REPUBLIC OF KENYA

VIRTUAL ASSETS (VAs) AND VIRTUAL ASSET SERVICE PROVIDERS (VASPs) MONEY LAUNDERING AND TERRORISM FINANCING RISK ASSESSMENT REPORT

September 2023

PRINTED BY THE GOVERNMENT PRINTER, NAIROBI

Virtual Assets (VA) and Virtual Assets Service Providers (VASPs) Money Laundering (ML) and Terrorism Financing (TF) National Risk Assessment Report

September, 2023

Disclaimer

The Virtual Assets (VAs) and Virtual Asset Service Providers (VASPs) Money Laundering (ML) and Terrorism Financing (TF) Risk Assessment Report of the Republic of Kenya for 2023 has been conducted as a self-assessment by the Kenyan authorities, using the Virtual Assets and Virtual Asset Service Providers National Risk Assessment Tool developed and provided by the World Bank Group. Data, statistics, and information used for completing the VA/VASP ML/TF risk assessment and the ensuing analysis, results, interpretation, judgment, and outcomes wholly belong to the Kenyan authorities and do not reflect the views of the World Bank Group.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

GLOSSARY

Custodial Wallet	A custodial wallet is an online virtual asset wallet that stores VAs on behalf of a VA owner and does not provide full control of VAs.
Fiat-To-Virtual	The conversion of government issued fiat currency to VAs
Non-Custodial Wallet	A non-custodial wallet is a virtual asset wallet that stores VAs and enables VA owners to have full control of their VAs. This wallet can be a program or a physical device.
Peer-To-Peer (P2P)	A form of virtual asset exchange that entails the transfer of virtual assets from one user to another.
Stablecoin	A stablecoin is a VA whose value is either backed by fiat currencies e.g., USD, commodities, or a basket of cryptocurrencies.
Virtual Asset (VA)	The Financial Action Task Force (FATF) defines a Virtual Asset as 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 that are already covered elsewhere in the FATF Recommendations.
Virtual Asset Brokers	VASPs that act as an intermediary for persons who want to exchange their fiat money for VAs.
Virtual Asset Exchanges	An online platform that facilitates virtual asset transfers and exchanges. Exchanges may occur between one or more forms of virtual assets, or between virtual assets and fiat currency.
Virtual Asset Investment Providers	The practice of providing an investment vehicle enabling investment in/ purchase of VAs via a managed investment scheme.

Virtual Asset Service Provider (VASP)	FATF defines a VASP as any natural or legal person that conducts the following activities or operations for or 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; IV. Safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and, V. Participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset."
Virtual Asset Wallet	A program or device that stores VAs
Virtual-To-Fiat	Conversion of VAs to fiat currencies
Virtual-To-Virtual	Conversion of one type of VA to another

ACRONYMS

AML	Anti-Money Laundering
BRS	Business Registration Service
CBK	Central Bank of Kenya
CFT	Counter Financing of Terrorism
CMA	Capital Markets Authority
DCI	Directorate of Criminal Investigation
DeFi	Decentralised Finance
DNFBP	Designated Non-Financial Businesses and Professions
ESAAMLG	Eastern and Southern Africa Anti-Money Laundering Group
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
ICO	Initial Coin Offering
LEA	Law Enforcement Agency
ML	Money Laundering
MLA	Mutual Legal Assistance
MOU	Memorandum of Understanding
NFT	Non-Fungible Token
NIS	National Intelligence Service
NRA	National Risk Assessment
P2B	Person to Business
P2P	Peer-to-Peer
STO	Security Token Offering
TF	Terrorist Financing
TOE	Traditional Obliged Entity
TWG	Technical Working Group
VA	Virtual Asset
VASP	Virtual Assets Service Provider

Foreword by the Cabinet Secretary, The National Treasury and Economic Planning

I am pleased to present the report of the inaugural Virtual Assets (VA) and Virtual Assets Service Providers (VASPs) Money Laundering (ML) and Terrorism Financing (TF) National Risk Assessment (NRA) for Kenya.

The objective of the risk assessment process is to aid the country in recognizing potential threats and vulnerabilities arising from the adoption of VAs and to formulate mitigating strategies aimed at safeguarding the integrity of the country's financial system. Without the right measures, VAs and VASPs can be abused for ML and TF.

In the spirit of collaboration and engagement, several stakeholders were engaged in the risk assessment, including financial sector regulators, law enforcement agencies, reporting institutions, relevant associations, virtual assets service providers (VASPs) and members of the public, to enable the widest possible range of information and views.

The risk assessment identified the VAs and VASPs in the Kenyan ecosystem and existing interaction with reporting institutions. It was noted that Kenya has a growing VA/VASP ecosystem supporting investments, transfer of value and remittances among others. The growth is driven by factors such as technology adoption, increasing interest in VAs, and emergence of blockchain start-ups and Fintech.

The global crypto winter experienced in 2022, caused by poor governance and accountability noted in some VASPs, led to loss of customer funds, and eroded public trust in the VA ecosystem. Accordingly, the risk assessment is a timely measure to examine the VA/VASP ecosystem in the country and potential ML/TF and other risks. The results of the risk assessment will guide Government’s response in combating money laundering and terrorism financing risks associated with VAs and VASPs.

I take this opportunity to thank all the stakeholders who participated in this important national exercise. The Government of Kenya is committed to implementing the recommendations of the VA and VASP risk assessment as set out in the resultant Action Plan.

PROF. NJUGUNA S. NDUNGU, C.B.S.
Cabinet Secretary, The National Treasury and Economic Planning.

Message from the National Co-ordinator: Director General, Financial Reporting Centre

The use of Virtual Assets (VAs) and Virtual Asset Service Providers (VASPs) for Money Laundering (ML) and Terrorism Financing (TF) is a concern to Kenya and many jurisdictions. This is primarily attributed to the inherent characteristics of VAs and VASPs, which may facilitate the obfuscation of the sources and destinations of funds.

Kenya, being cognizant of the adoption of VAs and their inherent vulnerabilities, constituted a technical working group comprising representatives from the financial sector regulators, law enforcement agencies, reporting institutions, and VASPs, to conduct the inaugural ML/TF risk assessment on VAs and VASPs. Data was collected from open-source intelligence, as well as survey questionnaires disseminated to the public, reporting institutions, regulators, law enforcement agencies, VASPs, and member organizations.

In conducting the risk assessment process, Kenya adopted the World Bank VA/VASPs 2022 risk assessment tool. The tool outlines the approach that countries should take in theidentification of ML/TF threats and vulnerabilities posed by the VA/VASPs and the mitigation measures in place to address the risks while taking into consideration the residual risk. The methodology outlined in the World Bank tool was used to assess VASP activities covered under both FATF Recommendations and non-FATF recommendations and their interactions with various players in the financial system.

The risk assessment will especially assist the country in identifying the gaps and deficiencies in Kenya's AML/CFT framework for VA&VASP and recommend relevant actions.

I would like to express my gratitude to the Cabinet Secretary, The National Treasury and Planning for the immense support accorded in the exercise, and for allowing the Financial Reporting Centre to coordinate this important national exercise. I would also like to thank the World Bank for availing the NRA tool and methodology that enabled us to undertake the NRA, and also, for their training and guidance on the use of the NRA tool. Finally, I thank the VA and VASP Technical working group (TWG), participating institutions, and personnel from both the public and private sectors for their, time, commitment, dedication, and effort which has enabled us to successfully complete this exercise.

Saitoti Maika, M.B.S.
Director General, Financial Reporting Centre

EXECUTIVE SUMMARY

The inaugural Kenya National Risk assessment on Money Laundering and Terrorism Finance (ML/TF) risks of Virtual Assets (VAs) and Virtual Asset Service Providers (VASPs) was conducted in 2023. The risk assessment is based on the Financial Action Task Force (FATF) Recommendation 15 which mandates jurisdictions, including their financial institutions to assess the ML/TF risks that may arise in relation to development of new products, business practices as well as technologies. The risk assessment process aimed to assist the country to identify threats and vulnerabilities that could pose risks as a result of emerging technologies such as VAs and other financial innovations in a bid to develop mitigating strategies and safeguard the country's financial system.

In conducting the risk assessment process, Kenya adopted the World Bank VA/VASPs' 2022 risk assessment tool, which outlines the approach that countries should take in the identification of ML/TF threats and vulnerabilities posed by the VA/VASPs ecosystem and the ability of the identified mitigation measures to address the risks in order to determine the country's residual risks. The methodology outlined in the World Bank tool was used to assess VASP activities covered under both FATF Recommendations and non-FATF recommendations and their interactions with various players in the financial system.

The assessment was caried out by a Technical Working Group (TWG) led by the Financial Reporting Centre (FRC) and comprising the public sector (including the Central Bank of Kenya, Capital Markets Authority, and law enforcement agencies), private sector (financial sector reporting entities) and VASPs. Data was collected from open-source intelligence, as well as survey questionnaires disseminated to the public, reporting institutions, regulators, law enforcement agencies, VASPs, and member organizations.

The risk assessment noted that Kenya does not have a legal and regulatory framework for the registration, licensing or supervision of VA-related activities and VASPs. However, circulars were issued by financial sector regulators from 2015, cautioning the public and prohibiting the regulated financial sector from dealing with VAs.

The TWG established that four major types of VASPs and eleven VASPs channels were operating in the Kenyan ecosystem. The types of VASPs identified were Virtual Asset Wallet Providers, Virtual Asset Exchanges, Virtual Asset Broking/Payment Processing, and Virtual Asset Investment Providers.

The risk assessment highlighted the use of VAs and VASPs in the country. Some of the VAs/VASPs identified as used by the country had anonymity-enhanced features. The complex traceability of VAs, speed of transactions and a notable susceptibility to tax evasion, among others, increased the risk for VAs being used for ML/TF. Additionally, the products offered by VASPs significantly determined the overall risk rating for ML and TF.

While a few cases of VA/VASP-related ML had been reported in the country, no cases related to TF had been reported by the time of risk assessment. However, some of the VAs and VASPs in use by Kenyans had been exploited for ML and TF in other jurisdictions.

The risk assessment findings highlighted that the use of VAs and VASPs was more prevalent among the younger population of ages of 18-40 years, with 75 percent of VA users from the public survey respondents falling in this age bracket. It was noted that students were major active participants of the VA/VASP ecosystem in Kenya. Majority of the survey respondents indicated that they used VAs for investment and speculation purposes. Most VA customers used peer-to-peer (P2P) mechanism to facilitate exchange from fiat to virtual and vice versa.

It was noted that at the point of company registration, some companies operating as VASPs failed to disclose their true nature of business to the Business Registration Service (BRS), and instead indicated they were consultancy firms or fintechs, among others. Accordingly, reporting institutions carried a residual risk related to VAs/VASPs due to presence of P2P mechanism for VA-related transactions, as well as on-boarding of VA/VASP-related customers who did not disclose the true nature of their businesses.

In view of the foregoing, the overall VA/VASPs ML risk for Kenya was rated as **Medium** while the TF risk was rated as **Low.**

Given the ML/TF risks identified, as well as consumer protection, data privacy, governance, and other concerns, it is recommended that the country regulates VAs/VASPs to mitigate the identified risks. It should be noted that banning VAs/VASPs would encourage an underground economy stemming from current usage of VAs/VASPs in the country. Accordingly, regulation of VAs/VASPs would pave the way for mitigation of the identified risks.

1. Background

1.1 Introduction

Virtual Assets (VAs) have attracted a growing interest in Kenya and globally due to their availability, speed, low costs, and anonymity/pseudonymity. The adoption of VAs and related services offer exciting opportunities for innovation and financial inclusion. However, VAs present inherent vulnerabilities which may be exploited for Money Laundering (ML) and Terrorist Financing (TF). These vulnerabilities include the ability to transact rapidly, pseudonymously/anonymously (using VAs with enhanced anonymity) and across borders. Such inherent vulnerabilities allow criminals to acquire, transact and store VAs outside the regulated financial system, thereby making it difficult for Law Enforcement Agencies (LEAs) to detect, investigate, trace, seize, and secure VAs related to criminal activities.

The Financial Action Task Force (FATF), an inter-governmental body which sets international standards for Anti-Money Laundering, Combating the Financing of Terrorism, and Counter-Proliferation Financing (AML/CFT/CPF) defines a Virtual Asset as *"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 that are already covered elsewhere in the FATF Recommendations."*[1][2]

Further, FATF defines Virtual Asset Service Providers (VASPs) as *"any natural or legal person who is not covered elsewhere under the Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person—*

(1) Exchange between virtual assets and fiat currencies;
(2) Exchange between one or more forms of virtual assets;
(3) Transfer of virtual assets;
(4) Safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and
(5) Participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset."

[1] FATF Glossary: https://www.fatf-gafi.org/en/pages/fatf-glossary.html#accordion-a13085a728-item-dd6de709ef
[2] The FATF Recommendations set out a comprehensive and consistent framework of measures which countries should implement in order to combat money laundering (ML), terrorist financing (TF), and the financing of proliferation of weapons of mass destruction (PF).

Recommendation 1 of the International Standards on Combating Money Laundering, Financing of Terrorism and Proliferation Financing requires Countries to identify, assess, and understand the ML/TF risks of the country, and take action, including designating an authority or mechanism to coordinate actions to assess risks, and apply resources, aimed at ensuring the risks are mitigated effectively. Based on that assessment, countries should apply a risk-based approach to ensure that measures to prevent or mitigate ML/TF are commensurate with the risks identified.

In October 2018, FATF adopted changes to its Recommendations to extend their application to VAs and VASPs. Recommendation 15 was updated to require countries and financial institutions to identify and assess the ML/TF financing risks that may arise in relation to:

(i) The development of new products and new business practices, including new delivery mechanisms; and,

(ii) The use of new or developing technologies for both new and pre-existing products.

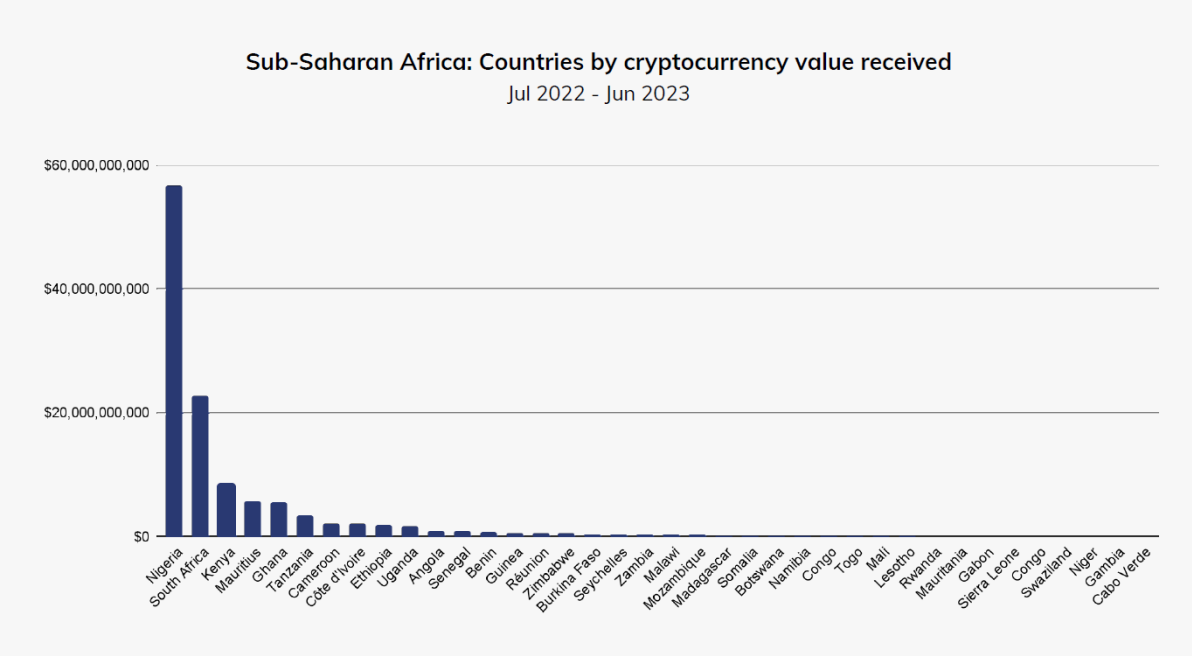
To manage and mitigate the risks emerging from VAs, Recommendation 15 additionally requires countries to ensure that VASPs are regulated for AML/CFT purposes, licensed or registered, subject to effective systems for monitoring or supervision, and ensuring compliance with the relevant measures called for in the FATF Recommendations.[3]

Based on open-source intelligence as well as information received from survey questionnaires issued to collect data for the risk assessment, Kenya has a growing VA/VASP ecosystem being used for various purposes including investment, remittances, cross-border payments and online transactions. The growth is driven by factors such as mobile money adoption, increasing interest in VAs, and emergence of blockchain start-ups and fintechs. The adoption of cryptocurrency in Kenya has been on a gradual rise over the past five years. The Chainalysis 2023 Geography of Cryptocurrency Report places Kenya as 3rd in Africa and 21st globally in crypto adoption, and 3rd globally in peer-to-peer (P2P) exchange.[4] Below is an illustration of the value of crypto assets received by Sub-Sahara African countries between July 2022 and June 2023.

[3] FATF (2012-2023), *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation,* FATF, Paris, France, www.fatf-gafi.org/recommendations.html

[4] The Chainalysis 2023 Geography of Cryptocurrency Report, October 2023: https://www.chainalysis.com/blog/2023-global-crypto-adoption-index/

Figure 1: Sub-Saharan Africa: Countries by Crypto Value Received



Source: Chainalysis

It is worth noting that VASPs with operations in Kenya could be licensed in different jurisdictions and may not have physical presence in the country due to the borderless nature of VA trading and accessibility of their platforms over the internet.

Kenya does not have a legal framework or a designated authority/agency to regulate and supervise VAs and VASPs on AML/CFT matters and other aspects. Therefore, use of VAs is neither expressly regulated nor prohibited in Kenya. Like many jurisdictions, Kenya is faced with ML/TF risks associated with the VAs due to their inherent vulnerabilities. Financial sector regulators have issued cautionary notices to the public[5] and Traditionally Obliged Entities (TOEs)/reporting institutions[6] on the risks associated with VAs. Accordingly, it is important to safeguard Kenya's economy by identifying and mitigating risks associated with VAs and VASPs and to take cognizance of any residual risks thereafter.

Kenya's AML/CFT Mutual Evaluation Report (MER), 2022, by the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG)[7] recommended that Kenya takes a policy decision regarding VASPs providing crypto and other virtual/digital assets services.

[5] https://www.centralbank.go.ke/images/docs/media/Public_Notice_on_virtual_currencies_such_as_Bitcoin.pdf

[6] https://www.centralbank.go.ke/uploads/banking_circulars/2075994161_Banking%20Circular%20No%2014%20of%202015%20-%20Virtual%20Currencies%20-%20Bitcoin.pdf

[7] https://frc.go.ke/downloads/send/6-for-your-information/156-mutual-evaluation-report-mer-for-kenya-september-2022.html

Accordingly, Kenya was expected to conduct the ML/TF risk assessment on VAs and VASPs to inform policy.

This report, therefore, sets forth Kenya's ML/TF risk assessment for VAs and VASPs. The risk assessment was conducted as per the World Bank's VA and VASP ML/TF Risk Assessment Tool (VA-RA)[8] which aims to assist countries in assessing the ML/TF risks of VA activities and the service providers in the financial and non-financial sectors involved in these activities. Further, the risk assessment considered FATF guidance on VAs and VASPs. The risk assessment was based on information provided by the Kenyan public, the financial sector regulators, TOEs/reporting institutions, Virtual Asset Service Providers, LEAs, open-source intelligence, and other key stakeholders.

1.2 Objectives of the VAs/VASPs ML/TF Risk Assessment

The key objective of undertaking the ML/TF risk assessment on VAs and VASPs is to identify, assess, and understand the ML/TF risks in order to inform policy pertaining to the AML/CFT regime. The main objectives for Kenya include the following:

(i) Identifying, understanding, and assessing the overall ML/TF risks related to VAs and VASPs ecosystems;

(ii) Identifying VA/VASP products/services/channels with high vulnerabilities;

(iii) Applying a risk-based approach to VAs/VASPs and proposing effective mitigation measures for the identified risks;

(iv) Developing action plans to strengthen AML/CFT controls in the VA/VASP ecosystem; and,

(v) Using the risk assessment as an opportunity to build capacity and raise awareness of competent authorities about the risks related to VAs and VASPs and strengthening interagency cooperation among them.

Understanding the potential ML/TF risks posed by VAs and VASPs is essential for gaining insights into the context in which VA/VASP-related predicate offenses (underlying criminal activities) occur and how the proceeds of VA/VASP-related crime are created, transferred, utilized, or reintegrated into the financial system. The inherent vulnerabilities of VAs may be manipulated by ML/TF threats, giving rise to risks that could adversely impact both society and the economy unless appropriate mitigation measures are put in place.

[8] https://thedocs.worldbank.org/en/doc/3ea7ffa49269eeee60ed6fb1a87507bb-0430012022/related/VA-Risk-Assessment-Tool-1.zip

2. Risk Assessment Methodology

2.1 Technical Working Group

Kenya set up a Technical Working Group (TWG) comprising representatives drawn from public and private sector organizations to conduct the National VAs/VASPs ML/TF Risk Assessment (NRA). The TWG comprised financial sector regulators, LEAs, VASPs, and TOEs. The TWG's membership was drawn from:

(i) Financial Reporting Centre (FRC) which is Kenya's Financial Intelligence Unit (FIU) as the national coordinator;

(ii) Financial sector regulators: Central Bank of Kenya (CBK) and Capital Market Authority (CMA).

(iii) Law Enforcement Agencies (LEAs);

(iv) Private sector reporting entities; and

(v) VASPs.

2.2 Scope of Risk Assessment

The scope of assessment was defined by, but not limited to, the World Bank VA and VASP risk assessment guidance tool and the FATF's updated guidance for a risk-based approach on VA and VASP, FATF (2021), Paris.[9]

To better understand the Kenyan VA and VASP ecosystem, the TWG undertook the following:

(a) Identified the VAs and VASPs accessed by Kenyans and how they interact with TOEs;

(b) Identified the potential VA/VASP vulnerabilities that could be exploited for ML/TF;

(c) Identified the potential VA/VASP threats and their impact on ML/TF;

(d) Assigned a risk level to each identified vulnerability and threat based on the World Bank tool;

(e) Identified existing controls in place to mitigate each identified risk with the aim of assessing their effectiveness; and

(f) Developed an action plan to mitigate the ML/TF risks identified.

2.2.1 The World Bank VA/VASP ML/TF Risk Assessment Tool

The World Bank VA/VASP ML/TF risk assessment tool considers seven (7) types of VASPs, twelve (12) services of VASPs, and twenty-seven (27) activities/channels with distinct assessment criteria for each product/service/activity. The TWG assessed potential interaction between the twenty-seven (27) activities and TOEs.

[9] https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html

Table 1: Types of VASPs and their Services

Type of VASP	Type of Services	Channel
Virtual Asset Wallet Providers	Custodial Services	Hot Wallet
	Non-Custodial Services	Cold Wallet
Virtual Asset Exchanges	Transfer Services	P2P
		P2B
	Conversion Services	Fiat-to-Virtual
		Virtual-to-Fiat
		Virtual-to-Virtual
Virtual Asset Broking / Payment Processing	Payment Gateway	ATMs
		Merchants
		Cards
Virtual Asset Management Providers	Fund Raising	Fund Management
		Fund Distribution
		Compliance, Audit and Risk Management
		Fiat-to-Virtual
		Virtual-to-Virtual
	Investment	Development of Product and Services
	Other Offerings	Security Token Offerings (STOs)
		Initial Exchange Offerings (IEOs)
Virtual Asset Investment Providers	Trading Platforms	Platform Operators
		Custody of Assets
		Investment into VA-related commercial activities
		Non-Security Tokens and Hybrid Trading Activities
		Stablecoins
	Emerging Products	Crypto Escrow service
		Crypto-custodian Services
Validators / Miners/ Administrators	Proof of Work	Fees
		New Assets

Source: World Bank

The VASPs as defined by FATF are as follows—

(a) **Virtual Asset Exchanges:** An entity engaged in the business of VA exchange for fiat currency, funds, or other forms of VA for a commission. The exchangers accept a wide range of payments, such as cash, wire transfers, credit cards, and other VAs. Individuals typically use exchangers to deposit and withdraw money from VA accounts.

(b) **Virtual Asset Wallet Providers:** Virtual Asset Wallet Providers, provide storage for VAs or fiat currency on behalf of others. It then facilitates exchanges or transfers between VAs and fiat currency. They include Custodian, hot wallet and the non-custodian, cold wallet.

(c) **Virtual Asset Broking:** Arranging transactions involving VAs or involving VAs and fiat currency. VA Broking involve ATMs (Automated Teller Machines), Merchants and Cards. An ATM dealing with VAs is a kiosk that allows a person to purchase VAs by using cash or debit card.

(d) **Initial Coin Offering (ICO) Providers:** Involve issuing and selling VAs to the public and may also involve participating in and providing financial services relating to the ICO. Further provide for services such as Security Token Offerings (STOs) offering equity in the form of tokens.

(e) **Virtual Asset Investment Providers:** They provide an investment vehicle that enables investment in or purchase of VAs (that is, via a managed investment scheme or a derivatives issuer providing VA options, or via a private equity vehicle that invests in VAs).

(f) **Virtual Asset Management Providers:** They focus on VAs as the underlying assets, typically involving fund management, fund distribution, audit, and risk management.

It is essential to constantly monitor such activities as they could evolve to that of a VASP and be subjected to AML/CFT regulations. Accordingly, the following VA/VASP activities that fall outside the FATF definition were also considered in this exercise.

(g) **Validators/Miners/Administrators (non-FATF):** An entity that receives VA rewards for being the first to validate transactions in a decentralized VA ledger. Miners use very high computing power in a distributed proof system to run complex algorithms which solve the highly challenging mathematical equations required to validate transactions. Mining could be undertaken by miners individually (solo mining) or as part of a pool (pooled mining) was traced among PI-network in Kenya.

While undertaking the assessment, the TWG considered the following factors—

(a) The VAs in the Kenyan ecosystem;

(b) VASPs with possible operations in Kenya and their specific risk factors which included the characteristics and nature of the VAs they deal with;

(c) VASPs operating in ML/TF high risk and other monitored jurisdictions[10] which are accessible to Kenyans;

(d) Interaction of VASPs with TOEs/reporting institutions, and Designated Non-Financial Businesses or Professions (DNFBPs);

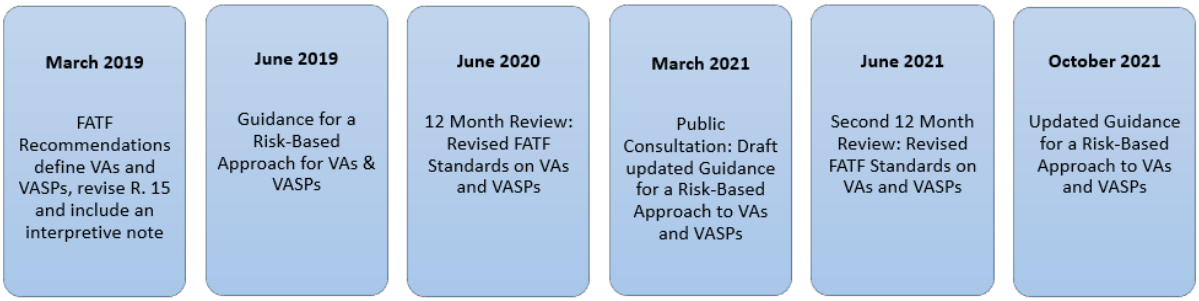
(e) Different types of tokens including non-transferable, non-exchangeable, and non-fungible tokens (NFTs), and how they might be used to aid fraud, ML/TF, or proliferation of crimes; and,

(f) The existence and adequacy of AML/CFT legislation and whether current provisions are sufficiently robust to mitigate ML/TF risks.

2.2.2 FATF Guidance and Recommendations on VAs and VASPs

In conducting the risk assessment on VAs/VASPs, the TWG considered FATF guidance and the Recommendations relating to VAs and VASPs. In 2019, FATF extended its AML/CFT standards to VAs and VASPs to prevent criminal and terrorist misuse of the sector. In October 2021, it updated its 2019 guidance for a risk-based approach to VAs and VASPs. The guidance helps jurisdictions to effectively implement FATF's requirements. The publications that were considered are shown below.

Figure 2: FATF Key Publications on VAs and VASPs



2.3 Data Collection and Analysis

The focus of the TWG was to ensure it gathered quantitative and qualitative data from multiple sources to attain an informed assessment of Kenya's VAs and VASPs ecosystem and its threats and vulnerabilities to the financial system. In addition to depending on both qualitative and quantitative data, several discussions were held to analyse and interpret the findings from the data to validate its accuracy before using the same for discussion in filling the World Bank risk assessment tool.

[10] https://www.fatf-gafi.org/en/topics/high-risk-and-other-monitored-jurisdictions.html

The TWG prepared data collection tools, specifically survey questionnaires. The questionnaires were disseminated to respondents including TOEs/reporting institutions, VASPs, LEAs, regulators, member associations and members of the public.

The questionnaires covered issues relating to inter-alia, governance, internal controls, operations, knowledge of staff, training across the threat, vulnerability, and mitigating measures dimensions.

The TWG received a total of **341** responses to the survey questionnaires as highlighted below.

Table 2: VA/VASP Questionnaire Survey Respondents

Category	**Number of Respondents**
Traditional Obligated Entities (TOEs)/reporting institutions	150
Regulators	4
VASPs	5
Law Enforcement Agencies	7
Member organizations/associations	5
Members of the public	170
Total	**341**

3. The VAs and VASPS Ecosystem in Kenya

The TWG noted interaction between TOEs and four (4) types of VASPs, six (6) services of VASPs, and eleven (11) activities/channels, as highlighted below.

Table 3: VASPs, Services and Channels identified in Kenya

VASP/SERVICE/CHANNEL		
VASP	**Type of Services**	**Channel**
Virtual Asset Wallet Providers	Custodial Services	Hot Wallet
	Non-custodial Services	Cold Wallet
Virtual Asset Exchanges	Transfer Services	P2P
		P2B
	Conversion Services	Fiat to Virtual
		Virtual to Fiat
		Virtual to Virtual
Virtual Asset Broking/Payment Processing	Payment Gateway	Merchants
Virtual Asset Investment Providers	Trading Platforms	Platform Operators
		Non-Security Tokens & Hybrid Trading Activities
		Stable Coins

While a 20% of the respondents indicated that they offered the services of a VA management provider, there was no evidence , and it was not clear whether this was happening in Kenya or other jurisdictions in which they operate. Accordingly, this category was not assessed in the risk assessment.

3.1 VA and VASP Regulatory Developments in Kenya

Kenya has an overarching AML/CFT legislative framework that addresses broad ML/TF risks. However, Kenya does not have a legal framework that governs/licenses VAs/VASPs' activities. Therefore, the VASPs that are operating in the country are not regulated for AML/CFT purposes. Below are key regulatory developments on VAs/VASPs in the country.

(a) CBK issued a public notice in December 2015, cautioning the public on cryptos such as bitcoin.[11] The caution primarily stemmed from the decentralized nature of crypto assets and their inherent risks. Further, it informed the public that virtual currencies were not legal tender in Kenya and therefore no protection existed in the event that the virtual currency platforms failed.

(b) A Banking Circular was also issued to all banks in 2015, by CBK cautioning them against dealing in virtual currencies or transacting with entities that are engaged in virtual currencies.[12]

(c) In 2018, CBK and other financial sector regulators (CMA, Sacco Societies Regulatory Authority (SASRA), Retirement Benefits Authority (RBA), Insurance Regulatory Authority (IRA) and Ministry of Trade and Cooperatives) issued notices to the public on fraudulent financial services, products and applications warning them against dealing with unlicensed and unregulated financial products and services.[13] The public was guided to verify the list of regulated financial institutions from the regulatory body websites.

(d) In August 2020, due to the re-emergence of fraudulent financial schemes in the wake of the COVID-19 pandemic, CBK and other financial sector regulators reiterated their warning against the use of unlicensed financial products and services.[14]

(e) In September 2020, CBK also issued circulars to banks and Payment Service Providers (PSPs) warning them against dealing with unlicensed entities. The circulars cautioned the institutions against the use, partnering and facilitation of services from unregulated and unlicensed entities, reminding them of the Public Notice of August 2020.

[11] https://www.centralbank.go.ke/uploads/banking_circulars/2075994161_Banking%20Circular%20No%2014%20of%202015%20-%20Virtual%20Currencies%20-%20Bitcoin.pdf

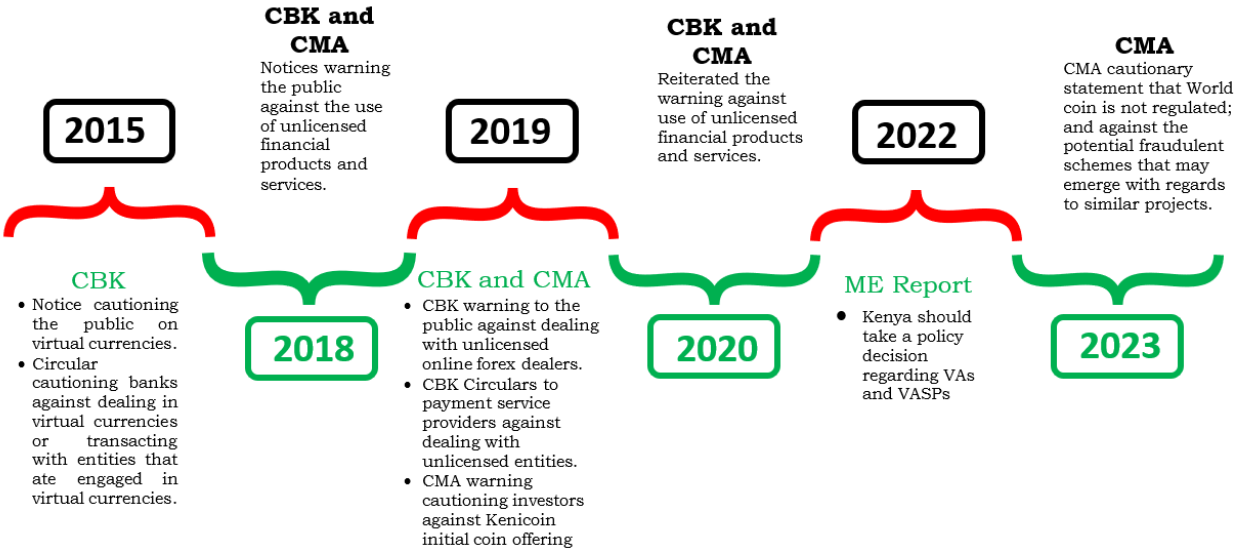
[12] https://www.centralbank.go.ke/uploads/banking_circulars/2075994161_Banking%20Circular%20No%2014%20of%202015%20-%20Virtual%20Currencies%20-%20Bitcoin.pdf

[13] https://www.centralbank.go.ke/uploads/press_releases/130503108_Public%20Notice%20-%20Fraudulent%20Financial%20Services%20Products%20and%20Applications.pdf

[14] https://www.centralbank.go.ke/uploads/press_releases/1843446732_Joint%20Press%20Release%20-%20Public%20Notice%20on%20Fraudulent%20and%20Unlicensed%20Financial%20Schemes.pdf

Below is a summary of the public notices and cautionary statements/circulars issued by financial sector regulators to create awareness and caution the citizens on risks associated VAs/VASPs.

Figure 3: VA/VASP-related Public Notices, Cautionary Statements and Circulars Issued by Financial Sector Regulators



Despite the various cautionary statements, there are reports that indicate that Kenyans continued to adopt VAs.[15] This was confirmed through feedback received from the NRA survey questionnaires. While the public cautionary notices and circulars to financial institutions limited access to financial services for crypto-related businesses or transactions, the effect was an increase of peer-to-peer VA transactions.

(a) In December 2022, the Joint Financial Sector Regulators (JFSR) Forum, a joint body of all financial sector regulators in Kenya, resolved to develop recommendations on the establishment of a comprehensive oversight framework on crypto assets activities and players in Kenya.[16]

(b) In 2023, the National Treasury and Economic Planning established a *Technical Working Group on Crypto Assets* to develop an oversight framework for crypto assets activities and players in Kenya with a view to addressing policy and regulatory gaps.

[15] Chainalysis 2023 Geography of Cryptocurrency Report

[16] https://www.centralbank.go.ke/uploads/press_releases/834999694_Communique%20on%20the%2013th%20Joint%20Financial%20Sector%20Regulators%27%20Board%20Meeting.pdf

(c) In March 2023, the *Capital Markets (Amendment) Bill 2023,* was tabled by a private member in Parliament. The proposal sought to amend amongst others, Section 2 of the Capital Markets Act to include definitions on blockchain, crypto currencies and crypto miners. The bill proposed an amendment to the definition of securities under the Act by including digital currencies. The Bill proposed to have a baseline of 10,000 customers and an operation period of two years for VA to be allowed to enter the Kenyan market by CMA. Moreover, the proposal provided that for a person to be granted a license to trade in digital currencies they must first register with CMA, keep a record of all transactions, and pay tax on any gains made on transactions carried out on the trading platform.

(d) In June 2023, CBK issued a *Technical Paper on Crypto Assets* as an annex to the report on *Discussion Paper on Central Bank Digital Currency: Comments from the Public*.[17] The technical paper summarized recent key developments on crypto assets. This was informed recent instability in the global crypto assets market, which amplified concerns and the need for a careful review of the innovation and technology risks.

(e) With regard to taxation, the Finance Act, 2023, introduced a 3 percent Digital Asset Tax payable by a person on income derived from the transfer or exchange of digital assets. The Act defines a digital asset (crypto assets and NFTs) as:

"digital asset" includes—

(i) anything of value that is not tangible and cryptocurrencies, 2023 Finance 85 No. 4 token code, number held in digital form and generated through cryptographic means or otherwise, by whatever name called, providing a digital representation of value exchanged with or without consideration that can be transferred, stored or exchanged electronically; and

(ii) (ii) a non-fungible token or any other token of similar nature, by whatever name called; and (b) "income derived from transfer or exchange of a digital asset" means the gross fair market value consideration received or receivable at the point of exchange or transfer of a digital asset[18].

(f) In July 2023, data privacy concerns were raised in Kenya when Worldcoin, an entity operating as a VASP, offered the Worldcoin token (a virtual asset) to Kenyans as an incentive in exchange for their biometric data. Consequently, in September 2023, the

[17] https://www.centralbank.go.ke/wp-content/uploads/2023/06/Discussion-Paper-on-Central-Bank-Digital-Currency-Comments-from-the-Public.pdf

[18] THE FINANCE ACT, 2023 No. 4 of 2023 Date of Assent: 26th June 2023

National Assembly *ad-hoc Committee on the Inquiry into the Activities of Worldcoin in Kenya* recommended, *inter alia*, for the development of a comprehensive oversight framework and policies on VAs/VASPs.

(g) Kenya's *Anti-Money Laundering and Terrorism Financing Mutual Evaluation Report* 2022 rated the country non-compliant with FATF Recommendation 15 on the general and comprehensive requirements of regulation and risk assessment of VAs and VASPs. The main reason for the rating was a lack of legal and enforceable regulation and policies to regulate the VA sector. *The Mutual Evaluation recommended that Kenya should take a policy decision as to whether to prohibit or allow VASPs in Kenya.* Where a position is taken to allow VASPs, licensing/registration requirements should be implemented, and a risk assessment relative to ML/TF risks with regards to their operations should be conducted. Additionally, the MER recommended that a framework for supervision of VASPs for AML/CFT should be set up.[19]

3.2 VA/VASP Regulatory Frameworks of Other Jurisdictions

Given the borderless nature of VAs/VASPs accessible to Kenyans, the risk assessment examined VA/VASP regulatory frameworks of select jurisdictions.

The regulatory approaches vary from country to country. The main competent authorities mandated to regulate VAs and VASPs include Central Banks, capital markets/securities regulatory bodies, and independent bodies such as Dubai's Virtual Assets Regulatory Authority (VARA) as summarized below.

Table 4: VA/VASP Regulatory Actions of Different Jurisdictions

No.	Regulation Status	Country
1.	Regulated by Central Banks or market conduct authority	• United Kingdom - Financial Conduct Authority (FCA) • Malta - Malta Financial Services Authority (MFSA) • Egypt – Central Bank of Egypt • Brazil
2.	Regulated by Capital Markets/Securities bodies or equivalent	• South Africa (Financial Conduct Services Authority) • Japan (Financial Services Agency) • Botswana (Non-Bank Financial Institutions Regulatory Authority)

[19] Mutual Evaluation Report of Republic of Kenya September 2022

No.	Regulation Status	Country
		• Seychelles - Seychelles Financial Services Authority (FSA) • Mauritius - Financial Services Commission (FSC)
3.	Independent bodies	• United Arab Emirates - Virtual Assets Regulatory Authority (VARA)
4.	No overall regulatory authority	• Uganda – VASPs are required to register as reporting entities for AML, but no overall regulations. • United States of America (USA) – varies per State: Security Exchange Commission (SEC), Commodities Futures Trading Commission (CFTC), FinCEN, and IRS
5.	Partial Ban/Cautionary Notices	• Kenya • Rwanda • Egypt • Nigeria
6.	Full ban	• China • Morocco

The motivations for the different approaches are primarily country context and the types of VASPs operating in the jurisdictions, among other factors. The jurisdictions who regulate VAs/VASPs aim to harness the benefits of VAs, for instance, promote innovation and financial inclusion, while mitigating the risks of ML/TF, consumer/investor protection, fraud, cyber risk, and other market conduct risks, and maintain financial stability.

The jurisdictions which banned VAs and VASPs cited the high volatility as the main financial stability risk, in addition to multiple consumer protection risks. Overall, where they are banned, the effect is VAs and VASPs will operate underground, leading to poor visibility on potential impact on financial stability, which might present additional regulatory and financial stability risks.

Of note is the United Arab Emirates (UAE), which has an advanced VA/VASP regulatory framework. In 2022, the Dubai Virtual Assets Law established the Dubai Virtual Assets Regulatory Authority (VARA) responsible for regulating, supervising, overseeing the issuance, offering and disclosure processes for VAs and NFTs.

UAE Onshore Companies are governed by Securities and Commodities Authority's (SCA) Decision No. 23 of 2020 concerning Crypto Assets Activities Regulation (CAAR). CAAR also lays down AML/CFT requirements. CAAR provisions require reporting entities to set up a solid AML/CFT compliance framework, define policies and procedures for KYC and AML monitoring, ensure that the deposits and withdrawals are made only from and to a designated bank account of the entity, and the bank account must be maintained with an authorized financial institution. The SCA must have explicitly approved the foreign financial institution. Firms are also required to ensure that the crypto assets are traceable. With regard to usage of VAs, the government owned licensing firm KIKLABB accepts bitcoin (BTC), Ether (ETH), and Tether (USDT) on behalf of Dubai Financial Services Authority to pay for various trade licenses and visas.

A detailed description of the VA/VASP regulatory framework of other jurisdictions is detailed in **Annex I**.

3.3 Regulatory Recommendations of International Standard-Setting Bodies

(a) Financial Action Task Force (FATF)

FATF adopted changes to its Recommendations which clarified that its recommendations apply to financial activities involving VAs and VASPs.[20] the Recommendations require that VAs and VASPs be regulated and supervised for AML/CFT.

(b) Financial Stability Board (FSB)

In July 2023, the Financial Stability Board (FSB) published a global regulatory framework for the international regulation of crypto-asset activities aimed at a comprehensive set of proposals for regulating and supervising crypto-asset activities. This framework comprised two sets of recommendations:

(i) High-level recommendations for the regulation, supervision and oversight of crypto-asset activities and markets.

(ii) Revised high-level recommendations for the regulation, supervision, and oversight of "global stablecoin" arrangements.

The recommendations include:

VAs and markets must be subjected to effective regulation and oversight proportional to their domestic and international risks;

[20] https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html

(i) VASPs must comply with existing legal obligations in the jurisdictions in which they operate;

(ii) Stablecoins should be subjected to robust regulations and supervision of relevant authorities if they are to be adopted as a widely used means of payment; and,

(iii) FSB members support the implementation of existing international standards on VA/VASP activities, notably the (FATF) Recommendation 15 on new technologies and Recommendation 16 on wire transfers (Travel Rule).

(c) International Organization of Securities Commissions (IOSCO)

In 2023, IOSCO published a consultation report on the policy recommendations for crypto and digital asset markets to address market integrity and investor protection issues in crypto-asset markets.[21] The report made 18 principles-based and outcomes-focused policy recommendations aimed at guiding the activities performed by VASPs and addressing key risks identified with VASP activities. Similarly, the report guides IOSCO members on how to ensure regulatory consistency in regulation and oversight of VA/VASP activities, given the cross-border nature of the markets, the risks of regulatory arbitrage, and the significant risk of harm to which retail investors are exposed to.

[21] https://www.iosco.org/library/pubdocs/pdf/IOSCOPD734.pdf

4. Survey Responses

4.1 Public Responses to the VA& VASP Survey

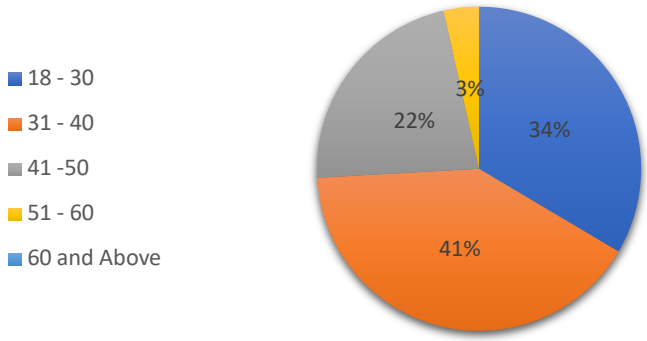
The TWG received one hundred and seventy (170) survey responses from the public with the 75% of the respondents aged between 31 – 40 years (41%) followed by 18 – 30 years (34%), an indicator that VA activities in Kenya are primarily carried out by the younger generation, which is more familiar with technology and the use of internet being an integral part of their lives. They are more comfortable navigating online platforms and understanding digital concepts, including VAs.

Advances in technology have made VAs more accessible and attractive. Blockchain technology, which underlies many VAs like cryptos and NFTs (Non-Fungible Tokens), is a novel and intriguing concept for the younger generation.

Additionally, they are more open to new forms of investment and are willing to take more risks to potentially reap higher rewards or returns. The younger generation might perceive VAs as a way to reduce reliance on traditional financial institutions and government-controlled currencies.

Social media platforms have played a significant role in popularizing VAs. Younger generations frequently use these platforms to discuss and share investment strategies, creating a sense of community and fostering interest in the space.

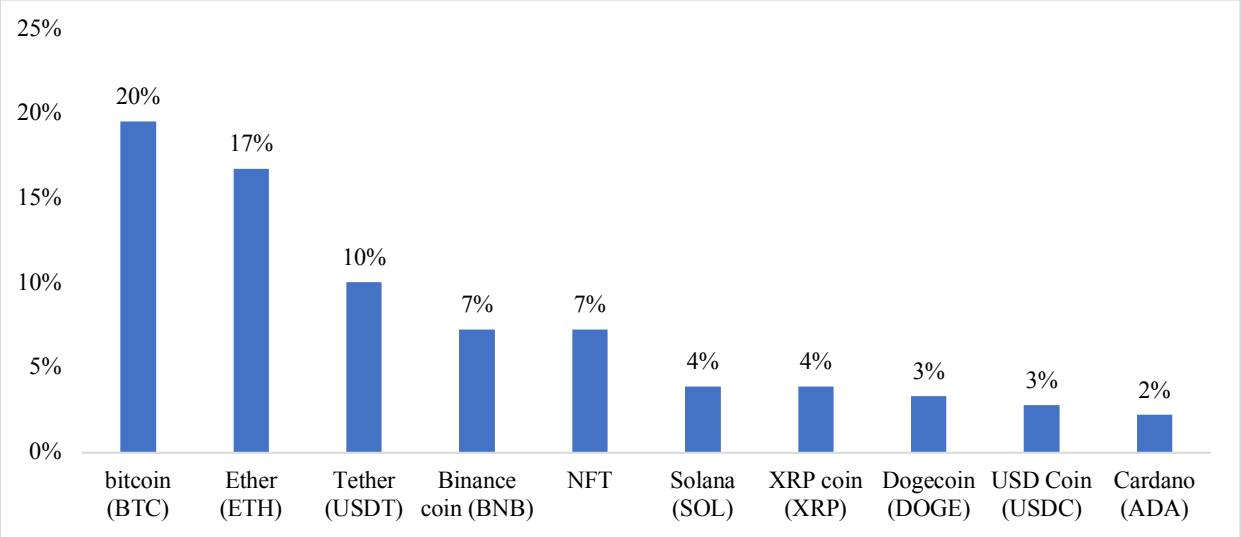
Figure 4: Age Bracket of Survey Respondents



Ownership VAs/VASPs: 86% of the respondents indicated that they are familiar with VAs (e.g., USDT, Bitcoin, Ether etc.) and VASPs (e.g., Binance, Coinbase, Luno). 33% of the respondents indicated that they owned or had ever owned Bitcoin.

The Chart below highlights the top 10 VAs owned by Kenyans.

Figure 5: Top 10 VAs in use in Kenya

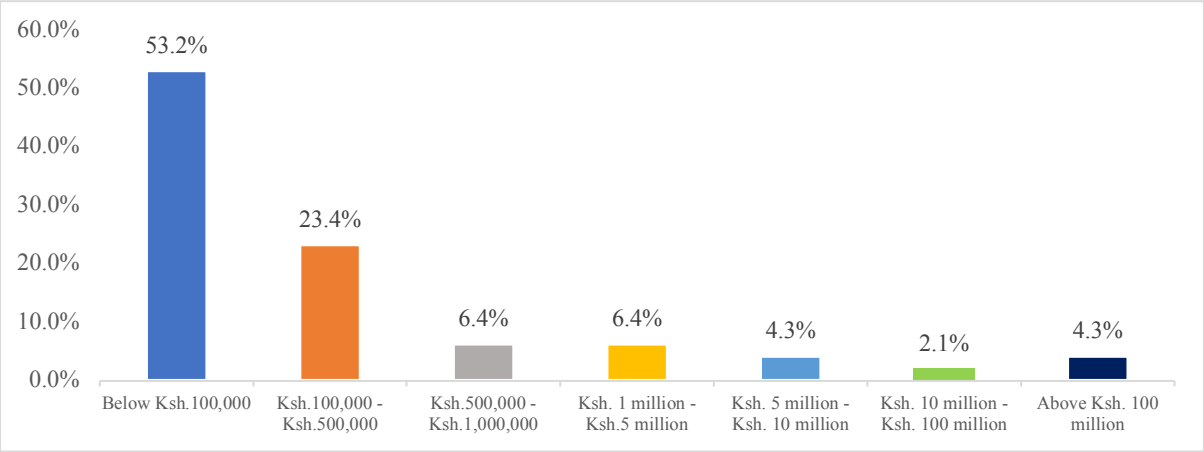


Numerous VASPs were actively used in Kenya, as illustrated in the image below.

Figure 6: VASPs Actively used in Kenya

53% of respondents had invested funds below KSh. 100,000, demonstrating a cautious approach to VAs investments aimed at risk mitigation as shown below.

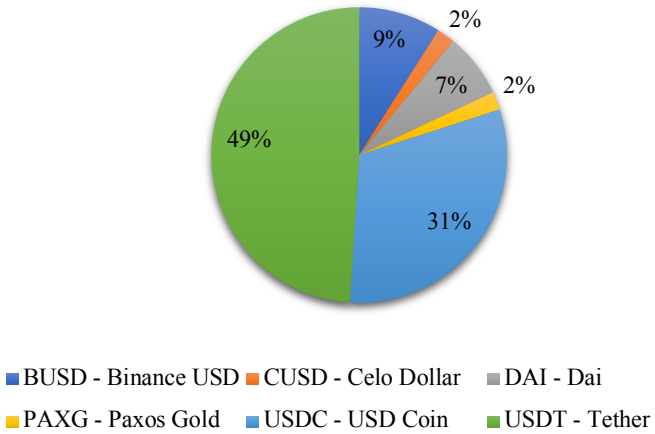
Figure 7: Value of VAs Invested by Respondents



A significant majority of individuals acquire their VAs through peer-to-peer trading, transfer from mobile and online wallets and utilize centralized exchanges to store their VAs, while others opt for self-custody or third-party solutions. Hot wallets are more prevalent than cold wallets in this context. The use of peer-to-peer mechanism was prevalent due to the prohibition of banks and PSPs from dealing with VAs and VASPs.

In their investment portfolio, respondents were observed to engage with various DeFi services, with stablecoins, lending and borrowing, and yield farming ranking as the most prominent choices. The main stablecoins used by Kenyans included USDT, USDC, DAI, BUSD, CUSD and Paxos Gold. Paxos Gold is backed by real gold reserves held by Paxos, DAI (an algorithmic stablecoin) is backed by multiple VAs, and the other stablecoins are backed by the US dollar.

Figure 8: Top Stablecoins used by Kenyans

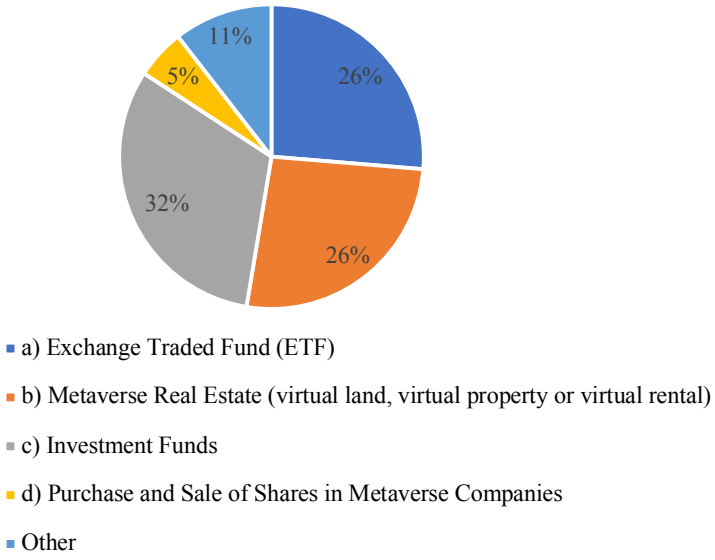


Apart from stablecoins, NFTs also offered an alternative avenue for investments and payments among the survey respondents, with the 27% utilizing NFTs for art or collectible acquisitions.

Some of the mentioned NFTs included BoredApes, Zed-Run horses, Music NFT's, Angry ape and Meme coin Kid called beast.

Further, 26% of the of the survey respondents dealing in VAs confirmed that they had traded or invested in the metaverse a virtual reality space where users can interact with each other and digital assets in a decentralized manner in the areas highlighted by the chart below.

Figure 9: Respondents' Trading or Investment Activities in the Metaverse

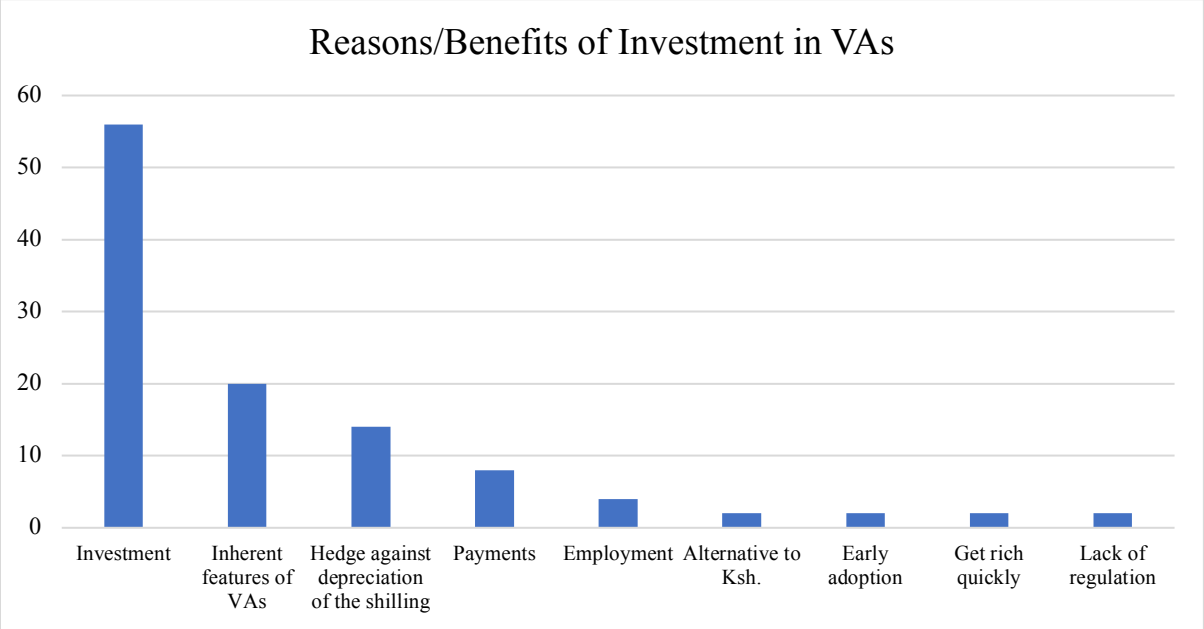


Source of Funding: A major source of funding for the VAs for Kenyans dealing in VA is income and savings with a minority taking loans and receiving gifts or grants.

Drivers for Adoption: A larger percentage of Kenyans had not ventured into VAs because they are not regulated, and the financial regulators had issued cautionary notices coupled with insufficient knowledge. Others viewed VAs as inherently risky and preferred not to commit their money to such ventures, while others found alternative investment opportunities more appealing.

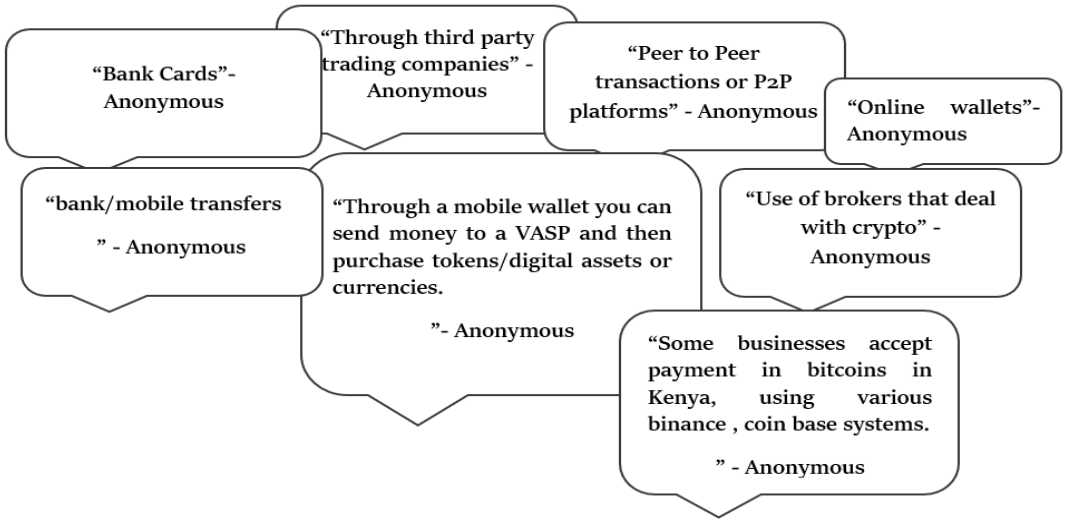
The main driver for VAs adoption was indicated as investment, hedge against currency depreciation, and attraction to the inherent features of VAs (Anonymity, cross border) as shown in the chart below.

Figure 10: Reasons/Benefits of Investment in VAs



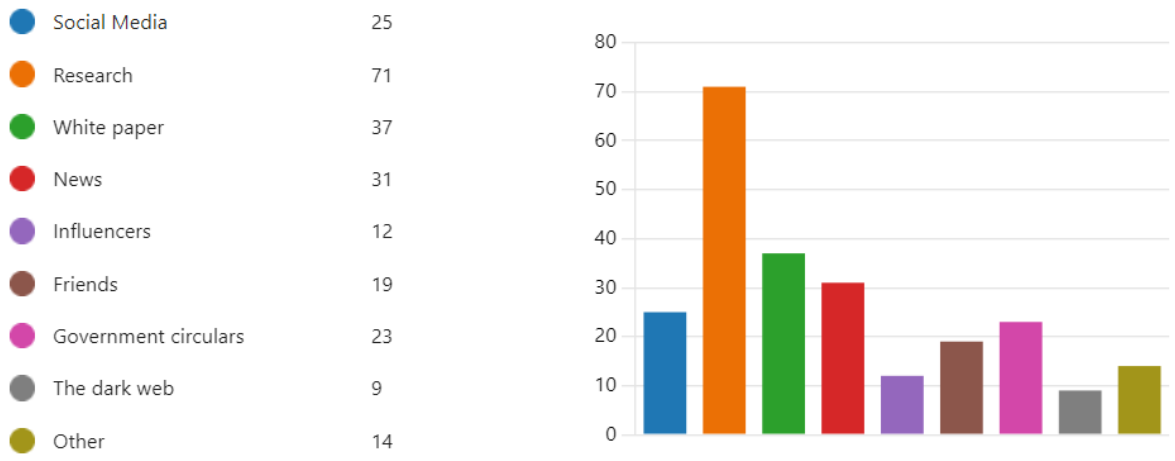
Despite the position taken by most TOEs of not allowing VA transactions due to the cautionary statements issued by financial regulators, respondents indicated that it was possible to convert fiat to VA and VA to fiat through the peer-to-peer mechanism, e-wallet intermediaries, brokers, card schemes.

Figure 11: Respondents' Means of Conversion of VAs to Fiat Currency and Vice Versa



The questionnaire findings also revealed that Kenyan traders in VAs confirm the legitimacy of their VA investments through research, social media, white papers, news outlets, and other sources as illustrated below.

Figure 12: Respondents' Due Diligence on VAs



Out of the 170 respondents, 23 confirmed that they had utilized the dark web to gather information about VAs to facilitate their buying or selling activities. A substantial majority of 110 respondents had not ventured into the dark web, while 30 individuals expressed unfamiliarity with what the dark web is.

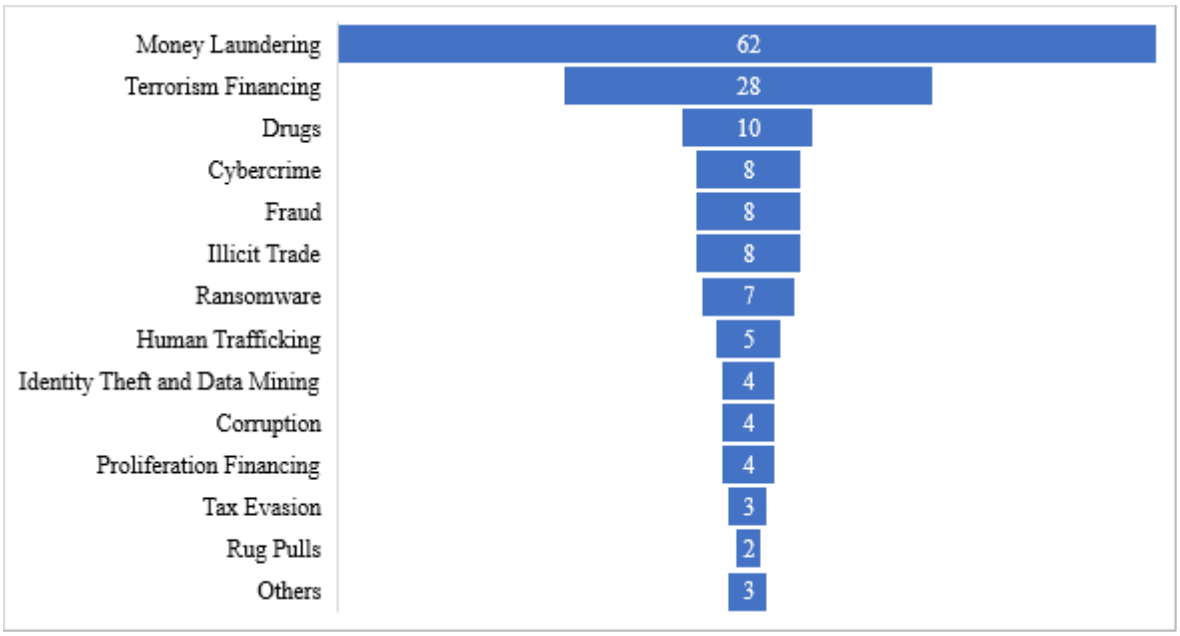
63% of the respondents confirmed that VAs are likely to be used for scams with 38% confirming they know someone who has been scammed through VAs. These scams like the pig-butchering[22], mostly occurs if one does not do their own due diligence before engaging in any VA trade with any companies or individuals. Some of the feedback received from respondents is indicated below.

Figure 13: Respondents' Experiences of VA Scams

[22] A type of VA scam that uses catfishing to gain the victim's trust and then convince them to join a financial investment scheme.

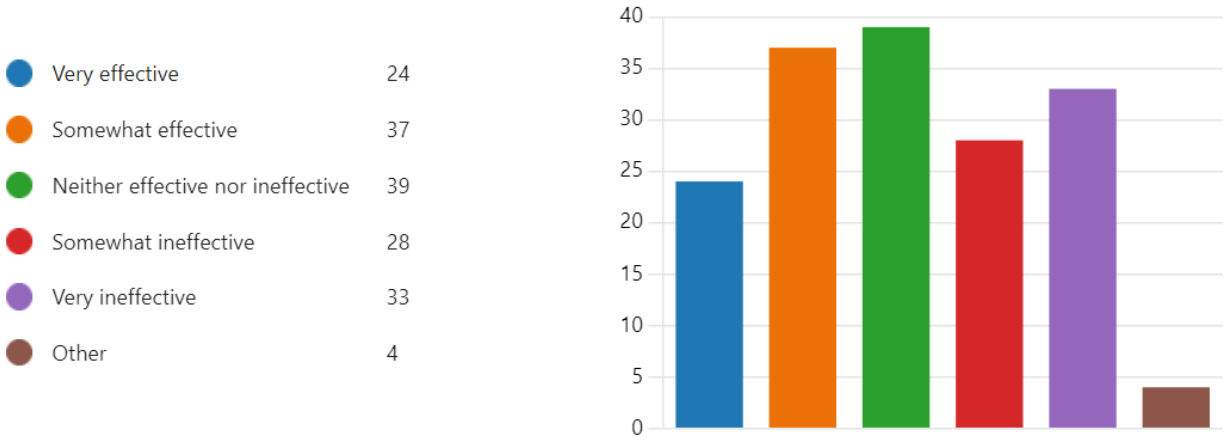
In addition to Ponzi schemes and scams, the respondents affirmed that the use of VAs presented a potential risk for facilitating ML and TF activities among others as shown below.

Figure 14: Criminal Activities Identified by Respondents



With regard to regulation, 24 respondents found the government cautionary notices to be effective, 37 considered them somewhat effective, and 39 believed they were neither effective nor ineffective, as demonstrated below.

Figure 15: Effectiveness of Government Cautionary Notices



4.2 Law Enforcement Agencies' Responses to the VA&VASP Survey

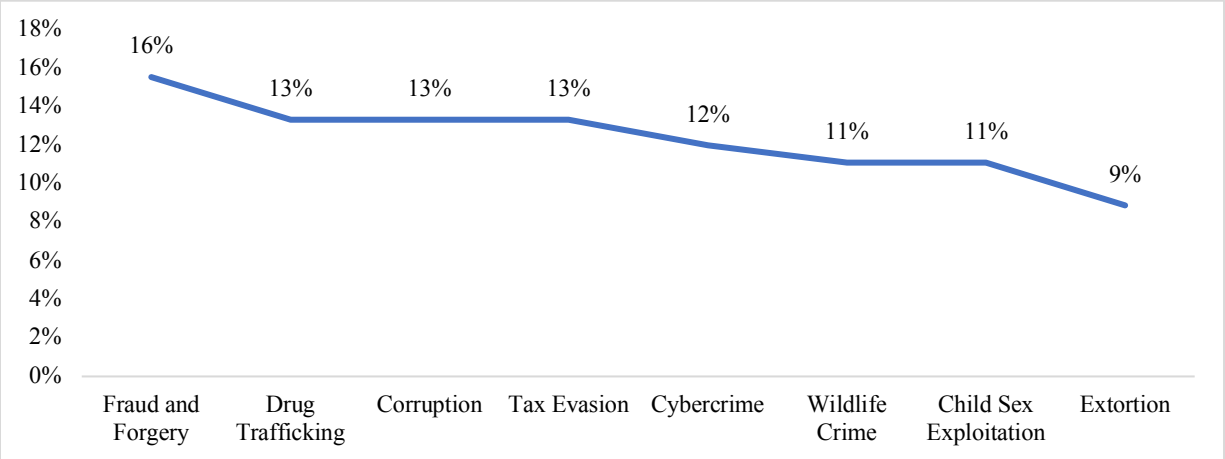
71% of the participating LEAs indicated that POCAMLA and other predicate offences laws enables them to conduct analysis, investigation, prosecution and recoveries of proceeds of crime from VAs and VASPs involved in ML/TF. However, they highlighted that Kenya has no laws for regulating VAs and VASPs.

All the LEAs that responded confirmed that there were no national laws that covered the mechanisms and functions of VASPs as per FATF recommendations. Further, the LEAs indicated that there were no legal provisions that obligate/compel VASPs to freeze, seize, or recover VAs upon suspicion of ML/TF and related predicate offences upon request by the LEAs.

86% of the LEAs confirmed they had limited capacity, resources, and technological tools to investigate, trace, prosecute and/or seize VAs. None of the LEAs had VA wallets to store and secure seized VAs.

The LEAs indicated that fraud and forgery, tax evasion, corruption, cybercrime and drug trafficking were among the top predicate offences associated with VA and VASPs as shown below.

Figure 16: Predicate Offences Associated with VA and VASPs



LEAs highlighted the following ways that criminals are likely to exploit VAs and VASPs to launder funds/assets or finance terrorism—

(a) Purchase of wildlife products using VAs.

(b) Purchase of real assets using VAs.

(c) Converting ill-gotten VAs into fiat currencies within a traditional financial system and vice-versa.

(d) Disguise and transfer of illegitimate sources of funds.

(e) Transferring assets to a terror network.
(f) Card fraud and identity theft.
(g) Moving VAs through mixers and exchanges.
(h) Online gambling sites.
(i) Buying and selling of illegal goods.
(j) Crypto smurfing schemes.
(k) Prepaid VA cards.
(l) Cryptocurrency P2P networks.

LEAs confirmed existence of formal/informal structures allowing them to cooperation within Kenya in relation to VA/VASPs, specifically through the Multi Agency Team (MT) and National Task Force on AML/CFT.

4.3 Regulators' Responses to the VA&VASP Survey

The participating regulators confirmed they did not have a legal or regulatory requirement for AML/CFT supervision or monitoring of VASPs.

All the regulators confirmed that they had conducted or participated in AML/CFT trainings with regard to VAs/VASPs in the past 2 years. 75% of the regulators indicated that they possessed a good understanding and appreciation of the ML/TF risks within the VASP/VA sector. Further, 75% of regulators indicated that they did not have the necessary resources to ensure VASPs/VA AML/CFT compliance (such as technical capacity, budget, and tools).

50% of the regulators maintained statistics on the number and type of complaints pertaining to VAs/VASPs to facilitate further investigations and sector risk analysis.

None of the regulators had assessed whether their licensees had conducted a thorough risk assessment to understand the risks of VAs and VASPs. CBK requires its licensees to undertake Customer Due Diligence (CDD) and counterparty due diligence. Once TOEs identify customers dealing with VAs/VASPs, steps are taken to de-risk the customers, based on the issued circulars.

The regulators indicated that they cooperated with other regulatory/supervisory authorities and/or LEAs with regard to VAs/VASPs for threat intelligence, information sharing and any other relevant aspect. The institutions also participate in interagency coordination and cooperation to develop policies and take measures to address VA/VASPs ML/TF risks.

4.4 Other Stakeholders' Responses to the VA &VASPs Survey

To gain deeper insights into the VA and VASP ecosystem and examine the potential facilitation of ML/TF, the TWG expanded its questionnaire distribution to include other industry stakeholders. These questionnaires were disseminated to a range of associations.

Eighty percent (80%) of respondents acknowledged their familiarity with VAs and VASPs, and sixty percent (60%) confirmed that they had engaged in VAs and VASPs activities. These interactions stemmed from the following reasons.

(a) Members of the association are VASPs; or,

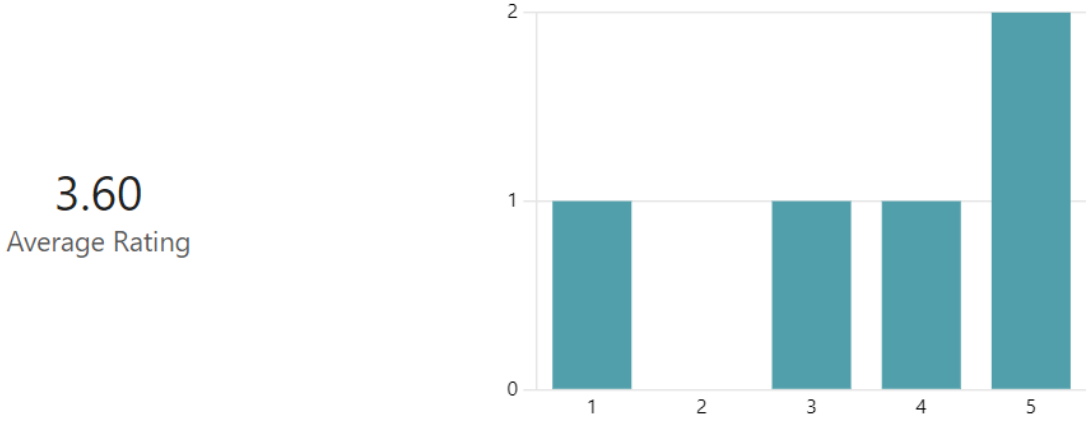
(b) Trading on the VASPs platforms mostly for speculation; or,

(c) Trainings as an emerging area of law.

Sixty percent (60%) of the respondents confirmed that they were not aware of the FATF recommendations and guidelines on VAs and VASPs and did not collaborate with LEAs or other institutions to share information related to VAs and VASPs. However, they expressed interest in exploring opportunities to collaborate with LEAs or other institutions.

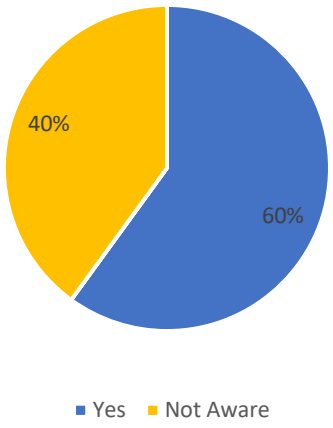
On a scale of 1 to 5, the respondents averaged 3.6 on the probability that VAs and VASPs could be used for ML/TF with 1 being low and 5 being high as shown below.

Figure 17: Possibility of use of VAs/VASPs for ML/TF



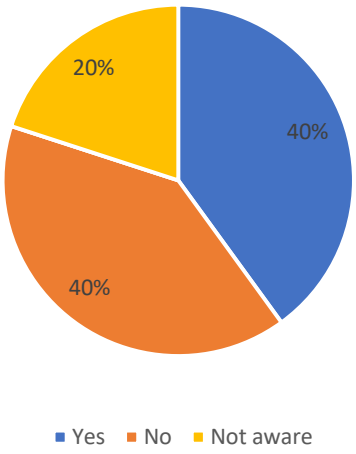
Sixty percent (60%) of survey respondents affirmed that their members participate in the purchase, sale, or exchange of VAs, either on their own behalf or on behalf of their customers or clients as illustrated below.

Figure 18: Other Organizations' Usage of VAs



It was essential to ascertain whether Kenya possesses a community that creates or accepts VAs as a means of conducting payment transactions. Forty percent (40%) of the respondents indicated that their members make or accept VAs for payment transactions as shown below.

Figure 19: Organizations' Members' Usage of VAs for Payments

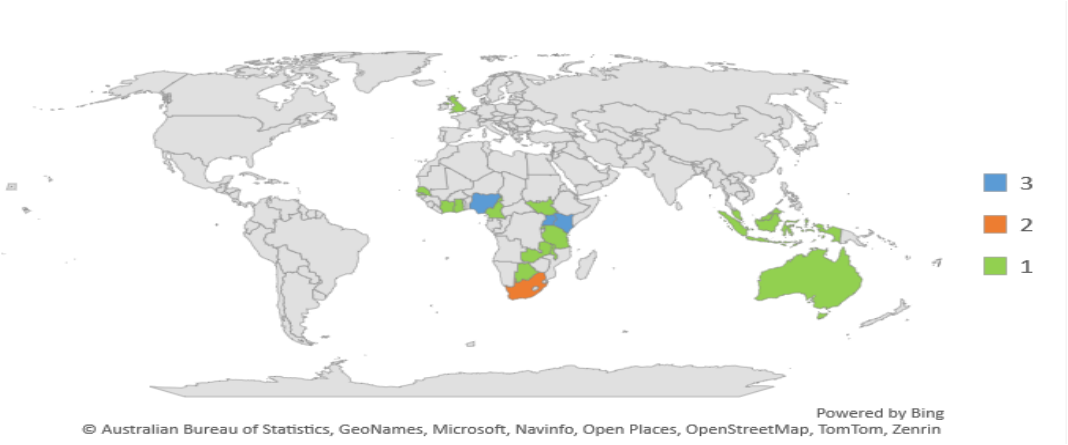


4.5 VASPS' Responses to the VA&VASP Survey

A number of VASPs participated in the survey. 80% of the VASPs operated in multiple jurisdictions including Kenya, Uganda, Tanzania, Rwanda, South Sudan, Nigeria, South Africa, Botswana, Cameroon, Ivory Coast, Ghana, Malawi, Senegal, Zambia, United Kingdom (UK), European Union, Malaysia, Indonesia, and Australia. None of these countries were identified as high-risk jurisdictions as of June 23, 2023.[23] The VASPs' jurisdictions of operations are illustrated below.

[23] https://www.fatf-gafi.org/en/publications/High-risk-and-other-monitored-jurisdictions/Increased-monitoring-june-2023.html

Figure 20: Jurisdictions of Operations of VASP Respondents



VASP Products and Services

All the respondents offered services through centralized exchanges. Further, they all offered the following services:

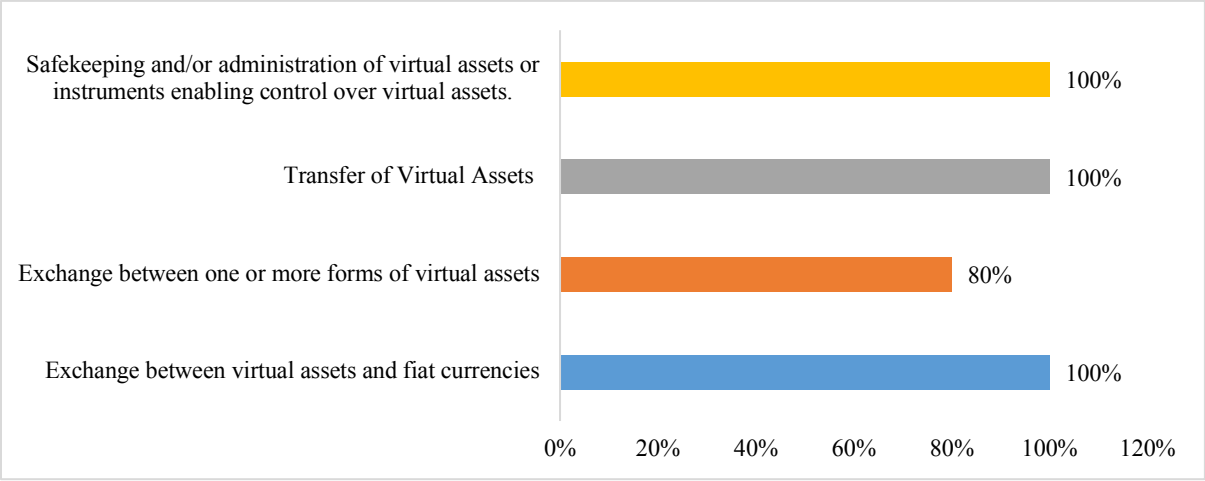
(i) Exchange between VAs and fiat currencies.

(ii) Transfer of VAs.

(iii) Safekeeping and/or administration of VAs or instruments enabling control over VAs.

80% of the VASPs offered services of exchange between one or more forms of VAs. None of the VASPs offered the services of Validators/Miners/Administrators. The figure below highlights the services offered by the respondents.

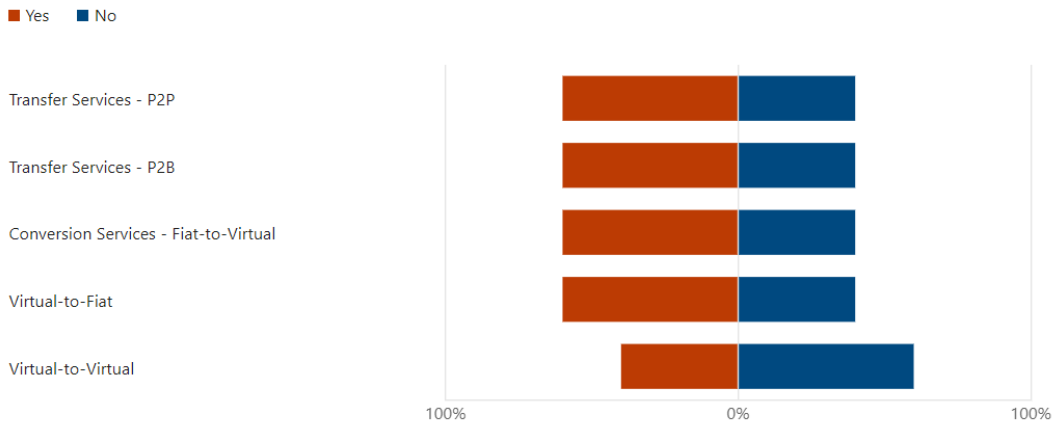
Figure 21: VASP Activities and Services Offered



With regard to specific services offered to within Kenya or to the country's nationals and legal persons incorporated in Kenya, respondents indicated the following:

(a) **Activities of a Virtual Asset Exchange Provider:** 60% of the VASPs offered Transfer Services - P2P, Transfer Services - P2B, Conversion Services - Fiat-to-Virtual, and Virtual-to-Fiat, while only 40% offered Virtual-to-Virtual conversion services as illustrated below.

Figure 22: Activities of a Virtual Asset Exchange Provider



Specific services offered included—

(a) Asset tokenization to enable trading in fractional security tokens.

(b) Exchange services.

(c) P2P payments.

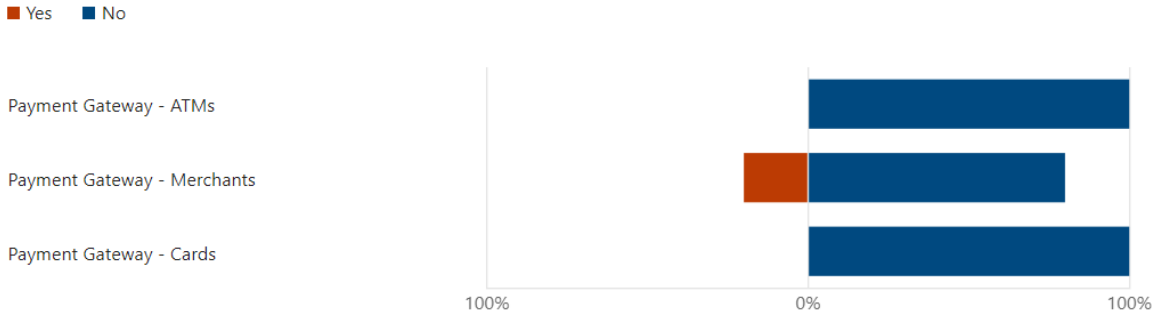
(d) Payments API.

(e) OTC services.

(f) Facilitating the integration of the platforms with in-country mobile money gateways in Africa.

(b) **Virtual Asset Broking/Payment Processing**: None of the respondents offered ATM or card payment gateways to customers. One offered a payment gateway for merchants by way of VA payment as illustrated below.

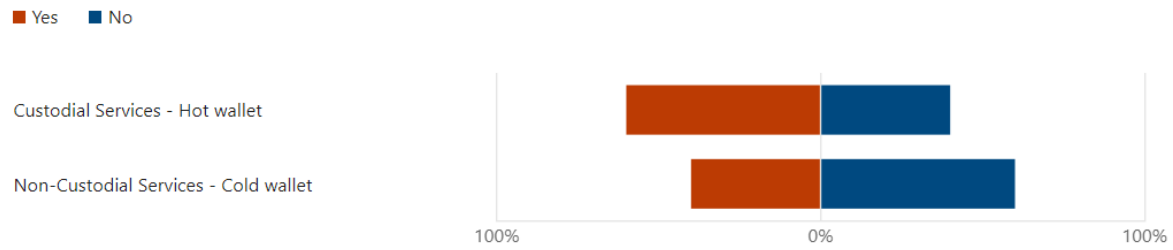
Figure 23: Virtual Asset Broking/Payment Processing



However, while the service was available, no merchants had been onboarded in Kenya yet.

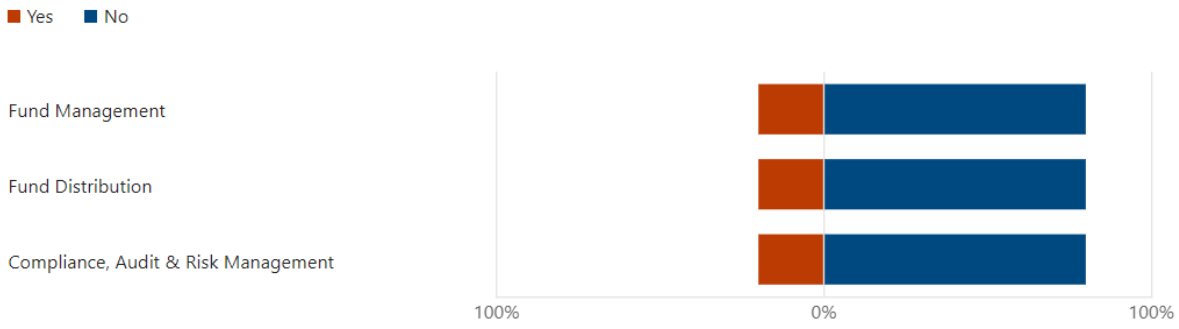
(c) Virtual Asset Wallet Provider: 60% of the respondents offered custodial services (hot wallets), while 40% supported non-custodial services (cold wallets). One of the respondents offered crypto-custodial services while another maintained an ownership registry for the digital assets on a private blockchain. The custodial and non-custodial proportion of VASPs is highlighted below.

Figure 24: Virtual Asset Wallet Provider



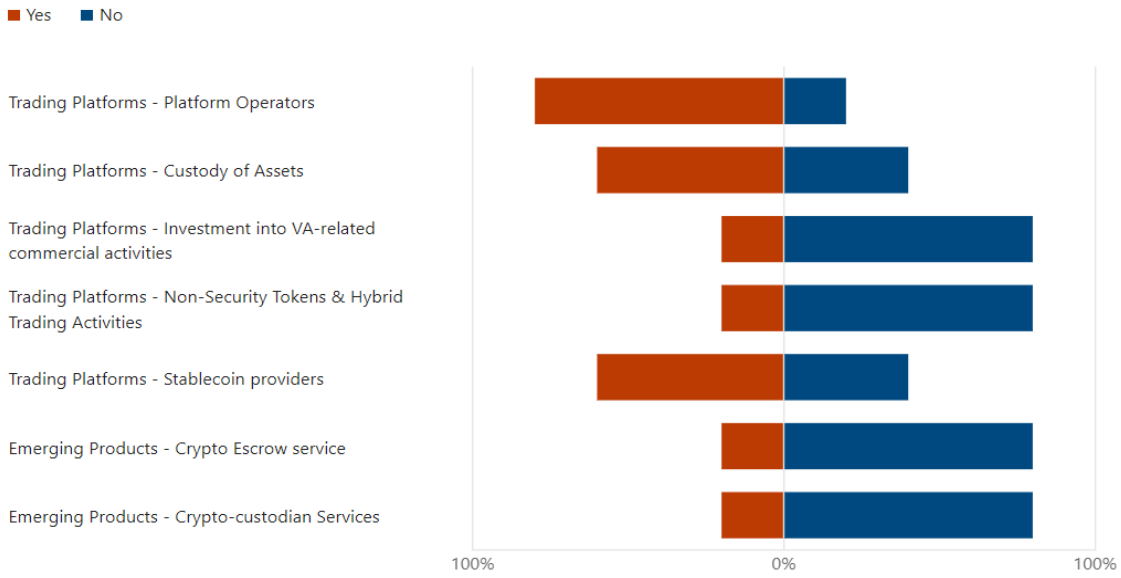
(d) Virtual Asset Management Provider: Only 20% of the respondents offered the services of a VA management provider. They tokenized real estate and managed the rental yield collected and distribute proceeds monthly to the security token holders for these properties. However, there was no evidence of this, and it was not clear whether this was happening in Kenya or other jurisdictions in which they operate. Accordingly, this category was not assessed in the risk assessment. The proportion of respondents who offer VA management provider services is illustrated below.

Figure 25: Virtual Asset Management Provider



(e) Virtual Assets Investment Provider: Of the respondents, 80% were platform operators, 60% offered custody of assets, and 60% were stablecoin providers. 20% offered Investment into VA-related commercial activities, Non-Security Tokens & Hybrid Trading Activities, Crypto Escrow service, Crypto-custodian Services as illustrated below.

Figure 26: Virtual Assets Investment Provider



Specific services for related to VA investment included—

(i) Securities token exchange.

(ii) Exchange services.

(iii) P2P transfers.

(iv) Payment API.

(v) OTC services.

(vi) Crypto-custodial services.

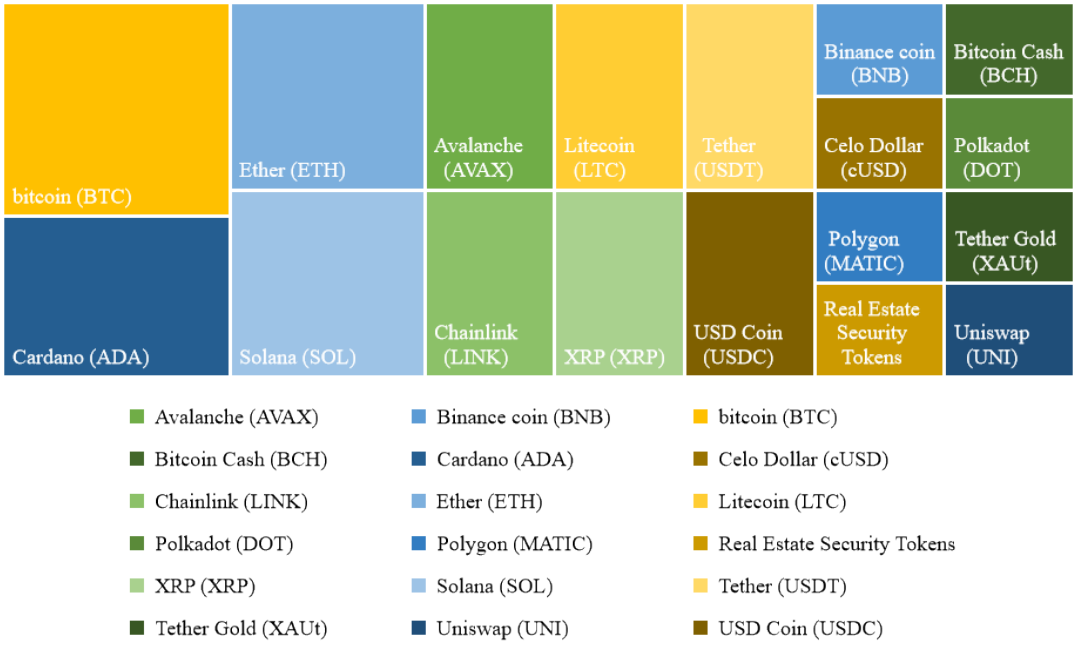
(vii) Investment in and trading of crypto assets on the platform.

(f) Validators/Miners/Administrators: None of the respondents offered the services of validators, miners or administrators.

VAs Offered by VASP Respondents

From the respondents, the estimated value of VAs held by Kenyan nationals or legal entities incorporated in Kenya from 2020 to September 2023 was KSh. 1.8 billion (USD12.2 million). The respondents indicated that they offered services in relation to the following most common VAs:

Figure 27: Top VAs Offered by VASP Respondents

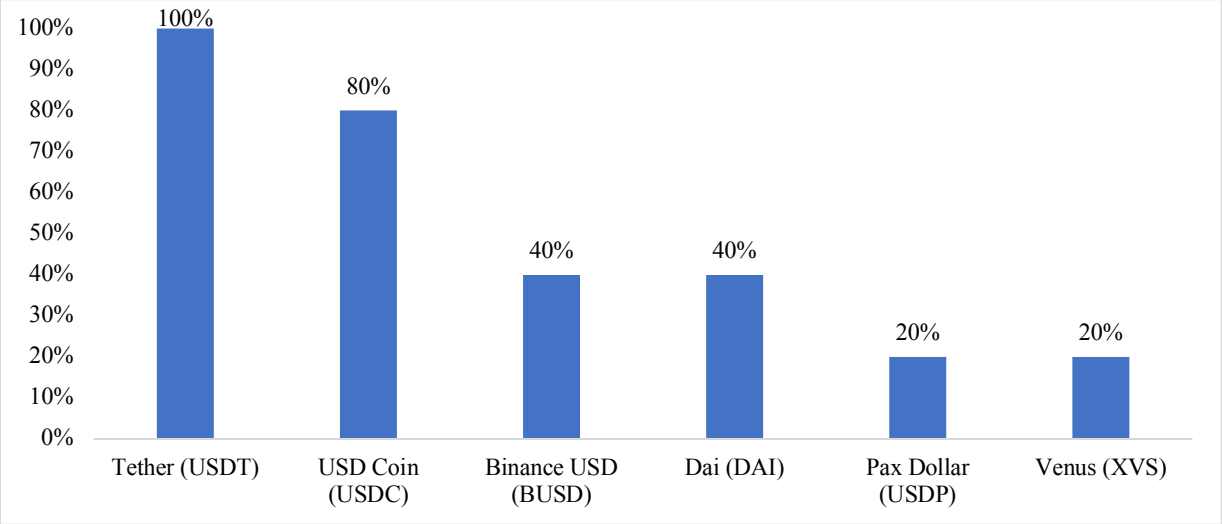


60% of the respondents indicated that they offered convertible VAs, 20% offered non-convertible VAs, and 20% offered both convertible and nonconvertible VAs.

80% of the VASPs avoided dealing with certain VAs due to higher AML/CFT risks. This was mostly because certain anonymity-enhanced cryptocurrencies or privacy coins were forbidden in some jurisdictions and where there are legislative restrictions, the coin in question was blocked for users in that jurisdiction. Only 20% of respondents allowed conversion or trading in anonymity-enhanced cryptocurrency or privacy coins. None of the respondents allowed the use of decentralized/un-hosted wallets, or offered decentralized platforms and exchanges, or mixing or tumbling services.

The VASPs identified the most common stablecoins held by Kenyans as Tether (USDT), USD Coin (USDC), Binance USD (BUSD), Dai (DAI), Pax Dollar (USDP) and Venus (XVS) as illustrated below.

Figure 28: Most Common Stablecoins held by Kenyans



Due to the CBK circular of 2015 to banks and PSPs prohibiting them from dealing with VAs/VASPs, banks and PSPs did not facilitate partnerships with VASPs. The VASPs indicated that they partnered with intermediaries to on-ramp and off-ramp VAs.

20% of the respondents indicated that they dealt with funds originating from DeFi sources. They also had platforms that supported investment activities in the metaverse i.e., stocks, gaming, real estate etc. The VASPs offered a platform for creation or trading of NFTs. NFTs were in use for both collectible and investment purposes. Further, the NFT platforms facilitated issuance and secondary sales of NFTs.

All the VASPs indicated that they applied AML/CFT risk-based mitigation measures, which included the following—

(a) Use of transaction monitoring systems for fiat transactions.
(b) Use of screening systems for adverse media, PEP and sanctions.
(c) Appointing of MLROs/compliance officers.
(d) Risk-based customer identification/verification.
(e) Mobile number verification.
(f) Integrating risk-based mitigation measures or tools on the application layer.
(g) Client funds segregation and daily reconciliation.

80% of the respondents had systems in place to flag and investigate transactions involving mixing or tumbling services used to obscure the source of VA funds.

All the respondents indicated that they effectively applied all AML/CFT processes in the jurisdictions in which they operated and compensated for any risks introduced by the cross-border nature of transactions. None of the VASPs provided VA services to individuals or

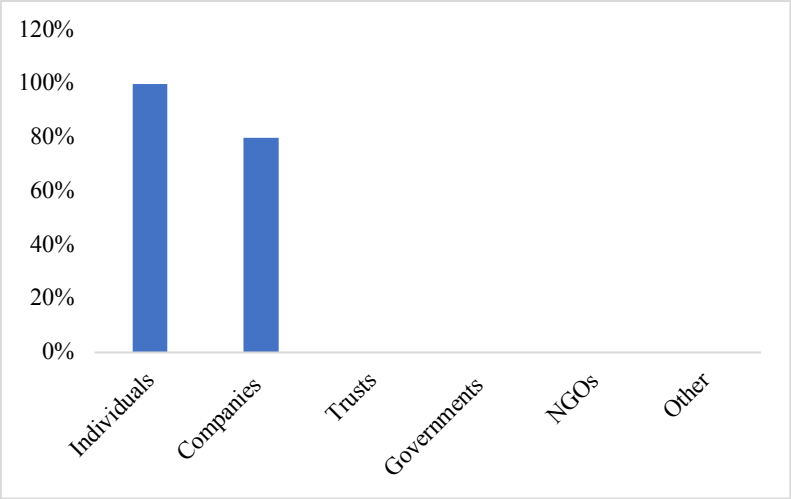
entities under UN/OFAC/EU/UKHMT sanctions. The VASPs considered sanctioned jurisdictions as part of geographic risks.

All the respondents kept their AML/CFT programmes up to date through tracking the VA landscape continuously and updating based on this as well as from engaging AML/CFT experts. The VASPs indicated that their compliance functions were, to a large extent, resourced, knowledgeable, and skilled to ensure adequate monitoring of VA/VASPs activities to detect and report suspicions of ML/TF to the authorities.

80% of the respondents had performed a comprehensive ML/TF risk assessment for all their VASP activities on an annual basis, and when triggered by key events with 40% indicating that their risk rating was high, 20% moderate and 20% low.

All the VASPs had individual customers, 80% had corporate customers (companies), while none had NGOs, trusts, and government customers as highlighted below.

Figure 29: Types of Customers Onboarded by VASPs



The respondents conducted CDD through non-face to face screening and onboarding using digital authentication services. The data required for CDD and onboarding is outlined below—

(a) **Personal Information:** Names, Mobile Phone Number (verified via text), Email (verified via email), Nationality, Address, pictures/selfies, liveness check, Country Location (IP capture) (20% of the VASPs).

(b) **KYC documents:** National ID, Passport, drivers' license or any other means of identification based on the jurisdiction, proof of source of funds, proof of address, KRA certificate. 20% of the VASPs included a questionnaire on purpose of wallet, employment status, or work industry.

(c) **KYB documents:** Certificate of Registration, shareholders and director register, applicable license.

(d) **EDD:** For high-risk customers i.e., OTC (Customers complete OTC questionnaire), API/B2B (Customers complete API/B2B questionnaire, Wolfsberg questionnaire, Recorded Virtual Meeting to assess their AML programme).

(e) UBO checks via corporate registries.

(f) AML/CFT sanctions/PEP screening for all customers against third party databases.

20% of the VASPs indicated that it may be possible for clients to potentially use their platforms to evade tax obligations. The VASPs indicated that they could assist their clients to comply with relevant tax laws in Kenya.

All the VASPs indicated that they had robust cyber risk governance measures that included business continuity, disaster recovery and contingency plans to handle emergencies, such as cyberattacks or security breaches affecting VA transactions.

80% of the surveyed VASPs had a documented annual training programmes to ensure all staff are made aware of AML/CFT laws, policies and procedures, risks and mitigations. This included significant training on ML/TF risks associated with VAs and VA related activities, including red flags for ML/TF. The trainings are offered annually for all staff and continually for those with specific compliance roles.

4.6 TOEs/Reporting Institutions' Responses to the Survey Questionnaire and Interactions with VAs/VASPs

A total of 150 reporting institutions submitted responses to the survey questionnaire.

4.6.1 Commercial Banks and Mortgage Finance Institution

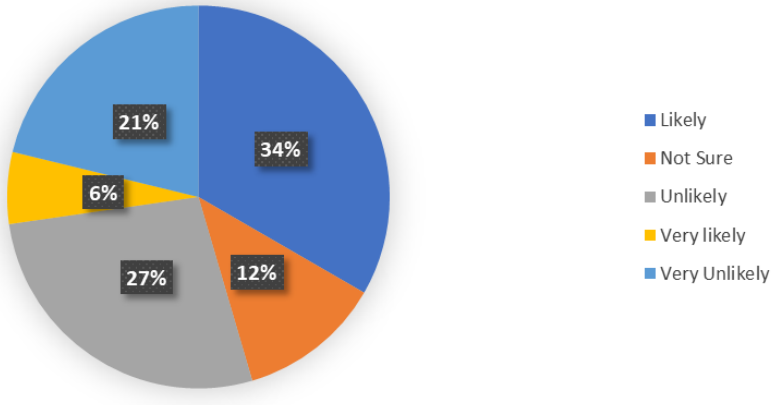
33 out 39 of commercial banks and mortgage finance institution responded to the survey, representing approximately 85 percent response rate. The survey findings indicated that the interaction between banks and VAs/VASPs was minimal as a result of the cautionary notices from the CBK which prohibited banks from interaction with VAs and VASPs. This led to a significant decline in their risk appetite for VAs/VASPs.

76% of the respondents indicated that none of their beneficial owners (BOs) had shares in VA/VASPs activities pointing to minimal interactions, while the remaining 24% were not sure or did not respond to this question.

While there was no direct integration between banks and VAs/VASPs, 40% of the respondents pointed to a possibility of their products and services being used to facilitate VAs and VASP activities as highlighted below. This likelihood was prompted by potential utilization of bank accounts for P2P offline settlements, cross-border payments, partnerships with Payment

Service Providers (PSPs) and Money Remittance Providers (MRPs), card schemes, and platform service providers.

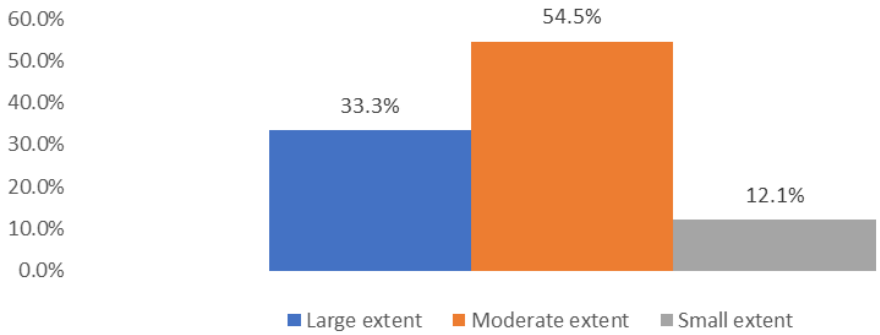
Figure 30: Likelihood of Commercial Bank's Products' Use for VAs/VASPs



None of the institutions confirmed to having customers who provide downstream financial services for VASP related activities.

88% of the banks demonstrated a good understanding of the VA/VASPs related risks especially for their compliance functions. The survey findings revealed that 91% of the compliance functions in the banks were well resourced, knowledgeable and skilled, with 73% of the institutions having carried out awareness on ML/TF risks and trends related to VAs and VASPs for staff at least annually. The institutions had an average understanding of the VAs/VASPs underlying technology with 47.5% confirming to have deployed technology solutions to detect criminal activities involving VAs and VASPs as shown below.

Figure 31: Commercial Banks' Compliance Functions' Understanding of ML/TF Risks of VAs/VASPs



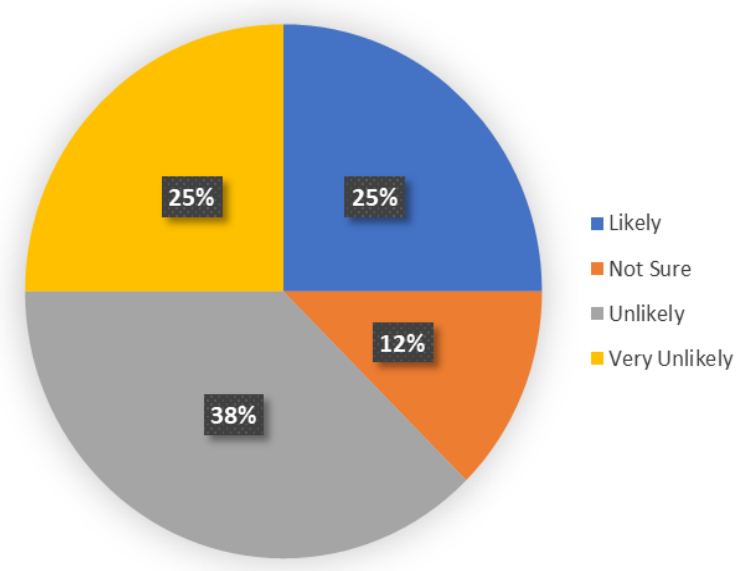
4.6.2 Microfinance Banks

8 out of 14 microfinance banks (MFBs) responded to the NRA survey, corresponding to a 57 percent response rate. None of the respondents engaged with the VA/VASP ecosystem. 75%

indicated that none of their BOs was involved in VA/VASPs activities both locally and internationally while the rest were not aware.

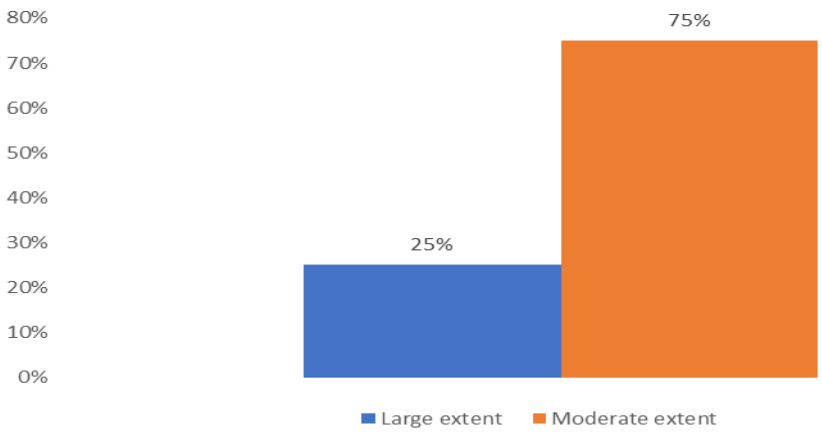
While MFBs restricted interaction with VAs/VASPs, 25% of the respondents confirmed that there was a likelihood of products and services being used to facilitate VA and VASP activities. This was as a result of interconnectedness of the payment ecosystem. This is summarized below.

Figure 32: Likelihood of Use of MFB's Products for VA/VASP Activities



50% of the respondents had a well-resourced, knowledgeable and skilled compliance staff with 25% carrying out awareness on ML/TF risk and trends related to VAs and VASPs for staff at least annually. The MFBs had an average understanding of the VA/VASPs underlying technology where 25% of the respondents had employed technology solutions to detect criminal activities involving VA and VASPs.

Figure 33: MFBs' Compliance Functions' Understanding of VA/VASP ML/TF Risks

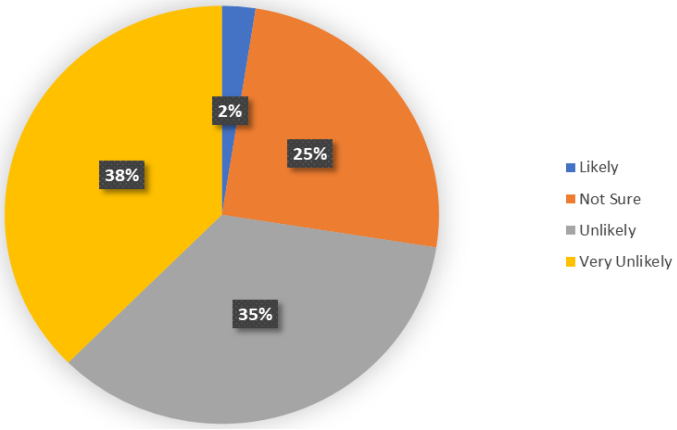


4.6.3 Forex Bureaus

40 out of the 73 licensed forex bureaus responded to the survey, representing 55 percent response rate. There was minimal interaction noted in terms of partnering or respondent institutions holding shares in VASPs.

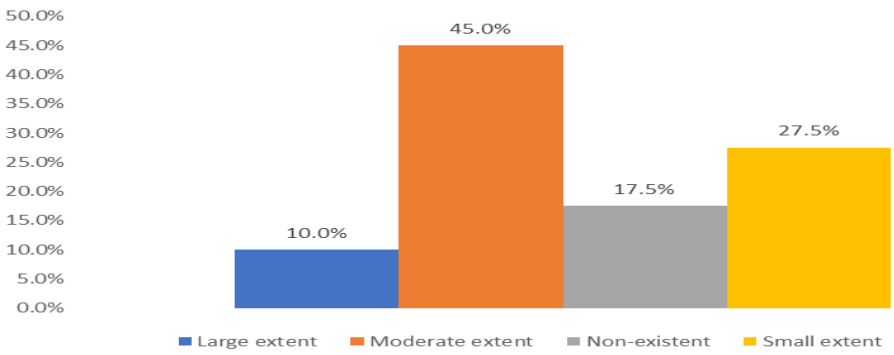
The survey indicated that the forex bureaus in Kenya do not allow for the usage or utilization of their products and services for VA/VASP activities. 2.5% of the respondents indicated that their services were likely to facilitate VA/VASPs related activities through technology service providers. 4.8% of the respondents pointed to a possibility of having customers that had invested in VAs and VASPs. The likelihood of interaction is summarized below:

Figure 34: Likelihood of Use of Forex Bureaus' Products for VA/VASP Activities



55% of the respondents indicated that they had a clear understanding of the ML/TF risks associated with VA/VASPs. The institutions demonstrated a low understanding of VAs/VASPs' underlying technology with 25% of the respondents employing technology solutions to detect criminal activities involving VA and VASPs. This is summarized below:

Figure 35: Forex Bureaus' Compliance Functions' Understanding of ML/TF Risks of VAs/VASPs



4.6.4 Securities/Capital Markets Participants

20 out of 202 institutions responded to the questionnaire representing 10 percent of the capital markets segment. The respondents indicated that their products did not interact with the VA/VASP ecosystem. They also indicated that it was unlikely that their products and services could be utilized to facilitate VA/VASP activities.

However, 90% of the respondents had not performed an ML/TF risk assessment related to VAs and VASPs despite indicating that they had appropriate measures to monitor customer activities in relation to VAs/VASPs.

50% of the respondents indicated that they understood ML/TF risks associated with VA and VASP activities.

4.6.5 Payment Service Providers

Of the 33 licensed PSPs, 7 responded to the survey, representing 21 percent of the total licensed entities. 56% of respondents confirmed that they did not interact directly with VASPs or VAs, nor provide products and services to customers to facilitate VA/VASP interactions. 67% of respondents confirmed that they did not allow usage of their products and services by VASPs. The institutions assessed indicated that they had a good understanding of ML/TF risks posed by VA/VASP activities. 33% of the respondents indicated that they had identified incidences where customers had used their platforms to engage in VA activities through P2P settlements between customers, organization accounts operating unlicensed activity such as VA trading, and cases of social engineering to facilitate fraudulent collection of funds used to purchase VAs. PSPs carry a residual risk where customers mis-declare their source of funding and account usage, thereby causing the PSPS to unknowingly facilitate VA transactions.

4.6.6 Money Remittance Providers

Of the 20 licensed MRPs, 16 responded to the survey questionnaire, representing 80 percent of the participants. The respondents indicated that their products did not interact with the VA/VASP ecosystem. However, one institution indicated that there was a likelihood of its products being used to facilitate VA and VASP related activities, specifically as a means for fiat payment between parties involved in P2P VA transactions.

The respondents indicated that they had a moderate understanding of the ML/TF risks posed by VA/VASP related activities. However, the respondents indicated that their staff had been trained on ML/TF risks associated with VAs and VA related activities, including red flags for ML/TF, with the frequency of such trainings being annually.

4.6.7 Digital Credit Providers (DCPs)

15 out of 32 licensed DCPs responded to the survey, representing 47 percent response rate. All the respondents indicated that they did not allow usage of their products and services by VASPs, and their products did not interact in any way with the VA or VASP ecosystem.

Due to the unregulated nature of VA/VASP ecosystem in Kenya and the nature of products offered by the DCPs, the respondents indicated that their customers did not carry out VASP activities. It was noted that all the respondents had not identified any customer engaged in VA or VASP-related activities.

4.6.8 Insurance Companies and Brokers

10 out of 58 licensed insurers and reinsurers and responded to the questionnaire, representing a 17 percent response rate. The respondents indicated that insurance companies in Kenya did not allow usage of their products and services by VASPs and their products did not interact with the VA/VASP ecosystem. All the respondents indicated that it was very unlikely for their products and services to be utilized to facilitate VA or VASP activities.

4.6.9 Sacco Society

Out of 33 Saccos that were sampled for the NRA, only one (1) responded, representing a 3 percent response rate. The respondents indicated that their products did not interact with the VA/VASP ecosystem. They also indicated that it was unlikely that their products and services could be utilized to facilitate VA/VASP activities.

4.6.10 Designated Non-Financial Businesses or Professions (DNFBPs)

DNFBPs did not respond to the questionnaires. However, there is a likelihood that VAs can be used in the purchase of DNFBPs products such as real estate, precious stones and in online casinos and gambling sites.

It was also note that there exists global DNFBP related markets outside of the Kenyan jurisdiction that accept VAs as a means of payment such as online betting/gambling sites, car dealers, real estate agents etc. These present channels via which Kenyans may use to conduct VA related ML/TF activities, albeit the likelihood of that happening remains low.

4.6.11 NPO Sector

No surveys were distributed to the Non-Profit Organizations (NPOs) sector to assess their interaction with the VA and VASP ecosystem within Kenya. Nevertheless, publicly available research revealed the possibility of NPOs located in Kenya or conducting activities in the country embracing VAs as a means of receiving donations.

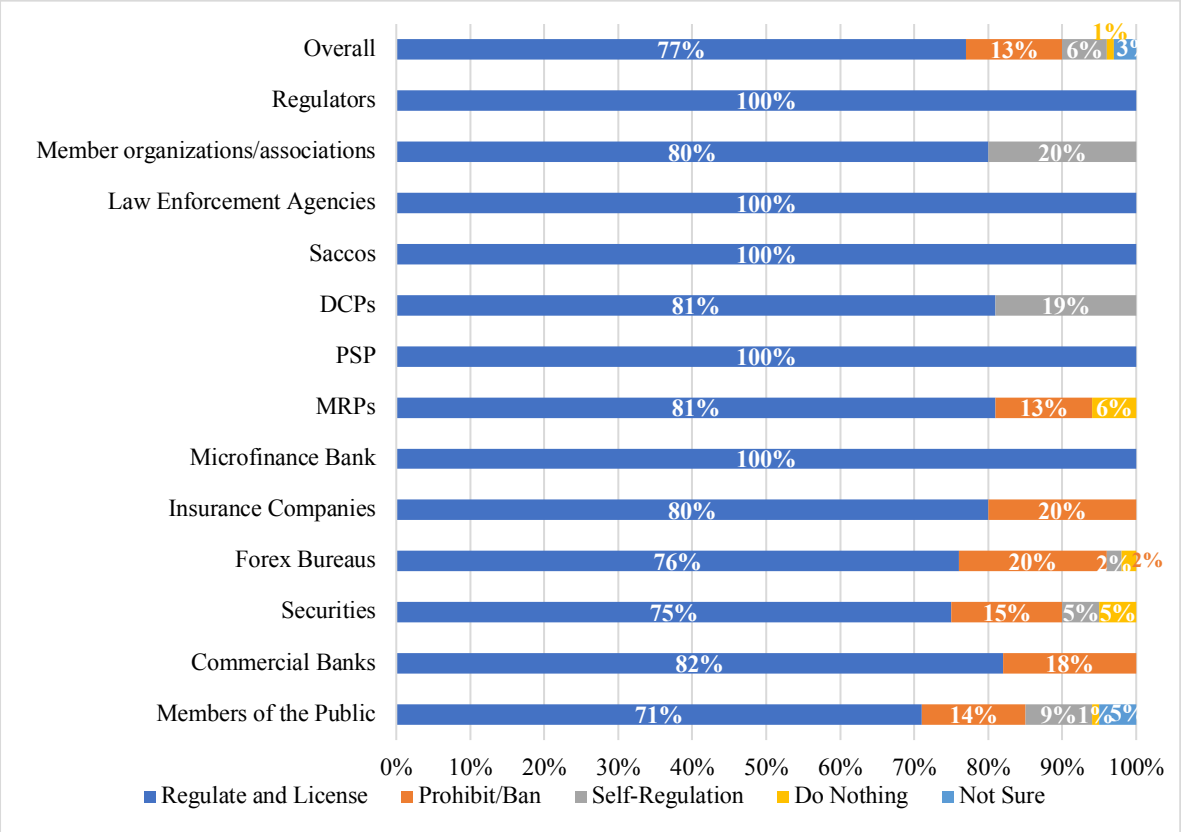
NPOs are considered high risk by the Financial Action Task Force (FATF) due to their susceptibility to being exploited for terrorism financing and money laundering activities.

Further, the CBK has issued guidance note on conducting ML/TF risk assessment for Banking sector which identifies foreign and domestic NGOs and Charities as customers posing high ML/TF risk to financial institutions[24]. The mutual evaluation of Kenya indicated that the sector is largely unsupervised and unregulated and has not been adequately assessed for TF risk. Therefore, the use of VAs might further enhance the risk taking into account the VAs inherent vulnerabilities like anonymity/pseudonymity, traceability, non-face to face, speed of transfer and cross border nature, among others.

4.7 Recommendations by Respondents on Treatment of VAs and VASPs

Overall, 77 percent of the respondents recommended the regulation and licensing of VAs/VASPs, while 13 percent recommended for prohibition of VA/VASP related activities as illustrated below.

Figure 36: Recommendations on Treatment of VAs/VASPs



Respondents noted that the decision to regulate or ban crypto assets in Kenya should be based on **people-centricity** (what problem does the solution solve), **country context** (given Kenya's advanced payments ecosystem) and the **balance between opportunities and risks**.

[24] https://www.centralbank.go.ke/wp-content/uploads/2018/03/Guidance-note-on-ML_TF-risk-assessment.pdf

Respondents identified potential benefits and risks of regulating VAs and VASPs as outlined below.

(a) Benefits of Regulation of VAs and VASPs

Kenya's payments ecosystem is advanced and comprises cross-sectoral players, and multiple use cases built upon the payment rails. The FinAccess Survey Report 2021[25] highlighted that Kenya's financial inclusion improved to 83.7 percent in 2021. Conversely, gaps were noted in the usage, quality, and impact of financial services. In this regard, Kenya should prioritize improving the financial health of its citizenry in the short to medium term. Potential benefits of regulating VAs and VASPs are as follows—

(i) Enhance consumer protection, given the potential investor losses from the high volatility and poor governance of crypto markets.

(ii) Ensuring the government undertakes its obligation in protecting the public, especially the vulnerable, from financial losses due to unregulated financial services.

(iii) Enhance AML/CFT measures in order to mitigate ML/TF risks and prevent predicate offences emanating from the use of VAs and VASPs in the country.

(iv) Reduction of financial crime related to VAs/VASPs.

(v) Financial inclusion and deepening of financial services: Protection of the existing gains of financial inclusion, so that the financial system is not adversely affected by contagion losses from VAs and VASPs, thereby reducing financial health and access.

(vi) Regulatory coherence.

(vii) Enhanced transparency, accountability, and governance of VASPs.

(viii) Enhanced financial transactions and services.

(ix) Economic growth and development.

(x) Financial innovation.

(xi) Solving current issues in the foreign exchange and cross-border transfer aspects of the financial sector.

(xii) Unlocking capital inflows into the market from players in the VA space.

(xiii) Enabling prosecution of offenders in VA/VASP-related criminal cases.

(xiv) Potential source of revenue for the government.

(b) Risks of Regulation of VAs and VASPs

Key risk considerations with regard to regulation of VAs/VASPs included—

[25] https://www.centralbank.go.ke/wp-content/uploads/2022/08/2021-Finaccesss-Survey-Report.pdf

(i) **Contagion Effect:** How do crypto assets interface with the rest of the financial sector and what are the potential contagion effects and how can they be mitigated to ensure continued financial stability? For instance, the risk of collapse of a VASP due to external events that may occur outside Kenya may lead to contagion risk.

(ii) **Effecting AML/CFT Considerations:** How will AML/CFT risks be addressed, given the anonymity of VAs and other inherent vulnerabilities?

(iii) **Consumer Protection Considerations:** How will consumer protection issues be addressed, given that most VASPs operate cross-border and are not necessarily domiciled in the countries of operation? It would be difficult to address market abuse and misconduct related to VAs and VASPS.

(iv) **Protection of the Vulnerable and Consumer Protection:** How will government ensure that the vulnerable, who do not have the capacity to do due diligence on VAs and VASPs, are offered protection from losses as a public good? How will deposit/investment protection be implemented?

(v) Lack of oversight of operations due to the complexity of supervising VASPs and VAs.

(vi) Increased cross-border activities and interactions between the regulated entities and non-regulated entities outside Kenya that could lead to an increase in the risks of ML, TF, fraud and other crimes.

5. VA/VASP Threat Assessment

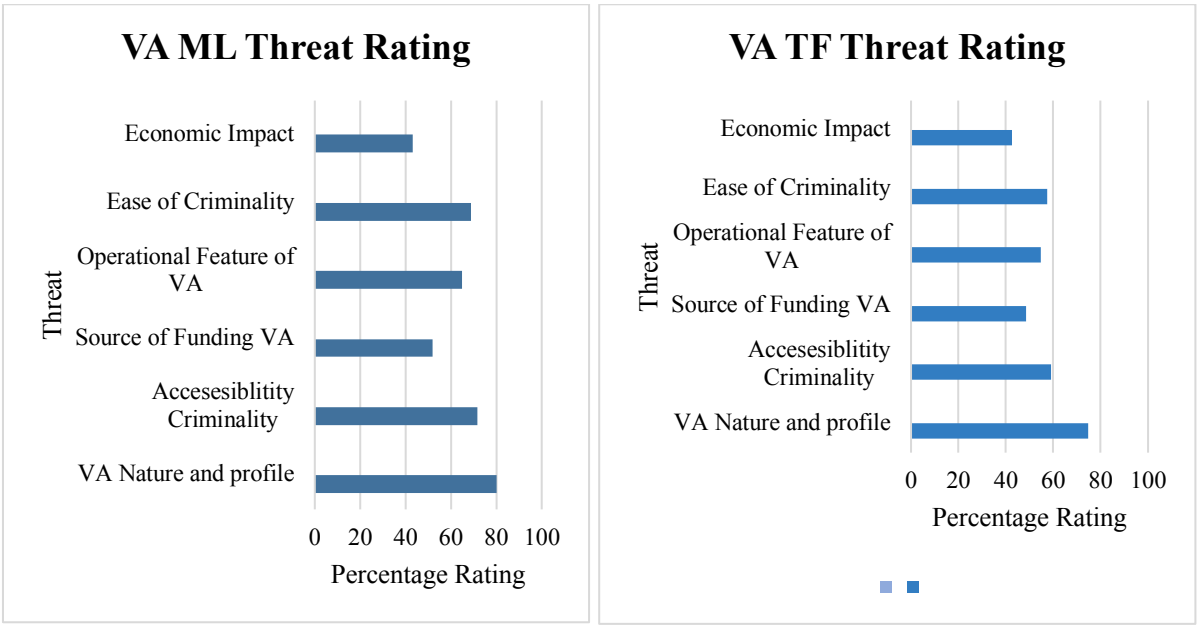
This section looks at the analysis of threats of both VAs and VASPs. The assessment considered intermediate and input variables of threats from a domestic and international perspective from various VAs/VASPs.

5.1 Threat Assessment Overview

Through the survey, a total of thirty-three (33) VAs were identified to be used by Kenyans. Six (6) percent of the VAs identified had anonymity enhanced features. An open-source search indicated that, thirty-three percent (33%) of the total VAs that were used in Kenya, had previously been exploited for ML in other jurisdictions, while twenty-four percent (24%) had been exploited for TF in other jurisdictions due to their inherent attributes. Open-source information indicated that VAs had been exploited domestically for ML.[26]

The assessment was based on six (6) intermediary variables of the threats related to VAs products as shown below.

Figure 37: VA ML and TF Threat Rating



The detailed explanation of the various variables considered in arriving at the ML and TF threat rating are as outlined below.

[26] https://nation.africa/kenya/news/revealed-how-billions-were-moved-in-sh25bn-suspected-racket-3798334

5.1.1 VA Nature and Profile

(i) Anonymity/Pseudonymity

The Kenyan ecosystem comprises of different types of VAs which were mostly convertible and characterized by anonymity and/or pseudonymity features which can obfuscate financial transactions thus presenting an ML/TF risk.

VAs such as Monero and Dash have anonymity-enhanced features and may be preferred by criminals for ML/TF.

The ML/TF risks presented by a wallet depend on, among others, the anonymity/pseudonymity characteristics of the VAs stored in the wallet. The survey indicated that most VAs in the Kenyan VA and VASP landscape are stored in hot wallets within centralized environment and there is no usage of mixers, tumblers or anonymizers that could increase obfuscation of financial flows. Hot wallets are held by a custodian and the owner does not have full control of the VA rather the funds are held by the custodian providing the VA Wallet Service. Cold wallets present a very high inherent risk especially when used to store anonymity enhanced VAs such as Monero which could provide an opportunity for exploitation by criminals.

The VASPs offering transfer and conversion services in the Kenyan ecosystem are mainly centralized exchanges who conduct customer due diligence and conduct transaction monitoring. Despite the space being non-regulated, the centralized environment increases the transparency of VAs transaction to some extent. With the existence of decentralized exchanges and the possibility of using privacy coins in the exchanges heightens the inherent risk to very high.

The use of (IP) anonymizers such as The Onion Router (TOR) or Invisible Internet Project (I2P) may further obscure transactions or activities and inhibit a VASP's ability to know its customers and implement effective AML/CFT measures.

The transparency of blockchains can complicate attempts to move or obfuscate funds even pseudonymously. However, the absence of a regulatory and supervisory framework increases the risk of Pseudonymous/anonymous VA transactions since they are not being monitored.

(ii) P2P Cross-Border Transfer and Portability

VAs by nature possess cross-border features with a global reach, making them attractive to criminals such as ransomware attackers, who receive payments from victims located around the world without having to go through a bank or other financial institution. Further, since they are internet-based, they can be accessed and transferred anywhere regardless of physical location.

The *2023 Geography of Cryptocurrency Report* by Chainalysis ranks Kenya the 3rd in peer-to-peer exchange trade volumes. The P2P cross-border transactions could therefore pose an ML/TF risk and illegal activities such as ransomware, could thrive in P2P transfers.

The VAs identified in Kenya are liquid, easily convertible and allow for use on decentralized platforms available across multiple jurisdictions. They can also be used for cross-border and cross-currency business, thereby posing high risks of transferability and portability.

A number of stablecoins were identified in Kenya with USDT leading as identified through the survey responses. There is therefore a possibility that the stablecoins could be used in cross-border business for remittance, payments, settlement and store of value.

The existence of cold wallets accessible to Kenyans may heighten the ML/TF risks due to their decentralized nature and ease of portability. On the other hand, at the time of risk assessment, no VA ATM was operating in the country. Moreover, the absence of a regulatory framework for VAs/VASPs further exacerbates the risk posed by P2P cross-border VAs transfers.

(iii) Absence of Face-to-Face Contact

The absence of face-to-face contact is an inherent risk with all the VAs identified in the Kenyan ecosystem. The degree of anonymity/pseudonymity together with existence of decentralized exchanges that provide peer to peer transferability with no regulatory controls makes the non-face-to-face activities pose a high inherent ML and TF risk. While some VASPs use different solutions such as *Notabene.id* to assist in the implementation of the travel rule, others, depending on the jurisdiction of operation. Such characteristics are appealing to criminals and thus may permit anonymous funding or not reveal the identity of the parties involved in such transactions.

Some of the VASPs with operations in Kenya lacked standard KYC while others gave users an allowance of 30 days to use the platform without any KYC. Due to the lack of a standard KYC, users could provide fake documentation. In addition, the absence of a regulatory framework makes it difficult to enforce AML/CFT measures since VASPs are not obligated to hold and keep the originator and beneficiary details.

(iv) Traceability

Blockchain technology provides transparency and traceability for all transactions in the chain. Most VAs in the Kenyan ecosystem had traceability features and transactions are recorded on a public DLT which can be traced with the right tools. Financial institutions, such as banks have controls in place to identify VA-related transactions and take appropriate action based on the cautionary statements by the CBK. Further, Kenya is among the many countries that have not yet implemented the travel rule for VASPs given that they are unregulated in the country.

Although there have been no cases where VAs have been seized, with appropriate tools and technical capacity, tracing and seizing them can effectively be managed. Kenya lacks dedicated tools to trace the VAs transactions effectively and efficiently on the blockchain. VAs such as Monero and Dash allow the user to decide their privacy features, thus increasing the risk of low traceability.

(v) Speed of Transfer

The speed of transfer of VAs is dependent on the blockchain protocol that supports it. Different types of VAs offer different transaction speeds with some being much faster than others. Some of the VAs were observed to be near instantaneous, taking 2 seconds to a few minutes to complete transactions, thereby posing a high risk. Although the speed of transfer in VAs is high as compared with other methods of transfers such as banks, the use of centralized exchanges and the ability to trace transactions mitigates this risk due to the controls/checks conducted by VASPs resulting in lower speed for transactions flagged as high-risk. Further, given that most of the VAs in circulation within Kenya's landscape are pseudonymous and not anonymous, the risk posed by rapid transaction settlement is mitigated by ability to trace transactions.

Overall, the speed of transfer, coupled with anonymity/pseudonymity, P2P mechanism, absence of face-to-face, cross-border nature and global reach of VAs presents an inherent ML/TF risk to the country.

5.1.2 Accessibility to Criminals

(i) Mining by Criminals

No mining pools were identified in Kenya. however, most VAs in circulation are majorly mined through staking which consumes less energy as compared to VAs mined through proof of work (POW). This makes it easier for criminals to mine the VAs in the ecosystem.

From a domestic perspective, the risk could be lower as few criminals could have the expertise and resources for mining. However, from an international perspective, there is a possibility of crypto jacking where hackers through malware would take advantage of Kenya's susceptibility to cyber-attacks to steal mining resources or VA wallets. The Communication Authority Cybersecurity Report Q2 2022-2023[27] indicated that cyber threat actors were observed to be advancing their tactics to distribute malware through phishing campaigns; fake forum pages; embedding malicious links in Ads such as Google Ads; infected software; and fake updates of apps. Further, a total of 249,991,852 cyber threats were detected by the National KE-CIRT/CC. Therefore, this raises the possibility of crypto jacking through malware.

[27] https://www.ca.go.ke/sites/default/files/2023-06/Cybersecurity%20Report%20Q2%202022-2023.pdf

(ii) Collection of Funds

Given the inherent nature of VAs coupled with the unregulated environment, there is a possibility of VAs being used to fund TF through various means to support international terrorism. VAs might be donated by supporters or collected through crowdfunding. The anonymity of some VAs makes them more appealing for TF. According to the National Risk Assessment for Kenya, the country is a target of Al-Shabaab, Islamic State and Al-Qaeda terrorist groups in Somalia. Given the country's uptake for VAs and absence of a regulatory framework, there is a possibility of abuse by terrorists. Although no information was available to support the use of VAs by the groups in the country, they could use VAs to collect and receive funds for TF.

Globally, there is an increasing trend of terrorist actors to adopt and use new technology to finance terrorism including the use of VAs. Terrorist groups, along with their sympathizers, are consistently exploring new methods to acquire and move funds discreetly, evading detection and monitoring by law enforcement agencies.

(iii) Transfer of Funds

Given the borderless nature of most VAs traced in the country and the fact that there is no regulatory framework in the country, the risk of transfer from and to unregulated jurisdictions is high. The anonymity of some of the VAs identified and ease of transferability increases the VAs' accessibility and exploitation by criminals.

No stablecoins had been issued or launched in the country and therefore, those accessed in the country are mainly dollar backed, and utilised for transactions including transfer of funds.

(iv) Dark Web Access

The pseudonymous nature of activities in the dark web creates an opportunity for criminal use. From the survey, Kenyans had the capability to access the dark web with 14% of the respondents confirming having used the dark web for various purposes.

The use of IP anonymizers, virtual private networks and onion router enable malicious actors to access dark web anonymously for VA related cybercrime like ML and TF. Proceeds of crime obtained through the use of the dark web may be laundered through anomality-enhanced VAs and the use of mixers or tumblers providing underground services. According to the U.S. Department of Justice, in November 2022 announced that it seized about $3.36 billion in bitcoin stolen from darknet market Silk Road[28]. VAs are the preferred mode of payment in the dark web to shield users' identity.

[28] https://www.cnbc.com/2022/11/07/feds-seize-3point36-billion-in-bitcoin-the-second-largest-recovery-so-far.html

(v) Expenditure of Funds

In absence of a competent authority to regulate innovations in the VA ecosystem, the rapid innovations my attract criminals to the ecosystem. According to the Kenyan Startup Ecosystem Report 2022,[29] Fintech is the leading sub-sector of the Kenyan start-up space in terms of levels of activity. Further, the report says Blockchain start-ups in Africa, raised US$91 million in the first quarter of 2022, and a total of US$127 million was raised throughout 2021. Of the funding raised in 2021, 96% went to Nigeria, Kenya, South Africa and Seychelles, making Kenya deserving of the spotlight when it comes to blockchain innovation and integration.

Despite there being no known instances where criminals had invested in technology infrastructure/fintech innovations in the Kenyan ecosystems, there is possibility that proceeds of crime can be used to support FinTech's in the VA arena. This presents an opportunity for use of proxies to launder ill-gotten proceed from crimes such as fraud, corruption and tax evasion. Criminals might also invest in trading platforms and disguise the proceeds as investments. According to BNN Bloomberg[30], a fintech owner in London faced allegations that he helped notorious drug traffickers attempt to launder hundreds of millions of Euros through a crypto exchange platform.

5.1.3 Source of Funding VAs

(i) Bank or card as source of funding VA

Noting that card issuers in the Kenyan ecosystem are regulated, traceability of card related transaction as a source of funding VAs is possible. CBK issued a circular to banks and PSPs prohibiting them against use of VAs. Based on this, banks and PSPs disallowed VA-related activities, lowering the risks of bank accounts and card schemes being used as a source of VA funding in Kenya. In addition, the contracts signed by banks with third-party service providers do not support the use of cards or bank transfers for VA related activities. However, banks and PSPs still carry a residual risk where accountholders mis-declare their source of funding and account usage as such unknowingly facilitating VAs transactions (*Ref Case A)*. Criminals therefore tend to shy off from exploiting this channel and thus limiting the potential for abuse.

[29] https://disrupt-africa.com/wp-content/uploads/2022/12/The-Kenyan-Startup-Ecosystem-Report-2022.pdf
[30] https://www.bnnbloomberg.ca/the-fintech-owner-accused-of-laundering-drug-money-in-huge-bitcoin-scheme-1.1968274

Figure 38: Case A - BitPesa Vs Safaricom

BitPesa Vs Safaricom case. BitPesa faced a legal challenge due to its service that permitted users to transmit funds using Bitcoin, which would subsequently be converted into Kenyan Shillings upon receipt. Safaricom alleged that BitPesa violated its anti-money laundering regulations by engaging in Bitcoin trading, an unregulated activity.

Source: http://kenyalaw.org/caselaw/cases/view/117270/

As the source of funds is mostly through regulated financial products, the risk of illicit funds being used to fund VAs is low due to existing controls in the products and banks. Most of the VAs used in Kenya passed through centralized exchanges which implemented preventive measures, despite not being regulated in Kenya. The prohibition through cautionary statements triggered banks to put in place adequate systems to detect VA-related activities and track payment cards connected to known fraud, extortion, ransomware schemes, and illicit websites, among others. Criminals therefore tend to refrain from exploiting bank and card channels, thus limiting the potential for abuse.

(ii) Cash Transfers, Valuable In-Kind Goods

No OTC traders were identified in Kenya. However, globally, the risk of OTC traders has been increasing with most of their CDD/KYC requirements being lower than the exchanges they operate in. This increases the risk of criminals using the service to launder and cash out funds. Due to lack of regulation and cautionary notes issued by various regulators, no known OTC business was identified to operate in Kenya. No information was availed to suggest usage of cash for purchase of the VAs identified in Kenya as trading is noted to be done mainly through peer to peer. This reduces the risk of cash transactions being exploited for ML/TF. In addition, VASPs offering VAs in the Kenyan ecosystem, conduct KYC with a view of confirming the identity of its customers which lowers the probability of mule accounts. However, there is the possibility of unlicensed brokers accepting cash in exchange for VAs.

(iii) Use of Virtual Currency

In Kenya, no stablecoins had been issued/launched to circumvent control imposed in other jurisdictions, an indicator that the country is not a preferred location for stablecoins. There is a possibility of proceeds from tax evasion being laundered through acquisition of other VAs. The majority of coins identified in the ecosystem do not use zero proof technology and therefore might not be a major threat to the country.

5.1.4 Operational Features

(i) Regulated

The legislative framework in Kenya has not provided for regulation of VAs and, therefore, this section of the criteria did not apply.

(ii) Unregulated

There is no regulatory framework in the country for VA or VASP related activities. The AML/CFT laws and consumer laws that exist apply to some extent making it possible for terrorist actors to misuse transfer and conversion services. However, no cases of TF funding by VAs had been reported in the country.

(iii) Centralized Environment

Majority of the VAs in Kenya operate in centralized environments which facilitate recording of the VA transactions. 62% of the public survey respondents dealing with VAs indicated that they used centralized exchanges, thereby presenting a lower risk.

(iv) Decentralized Environment

The public questionnaire identified the existence of users who utilized DeFi services/platforms such as Uniswap and MetaMask. Decentralised exchanges offer anonymity and might be misused to obfuscate sources of illicit funds. Additionally, un-hosted wallets could increase susceptibility to ML/TF abuse. These features increase privacy and security levels of VAs and thus increase their susceptibility to ML/TF abuse.

5.1.5 Ease of Criminality

(i) Tax Evasion

In an unregulated ecosystem such as Kenya, the inherent nature of VA informs a high threat rating for tax evasion. Tax evasion has been identified as a predicate offence for ML in the country. The anonymity/pseudonymity in the VAs could attract investors/traders/users in the crypto space who could easily avoid payment of taxes such as VAT, capital gains, stamp duty etc. due to lack of close scrutiny. Additionally, lack of traceability and portability especially, for cold wallets exacerbates the treat of tax evasion to very high.

(ii) Terrorist Financing

Anonymity, speed of transfer, absence of regulation, scalability, acceptance and usability makes VAs susceptible to misuse for TF purposes. Globally, there have been incidents where terrorist actors have raised funds through VA donations and crowdfunding. However, no cases were identified in the country. The existing TF measures, cautionary statements issued by financial sector regulators, stringent regulatory framework on terrorism through the Prevention of Terrorism Act (POTA) and implementation of the travel rule by reporting institutions,

downplay the possibility of the risk. Additionally, data collected during the assessment indicated that VASPs had put in measures to mitigate TF and ML risks.

(iii) Disguising Criminal Proceeds to VA not Regulated

In the absence of any regulations or reporting obligations by VASPs, it is possible for criminals to disguise and conceal proceeds of crime. Kenya's 2022, NRA, identified corruption to be among the country's top ML predicate offences. Therefore, there is a likelihood of VAs being used as a medium to conceal and disguise proceeds of corruption. Further, the inherent features of accessibility and anonymity heighten the risk.

The VASPs identified in the ecosystem conduct KYC during onboarding reducing the likelihood of the medium being used for kickback payments and to conceal and disguise the nature and source of illegal wealth. At the time of conducting this risk assessment no fiat backed stablecoins had been issued locally, therefore the risk related to stablecoins is minimal. The stablecoins in use in the country had been developed/launched in countries with a legal and regulatory framework.

(iv) Trace and Seize Difficulty

VAs transactions occur on DLT and can be traced and seized using the right tools and expertise. A majority of VASPs identified in Kenya conduct KYC, making it possible to trace the originators and beneficiaries of VA transactions. LEAs have legal authority to trace, freeze and seize VAs. However, they lack the expertise, technology, and knowledge of VAs/VASPs.

(v) Circumventing Exchange Control

Kenya repealed exchange control regimes in 1993 and moved to a fully market-determined exchange rate system. Therefore, the possibility of using VAs to circumvent exchange controls does not arise. However, the activities of foreign exchange dealing or trading are regulated services, respectively. VAs are not regulated in Kenya, and the conversion rate or costs are determined by the VASP or individual offering conversion or exchange services. Accordingly, customers dealing with VAs might be exposed to consumer protection and market conduct issues as they have no recourse for high conversion costs or unfair treatment. Conversely, stablecoins might be used by customers to protect themselves against unfavourable forex market conditions by holding value in foreign-denominated stablecoins, whose use would not be dependent on limits set by banks and other financial institutions.

5.1.6 Economic Impact

(a) Underground Economy – Impact on the Country's Monetary Policy

Kenya has a robust monetary policy framework that spurs financial stability and a stable market-based system. Kenya's financial access has increased from 26.7 percent in 2006 to 83.7 percent in 2021. Additionally, the adult population that is completely excluded from any form of financial services has declined from 41.3 percent in 2006 to 11.6 percent in 2021. This increased financial inclusion as highlighted by the growing use of formal financial services, has played a pivotal role in reducing the activities related to the underground economy.

5.2 ML Threat Assessment

The threat assessment analysis identified the nature and the exposure of VAs and VASPs in relation to ML predicate offences. The threat analysis considered the domestic predicate offences as identified in the NRA of 2021, foreign predicates identified in international and emerging typologies, and the exposure of Kenya's VAs and VASPs landscape to these predicate offences.

It further covered the threat analysis of each input variables that fed into the intermediate variables across the VASP channels as covered by the product dimension of the World Bank assessment methodology. The analysis considered the characteristics of VAs and how different types of VASPs in the VA value chain could be abused to commit predicate offences and launder proceeds generated either in fiat currency or VAs.

Based on Kenya's 2021 NRA findings, the main proceeds-generating predicate offences in the country that pose an ML threat include fraud and forgery, drug related offences, corruption and economic crimes, environmental and wildlife crime, counterfeiting, tax evasion and cybercrime offences.

VA/VASP related fraud and forgery related offences are usually characterized by fraudulent investment schemes, fake coin offerings and fake exchanges using imposter websites. In Kenya, there have been cases of VAs and VASP activities being used as part of ML schemes and are particularly associated with several predicate offences such as fraud, tax evasion and forgery. The assessment identified cases of VA-related fraud and forgery in Kenya as illustrated in the cases below.

Figure 39: Case B - Fraudulent ICOs

Wiseman Talent Ventures introduced its crypto coin called Kenicoin. The coin was initially available at Kshs 100.00 during the Initial Coin Offering (ICO) stage. However, it was later advertised as trading at Kshs 2,000 on its exchange. The Capital Markets Authority (CMA) flagged the potential inconsistencies in the information presented on the company's website and raised concerns regarding the accuracy of information provided by Wiseman Talent Ventures' leadership during interviews, regarding the number of Kenicoin units sold and the total amount of funds raised through the ICO. CMA believed that there were some irregularities in the information being offered to the public, which caused fraud risks. Wiseman Talent Ventures moved to court to challenge CMA's decision to ban their operation activities and the case was ruled in favor of CMA.

Figure 40: Case C - Fraudulent Investment

The Capital Markets Authority (CMA) in Kenya initiated an investigation into the activities of Nurucoin due to alleged irregularities in the collection of investor funds amounting to Kshs 2.7 billion. This case pertained to a Nurucoin scheme that has reportedly defrauded around 11,000 investors. The funds in question were gathered from investors who believed they were participating in an investment opportunity related to a virtual currency venture known as Nurucoin. The cryptocurrency issued an ICO which was supposedly closed in March 2018.

Figure 41: Case D - Crypto Ponzi Scheme

Kenya has witnessed several cases of crypto Ponzi schemes in the country. An example was BTCM, a crypto mining Ponzi scheme that collapsed with crypto investors' money. BTCM posed as an investment platform. The Ponzi scheme had promised investors to invest between Kshs 600 and Kshs.260,000.00 to buy bitcoin mining pools and in return get a profit of between 150% and 400% on investment after a couple of days. The investors were required to bring more people through referral programs to increase their returns, a common technic that most Ponzi schemes actors employ. Eventually the Ponzi scheme collapsed with people's money.

(Sources:

- *Letter from Africa: The lure of the get-rich-quick scam in Kenya - BBC News) and*
- *https://www.mariblock.com/btcm-kenyas-latest-crypto-mining-ponzi-scheme-collapses-leaving-investors-empty-handed/#:~:text=Be%20smart%3A%20Crypto%20Ponzi%20schemes,which%20defrauded%20several%20unsuspecting%20Kenyans.*

With regard to ransomware, a report by the Kenya Computer Incident Response Team (KE-CIRT) indicated that there had been cyber-attacks in the country conducted through ransomware. The attackers aimed to access sensitive data, which they steal, encrypt and threat to sell to the highest bidders or publish the information to data leaks if the victims fail to pay the ransom, usually in crypto currencies[31].

Against this backdrop, the TWG assessed the threat of VAs and VASPs to be exploited for ML activities as **Medium** as illustrated in the table below.

Table 5: ML Threat Exposure for VAs and VASPs

VASP/SERVICE/CHANNEL			**VA/VASP ML THREAT RATING**
VASP	**Type of Services**	**Channel**	**Threat**
Virtual Asset Wallet Providers	Custodial Services	Hot Wallet	Medium
	Non-custodial Services	Cold Wallet	High
Virtual Asset Exchanges	Transfer Services	P2P	High
		P2B	Medium
	Conversion Services	Fiat-to-Virtual	Medium
		Virtual-to-Fiat	High
		Virtual-to-Virtual	High
Virtual Asset Broking/Payment Processing	Payment Gateway	Merchants	Low
		Platform Operators	Medium

[31] https://ke-cirt.go.ke/wp-content/uploads/2021/07/Quarter-4-FY-2020_21-National-KE-CIRT_CC-Cybersecurity-Report-Public-Version.pdf

VASP/SERVICE/CHANNEL			VA/VASP ML THREAT RATING
VASP	**Type of Services**	**Channel**	**Threat**
Virtual Asset Investment Providers	Trading Platforms	Non-Security Tokens & Hybrid Trading Activities	Medium
		Stablecoins	Medium
Overall VA & VASPs ML Risk			**Medium**

5.3 TF Threat Assessment

VAs and VASPs are exposed to TF abuse in raising, moving, storing and using funds to finance terrorist attacks or support operations of terrorist cells or networks. VAs provide an alternative to fiat currency due to their inherent features such as anonymity/pseudonymity, global reach, absence of face-to-face contact, and high speed of transfer. The use of anonymity enhanced coins, "mixers" or "tumblers", Internet Protocol (IP) anonymizers and Invisible Internet Project (I2P) may further obfuscate transactions inhibiting customer identification and implementation of preventive measures by VASPs, making the channel attractive for criminals.

The 2021 NRA identified Al-Shabaab, ISIS and Lone Wolf actors as the major terrorist actors in the region. There has been no direct information available that links these actors to the usage of VAs to finance their attacks and operations. However, the United Nations Counter-Terrorism Committee Executive Directorate (UN-CTED) observed a rising trend where VAs, online exchanges and wallets were abused for terrorism financing. Further, it was possible to make donations through the abuse of social media, hosting services, crowdfunding platforms[32]. Similarly, FATF observed that ISIL, Al Qaeda and affiliates increased their usage of VAs to raise and move funds in Africa, Europe and the Middle East[33]. In November 2022, the US Department of State in a media note offered rewards for information leading to the

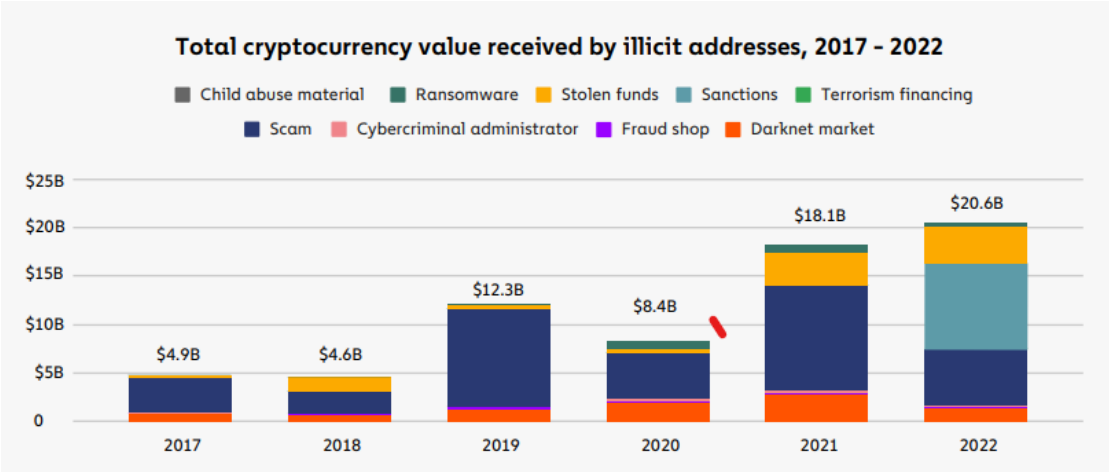
[32] https://www.un.org/securitycouncil/ctc/news/cted%E2%80%99s-tech-sessions-highlights-%E2%80%9Cthreats-and-opportunities-related-new-payment-technologies-0#:~:text=Examples%20of%20methods%20to%20raise,payments%20in%20fiat%20to%20cryptocurrencies)%2C

[33] https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/June2023-Targeted-Update-VA-VASP.pdf.coredownload.inline.pdf

identification and disruption of significant sources of revenue for Al-Shabaab, including the exploitation of VASPs[34].

Nevertheless, UN-CTED noted that cash and Hawala were the prevalent methods used to finance terrorism. This was equally supported by *The 2023 Crypto Crime Report* by Chainalysis, which highlighted that cryptocurrency was still not a preferred method for terrorist financing[35].

Figure 42: Total Crypto Value Received by Illicit Addresses, 2017-2022



Source: The 2023 Crypto Crime Report by Chainalysis

The TWG established that there were no TF cases reported by authorities in Kenya. However, there still exists a possibility of the TF actors in the region exploiting the VAs and VASPs to support their activities and operations.

In view of the foregoing, the overall TF threat exposure for VAs/VASPs for the country was rated as **Low** as shown below.

[34] https://www.state.gov/rewards-for-justice-reward-offers-for-information-on-key-leaders-of-al-shabaab-ahmed-diriye-mahad-karate-and-jehad-mostafa-and-the-disruption-of-its-financial-mechanisms/

[35] *The 2023 Crypto Crime Report* by Chainalysis

Table 6: VA/VASP TF Threat Exposure

VASP/SERVICE/CHANNEL			**VA/VASP TF THREAT RATING**
VASP	**Type of Services**	**Channel**	**Threat**
Virtual Asset Wallet Providers	Custodial Services	Hot Wallet	Medium
	Non-custodial Services	Cold Wallet	Medium
Virtual Asset Exchanges	Transfer Services	P2P	High
		P2B	Low
	Conversion Services	Fiat to Virtual	Medium
		Virtual to fiat	Medium
		Virtual to virtual	High
Virtual Asset Broking/ Payment Processing	Payment Gateway	Merchants	Low
Virtual Asset Investment Providers	Trading Platforms	Platform Operators	Low
		Non-Security Tokens & Hybrid Trading Activities	Low
		Stablecoins	Low
Overall VA & VASPs TF Threat			**Low**

6. VA/VASP Vulnerability Assessment

This section highlights the vulnerability assessment of both VAs and VASPs in the Kenyan ecosystem with regard to ML and TF. The assessment considered intermediate and input variables of vulnerabilities from a domestic and international perspective from various VASPs.

6.1 Vulnerability Assessment Overview

The analysis traced 66 VASPs accessed by Kenyans which offered multiple services. These VASPS fall under the following four (4) FATF-recognized VASP categories—

(i) Virtual asset wallet providers;

(ii) Virtual asset exchanges;

(iii) Virtual asset broking/payment processing; and,

(iv) Virtual asset investment providers.

Notably, out of the 66 VASPs, 49 were virtual asset exchanges, 42 were virtual asset wallet providers, 12 were virtual asset investments providers, and 2 offered virtual asset broking services. All the VASPs identified were neither registered nor licensed in the country owing to the absence of a VA/VASP regulatory framework. However, some were registered with the Business Registration Services (BRS) as Fintech companies whereas, others had misrepresented their business operations.

Globally, several cases of VASPs being used to launder illicit proceeds and finance terrorism through their products and services were noted.

Upon assessment, the country's vulnerability exposure for VASPs with regards to ML and TF were both established to be **High and Medium,** respectively. The assessment of VASPs considered the products and services provided, and the types of VASPs with the input variables highlighted below.

6.1.1 Products & Services Provided, and the Types of VAs

(i) Licensed in the country or abroad

The current AML/CFT legal framework in Kenya does not impose any limitations on the operations of VASPs licensed abroad. Additionally, there are no legal provisions that prohibit entities or individuals from functioning as VASPs, regardless of whether they are licensed overseas or unlicensed. Therefore, it is not possible to establish the fitness and propriety of the VASPs or assess their knowledge and measures concerning ML/TF risk. The lack of legislation governing VASPs in Kenya also means that it is not possible to establish the extent of transparency in the structure and shareholding of VASPs.

Survey responses from VASPs operating in Kenya indicated that they are licensed in other jurisdictions such as the UK or USA, where they are required to implement AML/CFT measures irrespective of the jurisdiction they operate in. However, Kenya cannot verify the effectiveness of such measures as it lacks a legislative framework to supervise them.

(ii) Nature, size, and complexity of business

The VASPs operating in the Kenyan ecosystem were noted to be diverse with some offering a single VA product while others offered multiple VA products including anonymity-enhanced VAs like Monero. All the VAs assessed had cross-border operations thereby allowing interaction with international customers from both regulated and unregulated jurisdictions. However, two Kenyan VASPs had plans to launch VA provision services through real estate tokenization.

(iii) Products and services

Anonymity-enhanced VAs, mixers, tumblers, and decentralized platforms increase the risk associated with VASPs because they facilitate reduced transparency and increased obfuscation of financial flows.

Given the absence of a regulatory framework in the country and the lack of supervisory authority, it was not possible to assess and verify the effectiveness of the VASPs' quality of internal oversight, the level of compliance with AML/CFT measures, and the quality of risk management with regards to products and services offered.

(iv) Method of delivery of products/services

Some of the products and services offered by VASPs such as privacy coins have enhanced anonymity, are cross-border and lack face-to-face interaction. The survey noted that Kenyans were able to access services from VASPs that had geo-blocked the Kenyan market. This is a possible indication of the use of IP anonymizers which may obfuscate transactions or financial flows and prevent the VASPs from identifying its customers to implement effective AML/CFT measures.

In contrast, the survey indicated that VASPs had appropriate measures to identify and verify their customers. Furthermore, VASPs applied additional measures to collect identity information to help in the identification of high-risk customers, for instance, IP address and associated time stamp, geolocation data, device identifiers, VA wallet addresses, transaction hashes, and transaction history. This was useful in further analysis of high-risk customers, and geo-restricting access to services from specific jurisdictions.

(v) Customer types

It was noted that there was a high likelihood of customers accessing VASPs such as virtual assets, virtual asset wallets, and virtual asset investment providers to exploit these platforms for ML and TF given the prominent adoption of peer-to-peer transfer, virtual to virtual transfer, and stablecoins. However, the data collected from VASPs indicated that they carry out CDD and implement risk management of their own volition or based on the regulations in the country of origin.

(vi) Country Risk

The geographical location of Kenya makes the country one of the most attractive investment destinations in the region. Furthermore, its proximity to UN-sanctioned countries, the populace's appetite for VAs, the absence of a regulatory framework, and non-adoption of the travel rule for VASPs exposes Kenya to an increased vulnerability to ML/TF risks.

From the survey conducted, VASPs indicated that they implement risk management on their own volition or based on the regulations in the country of origin. Financial services regulators issued cautionary statements and circulars to reporting institutions prohibiting them from direct engagement with VASPs.

Institutions Dealing with VASPs

VASPS can act as intermediaries hence exposing them to other VASPs that might have insufficient AML/CFT controls. However, most of the VASPs respondents indicated that they had measures to flag and investigate transactions involving mixing or tumbling services.

(vii) Rapid Transaction Settlement

The accessibility of VASPs that have rapid settlement VAs exposes the country to a high likelihood of ML and TF. However, following the cautionary notices issued by financial sector regulators, there had been no integration between the financial sector and VASPs for purposes of correspondent banking, thereby mitigating the risk of rapid transaction settlement.

(viii) Dealing with Unregistered VASP from Overseas

Most of the VASPs accessed by Kenyans were registered overseas. Kenya does not have a regulatory framework to license, register, or supervise VASPs thus posing a high vulnerability for the VASPs to be exploited for ML and TF. Furthermore, the borderless nature of VAs and VASPs provides an avenue for dealing with unregistered VASPs thus limiting the transparency of the VASP activities and governance structure.

6.2 ML Vulnerability Assessment

The overall ML vulnerability assessment for both VA and VASPs was established to be **High.** In assessing the ML vulnerability, the TWG considered the following:

(i) The 11 VASP types/channels identified to be operating in Kenya; and,

(ii) The vulnerability of different types of VAs accessed by Kenyans.

The assessment covered the factors that could attract criminals to opt for one type of VA or VASP over another for ML purposes. Below are detailed summaries of the vulnerabilities assessed for both VAs and VASPs.

6.2.1 VASP ML Vulnerability

Table 7: VASP ML Vulnerability Rating

VASP/Service/Channel			**VASP ML Risk Rating**
VASP	**Type of Services**	**Channel**	**Vulnerability**
Virtual Asset Wallet Providers	Custodial Services	Hot Wallet	High
	Non-custodial Services	Cold Wallet	High
Virtual Asset Exchanges	Transfer Services	P2P	High
		P2B	High
	Conversion Services	Fiat-to-Virtual	High
		Virtual-to-Fiat	High
		Virtual-to-Virtual	High
Virtual Asset Broking/Payment Processing	Payment Gateway	Merchants	Medium
Virtual Asset Investment Providers	Trading Platforms	Platform Operators	Medium
		Non-Security Tokens & Hybrid Trading Activities	Medium
		Stablecoins	High
Overall VASPs ML Risk			**High**

In view of the foregoing, the **High** vulnerability identified in the distribution channels was attributed to the inherent nature of VAs, the current Kenyan VA and VASP ecosystem, and their previous exploitation for ML domestically and globally**.**

6.2.2 VA Type Vulnerability

The overall VA vulnerability rating for ML was therefore found to be **High** based on the inherent vulnerabilities, notably anonymity/pseudonymity, irreversibility of transactions, difficulties in implementation of the travel rule, and the previous exploitation for ML globally and domestically. This is illustrated below.

Table 8: Vulnerability per VA Type

VA Type	Sub-type	Vulnerability
Exchange VAs	Anonymous/Pseudonymous	High
	Platform	Medium
	Stablecoins	High
Utility VAs	Utility	Low
Security VAs	Security	Medium
	Platform with Security features	Low

6.3 TF Vulnerability Assessment

The exposure of VASPs for TF purposes was covered in two parts: the vulnerability of different types of VAs, and VASP vulnerability assessment. The assessment covered the factors that could attract criminals to select one type of VA or VASP over another for TF purposes.

The survey respondents indicated minimal usage of anonymous coins. According to CoinTelegraph, an ISIS-affiliated news website linked to a jihadist movement solicited funds in 2020[36].

Based on the inherent characteristics of the VASPs operating in the Kenyan ecosystem, and taking into consideration the scalability, usability and security of various VAs and VASPs, the TF vulnerability was assessed as **Medium** as shown in the table below.

[36] https://cointelegraph.com/news/no-isis-does-not-have-300m-in-a-bitcoin-war-chest

Table 9: VA/VASP TF vulnerability Rating

VASP/Service/Channel			VA/VASP TF Vulnerability Rating
VASP	**Type of Services**	**Channel**	**Vulnerability**
Virtual Asset Wallet Providers	Custodial Services	Hot Wallet	High
	Non-custodial Services	Cold Wallet	High
Virtual Asset Exchanges	Transfer Services	P2P	High
		P2B	Medium
	Conversion Services	Fiat to Virtual	Medium
		Virtual to fiat	Medium
		Virtual to virtual	High
Virtual Asset Broking/Payment Processing	Payment Gateway	Merchants	Medium
Virtual Asset Investment Providers	Trading Platforms	Platform Operators	Medium
		Non-Security Tokens & Hybrid Trading Activities	Low
		Stable Coins	Low
Overall VA & VASPs TF Risk			**Medium**

7. Mitigation Measures

7.1 Government Measures

7.1.1 Comprehensiveness of AML/CFT Framework

Kenya has no AML/CFT legal and regulatory framework governing VAs/VASPs. However, POCAMLA defines property as "… *tangible or intangible*...". Therefore, VAs may be broadly interpreted to include intangible property under Section 2 of the POCAMLA. Additionally, financial sector regulators issued circulars to reporting institutions prohibiting the usage of VAs/VASPs and notices to the public warning them against engaging with VAs/VASPs related activities.

7.1.2 Availability and Effectiveness of Entry controls

The lack of entry controls such as licensing, registration, regulation, and other forms of authorization for VASPs to operate, increases the country's vulnerability to ML/TF. VASPS can open mule companies in the absence of any regulations or even operate from different jurisdictions to serve the Kenyan market due to the cross-border nature of their operations. This further exacerbated the ML/TF risk posed by the unregistered and unlicensed VASPs.

7.1.3 Adequate Supervision and Monitoring Mechanism

Kenya has no adequate legal or regulatory requirement for supervision or monitoring of VASPs and there is no competent authority tasked with regulating and supervising VASP operations. Furthermore, VASPs are not designated as reporting institutions under POCAMLA.

7.1.4 Regulation for CDD, Source of Funds and Availability of Reliable Identification Infrastructure

As per FATF Recommendations 10 and 15, VASPs are required to undertake CDD measures and scrutinise of the source of funds as an effective way of mitigating ML/TF risks. However, the existing AML/CFT legal and regulatory framework does not recognize VASPs as reporting institutions, and therefore VASPs are not required to undertake CDD and counterparty VASP due diligence.

7.1.5 Financial and Human Resource Capacity of LEAs to Investigate, Trace, Seize and Secure VA's

There have been efforts on the capacity of LEAs to investigate, trace, seize, and secure VAs. However, LEAs had inadequate skillset and tools for forensic investigations on VA transactions and DLT.

7.1.6 Effectiveness of International Cooperation

Kenya has an adequate framework for seeking international cooperation from and providing cooperation to LEAs in other jurisdictions with regard to criminal cases including VA cases. Kenya can successfully get information relating to VAs and VASPs from foreign jurisdictions based on MLA, MOUs, and other forms of international cooperation.

7.1.7 Quality of Guidance Issued to VASPs and Engagement with VASPs

Kenya does not have a competent authority to supervise and monitor the activities of VASPs. Therefore, no AML/CFT guidance had been issued to VASPs to enable them to understand ML/TF risks associated with VAs in the Kenyan ecosystem, put in place appropriate mitigation measures, and ensure compliance with AML/CFT requirements. However, financial sector regulators have been keeping abreast of emerging technologies and their potential benefits and risks to the financial sector, for instance, CBK issued a *Technical Paper on Crypto Assets* as an annex to the report on *Discussion Paper on Central Bank Digital Currency: Comments from the Public*.[37]

7.2 VASP Mitigating Measures

7.2.1 Transparency and Shareholder Structure

The Companies Act requires that a company must always disclose BOs and file returns as prescribed, which can be used to identify the shareholders. Responses received from the VASPs indicated that they held information pertaining to shareholders, investors, and other stakeholders. However, since they were not under the purview of any competent authority, this was not verifiable. It is possible that such information was available in the jurisdictions where they were registered/licensed.

7.2.2 Quality of Governance Structures and Level of Accountability of VASPs

VASPs' responses to the survey indicated they had put in place technological governance structures that ensured legitimacy and regular verification of information system integrity. Most of the VASPs also indicated that they had policies and procedures to ensure the safety of cryptographic keys and for AML/CFT. However, since they were not under the purview of any competent authority, this information was not verifiable.

7.2.3 Effectiveness of Compliance Function and Internal Control Mechanism

From the survey, VASPs indicated they had effective compliance functions that understood ML and TF risk and had implemented preventive and responsive measures through internal

[37] https://www.centralbank.go.ke/wp-content/uploads/2023/06/Discussion-Paper-on-Central-Bank-Digital-Currency-Comments-from-the-Public.pdf

control mechanisms. However, since they were not under the purview of any competent authority, this information was not verifiable.

7.2.4 AML/CFT Knowledge of VASP Staff

Responses from VASPs indicated that they on-going training programs to ensure their staff were aware of AML/CFT laws, policies and procedures, risks and mitigations, and identification of suspicious transactions.

7.3 TOEs/Reporting Institutions' Control Measures

7.3.1 Risk Assessment and Risk Mitigation Measures by TOEs/Reporting Institutions

From the TOEs' survey responses, only 16% of the respondents had identified and assessed ML/TF risks related to new and existing customers, products and services related to interaction with VAs/VASPs. Most of the TOEs de-risked customers identified to be dealing in VAs based on the circulars from regulators. TOEs noted that though their controls were optimal, VASPs could circumvent the mitigations by using mules and disguising their nature of business. Those who conducted risk assessments noted that they carried the residual risk of unknowingly facilitating VA settlements via P2P mechanism or providing traditional financial services to customers who disguised their business activities.

Other risk mitigation measures taken by TOEs included training and guidance on identifying and managing ML/TF risks associated with VAs/VASPs, and adoption of transaction monitoring systems to detect and report suspicious activities related to VAs/VASPs.

7.3.2 Effectiveness of Compliance Functions and Internal Control Mechanism

TOEs had compliance functions and internal control mechanisms to mitigate against ML/TF risks related to the nature of their businesses. However, the TWG observed that majority of TOEs had not employed technology solutions to detect transactions associated with criminal activities involving VA/VASP activities.

7.4 Rating of Mitigation Measures

Based on the foregoing, the ratings of mitigation measures were ranked **Medium** as highlighted below.

Table 10: Mitigation Measures

Mitigation Measure		Rating
Government measures	Comprehensiveness of AML/ CFT Legal Framework	Does not exist
	Availability and Effectiveness of Entry Controls	Does not exist
	Adequate Supervision & Monitoring Mechanism	Does not exist
	Regulation for CDD and source of funds & Availability of Reliable Identification Infrastructure	Does not exist
	Financial and human resource capacity of law enforcement authorities to investigate, trace, seize and secure virtual assets	Low Mitigation
	Effectiveness of international cooperation	Medium Mitigation
	Quality of guidance issued to VASPs and engagement with VASPs	Does not exist
VASP measures	Transparency of shareholder Structure of VASP	Low Mitigation
	Quality of Governance structure and Level of accountability of VASP	Low Mitigation
	Effectiveness of compliance function and internal control mechanism	Medium Mitigation
	AML/ CFT knowledge of VASP staff	Medium Mitigation
Financial Institution (FI) Measures and Designated Non-Financial Businesses and Professions (DNFBPs)	Risk assessment and Risk Mitigation measures by Financial Institutions (FIs) and DNFBPs. Referred in this guidance as Traditional Obliged Entities (TOE)	Medium Mitigation
	Effectiveness of compliance function and internal control mechanism	High Mitigation
Overall Rating of Mitigation Measures		**Medium**

8. Overall VA/VASP ML/TF Country Risk

In view of the threats and vulnerabilities as well as mitigating measures, the overall ML risk rating for VAs and VASPs in Kenya was **Medium** while the TF risk was rated as **Low**. Several factors have contributed to these risks, including the utilization of anonymity-enhanced VAs, accessibility to the dark web, adoption of P2P mechanism, complex traceability of VAs, speed of transactions and a notable susceptibility to tax evasion, among others. Additionally, a larger percentage of VASPs operating in the country effectively applied AML/CFT measures based on the parent jurisdiction regulations and compensated for any risks introduced by the cross-border nature of transactions thus significantly determining the overall risk rating for ML and TF.

A larger percentage of Kenyans had not ventured into VAs because they are not regulated, and the financial regulators had issued cautionary notices coupled with insufficient knowledge. The limited understanding of virtual assets amongst Kenyans may further reduce the risk of ML/TF, as criminals may not be aware of the opportunities to exploit for illicit purposes. Kenyans typically perceived virtual assets (VAs) as inherently risky and tended to avoid investing their money in such ventures, while others found alternative investment opportunities more appealing thus reducing the overall ML/TF risk.

A few cases of money laundering had been reported in the country, while no cases related to terrorism financing had been reported by the time of risk assessment. Moreover, some of the VAs and VASPs in use by Kenyans had been exploited for ML and TF in other jurisdictions. All these factors were taken into consideration in assessing the overall country ML/TF risk of VAs/VASPs. Below is a summary of the overall VA/VASP ML/TF National Risk Rating for Kenya.

Table 11: Overall VA/VASP ML/TF Risk

VASP/SERVICE/CHANNEL			OVERALL VA/VASP ML/TF RISK RATING									
VASP	**Type of Services**	**Channel**	**Threat**		**Vulnerability**		**Inherent Risk**		**Mitigating Measures**		**Risk Score after Mitigating Measures**	
			ML	**TF**	**ML**	**TF**	**ML**	**TF**	**ML**	**TF**	**ML**	**TF**
Virtual Asset Wallet Providers	Custodial Services	Hot Wallet	Medium	Medium	High	High	High	High	Medium	Medium	Medium	Medium
	Non-custodial Services	Cold Wallet	High	Medium	High	High	High	High	Medium	Medium	High	High
Virtual Asset Exchanges	Transfer Services	P2P	High	High	High	High	High	High	Medium	Medium	High	High
		P2B	Medium	Low	High	Medium	Medium	Medium	Medium	Medium	Medium	Low
	Conversion Services	Fiat to Virtual	Medium	Medium	High	Medium	High	Medium	Medium	Medium	Medium	Medium
		Virtual to Fiat	High	Medium	High	Medium	High	Medium	Medium	Medium	Medium	Medium
		Virtual to Virtual	High	High	High	High	High	High	Medium	Medium	High	High
Virtual Asset Broking/Payment Processing	Payment Gateway	Merchants	Low	Low	Medium	Medium	Medium	Medium	Medium	Medium	Medium	Low
Virtual Asset Investment Providers	Trading Platforms	Platform Operators	Medium	Low	Medium	Medium	Medium	Medium	Medium	Medium	Medium	Low
		Non-Security Tokens & Hybrid Trading Activities	Medium	Low	Medium	Low	Medium	Low	Medium	Medium	Medium	Low
		Stablecoins	Medium	Low	High	Medium	High	Medium	Medium	Medium	Medium	Low
Overall VAs & VASPs Risk			**Medium**	**Low**	**High**	**Medium**	**High**	**Medium**	**Medium**	**Medium**	**Medium**	**Low**

9. Conclusion

The NRA exercise confirmed the growing interest in VAs and VASPs activities in the country. However, the use of virtual assets, is still lower in terms of widespread adoption compared to other traditional financial forms. Factors such as technological infrastructure, regulatory frameworks, security concerns, high volatility, knowledge, and public trust play significant roles in the adoption of virtual assets. The relatively lower overall transaction value of virtual assets compared to other forms, coupled with the widespread use of cash and mobile money in Kenya, contributes to reducing the overall ML/TF risk for VAs and VASPs. In addition, the mitigating measures by different stakeholders were partly efficient in mitigating VA/VASP related ML/TF risks. However, the inherent nature of VAs and VASPS, coupled with their cross-border nature and lack of regulation, may increase the risk. Accordingly, the country should regulate VAs/VASPs in order to address the identified ML/TF and other risks and to strengthen the AML/CFT posture.

Annex I: Select VA/VASP Regulations by Other Jurisdictions

1. United Kingdom

Primary regulator with mandate – Financial Conduct Authority. FCA guidance CP 19/3 and PS 19/12 lay out the different market participants and the kind of the activities that would be regulated which includes e-money, securities and stable coins. The Financial Services Market Law contains provisions on stable coin and crypto currency.

2. United States

Regulations vary by state. ICOs and Crypto currency sales are only regulated by Security Exchange Commission (SEC) if they constitute the sale of a security under state of Federal Law or are considered money transmission under state law or an action that would make a person a money services under Federal Law. There is no overall regulatory authority. 2013 - FinCEN has issued guidance under BSA specifying that VASPs must register as MSBs. 2014 - IRS issued guidance on taxation of Virtual currencies, there is a task force created to look into transnational tax crimes and ML that extends to crypto. 2015 – New York State became the first to regulate. 2020 – US AML/CFT law updated with amendments to cover the VAs. 2022- enactment of Responsible Financial Innovation Act to give authority to Commodities Futures Trading Commission (CFTC) and clarify SEC roles. The Keep your Coins Act provides the legal framework for use of convertible virtual currencies.

3. Malta

Cryptocurrencies are legal and regulated under Virtual Financial Assets Act with additional regulation to come up with implementation of MiCA in 2023 and 2024. 2018 – passed 3 laws that form basis of cryptocurrency legislation: Digital Innovation Authority Act, The Innovative Technology Arrangements and Services Act and Virtual Financial Act. These provides regulations on the Prevention of ML/TF and amended the 1994 Prevention of ML Law.

4. South Africa

Cryptocurrency is legal in SA. 2022 – Financial Advisory and Financial Intermediary Services Act (FAIS) was amended to include appropriate definitions of crypto assets as Financial Products, create licensing, AML/CFT and consumer protection obligation for crypto asset providers. There is SARB cautionary statement in 2014 and it must be noted that cryptocurrencies are not recognized as legal tender in South Africa. Primary regulator is Financial Conduct Services Authority (FCSA).

5. Egypt

Central Bank issued a warning in 2020 stating that trading crypto without a license was an offence. However, the country has also taken a cautious approach, given the potential *Haram*

issues related to crypto assets, as guided by their religious bodies. The central bank was working on crypto regulations in 2020 but these have not been finalised.

6. Botswana

Feb 2022 – enacted an Act to regulate the sale and trade of VAs, licensing of VASPs and issuers of ITOs.

7. Rwanda

Partial ban – Central Bank issued a cautionary notice banning regulated Financial Service Providers from facilitating crypto transactions until a regulatory framework is in place.

8. Nigeria

Partial ban – Central Bank issued a cautionary notice banning FIs from using holding, or trading in crypto assets. 2021 – the central bank ordered local FIs to shut down all bank accounts associated with crypto trading claiming citing use for ML/TF. Ranks 11th globally in crypto adoption. 2022 – Launched the CBDC in Naira. Plans under to develop a regulatory framework.

9. Uganda

Not banned however, it is not considered a legal tender and the government has not licensed any entity to sell or facilitate trading in crypto.

(a) June 2021 – Central Bank launched a regulatory sandbox framework allowing Fintechs to test innovative financial solutions in a controlled sand box.

(b) 2022 – Central Bank sent notices to all payment providers in the country warning them against crypto transactions as they are an avenue for ML and scams.

(c) Dec 2020 – Financial Intelligence Authority (FIA) published a letter amending the AML act to include VASPs among the list of accountable persons subject to supervision and monitoring by FIA.

10. Namibia

2023 – enacted the VAs Act which requires a regulator to oversee crypto set ups and includes licensing requirements VASPs. Lays groundwork for more comprehensive laws. Is yet to designate a regulator to oversee VASPs activities and to take effect.

11. Tanzania

2017 – cryptocurrencies are not recognized as legal tender in the country.

12. Seychelles

Completed the VAs and VASPs ML/TF risk assessment in 2022. Legal regime for regulation still in development and ICOs and not regulated.

13. Mauritius

Has in place the VAs and ITOs Act. Completed the VAs and VASPs ML/TF risk assessment between 2021 – 2022. The residual risk rated as very high. Proposed mitigations included putting in a place a legal and regulatory framework for VAs and VASPs.

14. China

2021 - Declared all cryptocurrency related transactions as illegal objective being to maintain National Security and Social Stability.

15. Morocco

2017 – General ban on the back of foreign exchange controls and have introduced penalties and fines.