory argues that there is a difference in behaviour when people shift from one space to a new one. Suggestions of the theory are that people’s criminal behaviour can be suppressed while in the physical space though may have a tendency in cyberspace to perpetrate crime, because status and position physical space limits them. Decision to commit cybercrime comes from the fact that cyberspace gives anonymity, personality changes and general absence of prohibitive measures. Exporting unlawful conduct by criminals in cyberspace to real world is possible and vice versa, thus belonging to both space and time nature of cyberspace provide the chance to escape. Strangers are likely to unite in online to perpetrate illegal acts in real world. Colleagues are probable to connive in real world to commit crime in cyberspace. People in private society have higher chances of performing illegal acts online than people in accessible society.

Conflicting culture in real space against the online culture can result to cybercrime. Jaishankar (2008) further asserts that since online crime is now prevalent that scholars and professionals in the field of crime now view online platform as the new playground for illegal activities. The space transition theory presented above gives detailed analysis about illegal conduct in cyberspace.

2.11.2 Theory of Rational Choice

Rational Choice is a theory produced by Cornish and Clarke (1986) having three components. A person's belief to commit acts of criminality is based on that they can derive a benefit from it and the determination required a basic decision-making process. Simon (1957) assets that even though arriving at a decision with incomplete information, rationality processing is made for criminal decision making through weighing the reward of act with injury in line with excitement, pleasure and thrill derived. Which means that performing the criminal act is purely based on the act giving more benefits than the cost.

Cornish and Clarke (1986) suggested second component in rational choice theory required crime-specific focus that was critical to obtain the characterists of distinct requirements connected to a criminal act. More-so, this focus brought attention to the scenarios of the illegal act rather than the person and permitted for understanding the uniqueness in information critical for various crimes.

The third component was a vital difference being made between criminal participation and the crime incident. Criminal scenes and criminal participation recognised decisions made by a person to be involved in crime. On another note, criminal participation is the method that a person utilised to become engaged in a specific crime in the first place, or to persist and to stop.

2.12 Chapter summary

This chapter presented literature related to this study. This chapter presented the literature review of the study guided by objectives of the study such as to determine specific complexities encountered when investigating digital currencies from a sample of financial investigators, investigate if other developing countries who have adopted digital currencies coping, assess any international standards set by developed nations in investigating digital currencies that can also be adopted by developing countries like Zimbabwe and recommend action and guidelines to improve the current financial digital currency investigations eco-system. The next chapter present the methodology of the study.

Chapter 3: Methodology for Research

3.0 Introduction

The chapter before focused on presenting literature on the complexities digital currency has on financial investigations in relation to money laundering and terrorism financing. A case of Zimbabwe. This chapter focuses on presenting the research methodology of this study. In this chapter research philosophy, research design, targeted population, sample size, sampling method, research instruments, data collection procedure, data analysis and presentation methods, reliability and validity and ethical considerations will be presented.

3.1 Research philosophy

According to Creswell (2010) prior to selecting the research method and commencing with the research design, a suitable research philosophy should be identified, as it establishes the foundation for what follows. According to Mingers (2011); Mingers (2013); Orlikowski and Baroudi (2011) there are three key research philosophical or epistemology approaches or assumptions: positivist, interpretive, and critical research. The two main approaches used in financial research which are positivism and interpretivism (Chen and Hirschheim, 2014; Gregor, 2016; Guba and Linclon, 2014; Orlikowski and Baroudi, 2011; Myers, 2017).

However, amongst the two research philosophies, positivism is considered as the most popular one in financial research as it has been used in many financial research (Mingers, 2013; Orlikowski and Baroudi, 2011; Straub et al., 2014; Yin, 2013). In this research study positivism was adopted because it is used to test theory for understanding a certain phenomenon that is in research question (Orlikowski and Baroudi, 2011). Moreover, positivism assumes that the research study is undertaken in a value-free way. In this research study positivism was also adopted to scrutinize facts such as they are with no room for bias from the researcher. Positivism was adopted because it uses better coordinated methodology for the purposes that enable reproduction.

3.2 Research design

According to Avison et al., (2018) and Bryman (2014) research design refers to a framework or systematic approach to be adopted to fulfill the aim and objectives of this research. Research design can be exploratory, descriptive, and explanatory (Robson, 2012; Sekaran, 2013). For this study, the researcher adopted an exploratory research which enabled him to gain new insights on the concept of digital currency. The researcher conducted exploratory research through the search of literature from the internet's publications about digital currency adoption through searching on websites, research papers on financial investigations and by reading e-books about theories on technology adoptions and risks associated written by various authors. Cross sectional research design was also used in this research study because data was collected over a short period of time.

According to Kothari and Garg (2014) a research design is a blueprint for data collection, measurement, and analysis. As such the design includes an outline of what the researcher will do from writing the hypothesis and its implications for the final analysis of data (Kothari and Garg, 2014). Due to the nature of this research study cross-sectional survey design was adopted to accomplish the research objectives. The researcher adopted cross-sectional survey since it gives an effective manner on the gathering of huge volumes of information from a significant populace. Moreover, cross-sectional survey provides a quick, often inexpensive, efficient and accurate means of assessing data about a population (Zikmund and Babin, 2017).

3.3 Targeted population

Walliman (2018) state that target population refer to the individuals in a group that are drawn from the general population and share a common characteristic of interest to the researcher, and it should be defined ahead of time, clearly specifying the inclusion of eligibility criteria. The study population comprised of financial intelligence analysts, financial crime compliance investigators, and employees of digital currency agents in Harare, Zimbabwe. This figure of 130 people was drawn from the vital targeted organizations in Harare shown in table 3.1 below. The size of targeted population of this study which explains the reasoning for that certain number constituting relevant agencies responsible for subject matter in Zimbabwe as they are shown below.

Table 3.1 Organisations of targeted population.

Organization	Estimates of population
FINANCIAL INTELLIGENCE UNIT	50
ZIMBABWE POLICE (COMMERCIAL CRIMES)	50
GOLIX CURRENCY	20
CRYPTOCEM	10
Total	**130**

3.4 Sample size

In this research about the complexities digital currency has on financial investigations in relation to money laundering and terrorism financing. A case of Zimbabwe. Raosoft online sample size calculator was adopted. Raosoft Tool is powerful collection of more than 15 utilities for database and file management of research survey data gathered with Raosoft online survey software (http://www.raosoft.com). The researcher typed the url http://www.raosoft.com and entered 130 as population size and automatically the site calculated a sample size of 98 which was adopted in this study.

3.5 Sampling method and techniques

Sampling method is the strategy used to select participants into a study. Makanyeza (2016) state that, it is possible to enlist everyone into the study if the population is small but in most cases the population is so large that few participants from the population can be chosen to represent the whole population. Basically, there are two techniques for sampling exist which are non-probability and probability. The researcher adopted both non-probability and probability sampling techniques. Probability sampling is when all participants in the study have an equal opportunity to be selected (Easterby-Smith, Thorpe and Lowe, 2012). Probability sampling will use mathematics methods. Whilst non-probability sampling participant in the population are selected based on their availability or on the judgment of the researcher that they are information rich (Walliman, 2018).

Zikmund and Babin (2010) defined sampling as any procedure that draws conclusions basing on measurements of a portion of the entire population. This research study adopted convenience sampling because there are no available statistics of digital currency investigations in Zimbabwe at the time study was carried out hence convenience sampling was adopted to draw the sample, because of willingly available subjects invited to be part of research. Convenience sampling allowed the researcher to obtain the necessary number of completed questionnaires as the most of participants represent a sensitive section of individuals because of nature of their jobs so prior arrangements and clearance had been made due to the nature of the research study.

3.6 Research instruments

The major research instrument adopted in this research study was a google generated structured questionnaire consisting of 8 typed questions in a definite order or set. The questionnaires were used to collect data by asking respondents to respond the same set of questions. The structured questionnaire was adopted because it is the best study strategy for gathering explanatory and descriptive data on individual views. The structured questionnaire was adopted because they are quick to gather data, easier to complete and more readily amenable to structuring responses and quantitative analysis.

3.6.1 Key informant interviews

Primary qualitative data were acquired from key informant interviews through google generated open ended interview questions form for filling up answers because of covid-19 regulations and lock-down rules, 1 on 1 sessions were not possible. Interviews were meant to empower a more profound comprehension of digital currency investigations from officers who are responsible for financial investigations in Zimbabwe. Key informants for in-depth interviews are usually selected based on their first-hand knowledge about the subject of interest (Choy, 2014). Data was automatically collected through the space filling on forms noted by respondent. Participants were required to consent to being interviewed for security reasons that their responses are for academic purposes and were able to send back their answers within the shortest period of time to better facilitate for the completion of study.

3.6.2 Survey Questionnaires

Primary quantitative data was acquired through a draft of a survey questionnaire. A questionnaire is a set of questions with a selection of answers which is designed for use in a survey (gam, 2018). It gathers standardised data in the same way from a number of respondents. Data acquired from questionnaires can be generalised if the sampling is appropriately done. A profound comprehension of the research problem was acquired from literature and questions developed on this basis which addressed the research objectives of this study. The designed questionnaires were pre-tested to determine their effectiveness.

Participating pre-tests were done where respondents were informed that it was a pre-test. Respondents provided their feedback on the questions, their order and wording as well as how understandable they were. Questionnaires were administered during the research by the researcher to enable probing and clarification of questions and responses. To ensure confidentiality no respondent-identifying information was gathered and all questionnaires were totally anonymous. Questionnaires were administered to identified participants in Zimbabwe over a two-week period.

3.7 Data collection procedure

Once the questionnaire was designed, pilot tested and amended, the sample selected, the questionnaire was used to collect data. The researcher seeks permission from organizations before collecting data. The researcher self-administered through sending links on WhatsApp and email of the questionnaire to the target population. The questionnaire heading highlighted an introductory statement that respondent's feedback is for educational purposes and a brief of subject matter and clear instructions preceded each question in order to facilitate its completion. The questionnaires were then sent back to the researcher within 1 month from sending date. When conducting interviews, the researcher started by developing "an interview guide" whose content was derived from the three objectives of this study (Bernard, 2016).

The interview guide was administered and tested on three research participants who were selected using the purposive sampling method (Sifile, Mazikana, Chavunduka and Bhebhe, 2018). The researcher ensured that all the necessary steps involved in conducting an interview were done (Easterby-Smith, Thorpe and Lowe, 2012). Consent was made through texts on mobile communication application like WhatsApp because of geographical location differences. The interviewees had the choice to either partake or excuse themselves from participating any time they felt like and were also notified of the unavailability of material benefits to be derived by those who participated in the study.

3.8 Data analysis and presentation methods

Data analysis is the application of reasoning to understand the data that have been gathered (Kothari and Garg, 2014). After the data collection the quantitative data from the respondents was edited, structured, and processed. Descriptive analyses were performed. Descriptive statistics consist of measures of central tendency, including means, medians, and standard deviations (Salkind, 2012). Multiple regression analysis was performed to strengthen and give direction of the hypothesized relationships. One-way ANOVA was also adopted.

3.9 Reliability and validity

According to Kothari and Garg (2014) reliability is about the correctness and exactness of procedure for measurement. Coherent outcomes gauge the reliability of measuring instrument. Testing internal uniformity of instrument for research alpha coefficients by Cronbach were utilized. Having a high alpha coefficient implies that the validity of scale. 0.70 value and upwards shows pleasing reliability levels than a value between 0.50 to indicate an acceptable level of reliability. The measurement scales were reliable since all the Cronbach's alphas of the constructs were above 0.06 to ensure validity of the research instrument a thorough literature review was done.

3.10 Ethical considerations

Before data collection the researcher seek permission from the university to conduct a research study. During data collection the main objective of the study along with issues like privacy, discretion, consent that are ethical factors were highlighted in the introductory statement of the questionnaire. Voluntary participation and freedom to dropout from study any time was also indicated in the text's messages during communications with possible participants. After data collection presented the data as it was, and the collected data was solely used for academic research purposes.

3.11 Chapter Summary

This research study is on the complexities of digital currency on investigations in relation to money laundering and terrorism financing with participating institutions being Headquartered in Harare, Zimbabwe. This chapter focused on presenting the research methodology of this study. In this chapter research philosophy, research design, targeted population, sample size, sampling method, research instruments, data collection procedure, data analysis and presentation methods, reliability and validity and ethical considerations were presented. Data presentation and analysis of this research study is the focus for the next chapter.

Chapter 4: Results Presentation and Analysis

4.0 Introduction

This research was focused on the complexities digital currency has on financial investigations in relation to money laundering and terrorism financing. A case of Zimbabwe. The data for analysis was collected using qualitative and quantitative analysis methods. Descriptive style presented qualitative data, and then the researcher has used graphs, tables, and pie-charts to present quantitative data. The use of graphs, tables and charts was chosen to enable easy interpretation of the data collected. Data collected was analyzed and interpreted to provide answers to the research objectives and questions.

4.1 Response rate analysis

A total of 130 respondents were considered for contribution in this study. The researcher personally engaged respondents at organisations namely, Financial Intelligence Unit, Zimbabwe Police, Golix, Cryptogem. Out of the targeted 130 participants, 98 valid answered questionnaires were returned, and the response rate was 87%, with a 13% consists of non-respondents making the questionnaires that were never returned. The response rate is considered excellent by Makanyeza (2018) who noted that a response rate of 50% or above is deemed adequate for analysis and reporting; a rate of 65% is very pleasing, making 70% and over excellent.

4.2 Responsibility of respondents in investigative cycle.

The **table 4.1** below shows Responsibility of respondents and the positions which they hold in the organization targeted.

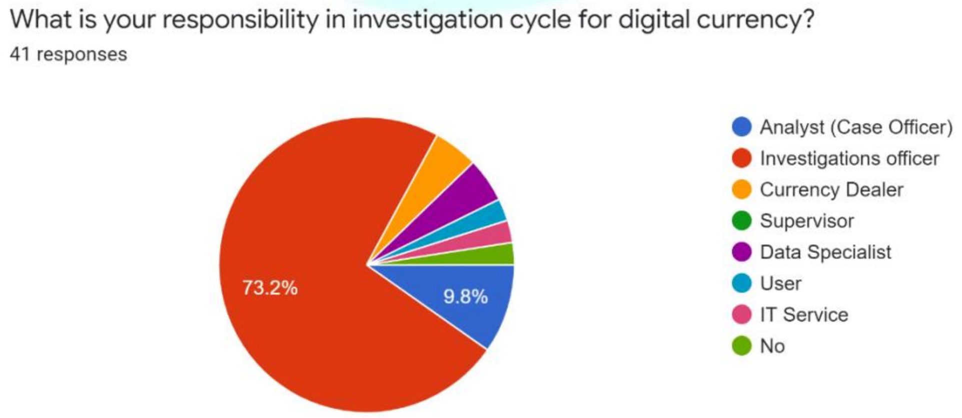
Table 4.1: Responsibility of respondents and position held.

	Frequency	Percent %	Cumulative Percent %
Compliance	40	32	40

Investigators			
Intelligence Analysts	43	35	40
Digital Currency Traders' Employees	15	20	20
Other	0	0	
Total	98	87	100

Table 4.1 above shows that 40 (32%) of the respondents were compliance investigators, 35 (35%) cited that they were intelligence analysts, 15 (20%) indicated they were employees of Digital Currency Agencies. The organization participants have much influence to make investigative decisions for their organizations pertaining to the use of digital currency and their contribution is fundamental to evidence gathering. Information displayed in **Table 4.1** above, it can infer that those are officers of organizations who are knowledgeable in digital currency issues.

Figure 4.1 Below also shows responsibility of respondents in targeted organizations.



Source: Study Questionnaire

Figure 4.1 displays that majority of respondents are from Financial Intelligence Unit (FIU) Investigations Analysts followed by Zimbabwe Police (Compliance Investigation), and Golix, Cryptogem (Currency Dealers) as the smaller number of respondents, who completed the questionnaire about the complexities of digital currency when investigating in the case of terrorism financing and money laundering in Zimbabwe indicating that they were participants. In a similar study conducted by Koreff (2018) on three studies examining auditors' use of digital currencies in Florida, United states of America, he noted that most employees in organizations constituted 80% of respondents of his study hence the results attained in this research were highly expected.

4.3 Level of understanding digital currency by organizations in Zimbabwe.

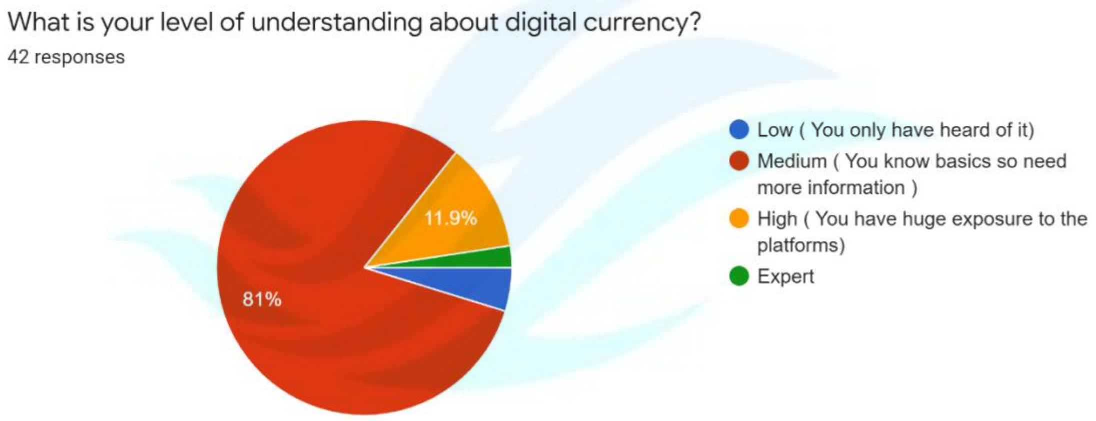


Figure 4.2: Source: Survey conducted for this study.

Respondents of this research on the complexities digital currency has on financial investigations in relation to money laundering and terrorism financing. A case of Zimbabwe asked about their level of understanding of digital currency and their responses were captured down in Pie Chart 4.3 above and it can be noted that majority of respondents (81%) indicated that they had a good understanding of digital currency. Idil, Halit & Koray (2018) conducted a study on digital currencies in Denmark. Idil, Halit & Koray (2018) noted that firms have a good understanding of digital currency. The research aimed to analyze the role and effects of digital currencies.

According to Idil, Halit & Koray (2018) the idea of using cryptographic technology to create digital currency can effectively transfer money without relying on any financial institution and intermediary agents. The ways of payment have transformed dramatically with the development of technology. Payment methods changed from cash payments to card payments, and then electronic payments appeared (Dennehy and Sammon, 2015). According to Idil, Halit & Koray (2018) the results were similar with the literature that firms have a good understanding of digital currencies and digital currencies had made payments easier. The responses show that according to our targeted participants understanding of digital currencies is very high which is important for the study as it requires articulation of the problem in the study.

In 2008, a paper written by Satoshi Nakamoto specifies the idea and underlying technology of a cryptocurrency called Bitcoin, including their solution to prevent double-spending using hash-based proof-of-work (Nakamoto, 2008). Bitcoin is implemented under open-source license and its network utilizes a form of distributed ledger technology called blockchain. Since its release, Bitcoin has been used for various transactions. As per 22 August 2018, Bitcoin network has processed on average 240,673 confirmed transactions per day.

4.4 Are the skills available to investigate digital currency platforms?

Research question two sought to find out if there are people skilled to investigates digital currency platforms operations.

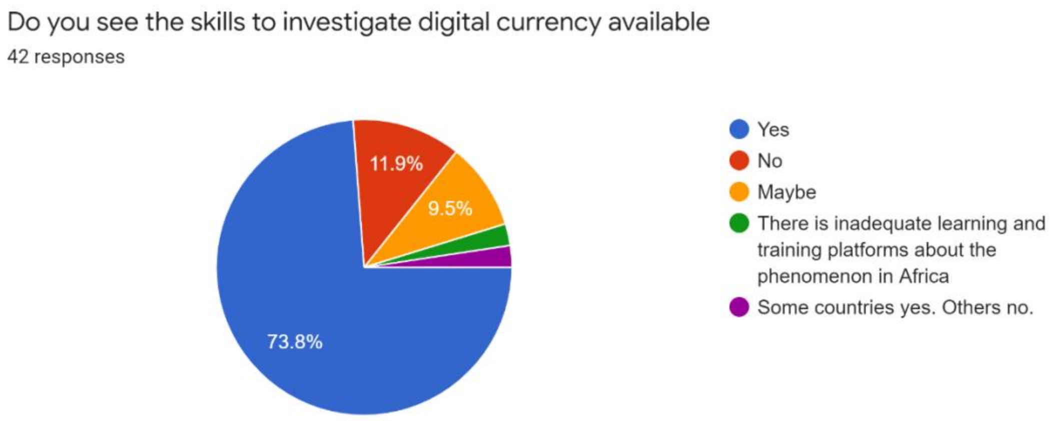


Figure 4.3 Source: Survey

It can be noted that 73.8% of the responses as shown above are confirming the availability of the skills base to investigate digital currency platform in Zimbabwe as the study wants to look at the vulnerabilities on digital currency platforms that make it difficult for investigations.11.9% view that there are no skills with 9,5% being not sure and the rest are of the opinion that there is inadequate learning and training platforms.

4.5 Is digital currency driven crime prevalent.

The question was aimed at understanding if the respondents were aware of criminal tendencies on digital currency platforms.

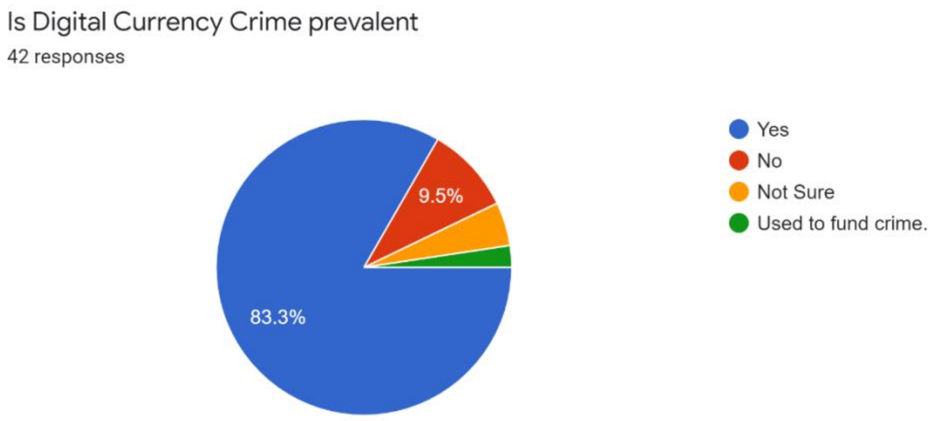


Figure 4.4 Source: Survey Pie chart

The above responses show data about the prevalence of criminality on digital currency platforms for the study on vulnerabilities of digital currency platforms which make investigations difficult. 83% admit that criminal activities are prevalent on digital currency platforms, with 9.5% saying prevalence is none and the rest not sure.

4.6 List of vulnerabilities digital currency platforms have

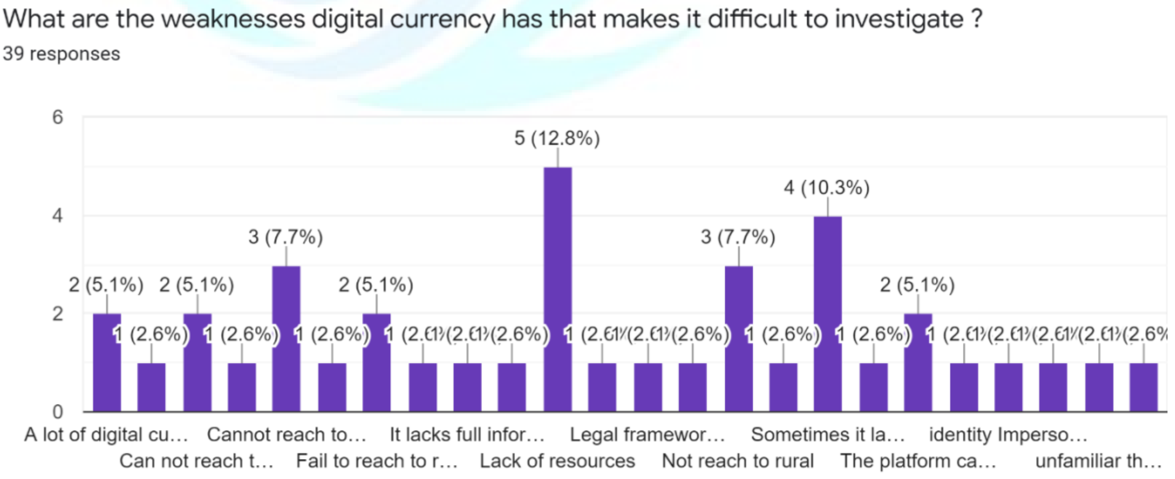


Figure 4.5 Source: Survey

Graph above shows that respondents who completed the questionnaire had various assertions about complexities digital currency has on financial investigations in relation to money laundering and terrorism financing. A case of Zimbabwe indicating that digital currency platforms can be difficult to investigate criminal activities facilitated by them. From the findings attained above 5(12.8%) cited lack of resources needed by investigators, 2(4.7%) cited lack of legal framework to regulate this kind of technology for the industry, 4 (10.3%) cited much about lack of enough information(actionable intelligence) critical to an investigation, 4 (10.3%) cited digital currency account holders use of anonymity through identity impersonation making traceability difficult (attribution) and 2 (4.7%) cited that it is a new phenomenon in academia in Zimbabwe which makes understanding of it by investigators difficult, 2(4.7%) citied that there are no main stream banks or institutions that deal with digital currency and that its unfamiliarity from fiat currency operations makes it difficult to investigate, 2(5.1%) cited remote access (transnational nature) of digital currency an investigative headache because of jurisdiction issues, 2(4.7%) cited the use of dark net(internet black-market) which further complicates nature of these transactions, 3(7.3%) cited encryption, lack of accountability and proneness to hacking as complexities that make it difficult for investigators and 11(35,4) cited issues that did not really reflect on the question asked with issues to do with reaching to rural areas, reach to different people.

According to Shi & Zhou (2020) inspired by the digital revolution to the financial industry, the discussion around central bank digital currency also attract attention from academics and central banks. According to Jad Mubaslat (2017), who was a Wright State University graduate student and creator of BitQuick.co, concurred with the outcome of this survey as he postulates that, other cryptocurrencies, such as Monero, are becoming popular for dark web uses including drug trafficking and human trafficking and also according to a 2015 Europol article, bitcoin had featured in high-profile investigations involving payments between criminals, and was used in over 40% of illicit transactions in the European Union.

It is therefore noticeable that when terrorists and money laundering criminals use digital currencies for their operations, it is difficult for investigators to trace and apportion responsibility for the illegal actions (attribution)given the absence of regulatory frameworks that gives motion to the wheels of criminal justice coupled mainly with the nature of digital currency transactions that offer use of pseudo identities raising anonymity levels, also necessitated with its access that can be done anywhere in the world remotely which criminals favour as they usually go to places called safe havens which have laxity in law enforcement and more-so internet platforms like darknet give investigations torrid time as criminals are always a step ahead of officers of law with the use of technology. It is also highly difficult to have reliable information that is actionable that an investigator can use because most of the communication used is facilitated by heavily encrypted messages which can take time for investigators to decode as information and timely reaction are fundamental aspects to all investigations. From the responses of this question, it shows that digital currency platforms are attracting a lot of scrutiny by law enforcement and financial policy regulators because of their potential to offer more to similar benefits of trust, reliability, and credibility as the traditionally used hawala financial system that money launders and terrorism operators had become accustomed to.

4.7 Interview Responses Outlook

4.7.1 Some argue that digital currency use needs financial authorities' involvement, how can this help investigators?

Responses

i) To get access to all the needed information which will be used as evidence.

ii) Maybe more visibility into transactions and an attempt to identify locations of transactions.

iii) In order to have rules and guidelines of operation.

iv) It is recognition by authorities means budgets are provided for training to combat it and there will be legislative progression to help in prosecution.

v) This will assist to know the people behind or proponents of the digital currency for easier follow up when customers are fleeced or in case of fraudulent transactions.

4.7.2 Given the crossing of borders of cyber space, how is the cooperation situation with other countries when investigating?

Responses

i) It is a complex situation as other countries are not cooperative.

ii) For individual cases, not great. For large scale operations that already have an international component then cooperation is better.

iii) It is a challenge because you do not know who exactly to contact for cooperation.

iv) Cooperation is important since cyber space is borderless and digital currency is used to fund international criminal activities and terrorism however due to fragmented policing and legislation particularly in Africa cooperation is minimal and difficult.

v) The use of Interpol and other organs such as SARPCCO assist so much in cross border investigations on these transnational incidences. However, there are some hiccups with some member states whose cooperation is not that pleasing as they take time to respond, or their statutes will be different from the requesting country hence that will pose as a challenge.

4.7.3 What are the consequences for investigators when digital currency use is banned though trade still goes on?

Responses

i) Their source of information and cooperation will be hindered.

ii) Investigators loose KYC data from local exchanges. They will have to rely on international cooperation.

iii) Work is very difficult for investigators because it is an unknown territory.

iv) The banning entails that the official system ignores it is existence and thus do not budget for it or legislate to combat it and yet it is a reality on the ground.

v) The investigators must stop the trade of the currency but in so doing there will be so much resistance from the transacting public who will be holding the digital currency.

4.8 Descriptive statistics

This section presents results on descriptive statistics (mean and standard deviation) of the study constructs). Five-point Likert scale was used on each of the four constructs that is to determine specific complexities encountered when investigating digital currencies from a sample of financial investigators, to investigate if other developing countries who have adopted digital currencies are coping, to assess any international standards set by developed nations in investigating digital currencies that can also be adopted by developing countries like Zimbabwe and to recommend action and guidelines to improve the current financial digital currency investigations eco-system. The response points being disagree firmly, disagree, impartial, agree, firmly agree.

4.8.1 To determine specific complexities encountered when investigating digital currencies from a sample of financial investigators.

Table 4.2: Mean and standard deviation for determining specific complexities encountered when investigating digital currencies from a sample of financial investigators.

Item	**Mean**	**Std. Deviation**	**N**
Unharmonized local regulations and international standar ds	4.13	.963	100

Criminal offences associated with virtual currencies	4.17	.933	100
Unavailability of tools and software's to trace transactions	4.03	.941	100
Privacy Rights (Apportioning responsibility of crime)	4.16	1.033	100

Overall mean =4.1225; Standard deviation= 0.9675

Results in Table 4.2 above shows the lowest mean rate that is 4.03 and standard deviation that is 0.941 as compared to the highest mean rating of 4.17 with a standard deviation 0.933. Descriptive statistics of determining specific complexities encountered when investigating digital currencies from a sample of financial investigators showed an average mean of 4.1225 with a standard deviation of 0.9675. On average, respondents were agreeing that there are some criminal offences associated with virtual currencies.

The results are similar to United Nations Office on Drugs and Crimes who noted that digital currencies by nature, may possibly be related to a variety of criminal crimes. Their focus was on money laundering offences involving virtual currency, they noted the vitality to quickly give a larger scope to which these offences could be looked at. This does not exclude worry on the relations that exist between digital currencies and cybercrime. Dyson & Bell (2020) conducted a study on the challenges of investigating cryptocurrencies and block chain related crime. They noted that we are incrementally living in a society seeking balancing need for consent and rights to privacy along with the obligation of the state to protect its citizens. Within this ever-evolving society, it is increasingly fundamental need to guard a person's financial trail of transactions which at the same time makes it problematic for financial crime agencies when investigating fraud or money laundering.

4.8.2 To investigate if other developing countries who have adopted digital currencies are coping.

Table 4.3 below shows descriptive statistics for investigating if other developing countries who have adopted digital currencies are coping.

Table 4.3: Mean and standard deviation for investigating in other developing countries who have adopted digital currencies are coping.

Item	Mean	Std. Deviation	N
Effective internet control	4.00	.878	100
Use of regulatory instruments	4.04	.893	100
Cryptocurrency regulatory institutions	3.92	.979	100
Financial Crimes agencies in place	3.99	.975	100

Overall mean =3.9875; Standard deviation= 0.93125

Results in Table 4.7 above shows the lowest mean rating of 3.92 with a standard deviation of 0.979 as compared to the highest mean rating of 4.04 with a standard deviation 0.893. Descriptive statistics of investigating if other developing countries who have adopted digital currencies are coping showed an average mean of 3.9875 with a standard deviation of 0.93125. On average, respondents were agreeing that other countries have adopted the use of regulatory instruments. The results were like Marian (2018) who presented a conceptual framework for the regulation of cryptocurrencies and noted that the write up proposed a conceptual framework for the regulation of transactions involving cryptocurrencies. Cryptocurrencies offer tremendous opportunities for innovation and development but are also uniquely suited to facilitate illicit behaviour (Marian, 2018). Marian (2018) proposed a monitoring legal concept which enforces costs on features of cryptocurrencies that define their facilitation for crime behaviour but leave out enforcing on key aspects that make it possible, especially transfer processes of value decentralisation. Using a basic utility model of criminal behaviour as a benchmark Marian (2018) clarifies on how the legal framework can be constructed. An example of a tax anonymity that is elective on transactions that makes one user not anonymous.

4.8.3 To assess any international standards set by developed nations in investigating digital currencies that can also be adopted by developing countries like Zimbabwe.

Table 4.4: Mean and standard deviation for assessing any international standards set by developed nations in investigating digital currencies that can also be adopted by developing countries like Zimbabwe.

Item	Mean	Std. Deviation	N
Rules for exchanges	3.83	.886	100
Taxation levels	3.76	1.068	100
Cohesive approaches on cryptocurrencies in form of policies guiding and regulating it.	3.92	.934	100
Approval of financial institutions that handle Bitco in transactions	3.96	1.031	100

Overall mean =3.8675; Standard deviation= 0.97975

Results in Table 4.2 above shows the lowest mean rating of 3.76 with a standard deviation of 1.068 as compared to the highest mean rating of 3.96 with a standard deviation 1.031. Descriptive statistics for assessing any international standards set by developed nations in investigating digital currencies that can also be adopted by developing countries like Zimbabwe showed an average mean of 3.8675 with a standard deviation of 0.97975. On average, respondents were agreeing that there should be an approval of financial institutions who handles Bitcoin transactions as a standard that enhances digital currency investigations. According to Kyc (2021) major governments across the globe have taken very different approaches to the regulation of cryptocurrency. The landscape is still evolving, but given the bureaucratic tendencies of governments, much remains to be seen.

These examples of countries around the world on how they are regulating cryptocurrency. In United States, while cryptocurrencies are legal, there does not seem to be a consistent legal approach to them. Laws vary greatly state by state, and federal laws cannot seem to agree as to what cryptocurrency is. For example, the Financial Crimes Enforcement Network considers cryptocurrencies to be money transmitters, while the IRS regards them as property. Cryptocurrency exchanges also face much uncertainty when it comes to regulation. Several different regulators claim jurisdiction, and there has yet to be a cohesive approach. Policies vary greatly. The US though, is beginning to take steps to create overarching crypto regulation. The US Treasury has been outspoken regarding the regulation of cryptocurrencies to combat criminal activities, and change may be on the horizon.

According to Kyc (2021) in the European Union cryptocurrency is widely considered legal across the EU, but the rules for exchanges differ across member states. Taxation also varies, ranging anywhere from 0% to 50%, and crypto is subject to capital gains tax. To date, the EU Parliament has passed no specific legislation regarding cryptocurrencies. Exchanges are required to register with their local financial authority, and from there can operate across the entirety of the EU. The 5th AML Directive now requires that crypto exchanges follow the EU's anti-money laundering regulations. Luckily for some, exchanging FIAT currency to crypto is not subject to VAT.

While UK divorced itself from EU through Brexit, they have created their own regulations for cryptocurrencies. Currently, crypto is not considered to be legal tender, although cryptocurrency exchanges are legal. The potential taxability of cryptocurrency depends on the activities and parties involved, although gains or losses on cryptocurrency are subject to capital gains tax. Cryptocurrency exchanges will need to register with the Financial Conduct Authority (FCA, however, some exchanges may be able to apply for an e-license. As of January 2020, the FCA now has the power to supervise how cryptocurrency businesses deal with terrorism financing and money laundering associated risks. In the grand scheme of things, the UK is far from the target and post-Brexit it becomes interesting how the legal framework moves.

In Russia there has a complicated history regarding cryptocurrency, and now seems to be taking actions against its use. In Russia, crypto is considered to be a money substitute, and recent laws of 2019 have now made money substitutes illegal in the country. It is still unclear what crypto is defined as and can be used for. New proposals are being made that could allow crypto to be confiscated, and these proposals are rumored to soon be made into law. It is unclear as to how the Russian government plans to confiscate crypto, especially Bitcoin which is anonymous and decentralized.

4.8.4 To recommend action and guidelines to improve the current financial digital currency investigations eco-system.

Table 4.5 below shows descriptive statistics for recommendations on action and guidelines to improve the current financial digital currency investigations eco-system.

Table 4.5: Mean and standard deviation for recommendations on action and guidelines to improve the current financial digital currency investigations eco-system.

Item	**Mean**	**Std. Deviation**	**N**
Improving mutual legal assistance approaches	3.48	1.175	100
Clear financial intelligence network in place	3.49	1.199	100
Capacity building through training investigators	3.74	.996	100
Setting up a regulatory authority	3.90	1.037	100

Overall mean =3.6275; Standard deviation= 1.101

Results in Table 4.9 above shows the lowest mean rating of 3.48 with a standard deviation of 1.175 as compared to the highest mean rating of 3.90 with a standard deviation 1.037. Descriptive statistics for recommendations on action and guidelines to improve the current financial digital currency investigations eco-system showed an average mean of 3.6275 with a standard deviation of 1.101. On average, respondents were agreeing on setting up a central regulatory authority. According to Mazikana (2018) a popular narrative noticed in his survey was the government giving warnings about dangers of relying on cryptocurrency investment which would be meant for educational purposes focusing on the non- government guarantee aspects of cryptocurrencies. These government notices tell people that most of the agencies facilitating cryptocurrency are unregistered and the unpredictability risks of cryptocurrency as such investing in at own risk with no legal action for restitution.

Table 4.6 Direction of the relationship between ways of adopting digital currency and investigations performance.

Chi-Square Tests	Value	Df	Asymp. Sig. (2-sided)
Pearson Chi-Square	78.079[a]	4	.000
N of Valid Cases	100		
a. 2 cells (20.0%) have expected count less than 5. The minimum expected count is 3.45.			

		Value	Approx. Sig.
Ordinal by Ordinal	Gamma	-.683	.000
N of Valid Cases		100	
a. Not assuming the null hypothesis.			
b. Using the asymptotic standard error assuming the null hypothesis.			

Tables 4.6 above shows there is an association between ways of adopting digital currency and investigations performance. Gamma -.683 displays a negative relationship that is strong. This means that as adopting digital currency in Zimbabwe

become more and more formal, it would influence investigations outcomes. From the above statistical analysis conducted on the adoption of digital currency and its impact on investigations outcomes, conclusion can be drawn that there is association between adopting digital currency and investigations performance as measured by prohibition orders per year.

4.9 Testing Research Hypotheses

This section presents results of research hypotheses.

4.9.1 Testing hypotheses (H1, H2, H3, H4)

The study seeks to test the following hypotheses.

H1: Expected performance possess a positive impact on the intention by criminals to use digital currency.

H2: The greater the effort expectancy in investigating the greater the intention by criminals to use digital currency.

H3: Influence of society has a positive impact on the intention by criminals to use digital currency.

H4: The greater the facilitating conditions digital currency has the higher the intention by criminals to use digital currency.

Multiple-regression analysis was used to test the hypotheses and results are shown in Table 4.7, Table 4.8 and Table 4.9 below

Table 4.7 Model summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.344[a]	.118	.091	1.67549

a. Predictors: (Constant), H1, H2, H3, H4

b. H1 Performance expected

c. H2 Effort expected

d. H3 Social influence

e. H4 Facilitating conditions

Results in Table 4.7 show that the four constructs explain about 12% of changes in behavioural intention. This is shown by the R square value of 0.118. This implies that there are other factors that influence the adoption of digital currency by individuals with criminal intentions. Table 4.8 below shows the ANOVA test results.

Table 4.8 ANOVA

ANOVA[a]						
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	48.189	4	12.047	4.291	.003[b]
	Residual	359.330	128	2.807		
	Total	407.519	132			
a. Dependent Variable: Behavioural Intention						
b. Predictors: (Constant)						

Results in Table 4.8 above show that the model is statistically significant (F= 4.219; p= 0.003). This implies that the regression model is relied upon. **Table 4.9 below** presents coefficients results for factors influencing behavioural intention.

Table 4.9 Coefficients

Coefficients[a]						
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	8.126	1.240		6.552	.000
	Performance Expected	.125	.065	.190	1.927	.056

	Effort Expected	.053	.062	.077	.841	.402
	Social Influence	.077	.068	.112	1.133	.259
	Facilitating Conditions	.055	.048	.099	1.146	.254
a. Dependent Variable: Behavioural Intention						

Results in Table 4.9 above show that performance expectancy has a partial effect on behavioural intention (Beta= 0.190, t= 1.927, p= 0.056). However, since the p-value of 0.056 is above the expected p-value of 0.050, H1 is not supported. This implies that performance expectancy does not influence behavioural intention to adopt digital currency among individuals with criminal intentions in Harare. These results contradict Venkatesh et al. (2003) who found a significant relationship between performance expectancy and behavioural intention. The reason could be that the study by Venkatesh et al. (2003) focused on the utilization of technology in general, while the current study focused only on a specific financial technology and criminality.

Results in Table 4.9 show that effort expectancy has an insignificant effect on behavioural intention (Beta= 0.077, t= 0.841, p= 0.402). Therefore, H2 is not supported. This implies that effort expectancy when investigations does not influence behavioural intention by criminals to adopt digital currency. This contradicts Venkateshet al. (2003) who claims that effort expectancy influences behavioural intention. The reason could be that the study by Venkatesh et al. (2003) focused on the adoption of technology such as machinery while the current study focused on digital financial application.

Results in Table 4.9 above indicate that social influence has an insignificant effect on behavioural intention (Beta= 0.112, t= 1.133, p= 0.259). Therefore, H3 is not supported. This implies that social influence does not influence behavioural intention by criminals to adopt digital currency. For this reason, one's environment do not have an impact on an individual to adopt digital currency use for criminality.

Results in Table 4.9 above show that facilitating conditions has an insignificant effect on behavioural intention (Beta=0.099, t= 1.146, p= 0,254). Therefore, H4 is not supported. This implies that facilitating conditions on digital currency does not influence behavioural intention by criminals to adopt digital currency. These findings differ from those of Venkatesh et al. (2003) showing that conditions for facilitating possess a positive impact on behavioural intention to adopt a technology. However, the findings are similar to those of Alshehri, Drew and Alghamdi (2012) which established no significant effect of facilitating conditions on behavioural intention to accept e-government services.

4.10 Chapter summary

In this chapter, quantitative data and qualitative data were presented. Pie Charts, Tables, Bar graphs were utilized to present data. The research adopted a mixed approach to collect quantitative and qualitative data. Quantitative data was presented by utilizing the sequence based on the research questions from questionnaire. The response rate which was recorded for this study was 87%, with a 13% non-response rate are questionnaires not returned.

Chapter 5: Recommendations and Conclusions

5.0 Introduction

This research focused on the complexities digital currency has on financial investigations in relation to money laundering and terrorism financing. A case of Zimbabwe. The previous chapter looked at research results presentation, statistical analysis, and discussion. This final chapter of the study shall dwell on the recommendations by researcher and lastly offer conclusive statements based on the research questions and guided by the objectives of study.

5.1 Recommendations

The researcher makes the following recommendations as a direct outcome of this study.

5.1.1 Recommendation 1

Financial Investigations Agencies in Zimbabwe are encouraged to adopt a strategic approach to investigating digital currency platforms through the promotion of world best practices. It can be achieved by deliberate implementations of Financial Action Task-force (FATF) evaluation reports and United Nations Office on Drugs and Crime (UNODC) proposed virtual currency investigation manual and ask for assistance for capacity building initiatives as these international bodies have the funding and budgets aimed at helping developing countries like Zimbabwe be trained and be exposed to keeping abreast with emerging trends, tools and software's being used for investigative purposes.

5.1.2 Recommendation 2

Legislature and Judiciary should foster the creation and implementation of harmonisation of laws such as the Cyber Security, Crime and Data Protection Bill, Criminal Procedure and Evidence Act and Criminal Law Codification Act, for instance, to facilitate the plugging of legal impediments for investigators when seeking court orders to confiscate possible items or gadgets that may contain digital evidence and also to be able to effect arrests through clearly defined legal breaches when investigating digital currency platforms. This is possible when policy makers deliberately embrace these digital currency technology innovations and create a digital currency regulatory framework that encourage technology development.

5.1.3 Recommendation 3

Reserve Bank of Zimbabwe as the financial regulator through a piece of legislation formulated to promote bank use and suppression of money laundering should speedily formalise digital currency practices operations in order to adopt a professional stance which would make it easier to institute compliance and monitoring initiatives for basic anti-money laundering and terrorism financing modalities that would result in Financial Intelligence Unit (FIU) duties of supervision more effective as they would operate within the margins of regulatory guidelines. Formalisation of digital currency industry entails bringing more currency security and stability for the country.

5.1.4 Recommendation 4

Financial investigators in Zimbabwe should increase liaison with regional fundamental structures for cooperation such as Southern African Region Police Chiefs Coordination Organisation(SARPCCO), Southern Africa Organ on Politics, Security and Defence, Interpol Sadc Regional Headquarters, National Cyber Bureau (NCB) in Zimbabwe which should be utilised for digital currency investigations as they have an already existing cooperating network and infrastructure that can make facilitation of mutual legal assistance request be processed in time as a measure to curtail on bureaucratic tendencies involved when filing for cross border operations.

5.2 Conclusions of the Study

5.2.1 Conclusion: Research objective 1: To determine specific complexities encountered when investigating digital currencies from a sample of financial investigators.

This study did establish specific legal and technological issues surrounding digital currency platforms use which make investigations of money laundering and terrorism financing complicated to achieve arrests and prosecutions in developing countries like Zimbabwe chiefly being laxity in cyber regulatory framework and lack of tools and understanding on how to investigate new technology like blockchain. It was noted that criminals could be favouring the use of virtual currencies mainly because of their very nature which involve, increased ability to use pseudo-names which promote high chances of anonymity with platforms like darknets facilitating easy movement and illegal payments of services coupled with the transnational nature of digital technology facilitated by internet. Hence this objective was achieved.

5.2.2 Conclusion Research Objective 2: To investigate how other developing countries who have adopted digital currencies are coping.

The study established that other countries use regulatory instruments and are at an advanced stage to adopt centralised digital currency operations. It also established that there should be a framework to facilitate harmonisation of laws for better cooperation as the use of digital currencies by criminals has transnational characteristics that require use of existing bodies like INTERPOL, FATF and UNODC set standards. Cryptocurrencies give huge prospects for developments and inventions but at the same time are distinctively positioned to aid money laundering and terrorism financing as shown with cases in South Africa of illicit flows investigations increasing with identified individuals being on wanted lists. This objective was partially achieved as more work still needs to be from a developing countries perspective.

5.2.3 Conclusion Research objective 3: To assess any international standards set by developed nations in investigating digital currencies that can also be adopted by

developing countries like Zimbabwe.

This study noted the Basic Manual on Detection and Investigation of Laundering of Crime Proceeds by Virtual Currencies UNODC and the Train the Trainers Course in 2018 by UNODC could be considered as best set practices for investigations of digital currency platforms so far. Another important set standard is the governing of financial institutions that handles digital currency transactions which would help investigators when tracking and monitoring operations. It was also noted that major governments across the globe have taken very different approaches to the regulation of cryptocurrency as the digital currency technology is still evolving so much remains to be seen but otherwise the objective was achieved.

5.2.4 Conclusion Research Objective 4: To recommend action and guidelines to improve the current financial digital currency investigations eco-system.

The study asserts that an effective digital currency investigation eco-system involves various stakeholders who are Policy makers, Regulators, Law enforcement, International Bodies, General Public and the Criminal Justice System as a whole. As a matter of priority there should be a setting up of a regulatory authority that result in central governing of digital currency operations than to have warnings issued by government on the disadvantages of cryptocurrency investments. Financial Intelligence Unit should be given arresting powers for financial breaches than investigative powers only as this would smoothen the chain of custody for digital currency evidence. Judiciary should also compliment investigators through being trained on how to recognize digital evidence of financial nature in court proceedings from arrest to trial and fundamentally the educating the citizenry is critical by emphasizing on reporting any suspicions transaction on any platform on time which influences investigations.

5.3 Further suggestions for future research

This research focused on the complexities digital currency has on financial investigations in relation to money laundering and terrorism financing. A case of Zimbabwe. The author for this study suggests that the following areas be examined to generate more knowledge on digital currency platforms investigations:

(a) The attitude of senior or older investigators who were used to traditional guidelines of fighting financial crime, as a barrier to adoption of digital currency technology investigations tools and software's.

(b) The contribution of capacity building programmes for digital currency investigation to the anti-money laundering and terrorism financing regime in Zimbabwe.

(c) The effect of formalising digital currency to financial investigations in Zimbabwe.

References

Adrian, A., (2018). Data Challenges. Database Systems Journal, 4(3), pp. 31-40.

Alles, M., (2015). Drivers of the Use and Facilitators and Obstacles of the Evolution of Data by the Audit Profession. American Financial Association, 29(2), pp. 439-449.

Alves, M. D. C. G., Matos, S. I. A. (2010). Adoption of enterprise resource planning system – some preliminary results. Proceedings of the European Conference on Information Management & Evaluation

Brown-Liburd, H., Issa, H. & Lombardi, D., (2015). Behavioral Implications of Data's Impact on Audit Judgement and Decision Making and Future Research Directions. Financial Horizon's, 29(2), pp. 451-468.

Business.com, (2017). business.com. Available at: https://www.business.com/articles/-data--problem-coping-with-shortageof-talent-in-data-analysis/ Assessed 15 May 2017].

Byrnes, P., Criste, T., Stewart, T. & Vasarhelyi, M., (2016). Reimagining Technology in a Wired World. Available at: http://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/DownloadableDocuments/Whitepaper_Blue_Sky_Scenario-Pinkbook.pdf

Boerkamp, F., & Soerjoesing, S. (2010). Data-analyse als procesgericht controlemiddel. De IT-Auditor, 2, 29-34.

Byrnes, P., Ames, B., Vasarhelyi, M., & J.D. Warren, J. (2012). The Current State of Continuous Technology and Continuous Monitoring.

AICPA. Byrnes, P., Criste, T., Stewart, T., & Vasarhelyi, M. (2014). Re-imagining Technology in a Wired World. Chan, D., & Vasarhelyi, M. (2011). Innovation and practice of continuous technology. International Journal of Financial Information Systems, 12, 152-160.

Cao, M., Chychyla, R. & Stewart, T., (2015). Digital currenciesin Financial Statement Audits. Financial Horizons, 29(2), pp. 423-429.

Coyne, E., Coyne, J. & Walker, K., (2017). Data Information Governance by Accountants. International Journal of Financial and Information Management (forthcoming), Volume Working paper, pp. 1-34.

Crawford, K. & Boyd, D., (2016). Six Provocations for Data. Oxford Internet Institute's, p. 17.

Cobbin, P. E. (2012). International Dimensions of the Audit Fee Determinants Literature. International Journal of Technology, 6, 53-77.

Coderre, D. (2015). Continuous Technology: Implactions for Assurance, Monitoring and Risk Assessment. IIA.

Craswell, A. T., Francis, J. R., & Taylor, S. L. (2015). Auditor brand name reputations and industry specilizations. Journal of Financial and Economics, 20, 297-322.

Culotta, Aron. (2010). "Towards Detecting Influenza Epidemics by Analyzing Twitter Messages." In Proceedings of the First Workshop on Social Media Analytics, 115–22. SOMA '10. New York, NY, USA: ACM. doi:10.1145/1964858.1964874.

Das, Sanjiv R., and Mike Y. Chen. (2017). "Yahoo! For Amazon: Sentiment Extraction from Small Talk on the Web." Manage. Sci. 53 (9). Institute for Operations Research; the Management Sciences (INFORMS), Linthicum, Maryland, USA: INFORMS: 1375–88. doi:10.1287/mnsc.1070.0704.

DeAngelo. (2011). Audit size and reducing liquidity crunch. Journal of Financial and Economics, 3, 183-199.

Zimbocash. (2010). Continuous monitoring and continuous technology: From idea to implementation. Zimbocash.

Dean, Jeffrey, and Sanjay Ghemawat. (2018). "MapReduce: Simplified Data Processing on Large Clusters." Commun. ACM 51 (1): 107–13. doi:10.1145/1327452.1327492.

Domingos, Pedro. (2012). "A Few Useful Things to Know About Machine Learning." Commun. ACM 55 (10). New York, NY, USA: ACM: 78–87. doi:10.1145/2347736.2347755

Earley, C. E., (2015). Digital currenciesin technology: Opportunities and Challenges. Business Horizons, Volume 58, pp. 493-500.

Gershkoff, A., (2015). techcrunch. [Online] Available at: https://techcrunch.com/2015/12/31/how-to-stem-the-global-shortage-of-datascientists

Ginsberg, Jeremy, Matthew Mohebbi, Rajan Patel, Lynnette Brammer, Mark Smolinski, and Larry Brilliant. (2019). "Detecting Influenza Epidemics Using Search Engine Query Data." Nature 457: 1012–4. http://www.nature.com/nature/journal/v457/n7232/full/nature07634.html

Hay, D., Knechel, R. & Wong, N., (2016). Audit Fees: A Meta-analysis of the Effect of Supply and Demand Attributes. Contemporary Financial Research, 23(1), pp. 91-141.

Hayes, R., Gortemaker, H. & Wallage, P., (2017). Principles of Technology. 3e ed. Harlow: Pearson Education Limited.

Halevy, Alon Y., Peter Norvig, and Fernando Pereira. (2019). "The Unreasonable Effectiveness of Data." IEEE Intelligent Systems 24 (2): 8–12. doi:10.1109/MIS.2009.36.

Kessel, P. v., (2017). Data: Changing the way business operate, United Kingdom: Ernst & Young.

Loukides, Michael. (2012). What Is Digital currency. Sebastopol, California: O'Reilly.

Liddy, J., (2015). How Data and Analytics Are Enhancing Reducing liquidity crunch and Value. The CPA Journal, 85(5), p. 80.

Manson, S., McCartney, S. & Sherer, M., (2017). Audit automation: Improving quality or keeping up. In: M. Sherer & S. Turley, eds. Current Issues in Technology. Thousand Oaks,:Sage Publications.

Mayer-Schönberger, Viktor, and Kenneth Cukier. (2013). Data: A Revolution That Will Transform How We Live, Work, and Think. Second. New York, NY: Houghton Mifflin Harcourt.

Nasser, T. & Tariq, R., (2015). Data Challenges. Journal of Computer Engineering & Information Technology, 4(3), p. 10.

NBA, (2015). four investeren fors in data. Accountant, 13 11, p. 2.

Patil, Dhanurjay (2012). Data Jujitsu. Sebastopol, California: O'Reilly.

Patil, Dhanurjay (2011). Building Digital currency Teams. Sebastopol, California: O'Reilly.

Pepping W & Nooitgedagt (2014). Digital currenciesin financial statement audit: Does digital currenciesimprove the efficiency of an audit?

FINANCIAL INTELLIGENCE UNIT, (2015). Financial Intelligence Unit .com Available at: https://www.Financial Intelligence Unit .com/gx/en/audit-services/publications/assets/Financial Intelligence Unit -fact-sheet3-summary-of-eu-audit-reform-requirements relating-to-nas-feb-2015.pdf

Ramlukan, R., (2015). Available at: http://www.ey.com/gl/en/services/assurance/ey-reporting-issue-9-how--dataand-analytics-are-transforming-the-audit#item1

Ruhnke, K. & Schmidt, M., (2017). The audit expectation gap: existence, causes and the impact of changes. The audit expectation gap

Siegel, Eric. (2013). Predictive Analytics. New Jersey: John-Wiley; Sons.

Vasarhelyi, M. A., & Romero, S. (2014). Technology in audit engagements: a case study. Managerial Technology Journal, 29(4), 350-365.

Whitehouse, T., (2017). Technology in the Era of Data. Compliance Week, 29 April, p.

2.

Pîrjan, A., Petrosanu, D.-M., Huth, M., and Negoita, M. 2015. "Research Issues Regarding the Bitcoin and Alternative Coins Digital Currencies," Journal of Information Systems & Operations Management (9:1), pp. 1-14

Glaser, F., and Bezzenberger, L. 2015. "Beyond Cryptocurrencies-a Taxonomy of Decentralized Consensus Systems," 23rd European Conference on Information Systems (ECIS), J. Becker, J.V. Brocke and M. De Marco (eds.), Münster, Germany.

https://www.investvoyager.com/blog/peer-to-peer-transactions-spike-in-zimbabwe-following-foreign-currency-ban/

https://www.nasdaq.com/articles/the-future-of-digital-currency-2021-02-12

https://www.csis.org/analysis/train-leaving-station-digital-currency-sub-saharan-africa

https://www.unodc.org/unodc/en/drug-trafficking/crimjust/news/unodc-delivers-the-first-cryptocurrency-investigation-training-course-in-latin-america.html

https://bitcoinist.com/zimbabwe-finally-regulates-cryptocurrency/

https://www.imolin.org/pdf/UNODC_VirtualCurrencies_final_EN_Print.pdf

Frank Schmalleger & Michael Pittaro 2015, Crimes of the Internet, published by

Prentice Hall (2008: 283-301).

Jaishankar, K. (2008). Space Transition Theory of cybercrimes. In Schmallager, F., & Pittaro, M. (Eds.), Crimes of the Internet. (pp.283-301) Upper Saddle River, NJ: Prentice Hall.

Cornish, D., & Clarke, R. V. (1986). The reasoning criminal: Rational choice perspectives in offending. Springer-Verlag: New York, NY.

http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf

https://thenextweb.com/hardfork/2019/12/26/bitcoin-cryptocurrency-criminals-law-enforcement/

https://www.reuters.com/article/bc-finreg-aml-cryptocurrency-idUSKCN1FX29I

https://coinidol.com/african-countries-cryptocurrency/

https://businesstech.co.za/news/technology/228769/hawks-investigating-multi-million-rand-bitcoin-scam-in-south-africa-report/

https://www.fincen.gov/sites/default/files/advisory/2019-05-10/FinCEN%20Advisory%20CVC%20FINAL%20508.pdf

Appendix 1

Questionnaire: Digital Currency Investigations Survey

Academic study by collection of financial investigators views about digital currency.

1.What is your level of understanding about digital currency?

Low (You only have heard of it)

Medium (You know basics so need more information)

High (You have huge exposure to the platforms)

Other

2.Which organization do you belong to?

Police

Financial Intelligence Unit

Bank Loss Control and Security

Anti-Corruption Unit

Currency Agent

Other

3.What is your responsibility in investigation cycle for digital currency?

Analyst (Case Officer)

Investigation’s officer

Currency Dealer

Other

4.Is Digital Currency Crime prevalent?

Yes

No

Not Sure

5.What are the weaknesses digital currency has that makes it difficult to investigate?

....

6.Do you see the skills to investigate digital currency available?

Yes

No

Maybe

7.How can authorities stop unregulated digital currency trade?

....

8.Do you believe in the regulatory framework available for digital currencies?

..

Appendix 2

Interview guide for Digital Currency Investigation

1) **Some argue that digital currency use needs financial authorities' involvement, how can this help investigators?..**

2) **Given the crossing of borders of cyber space, how is the cooperation situation with other countries when investigating?..**

3) **What are the consequences for investigators when digital currency use is banned though trade still goes on?...**

디지털 화폐 플랫폼 수사의 복잡성에 관한 연구.

짐바브웨의 자금세탁 및 테러자금조달 사례.

2021년 6월 15일

정보법과학 석사학위 논문

럭슨 타파드와 즈비리쿠제

국제학과

지도교수: 장윤식

요약

주된 목적은 비트코인과 같은, 블록체인 기술을 활용해 금융 조사를 복잡하게 하고, 규제 기관과, 특히 자금 세탁과 전세계와 짐바브웨와 같은 개발도상국에 테러자금조달과 관련된 금융 시스템의 확산을 통찰하는 것이다.

본 논문은 짐바브웨에서 디지털 통화 플랫폼 내 거래가 실생활과 밀접함을 밝히며, 플랫폼 내에서 이뤄지는 자금 세탁과 테러 자금 조달의 범죄성을 보여주는 조사 통계가 아직 완전하지 않기 때문에, 조사 중에 금융 조사관에게 벽으로 다가오는 디지털 통화 플랫폼의 몇 가지 복잡성을 강조한다.

이 연구는 인터폴과 같은 기존 협력 기관과 디지털 화폐 거래 플랫폼 내의 모든 거래의 유동과 주소를 추적할 수 있는 소프트웨어 및 툴들을 이용한 법적 프레임워크로 도출되

는 전략적 접근 방식을 채택할 필요성을 강조하고, UNODC 와 KOICA 와 같은 국제 기구가 디지털 화폐 거래 플랫폼 관련 수사관을 양성해야한다 조언하며, 질문과 인터뷰, 주제와 관련된 오픈 소스 자료를 통해 자금 세탁과 테러 자금 지원을 수사하는 금융 정보 조사관들의 관련 자료를 통해 금융 디지털 통화 조사의 생태계를 개선하기 위한 구체적인 실현 가능한 조치와 지침을 결정하기 위해 혼합 연구 전략을 이용했다.

. 키워드: 디지털 통화, 자금 세탁, 테러자금조달, 금융 수사, 복잡성

Study about Complexities on Digital Currency Platforms Investigations. Case of Money Laundering and Terrorism Financing in Zimbabwe.

2021 June 15, 2021
Master's Degree Legal Informatics and Forensic Science
Luckson Tafadzwa Zvirikuzhe
Department of International Studies
Advisor Prof Yunsik Jake Jang

Abstract

The main objective was to provide an insight on the proliferation of digital currency platforms like Bitcoin that uses blockchain technology that has brought with it some complications for financial investigations, regulatory authorities, and the financial system especially in relation to combating money laundering and terrorism financing the world over and developing countries like Zimbabwe have not been spared also. This paper highlighted some of the complexities about digital currency platforms that exist for financial investigators during investigations, undertaken because of the declarations that digital currency platforms for trade are a reality in Zimbabwe and investigations statistics on money laundering and terrorism financing that display criminality on these platforms are not yet fully available. A mixed research strategy was adopted for this study to determine specific possible recommendable actions and guidelines to improve the current financial digital currency investigations eco-system with relevant data drawn from mainly Financial Intelligence officers who are mandated to investigate money laundering and terrorism financing through questionnaires and interview forms and supported by open source material on the subject matter thereby necessitating to draw conclusions that there is need to adopt a strategic approach that is guided by legal frameworks, using existing cooperation bodies like Interpol, adoption of software's and tools that can be able to trace movements and addresses of transactions on any digital currency platform and the need to train investigators through capacity building programs by international bodies like UNODC and KOICA for skills development.

Keywords: digital currency, money laundering, terrorism financing, financial investigations, complexities