ZIMBABWE

MONEY LAUNDERING/ TERRORIST FINANCING / PROLIFERATION FINANCING NATIONAL RISK ASSESSMENT

VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS

2024

TABLE OF CONTENTS

List of Tables

List of Figures

ACRONYMS

AEV	Anonymity Enhanced Virtual Assets
AML	Anti-Money Laundering
CDD	Customer Due Diligence
CFT	Counter Financing of Terrorism
CSAM	Child Sexual Abuse Material
DeFi	Decentralised Finance
DNFBP	Designated non-financial business and profession
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
ICO	Initial Coin Offering
LEA	Law Enforcement Agencies
ML	Money Laundering
NPO	Non-Profit Organisation
NPA	National Prosecuting Authority
NRA	VA and VASP National Risk Assessment
P2P	Peer to Peer
P2B	Platform to Business
PEP	Politically Exposed Person
PF	Proliferation Financing
PoW	Proof of Work
RBA	Risk-Based Approach
RBZ	Reserve Bank of Zimbabwe
SECZim	The Securities Exchange Commission of Zimbabwe
STO	Security Token Offerings
TOE	Traditional Obliged Entities
TF	Terrorists Financing
UBO	Ultimate Beneficial Owner
USD	United States Dollar
VA/VAs	Virtual Assets
VASPs	Virtual Assets Service Providers
WB	World Bank
WG	Working Group
ZIMRA	Zimbabwe Revenue Authority
ZRP	Zimbabwe Republic Police

DEFINITIONS

Bitcoin	The most prominent and widely recognized cryptocurrency, identified by the ticker symbol BTC.
Blockchain	The fundamental technology behind most cryptocurrencies, functioning as a comprehensive ledger of transactions maintained simultaneously by multiple nodes in a network.
Centralised Exchange	A cryptocurrency exchange operated by a single company that controls the platform.
Mixer	Services that blend transactions between various cryptocurrency addresses to obscure their origins, making them untraceable.
Custodial	Service providers that manage customers' private keys, thereby taking responsibility for the security of their virtual assets.
Dark Web	The portion of the internet that is intentionally hidden and requires specific software to access, often associated with illegal activities.
Ethereum	The second-largest blockchain platform by market capitalisation, after Bitcoin.
Fiat Currency	Government-issued currencies that are recognized as legal tender, such as the ZWG, US dollar, Euro, or British pound.
ICO (Initial Coin Offering)	Is a fundraising method used by blockchain projects to raise capital by issuing and selling new cryptocurrency tokens to investors.
Miners	Individuals or organizations that perform proof-of-work operations to validate cryptocurrency transactions.
Non-Custodial	Self-management of private keys, where the user directly holds their own keys.
P2P (Peer-to-Peer)	Transactions conducted directly between two individuals without the involvement of intermediaries or central authorities.
Ransomware	Malicious software used by hackers to encrypt victims' files, demanding a ransom often paid in VAs, for decryption or restoration.
Token	A unit of cryptocurrency that operates on a specific blockchain, such as XRP on the Ripple blockchain.
Virtual Assets	A digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities and other financial assets.
VASP	Any natural or legal person that, as a business, conducts one or more of the following activities or operations on behalf of another natural or legal person: i. Exchange between virtual assets and fiat currencies; ii. Exchange between one or more forms of virtual assets; iii. Transfer of virtual assets; and

	iv. Safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; v. Participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.
Virtual Asset Exchanges	Provide a digital online platform facilitating virtual asset transfers and exchanges. Exchanges can be online platform-based operating from different jurisdictions or in person, such as trading platforms that facilitate peer to peer exchanges or kiosk based exchanges. These exchanges offer services such as Fiat to Virtual Assets, Virtual Assets to Fiat, Virtual to Virtual, e.g. Luno, Coinbase, Kucoin, Kraken, Binance.
Wallet	A digital storage solution for securing cryptocurrency assets, which can be online (hot wallet) or offline (cold wallet).
Wallet providers (Custodial Wallets/ Hot wallet)	These entities provide storage for VAs or fiat currency on behalf of others. They facilitate exchanges or transfers between VAs and fiat currency. They include custodial wallets, and non-custodial wallets e.g. Metamask, Coinbase wallet, Trezor etc.

FOREWORD

In the rapidly evolving landscape of financial services and products, the rise of Virtual Assets (VAs) and Virtual Asset Service Providers (VASPs) signifies both opportunities and challenges to the economy. VAs and VASPs utilise advanced technologies that present new risks, particularly in areas such as money laundering, terrorist financing, and other forms of illicit financial activities.

It is within this context that I present the VA and VASP Risk Assessment Report. This report serves as a crucial tool for competent authorities and policymakers, as well as a valuable resource for industry participants who are interested in venturing into this business.

This document is a culmination of extensive research, analysis, and collaboration among key stakeholders from both the public and private sectors. The objective of this assessment is to provide a comprehensive overview of the current money laundering, terrorist and proliferation financing risks associated with VAs and VASPs in Zimbabwe. By understanding the risks inherent in the virtual asset ecosystem, robust frameworks can be developed that ensure integrity of our financial systems while fostering innovation and growth.

I extend my gratitude to all who contributed to this assessment. Your expertise and dedication are instrumental in our ongoing efforts to address the challenges and harness the opportunities presented by VAs and VASPs.

O. Chiperesa
National Task Force Chairperson
Director General, Financial Intelligence Unit

EXECUTIVE SUMMARY

Zimbabwe conducted its inaugural national money laundering, terrorist and proliferation financing risk assessment focused on the Virtual Asset (VAs) and Virtual Asset Service Providers (VASPs) for the period 2019-2024. This was necessitated by the increasing risks associated with virtual assets which have become a global concern.

The objective of this assessment was to identify, assess, and understand the money laundering, terrorist and proliferation financing (ML/TF/PF) risks posed by VAs and VASPs to Zimbabwe. This is a crucial step towards fulfilling the country's obligations under FATF Recommendation 15. The findings of the assessment will inform the development of a national policy framework for VAs and VASPs.

Zimbabwe employed the World Bank's tool and methodology to identify and assess the ML/TF/PF risks of VAs and VASPs. Representatives from both the public and private sectors contributed to the assessment. The country also engaged a United States-based blockchain explorer company to analyse the flow of virtual assets in and out of the country, covering both on-chain and off-chain activities.

The assessment revealed the existence of a Virtual Assets (VA) market with limited Virtual Asset Service Providers (VASPs) activities. The overall ML/TF/PF risk for VAs and VASPs in Zimbabwe was rated **Medium Low** as shown in the matrix below.

Risk score matrix

Overall, Threat						
	H	M	M	MH	H	H
	MH	M	M	MH	MH	H
	M	ML	M	M	MH	MH
	ML	ML	ML	M	M	M
	L	L	ML	ML	M	M

VA and VASP ML/TF/PF Risk level

L ML M MH H

Overall Vulnerability

key: L = low; ML = medium-low; M=medium; MH = medium-high; H = high

The medium low risk level was based on medium low threat level and medium low vulnerability level of the sector. These ratings for the ML/TF/PF risks in VA and VASP sector were due to its nascent stage, limited adoption of the products, which keep the sector relatively small. Additionally, the minimal interaction between VASPs, VA transactions, and the traditional financial sector further reduces the ML/TF/PF risks. The absence of significant ML or TF abuse incidents and the country's limited international integration in VA markets further reduce the risk. Though the overall ML/TF/PF risk was assessed as medium low, the potential for abuse is significant in the absence of a regulatory framework and the prevalence of peer-to-peer transactions.

The assessment identified four primary VASP categories operating in Zimbabwe namely wallet providers, exchanges, initial coin offerings, and information providers. The risk assessment determined that non-custodial wallets pose a medium risk for ML/TF/PF, while initial coin offerings (ICOs) present a medium low risk. Virtual asset exchanges were assessed as having a medium risk, whereas custodial hot wallets and information providers were considered to have a low risk of ML/TF/PF. Based on these findings the overall ML/TF/PF risk was rated medium low. The table below summaries the results.

Table 1: Summary of results

VASP	Types of Services	Sub-type	Threat	Vulnerability	Inherent Risk	Residual Risk
Wallet Provider	Custodial Wallet	Hot Wallet	Medium low (0,4)	Medium low (0,35)	Medium low (0,38)	Low (0,2)
	Non-Custodial	Cold Wallet	Medium High (0,69)	Medium High (0,75)	Medium High (0,72)	Medium (0,54)
VA Exchanges	Transfer Services	P2 P	Medium High (0,63)	Medium (0,58)	Medium (0.59)	Medium (0,42)

		P2B	Medium (0.50)	Medium low (0.38)	Medium (0,44)	Medium Low (0,32)
	Conversion Services	Virtual-to-Fiat	Medium High (0,63)	Medium (0,58)	Medium (0.59)	Medium (0,42)
		Virtual-to-Virtual	Medium High (0,63)	Medium (0,58)	Medium (0.59)	Medium (0,42)
		Fiat-to-Virtual	Medium High (0,63)	Medium (0,58)	Medium (0.59)	Medium (0,42)
Initial Coin Offering	Investment	Development of Product & Services	Medium (0,41)	Medium (0,42)	Medium low (0,31)	Medium low (0,31)
Information Providers	Educational content and Investment Advise		Low (0,2)	Low (0,19)	Low	Low

In terms of the VAs, the assessment established a high preference for stable coins such as USDT and USDC, with Bitcoin and other prominent cryptocurrencies also dominating. Privacy focused or anonymous coins, such as Monero, Zcash have shown limited interest and adoption in the country.

To mitigate the risks identified in the VAs and VASPs sector, Zimbabwe is recommended to establish a robust regulatory framework, enhance public awareness, and strengthen inter-agency cooperation. Implementation of these measures will go a long way in effectively combating ML/TF/PF within the emerging virtual asset ecosystem and complying with international standards.

CHAPTER ONE

1. INTRODUCTION

The primary purpose of carrying out a money laundering, terrorist financing and proliferation financing (ML/TF/PF) on VAs and VASPs was to identify, assess, and understand the risks associated with these activities. FATF Recommendation 15 require countries to identify, assess, and understand the money laundering, terrorist and proliferation financing risks emerging from virtual asset activities and the activities or operations of VASP. The results of the assessment will be used to shape policies that strengthen Zimbabwe's Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) regime. It is important to mention that this is a maiden assessment of the VAs and VASPs sector in Zimbabwe.

1.1 Background

Virtual assets (VAs), often referred to as cryptocurrencies, are virtual or digital representation of value that use cryptography for security.1 They operate independent of central banks or governments. The notable global growth of VAs reflects a significant shift in the global financial landscape, with the market capitalization of virtual assets, including stablecoins and tokens, soaring to nearly US$ 2.4 trillion by July 2024. This surge from US$ 640.24 billion in 2018 indicates a significant upward trajectory, with the number of virtual assets being traded across the globe, exceeding 2 million in 20242. Bitcoin, the first and most well-known cryptocurrency, was introduced in 20093. Since then, thousands of other virtual assets have emerged, each with its unique characteristics and functionalities.4 The global rise of VAs continues to ignite international debates concerning their potential role in facilitating money laundering and other illicit financial activities. Due to their decentralised nature, anonymity, and

[1] Virtual Assets - FATF

[2] https://coinmarketcap.com/

[3] Bitcoin Price History: 2009 to 2024 – Bankrate: www.bankrate.com

[4] Cryptocurrency Explained with Pros and Cons for Investment – Investopedia: www.investopedia.com

cross-border capabilities, virtual assets have attracted significant attention, both for their potential benefits and associated risks.5

To address these concerns, the Financial Action Task Force (FATF) revised Recommendation 15 in 2018, urging countries to evaluate and comprehend the risks associated with VAs activities and VASPs.

1.2 Virtual Assets Market survey in Zimbabwe

While the global landscape has been rapidly evolving with various cryptocurrencies since 2009, the country's adoption was limited until the establishment of a virtual asset exchange around 2017. This marked a significant turning point, signalling the country's entry into the world of digital currencies. Several factors, including economic instability and the need for more efficient remittance options, drew Zimbabweans into the VA sector as discussed below.

a) **Economic environment:** The country's economic challenges, including hyperinflation and currency fluctuations, allegedly drove people to seek for alternative forms of storing value of their investments.

b) **Remittances:** A significant portion of the Zimbabwean population relies on remittances and virtual assets offer a faster and potentially cheaper way to transfer funds across borders. While remittances are important to the economy, the use of VAs as remittance solution remains small and fragmented, often operating through informal channels like WhatsApp groups.

c) **Technological advancements:** The wide use of smartphones and internet connectivity facilitated the adoption of digital technologies, including virtual assets. However, this nascent market was also marred by fraudulent activities, such as scams and Ponzi schemes, which resulted in financial losses. Moreover, a general lack of

[5] Shielding Against Illicit Activities: Curbing Anonymous Transactions with Virtual Assets: financialcrimeacademy.org

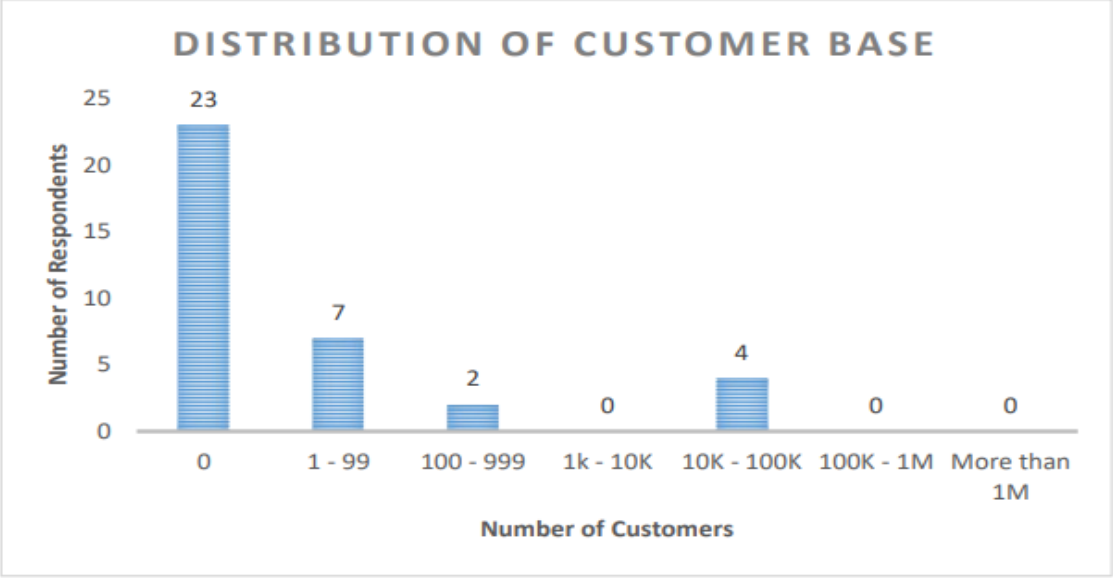
technical literacy regarding cryptographic principles and VAs operations hindered widespread adoption.

The identification of VASPs was a challenge since the country had no regulatory framework in place. Nevertheless, the assessment revealed that the VA market in Zimbabwe is characterised by limited penetration, informal trading, and underdeveloped infrastructure.

Despite the above, a few cryptocurrency exchanges and custodial wallet providers emerged in Zimbabwe. A study conducted by a United States of America based company, revealed that there were six cryptocurrency exchanges that originated from Zimbabwe since 2018. However, some of these exchanges ceased operations around 2020 except for two. The study also noted that, at the peak of their operations, none of these exchanges had more than 3,000 subscribers.

Survey responses indicated that most VASPs operating in Zimbabwe serve less than one thousand customers, with the exception of four entities that have customer base ranging from ten thousand to one hundred thousand, primarily operating outside of Zimbabwe but serving Zimbabweans, as shown below.

Fig 1: Distribution of customer base

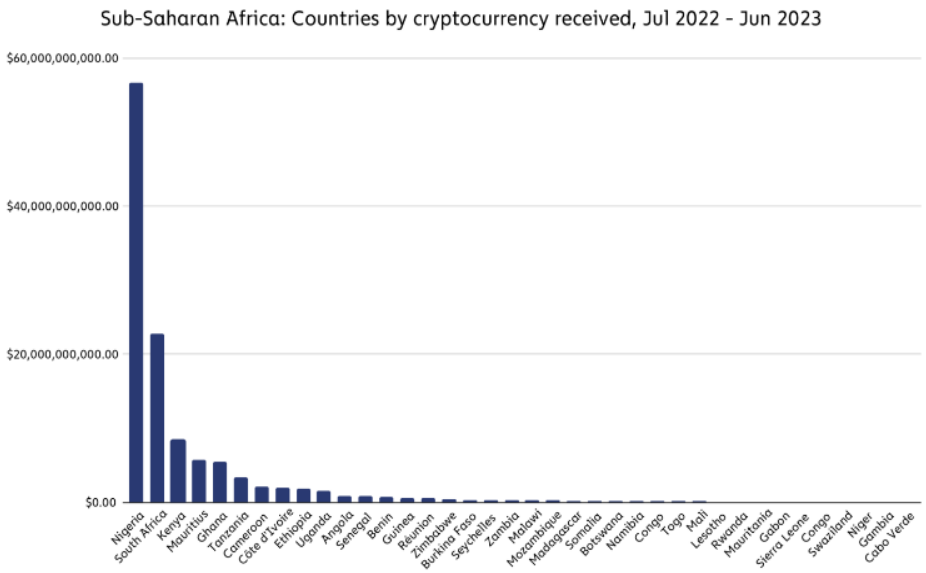


Source: VASPs Survey

The market also saw a handful of initial coin offerings (ICOs), such as Big Five Token. The country's VA exchange and mining infrastructure were also considered to be underdeveloped and minimal, at the time of the assessment.

There was absence of mixers or VA anonymizers, which was attributed to a lack of demand and the requisite technical expertise and software for such services. In addition, VASPs in the country involve individuals managing virtual assets on behalf of others through manual custody arrangements. This is consistent with the study conducted by Chainalysis on cryptocurrency adoption trends in Sub-Saharan Africa, which was released on 19 September 2023. The report showed that Zimbabwe has little virtual assets activities as compared to other countries in the region. The Chainalysis study revealed that Sub-Saharan Africa has the smallest crypto economy among all regions, accounting for just 2.3% of global transaction volume between July 2022 and June 2023. The study also showed that, across the region, centralized exchanges were the most widely used platform type, facilitating over half of all transaction volume.

Fig 2: Countries by cryptocurrency received 2022–2023

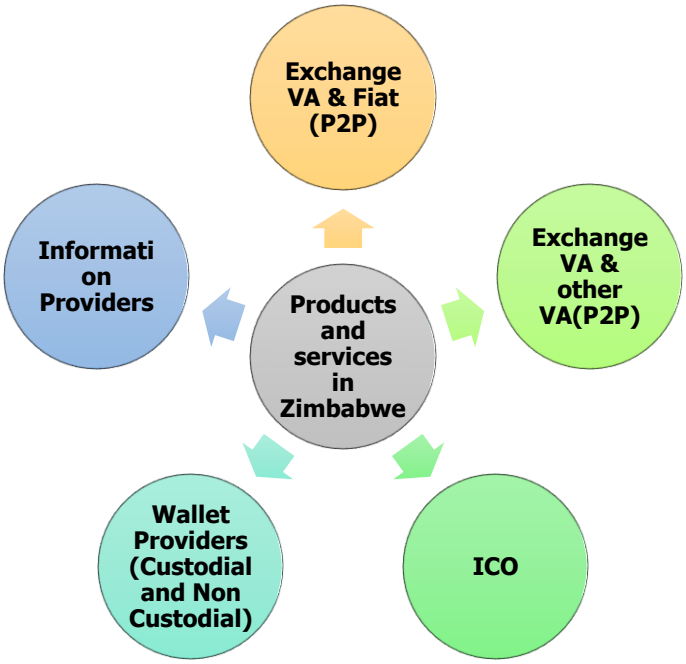


Source: Chainalyisis

1.3 Products and Services offered by VASPs in Zimbabwe

VASPs in Zimbabwe were noted to offer a variety of services as shown below.

Fig 3: Services offered by VASPs



These products and services are defined as follows;

a) Wallet providers (Custodial wallets/ Hot wallet)- These entities provide storage for VAs or fiat currency on behalf of others. They facilitate exchanges or transfers between VAs and fiat currency. They include custodial wallets and non-custodial wallets. A custodial wallet is a type of cryptocurrency wallet where a third party in most cases a VASP holds and manages the private keys on behalf of the user. This means the user does not have full control over their funds but benefits from convenience and security features provided by the custodian. Examples include, Binance Wallet (Binance Exchange), Coinbase Wallet (Coinbase Exchange) etc. A non-custodial wallet gives the user full control over their private keys, meaning they are solely responsible for securing their funds. Transactions are directly

managed by the user without reliance on third parties. Examples include MetaMask, Trust Wallet, Ledger Nano X, Trezor.

b) Virtual Asset Exchanges - provide a digital online platform facilitating virtual asset transfers and exchanges. Exchanges can be online platform-based exchanges operating from different jurisdictions or in person, such as trading platforms that facilitate peer to peer exchanges or kiosk-based exchanges. These exchanges offer services such as Fiat to Virtual Assets, Virtual Assets to Fiat, Virtual to Virtual for example Luno, VALR, Coinbase, Kucoin, Kraken, Binance, Cryptogem.

c) Initial Coin Offering (ICO)- is a type of fundraising activity where providers issue and sell virtual assets to the public. In Zimbabwe, ICOs primarily involve the issuance and sale of coins, without typically offering additional benefits such as equity, dividends, or voting rights commonly associated with traditional fundraising methods.

d) Information Providers- mainly provide educational content on cryptocurrency. They also offer ratings and reviews of cryptocurrencies, exchanges, wallet and other related services to assist users in making informed decisions.

Specific virtual assets such as Bitcoin, Ethereum, USDC and USDT stood out as the most traded, with a focus on investment and trading gains rather than payment solutions. Privacy focused coins like Monero have generated little interest and face negligible demand.

CHAPTER TWO

2. METHODOLOGY

Zimbabwe employed the World Bank's risk assessment tool to conduct the risk assessment of VAs and VASPs. The assessment identified and evaluated the ML/TF/PF threats and vulnerabilities of VA/VASPs operations in Zimbabwe. It also considered mitigatory measures to determine a national residual risk rating. Subsequently, a strategic action plan was developed, recommending further steps to be adopted at national level.

2.1 Stakeholders involved

VAs and VASPs Working Group was established in accordance with the World Bank's methodology. The Working Group comprised of relevant public and the private sector participants with representation from the following:

a) Ministry of Finance, Economic Development and Investment Promotion;
b) Financial Intelligence Unit;
c) Reserve Bank of Zimbabwe;
d) Securities and Exchange Commission of Zimbabwe;
e) Zimbabwe Revenue Authority;
f) Zimbabwe Republic Police;
g) Bankers Association of Zimbabwe;
h) Mobile Money Operators;
i) Virtual Assets Service Providers; and
j) Academia.

Consultations with the private sector were conducted, providing valuable data, and useful insights in developing recommendations for the national risk assessment. A blockchain explorer company based in the U.S.A, also conducted an independent study on VAs and VASPs activities in Zimbabwe, the results of which were incorporated into the report.

World Bank Tool

Zimbabwe received technical assistance from the World Bank Group as part of national efforts to capacitate the relevant stakeholders. The World Bank also provided the risk assessment tool which was comprehensive and focused on components deemed relevant to the national context, as highlighted below.

Table 2: VA and VASPs operating in Zimbabwe

VASP	TYPE OF SERVICE	CATEGORY
Virtual Asset Wallet providers	Custodial	Hot
	Non-Custodial	Cold
Virtual Asset Exchanges	Transfer Services	P2P
		P2B
	Conversion Services	Fiat-to-Virtual
		Virtual-to-Fiat
		Virtual-to-Virtual
Initial Coin Offering (ICO)	Fund Raising	Fiat-to-Virtual
		Virtual-to-Virtual
	Investment	Development of Product & Services
	Other Offerings	Security Token Offerings (STOs)
		Initial Exchange Offerings (IEOs)
Information Providers		

2.2 Data collection

The Working Group used data collection methods such as:

a) Questionnaires that were sent to virtual assets service providers, supervisors, traditionally obliged entities and law enforcement agencies;

b) Interviews and discussions with VASPs and the private sector;
c) Open-source - research;
d) Reports from block chain explorer;
e) Criminal case studies on VAs;
f) A public notice was issued to the public inviting service providers and other participants to volunteer information since Virtual Asset activities in the country are mainly informal and
g) Dummy transactions to understand the registration and transaction flow of the products.

2.3 Interpretation of risk assessment results

The overall ML/TF/PF risk was calculated by combining the threat and vulnerability ratings for each category of virtual asset service providers. The risk rating also considered the residual ML/TF/PF risk rating for each category of VASP, after taking into consideration mitigatory measures by VASPs, Government and Traditionally Obliged Entities (TOEs). The Heat map below was used to illustrate the final results.

Overall Threat					
H	M	M	MH	H	H
MH	M	M	MH	MH	H
M	ML	M	M	MH	MH
ML	ML	ML	M	M	M
L	L	ML	ML	M	M
	L	ML	M	MH	H

Overall Vulnerability

NB: *L = low; ML = medium-low; M=medium; MH = medium-high; H = high*

Risk levels were classified into five categories: High, Medium High, Medium, Medium Low, and Low. Similarly, the effectiveness of mitigating measures was rated from Very High to Does Not Exist. The key below was used to interpret the risk levels.

Table 3: Key for result interpretation

Scale	Interpretation
0 – 0.2	Low
0.21 – 0.4	Medium low
0.41 – 0.6	Medium
0.61 – 0.8	Medium high
0.81 – 1	High

2.4 Limitations of the data collection process

Challenges faced included the following;

a) Lack of detailed information from some of the questionnaire responses.
b) Lack of a legal framework for regulating VAs activities contributed to the scarcity of information on VA and VASPs.
c) Unavailability of officially compiled VA/VASP data in the country.

CHAPTER THREE

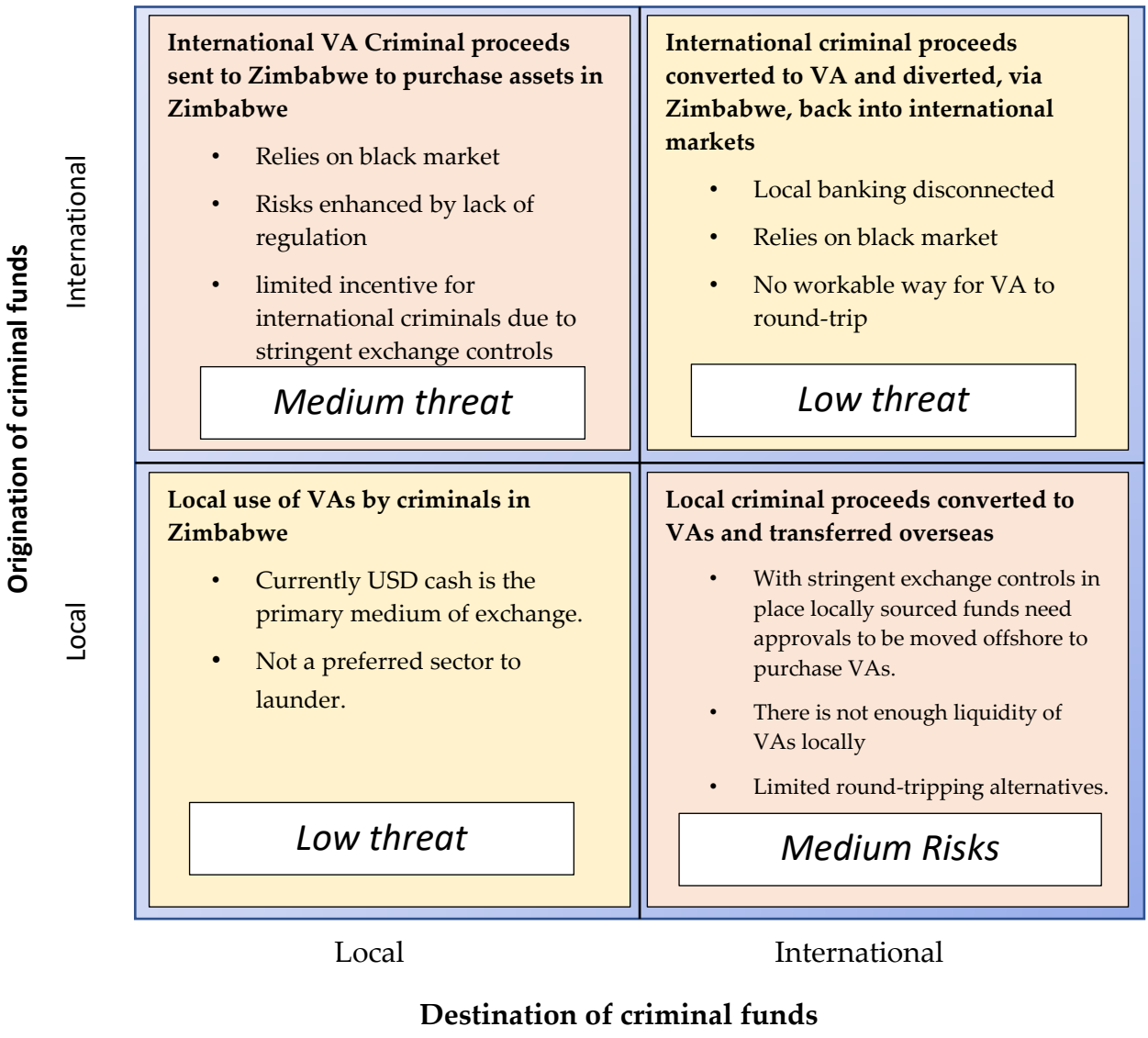
3. DETAILED FINDINGS

3.1 Threat Assessment

VA and VASPs threat arise from predicate offences associated with their ecosystem. The threat level for each identified VASP was assessed based on the different input variables from the World Bank tool.

The threat of ML/TF/PF was also assessed by categorising and distinguishing the possible sources and destinations of illicit funds, both domestically and internationally, as outlined in the following matrix.

Fig 4:Qualitative matrix of illicit money flows



3.1.1 Local to Local illicit flows

In Zimbabwe, the incentive for criminals to engage in money laundering using virtual assets is minimal due to the predominance of cash-based transactions within the economy. The widespread use of USD cash over any other form of payment such as virtual assets contribute to the low threat level. There are no known shops or outlets that accepts VAs as a form of payment.

3.1.2 International to Local illicit flows

In this scenario, the proceeds of criminal activities that are originated internationally, are brought into Zimbabwe as VAs and used to purchase assets in Zimbabwe. This activity relies on the parallel market to trade in VAs since banks and other regulated institutions are prohibited from processing VAs transactions.

Zimbabwe has a significant number of nationals based in the diaspora who have access to VAs which can be sent home through the informal/parallel market. The threat for this scenario was therefore rated medium.

3.1.3 International via Zimbabwe to International illicit flows

This risk emanates from criminals bringing in illicit proceeds of fiat currency into the country, which are then used to purchase VAs and transferred back into international markets. There is no feasible way for international funds in the form of cash to flow into the country, other than via formal banking channels.

Locally, acquiring VAs requires buying them with fiat currency on international markets, which inherently restricts this trade where Zimbabwe is used as an intermediary.

3.1.4 Local to International illicit flows

In this quadrant, proceeds sourced locally are destined internationally to some other jurisdiction. Local criminals may launder money by converting their proceeds in VAs and transferring them internationally, posing various challenges. Exchange controls prevailing in the country restrict

moving local funds abroad to acquire VAs, affecting both criminals and intermediaries thus inhibiting other round-tripping methods.

Further, sourcing VAs often depends on an unregulated informal market, which discourages many users from placing large sums of money to participate in the VA sector. In addition to the above quadrant, the threat arising from predicate offences was also analysed as follows.

3.1.5 Predicate offences to ML/TF/PF threat to VAs and VASPs

3.1.5.1 Fraud

The demand for VAs in Zimbabwe is rising due to a widespread "get rich quick" mentality, largely fuelled by social media. This mindset has led individuals with limited knowledge to enter the market by purchasing cryptocurrencies for investment purposes using third parties. Research has shown that individuals often share their private keys with agents when buying crypto or hire experts to invest on their behalf, hoping to realize profits. In most cases, the agents or experts defraud the ignorant investors.

The absence of regulatory oversight and the anonymity of cryptocurrency transactions have made it easier for fraudulent activities to proliferate. This situation underscores the need for increased public awareness and education about cryptocurrency, as well as establishment of clear regulatory frameworks to protect investors and curb fraudulent activities. Cases of fraudulent activities were recorded in the period under review 2020-2024.

Case Study 1: Fraud on Cold Wallet

A few cases were reported at the CID Commercial Crime Division such as the fraud case involving a complainant whose cryptocurrency worth US$108, 000.00 was allegedly stolen by a well-known crypto currency dealer. The case is before the courts and the accused was granted bail by the High Court. The challenge of the case is that there is no legal framework to prosecute crypto currency. To facilitate the investigation of the case, the accused was charged with fraud and the equivalent value of the cryptocurrency in USD was used. The case can be accessed through this link: https://www.herald.co.zw/top-eye-specialist-loses-us108-000-in-crypto-deal/

3.1.5.2 Kidnapping

Kidnapping for ransom involves abducting individuals and demanding payment in cryptocurrency. Criminals prefer this method due to the anonymity that cryptocurrencies provide, making it harder for authorities to trace the proceeds. Reports suggest a growing trend in the use of cryptocurrency for ransom payments worldwide.

3.1.5.3 Robbery

VAs can also be targeted during physical robbery, where perpetrators steal the individual's hardware wallets, private keys, user passwords and other personal information to access online accounts. In Zimbabwe no such cases were reported.

3.1.5.4 Ransomware Attacks

Ransomware attacks have surged in recent years, with cybercriminals preferring cryptocurrency as the payment method. Victims are often left with little choice but to pay the ransom, leading to increased criminal activity.

Case Study 2: Kidnapping and Ransomware

Another interesting case involves a Zimbabwean businessman based in South Africa. The victim was kidnapped by eight criminals who took him from South Africa to Zimbabwe, intending to rob him of his cryptocurrency worth US$13.9 million. The matter is currently before Zimbabwean courts. The case can be accessed through this link: https://www.zimlive.com/crypto-couple-kidnapped-in-sa-and-smuggled-into-zimbabwe/

3.1.5.5 Violation of the Exchange Control Act and Taxation in Zimbabwe

Crypto currency transactions are being done clandestinely through any mode of payment available in Zimbabwe i.e. formal banking channels, mobile money operators and mainly cash in USD. When using formal payment systems, the purpose of funds or types of transaction is not declared correctly, making it difficult to apply any form of tax. In this regard and due to the lack of regulation, all crypto currency transactions are not being subjected to tax.

3.1.5.6 Crypto Currency Scams/Schemes

Fraudulent crypto currency websites have flooded the social media with purported lucrative investment return and most Zimbabweans are falling victim to these scams which are brought by purported Crypto Information Providers.

Case Study 3: Crypto Currency Scams / Schemes

Victims have fallen prey to fraudulent websites like Blue Wallet, resulting in financial loss. Additionally, scammers have posed as cryptocurrency investors, with companies like Bitcoin Interchange which operated during the COVID-19 pandemic as a prime example. These scammers exploited the public's limited knowledge of cryptocurrency trading in Zimbabwe, where they took deposits from the public purporting to invest in crypto and then closed shop leaving the investors stranded with no access to their funds . The picture below shows the cards which were given to people by Bitcoin Interchange as wallets.

3.1.6 Summary results of threat assessment

Based on the above assessment of predicate offences, the quadrant analysis, and other variables from the tool, the threat level for VAs through each assessed VASP channel is shown below.

Table 4: Summary of threat rating results

VASP	Types of Services	Sub-type	Threat
Wallet Provider	Custodial Wallet	Hot Wallet	Medium low (0,4)
	Non-Custodial	Cold Wallet	Medium High (0,69)
VA Exchanges	Transfer Services	P2P	Medium (0,59)
		P2B	Medium (0.50)
	Conversion Services	Virtual-to-Fiat	Medium (0,59)
		Virtual-to-Virtual	Medium (0,59)
		Fiat-to-Virtual	Medium (0,59)

Initial Coin Offering	Investment	Development of Product & Services	Medium (0,41)
Information Providers	Educational content and Investment Advise		Low (0,2)

The overall threat level was rated as medium low. While there have been some cases involving virtual assets, their prevalence in Zimbabwe remains low, including the use of anonymising virtual assets such as Monero, Dash, and Zcash which are regarded as high risk.

3.2 Vulnerability Assessment

An analysis of the ML/TF/PF vulnerability of VA and VASPs looked at the gaps in regulatory frameworks. The following variables were assessed:

a) Licensed in the country or abroad;
b) Nature, size and complexity of business;
c) Products/services;
d) Methods of delivery of products/services;
e) Customer types;
f) Country risk;
g) Institutions dealing with VASP;
h) VA (Anonymity/pseudonymity);
i) Rapid transaction settlement; and
j) Dealing with unregistered VASP from overseas.

Zimbabwe is exposed to licensed/unlicensed as well as regulated /unregulated VASPs from outside the country. At the time of the assessment, there were no registered or licensed VASPs operating within Zimbabwe due to the absence of a legal framework for licensing and registration. This lack of a regulatory framework implies that VASPs offering services in Zimbabwe may either be licensed elsewhere or unlicensed, thereby increasing the risk exposure. The following are the VASPs which were identified and assessed.

3.2.1 Wallet Providers (Custodial Wallets/ Hot wallet)

The lack of regulatory oversight of VASPs in Zimbabwe and limited visibility into the flow of funds to and from wallets may attract overseas VASPs looking to exploit jurisdictional arbitrage opportunities. Several wallet providers offer custody services for high-risk VAs, including pseudo-anonymous or anonymous VAs. It is possible that in Zimbabwe, criminals might use unregulated hot wallets to perform peer-to-peer (P2P) transactions. Wallet providers are vulnerable to money laundering, terrorist and proliferation financing (ML/TF/PF) abuse, as criminals can exploit them to store and transfer illicit funds.

However, it was noted that most Zimbabweans with Hot wallets use international custodial exchanges such as KuCoin, Binance, OKX etc, that are licensed internationally, and they perform Know Your Customer (KYC) and Customer Due Diligence (CDD) during onboarding.

The vulnerability levels for hot wallets in Zimbabwe were assessed as low at 0.35. Moreover, there was only one VASP offering custodial wallets in the country, and it had not commenced operations at the time of the assessment. Zimbabweans can only register when the platform opens.

Additionally, the funding of these wallets is primarily done through cash (USD) transactions, as the VASP's ecosystem is not integrated with the formal financial sector. This lack of integration further mitigates the risk, as it limits the ability to move large sums of money undetected. Consequently, the economic impact of hot wallets in Zimbabwe remains insignificant.

3.2.2 Wallet Providers (Non-Custodial/ Cold wallets)

The vulnerability level for cold wallets in Zimbabwe was rated medium high. This high threat and vulnerability level is primarily attributed to the anonymity of cold wallets, the difficulty of tracing and seizing them, and the lack of face-to-face contact during transactions.

At the time of assessment, an online company operating in Zimbabwe offered ledger nano cold wallets. Some individuals in the country use MetaMask and Trust wallet as their cold wallets because they are free to download, use and offers robust security features. The pictures below shows some of the cold wallets.

Non-Custodial Wallets

The security features of cold wallets make them appealing to legitimate users and also to those with malicious intent, facilitating the concealment and movement of illicit funds. Few Zimbabweans use cold wallets compared to hot wallets, primarily due to a lack of knowledge.

3.2.3 Virtual Exchanges

The level of vulnerability arising from virtual exchanges was rated medium. The exchange in Zimbabwe largely offers P2P transactions and brokerage services as it matches buyers and sellers. It is also involved in other services such as Fiat-to-Virtual, Virtual-to-Fiat and Virtual-to-Virtual exchange. The exchanges are highly vulnerable to money laundering since they are not regulated. Some of these exchanges have not implemented any AML/CFT measures posing a high risk of ML/TF/PF, externalisation and tax evasion due to its anonymous customer base. Categories such as P2B and fiat-to-virtual transactions, were rated as medium. This exchanges primarily operates as a P2P exchange.

3.2.4 Initial Coin Offering

There were approximately 20 tokens that were introduced by Zimbabweans which includes Tac Token, Survivor Token, Stockvel Coin, Simba Coin, Ubuntu Coin, Bullrun Coin, Big Five Token, Catpump, Zombracoin, Solama, and Iketecoin among others and only Big Five Token (BFT) successfully penetrated the market. Other tokens have not succeeded as they turned out to be fraudulent or poorly issued. Some of the failed tokens were associated with or showed synonymous activity to fake coins or scam coins.

The vulnerability rating for the successfully issued ICOs was rated medium. However, the overall vulnerability level does not negate the potential for financial losses and fraud faced by investors.

3.2.5 Information Providers

Information providers pose low vulnerability rating of ML/TF/PF. In Zimbabwe information providers only provide educational content on cryptocurrency. They also offer ratings and reviews of cryptocurrencies, exchanges, wallet and other related services to assist users in making informed decisions. The table below summarise the vulnerability ratings.

Table 5: The vulnerability assessment results

VASP	Types of Services	Sub-type	Vulnerability
Wallet Provider	Custodial Wallet	Hot Wallet	Medium low (0,35)
	Non-Custodial	Cold Wallet	Medium High (0,75)
VA Exchanges	Transfer Services	P2P	Medium (0,58)
		P2B	Medium low (0.38)
	Conversion Services	Virtual-to-Fiat	Medium (0,58)
		Virtual-to-Virtual	Medium (0,58)
		Fiat-to-Virtual	Medium (0,58)
Initial Coin Offering	Investment	Development of Product & Services	Medium (0,42)

Information Providers	Educational content and Investment Advise		Low (0,19)

3.3 Vulnerability Assessment Based on Type of Transactions

3.3.1 Peer To Peer Crypto Transactions

Crypto activities in Zimbabwe are mostly peer to peer, mainly due to the absence of a formal platform for interaction between formal banking channels and VASPs. This followed the warning from Reserve Bank of Zimbabwe for banks not to facilitate cryptocurrency transactions in the absence of a regulatory framework. As a result, crypto transactions are conducted outside the formal market on a willing buyer willing seller basis. This involves "crypto currency dealers" trading at a premium fee of 10% to 15%. Cryptocurrency dealers have established backyard offices where they sell VAs to individuals, with transactions primarily involving the purchase of VAs using fiat currency, mainly USD cash.

Research conducted revealed that most P2P platforms commonly used are Paxful, Poloniex and Binance. These platforms facilitate the buying, selling, and trading of digital assets, including Bitcoin and stablecoins, enabling users to conduct international transactions.

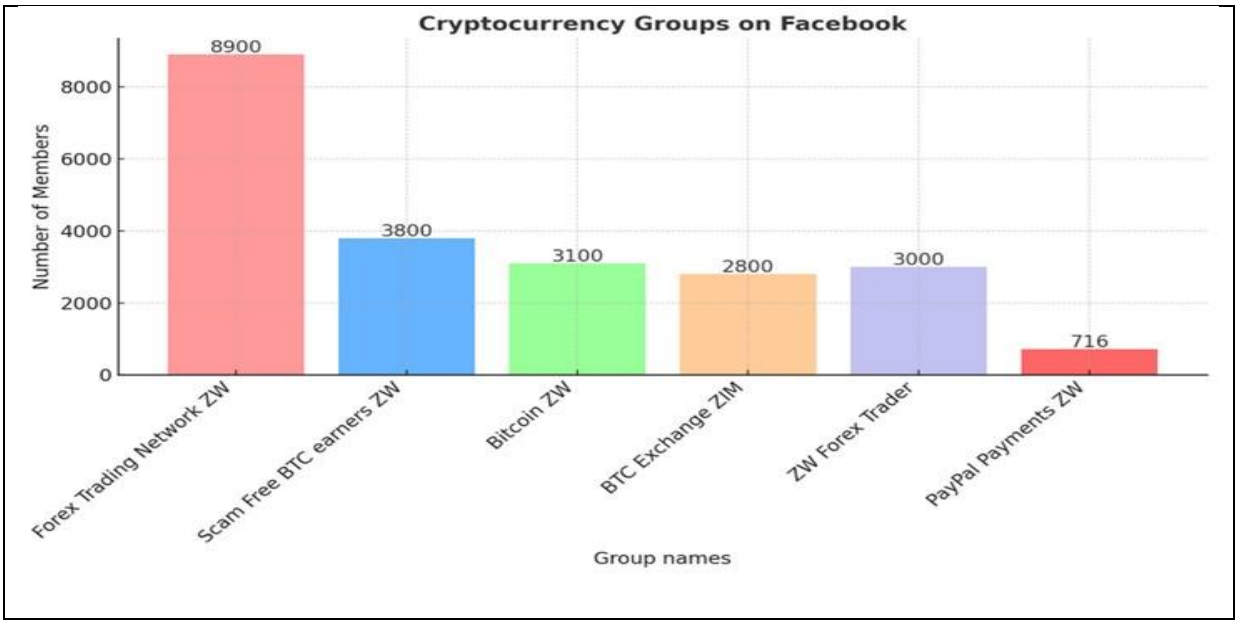
They also connect users with vendors from neighbouring countries like Kenya, Nigeria, and South Africa. While these platforms provide financial inclusion and cross-border transaction capabilities, they also present vulnerabilities to illicit financial activities. Blockchain analysis has identified links between some transactions and potentially illicit activities. However, there is no recorded evidence of terrorist financing cases in Zimbabwe, and transactions linked to the darknet were not necessarily indicative of money laundering or terrorism financing. The overall risk ratings assigned to these platforms was medium high.

3.3.2 Role of social media on P2P transactions

Social media platforms like telegram, WhatsApp, and Facebook play a significant role in enhancing P2P transactions in Zimbabwe. Over 25,000 active Zimbabweans were identified in various social media platforms related to cryptocurrency trading. These platforms allow for encrypted and direct communications between traders without having to rely on a third-party platform.

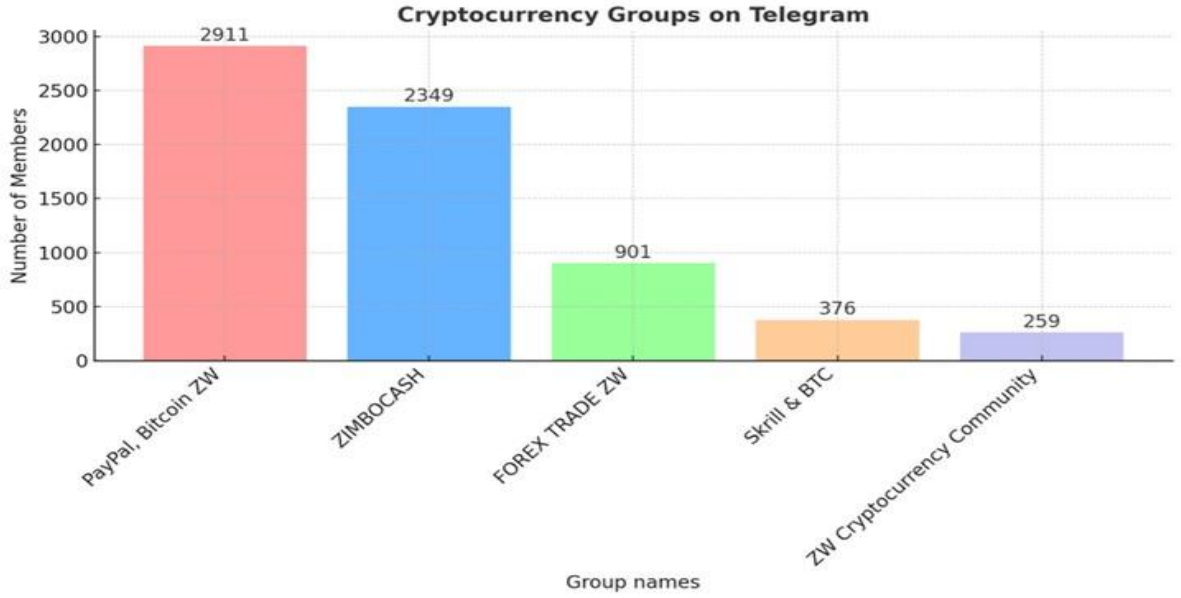
The chart below displays the six Zimbabwean Facebook cryptocurrency groups that were analysed. It shows over 20,000 combined members in the various group.

Fig 5: Cryptocurrency groups on facebook



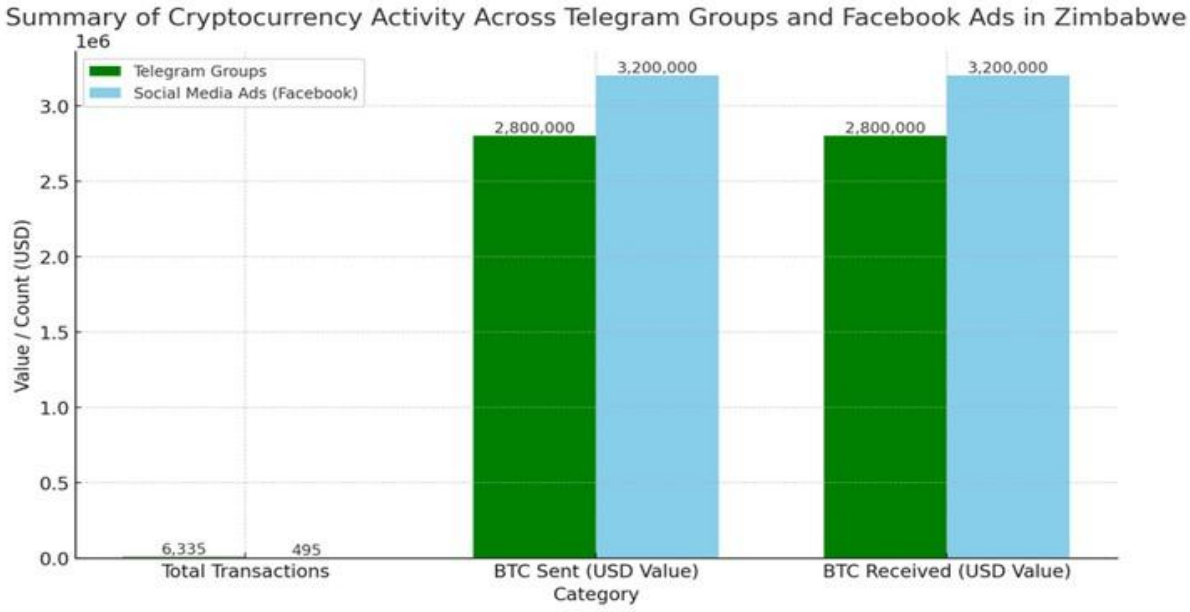
The chart below displays five Zimbabwean Telegram cryptocurrency groups that were analysed. It shows over 6,500 combined members in the various groups.

Fig 6: Cryptocurrency groups on telegram



The following chart summarizes cryptocurrency activity across various social media platforms in Zimbabwe.

Fig 7: Summary of cryptocurrency activity across social media platforms



The above shows that cryptocurrency activities in Zimbabwe remain limited, with a small portion of the adult population engaging in such transactions. While precise figures are unavailable, estimates suggest that fewer than 20,000 individuals actively participate in the cryptocurrency

market compared to the country's total population 16,67 million in 2023.This indicates that cryptocurrency adoption has not achieved significant penetration in the country. Consequently, the contribution of cryptocurrencies to the country's GDP is not known since it has not been calculated.

3.4 Interaction Between VASPS and Banks

A survey targeting the traditionally obliged entities (TOEs) such as banks revealed that they do not have any relationship or accounts with VASPs. This was as a result of the cautionary statements that prohibited banks from establishing any relationship with a VASPs including opening an account. Traditionally obliged entities thus put in place various controls in response to the 2017 and 2018 cautionary statements, including robust KYC mechanisms and ongoing monitoring tools to ensure they do not maintain accounts or establish any relationship with a VASP.

Traditionally obliged entities, however, acknowledged the possibility that some of the virtual asset's payments were processed using their platforms due to limitations in detecting these transactions which are largely conducted on P2P basis.

The survey further established that 18% of the respondents from TOEs, indicated having detected transactions involving virtual asset related activities by individuals on a P2P basis.

3.5 Terrorist and Proliferation Financing Risk through VAs and VASPS

Terrorist groups and proliferators exploit the anonymous and borderless nature of VAs to circumvent traditional financial controls. Unregulated or poorly regulated VASPs can facilitate these illicit activities by providing platforms for buying, selling, and transferring VAs with minimal oversight. The decentralized structure of many cryptocurrencies further complicates tracking and enforcement efforts.

Terrorist organizations and proliferators may also utilize VASPs to solicit funds from supporters worldwide through social media and other online channels. Weak Know Your Customer (KYC) and Customer Due Diligence

(CDD) procedures at some VASPs enable anonymous account creation and transactions, enabling the unobstructed flow of terrorist financing.

Despite the presence of stablecoins in Zimbabwe, there is no evidence linking them to TF and PF activities within the country. No concrete cases of TF and PF through VAs and VASPs, have been recorded in the country to date. While international typologies highlight the potential risks of terrorist and proliferation financing (PF) through virtual assets (VAs), there is no direct indication of such activities occurring domestically. As a result, the overall TF and PF risk associated with VAs in Zimbabwe has been assessed as low.

CHAPTER FOUR

4. MITIGATION MEASURES

4.1 Mitigation measures by government

In response to fraud cases purported to be linked with the use of VAs, government implemented several measures. These included directing banking institutions, in 2018, to cease providing services related to virtual currencies until appropriate regulations were in place. Additionally, a public warning was issued, in 2018, cautioning against the risks associated with cryptocurrency trading. To address the broader issue, the government collaborated with regulatory bodies and both public and private sectors to develop strategies for safeguarding the country and its citizens, which include establishment of fintech department in the central bank where players were invited to participate in a sandbox project.

4.2 Mitigation measures by the VASPs

VASPs in Zimbabwe have not yet implemented AML/CFT obligations in line with international standards. There is no comprehensive regulatory framework requiring VASPs to conduct CDD, transaction monitoring, or suspicious transaction reporting (STR) among others. As a result, these platforms are unregulated.

However, some VASPs who were in the sandbox do conduct CDD, but primarily for business and operational purposes rather than for AML/CFT compliance.

4.3 Mitigation measures by Financial Institutions

Some financial institutions have implemented automated detection systems to identify abnormal customer behaviour indicative of cryptocurrency trading. Policies have been updated to incorporate cryptocurrency management, and staff have undergone training, awareness campaigns, and certifications.

Additionally, governance structures have been established to address the emerging risks associated with cryptocurrency. Furthermore, financial institutions are now evaluating the risks associated with the use of new technology and products in their institutional risk assessments.

CHAPTER FIVE

5. RECOMMENDATIONS AND CONCLUSION

5.1 Recommendations

Based on the assessment a number of recommendations were made. Implementation of the recommendations below can result in effective management of the ML/TF/PF risks associated with virtual assets while fostering innovation and protecting consumers.

5.1.1 Regulatory Framework and Oversight

a) Develop a legal framework for VAs and VASPs encompassing licensing, supervision, and monitoring.
b) The regulatory framework to cover issues of consumer protection, data protection, market discipline and taxation.
c) Alternatively, establish a controlled environment(sandbox) for VASPs to operate under regulatory supervision while a comprehensive legal framework is being developed. This approach fosters innovation while mitigating risks.

5.1.2 Capacity Building and Awareness

a) Conduct capacity building programs for law enforcement agencies, financial institutions, judiciary and other relevant stakeholders to enhance their understanding of VAs.
b) Launch public awareness campaigns to inform the public about the risks associated with virtual asset trading.

5.1.3 Implementation of AML/CFT requirements

After the legal framework has been put in place, require VASPs to implement robust AML/CFT frameworks tailored to mitigate the specific risks associated with virtual asset activities.

5.2 Conclusion

The assessment provides insights into the emerging VAs and VASPs sector in Zimbabwe, highlighting both opportunities and challenges. It is important to have a regulatory and supervisory framework for this sector. Infrastructure improvements, and increased public awareness, to better combat ML/TF risks associated with VAs and VASPs is of paramount importance.