THE REPUBLIC OF UGANDA

NATIONAL MONEY LAUNDERING AND TERRORISM FINANCING RISK ASSESSMENT REPORT ON VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS FOR UGANDA

SEPTEMBER 2025

TABLE OF CONTENTS

06 Va and vasp interaction with traditional obliged entities

07 Key findings

08 Uganda's policy options for virtual asset service providers under fatf recommendation

A "Virtual Asset" is any digital representation of value that can be traded or transferred online and used for payment or investment. Digital forms of fiat currency, securities, or other financial assets are not regarded as VAs.

LIST OF FIGURES

LIST OF TABLES

ACRONYMS

ACAMS	Association of Certified Anti-Money Laundering Specialists
AEV	Anonymity Enhanced Virtual
ALCTR	Attempted Large Cash Transaction Report
AML	Anti-Money Laundering
AMLA (Cap 118)	Anti-Money Laundering Act (Chapter 118, Laws of Uganda)
ARINSA	Asset Recovery Inter Agency Network of Southern Africa
ATM	Automated Teller Machine
BO	Beneficial Ownership (or Beneficial Owner)
BoU	Bank of Uganda
CBDCs	Central Bank Digital Currencies
CDD	Customer Due Diligence
CFCS	Certified Financial Crime Specialist
CEX	Centralised Exchange
CFT	Combating the Financing of Terrorism
CID	Criminal Investigations Directorate
CMA	Capital Markets Authority
DLT	Distributed Ledger Technology
DeFi	Decentralised Finance
DEX	Decentralised Exchange
DNFBP	Designated Non-Financial Businesses and Professions
DPMS	Dealers in Precious Metals and Stones
ESAAMLG	Eastern and Southern Africa Anti-Money Laundering Group
FATF	Financial Action Task Force
FIA	Financial Intelligence Authority (Uganda)
FIU	Financial Intelligence Unit
FITSPA	Financial Technologies Service Providers Association
GCCS	Global Centre on Cooperative Security
goAML	IT platform used by FIUs to receive/analyse STRs/SARs
IG	Inspectorate of Government
ICO	Initial Coin Offering
IVO	Initial Virtual Asset Offering
IMF	International Monetary Fund
IP	Internet Protocol
ISCAP	Islamic State – Central Africa Province
IWTR	International Wire Transfer Report
KYC	Know Your Customer
LATF	Lusaka Action Taskforce
LCTR	Large Cash Transaction Report

LEA(s)	Law Enforcement Agencies
ML/TF	Money Laundering / Terrorist Financing
MoFPED	Ministry of Finance, Planning & Economic Development
MoJCA	Ministry of Justice and Constitutional Affairs
NFT	Non-Fungible Token
NITA-U	National Information Technology Authority – Uganda
NPS Act	National Payment Systems Act, 2020
ODPP	Office of the Director of Public Prosecutions
OECD	Organisation for Economic Co-operation and Development
OFAC	Office of Foreign Assets Control
P2P	Peer-to-Peer
PEP	Politically Exposed Person
PF	Proliferation Financing
PSO	Payment System Operator
R.1 / R.15	FATF Recommendation 1 / FATF Recommendation 15
RBA	Risk Based Approach
RBS	Risk Based Supervision
RFSP	Regulated Financial Service Provider
SAR	Suspicious Activity Report
STO	Security Token Offering
STR	Suspicious Transaction Report
TF	Terrorist Financing
TOE	Traditional Obliged Entities
UCC	Uganda Communications Commission
URA	Uganda Revenue Authority
URSB	Uganda Registration Services Bureau
USD	United States Dollar
UWA	Uganda Wildlife Authority
VA (plural VAs)	Virtual Asset(s)
VASP	Virtual Asset Service Provider
VPN	Virtual Private Network
WG	Working Group

FOREWORD by the Minister

The Government of Uganda remains unwavering in its commitment to Countering Money Laundering, Terrorism Financing, and other financial crimes that threaten the integrity of the national and global financial systems.

The global evolution of digital technologies in the financial sector has led to the emergence of Virtual Assets which are not any established legal and regulatory framework.

Virtual Assets have gained prominence as transformative financial instruments, and Ugandans are actively participating in this trend. The increasing adoption of Virtual Assets (VAs) and the rise of Virtual Assets Service Providers (VASPs) within Uganda have underscored the need to thoroughly examine and comprehend the risks associated with these emerging technologies.

While the use of VAs and VASPs offers considerable opportunities, it also introduces substantial risks, particularly in the context of Money Laundering and Terrorist Financing. This assessment serves as a foundational step in addressing these concerns, ensuring that Uganda's financial system remains secure, reliable, and positioned for sustained growth in an increasingly competitive global environment.

This report therefore, presents Uganda's inaugural comprehensive National Money Laundering and Terrorism Financing Risk Assessment on VAs and VASPs, aligned with the Financial Action Task Force (FATF) Recommendations 15 and 1, and marks a significant milestone in safeguarding the financial sector.

The findings of this report underscore Uganda's dedication to adopting International Standards in the fight against Money Laundering/Terrorism Financing (ML/TF) and other financial crimes. This Assessment demonstrates Uganda's determination to establish a robust regulatory framework that encourages technological advancement as well as upholding the integrity of the financial system. Striking this balance is essential for fostering an environment where legitimate investments and businesses can thrive, and innovation flourishes, within a framework of effective oversight.

Uganda has proactively identified vulnerabilities, and counter-measures to mitigate the risks posed by Virtual Assets and VASPs to support responsible growth of digital financial services. I believe this approach, will strengthen public confidence in the financial system and facilitate the adoption of digital financial technologies in a manner that aligns with regulatory expectations. Implementation of the recommendations in this report is expected

to reinforce Uganda's ability to combat Money Laundering, Terrorism Financing and other financial crimes, in addition to attracting legitimate investments, and drive economic growth.

I therefore, extend my sincere gratitude to the Financial intelligence Authority, MDAs, and other stakeholders who dedicated their time and expertise to this critical exercise. I also acknowledge the support rendered during the finalization of this Assessment by the World Bank, United Nations Office on Drugs and Crime, and the commercial blockchain analytics company.

Finally, I call upon all stakeholders to implement the actions and measures identified in the report to ensure that Uganda's financial system is well prepared to counter the challenges posed by the rapidly evolving digital economy, including complying with International Standards.

Matia Kasaija (MP)
MINISTER OF FINANCE, PLANNING AND ECONOMIC DEVELOPMENT

> ***"Virtual Assets have gained prominence as transformative financial instruments, and Ugandans are actively participating in this trend. The increasing adoption of Virtual Assets (VAs) and the rise of Virtual Assets Service Providers (VASPs) within Uganda have underscored the need to thoroughly examine and comprehend the risks associated with these emerging technologies."***

FOREWORD by the Executive Director, FIA

> ***The adoption of Virtual Assets as an innovative financial tool presents both opportunities and challenges, as their growing use signals technological progress and new investment potential, yet it also raises concerns, particularly in the areas of money laundering and terrorist financing.***

The fight against money laundering, terrorist financing, and related financial crimes remains a priority for the Government of Uganda, recognising the critical importance of maintaining the stability, integrity, and resilience of our financial system. With the increasing use of Virtual Assets (VAs) and the rise of Virtual Asset Service Providers (VASPs) in Uganda, it is essential to understand the associated risks and develop robust measures to address them. This report, Uganda's first comprehensive national risk assessment of VAs and VASPs, reflects our commitment to tackling these challenges in alignment with the global standards set out in FATF Recommendations 15 and 1.

The adoption of Virtual Assets as an innovative financial tool presents both opportunities and challenges, as their growing use signals technological progress and new investment potential, yet it also raises concerns, particularly in the areas of money laundering and terrorist financing.

This ML/TF risk assessment has identified vulnerabilities within the VA ecosystem and the unregulated activities of many VASPs, while also highlighting the emerging shadow financial system created by the restriction of VA transactions in the formal financial sector, underscoring the need for coordinated efforts to address these gaps.

Through this exercise, Uganda has demonstrated its commitment to international best practices by taking the first step toward establishing a comprehensive regulatory framework for VAs and VASPs. The findings emphasise the need to balance innovation with

financial integrity, which is crucial for fostering trust and confidence in our financial sector. When implemented, the proposed measures will not only help mitigate ML/TF risks but will also position Uganda as a responsible and competitive player in the rapidly evolving digital financial space.

This initiative goes beyond a compliance exercise and forms part of Uganda's broader strategy to strengthen the financial sector and enhance its reputation as a trusted and innovative financial hub. By addressing these risks proactively, Uganda can attract legitimate investment, promote economic growth, and encourage responsible innovation in the digital economy.

I would like to express my sincere gratitude to all the stakeholders who contributed to this important exercise, as their expertise and contributions have played an essential role in shaping the findings of this assessment and providing a solid foundation for the actions we will take moving forward.

Mr. Samuel Were Wandera
Executive Director Financial Intelligence Authority

EXECUTIVE SUMMARY

This first National Risk Assessment exercise of Money Laundering and Terrorist Financing risks of Virtual Assets and Virtual Asset Service Providers in Uganda builds on a comprehensive understanding of the threats and vulnerabilities associated with these emerging financial systems. It highlights the critical ML/TF impact they present and provides Ugandan authorities and the private sector with a solid foundation to address these risks. The findings aim to guide the development of appropriate actions at both the national and sectoral levels, ensuring the protection of the country, its citizens, businesses, and society against these unwanted risks. This assessment is a cornerstone of Uganda's commitment to meeting international AML/CFT standards and developing legislation dedicated to Virtual Assets and Virtual Asset Service Providers.

> *The findings aim to guide the development of appropriate actions at both the national and sectoral levels, ensuring the protection of the country, its citizens, businesses, and society against these unwanted risks.*

The assessment rated Uganda's overall ML/TF risks in this sector as high. This risk level was influenced by the mitigating measures put in place by the Bank of Uganda, which restricted all financial institutions and payment system operators—referred to in this report as traditional obliged entities—from facilitating the conversion of Virtual Assets into fiat currency or integrating them into the financial system. This measure significantly reduced the ML/TF risk exposure of Virtual Assets within the traditional financial sector, limiting their ability to exploit the regulated financial system for illicit activities. However, this mitigating measure also has a notable downside. By banning Virtual Asset transactions within the financial system, a shadow financial system has emerged, particularly involving stablecoins and traditional Virtual Assets like Bitcoin. These transactions operate outside the oversight of AML/CFT supervisors and law enforcement agencies, thereby increasing ML/TF risks in unregulated and unmonitored spaces.

The assessment found that while banks and Designated Non-Financial Businesses and Professions have limited direct involvement with Virtual Assets, their indirect exposure is significant, primarily due to weak prevention and detection mechanisms in traditional AML/CFT systems. The interconnectivity between traditional financial institutions and Virtual Asset activities, including their support of peer-to-peer transactions and Virtual Asset

Service Provider operations through fiat currency mediums, underscores the need for a proactive and forward-looking approach to regulation, oversight, detection and prevention of ML/TF. If left unaddressed, this evolving landscape could see traditional financial entities inadvertently facilitating unregulated activities, triggering systemic ML/TF risks that could adversely impact the broader economy.

Currently, Uganda lacks a licensing regime for Virtual Asset Service Providers, and this gap has enabled hundreds of unlicensed entities to operate within the Non-Banking Financial Institution sector. These entities offer a range of services, from token trading and cloud mining to decentralised exchange platforms, exploiting the absence of bespoke legislation and disclosure requirements. This has resulted in the emergence of a shadow financial system centreed around Virtual Assets, which must be urgently brought under regulatory oversight to prevent the exploitation of customers and preserve Uganda's reputation as a trustworthy financial hub.

The assessment also shed light on the types of Virtual Asset Service Providers operating in Uganda and the concerns raised about them by international regulators and organisations such as Interpol. Many of these providers offer services related to Bitcoin, Ethereum, stablecoins and privacy coins, in addition to cloud mining, decentralised finance exchanges, and non-fungible tokens. These activities have given rise to new market participants, including Virtual Asset exchanges and investment service providers, which cater not only to retail clients but also to institutional investors such as investment funds. These entities require close regulatory scrutiny and should be subjected to oversight frameworks consistent with AML/CFT legal requirements and FATF recommendations to ensure their operations do not pose undue risks.

The findings of the assessment highlight the urgent need for Uganda to develop and implement a comprehensive regulatory framework for Virtual Assets and Virtual Asset Service Providers. This includes establishing a licensing regime, strengthening cross-sector collaboration for monitoring and oversight, and enhancing AML/CFT measures to address the specific challenges posed by these financial innovations. Improved customer due diligence, transaction monitoring, and public awareness campaigns are critical components of this effort.

The findings of the assessment highlight the urgent need for Uganda to develop and implement a comprehensive regulatory framework for Virtual Assets and Virtual Asset Service Providers.

Key DEFINITIONS

Virtual Asset

As defined by the FATF, a "Virtual Asset" is any digital representation of value that can be traded or transferred online and used for payment or investment. Digital forms of fiat currency, securities, or other financial assets are not regarded as VAs.

VAs possess distinct technological attributes that enable pseudo-anonymous and anonymous transactions, rapid cross-border value transfers, and remote (non-face-to-face) business relationships. These capabilities can enhance an array of financial products and services, including trade finance, international payments, and the settlement of financial instruments.

Global typologies reveal that organised criminal groups may exploit VAs to obtain laundered proceeds by making numerous deposits and withdrawals. It is not only cybercriminals who utilise VAs, other criminal enterprises, such as drug traffickers, also use them to move and launder illicit proceeds. VAs allow these groups to access cash discreetly and conceal transaction histories, and criminals may gain control of e-wallets or withdraw cash from ATMs.

Some VAs, such as Monero, are structured as privacy coins to hide the identities of both sender and recipient, as well as the transaction details. These VAs directly challenge customer due diligence measures, making them particularly attractive to criminals. Additionally, the use of mixing and tumbling services suggests attempts to mask the flow

of illegal funds between wallet addresses and darknet markets.

Virtual Asset Service Provider

"Virtual Asset Service Provider," according to the FATF, is a natural or legal person who is not covered elsewhere under the FATF 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:

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 Providers

Virtual Asset Wallet Providers are entities that offer a virtual asset wallet for holding, storing, and transferring bitcoins or other virtual assets. These providers enable users, exchangers, and merchants to participate more easily in a VA system by maintaining the customer's virtual asset balance and generally ensuring storage and transaction security. Well-known Wallet Providers include Bitcoin Core protocol, Electrum, Exodus, Jaxx, Coinbase, and Blockchain.

Virtual Asset Exchanges

Virtual Asset Exchanges are entities engaged in the business of exchanging virtual assets for fiat currency, funds, or other forms of virtual assets in return for a commission. These exchanges typically accept a wide range of payment options, such as cash, wire transfers, credit cards, and other virtual assets. Users commonly utilise these platforms to deposit and withdraw money from their virtual asset accounts. Notable examples of Virtual Asset Exchanges include Kraken, Bitfinex, Coinbase, Bitstamp, Binance, Coinmama, and CEX.IO.

Virtual Asset Broking

Virtual Asset Broking involves arranging transactions that either exchange virtual assets with fiat currency or exchange one form of virtual asset for another. This can involve the use of virtual asset ATMs, where individuals can purchase or sell VAs using cash or a debit card, and sometimes both buying and selling are supported. Merchants also engage in broking by exchanging fiat currency for VAs. Cards linked to virtual asset balances may be used to conduct transactions in a similar manner to traditional financial cards.

Virtual Asset Management Providers

Virtual Asset Management Providers offer services relating to the management of virtual asset investments. This includes fund managers who invest in virtual assets, firms that distribute funds investing partly or entirely in VAs, and broader support on risk management, management of liquid capital, segregation of assets, custodianship, fund structure, and legal considerations.

Initial Coin Offering (ICO) Providers

Initial Coin Offering (ICO) Providers issue and sell virtual assets to the public, often for the purpose of fundraising. These offerings may also involve Security Token Offerings (STOs), where the tokens represent equity. In addition to hosting the sale of tokens, these providers may participate in and offer financial services related to the ICO, including compliance, advisory, and marketing.

Virtual Asset Investment Providers

Virtual Asset Investment Providers create investment vehicles that enable the purchase or investment in virtual assets. These vehicles may include managed investment schemes, derivatives (such as virtual asset options), or private equity funds focused on virtual assets. They provide an avenue for investors seeking exposure to this emerging asset class.

Validators / Miners / Administrators

Validators, miners, and administrators are entities that maintain the security and integrity of decentralised virtual asset ledgers. They receive VA rewards for being the first to validate transactions, typically by employing significant computing power to solve complex mathematical equations. This process, often referred to as mining, underpins the blockchain's consensus mechanism and ensures that transactions are verified and recorded accurately.

Stablecoins

Stablecoins typically claim to have a mechanism which seeks to stabilise their value by backing them with fiat currencies, commodities or a basket of cryptocurrencies. These virtual assets have given rise to significant regulatory concerns among global central bankers and financial regulators, particularly where they are intended to be adopted on a global scale.

Non-Custodial Wallet

A non-custodial wallet is a wallet in which the private keys are held by the virtual asset owner, who has complete control over the virtual assets. Non-custodial wallets include the Bitcoin.com client, BRD, Blockchain, BTC.com, Electron Cash, Copay, Jaxx, Coinomi, Edge, and many more because these platforms give users the ability to store their own private keys.

Custodial Wallet

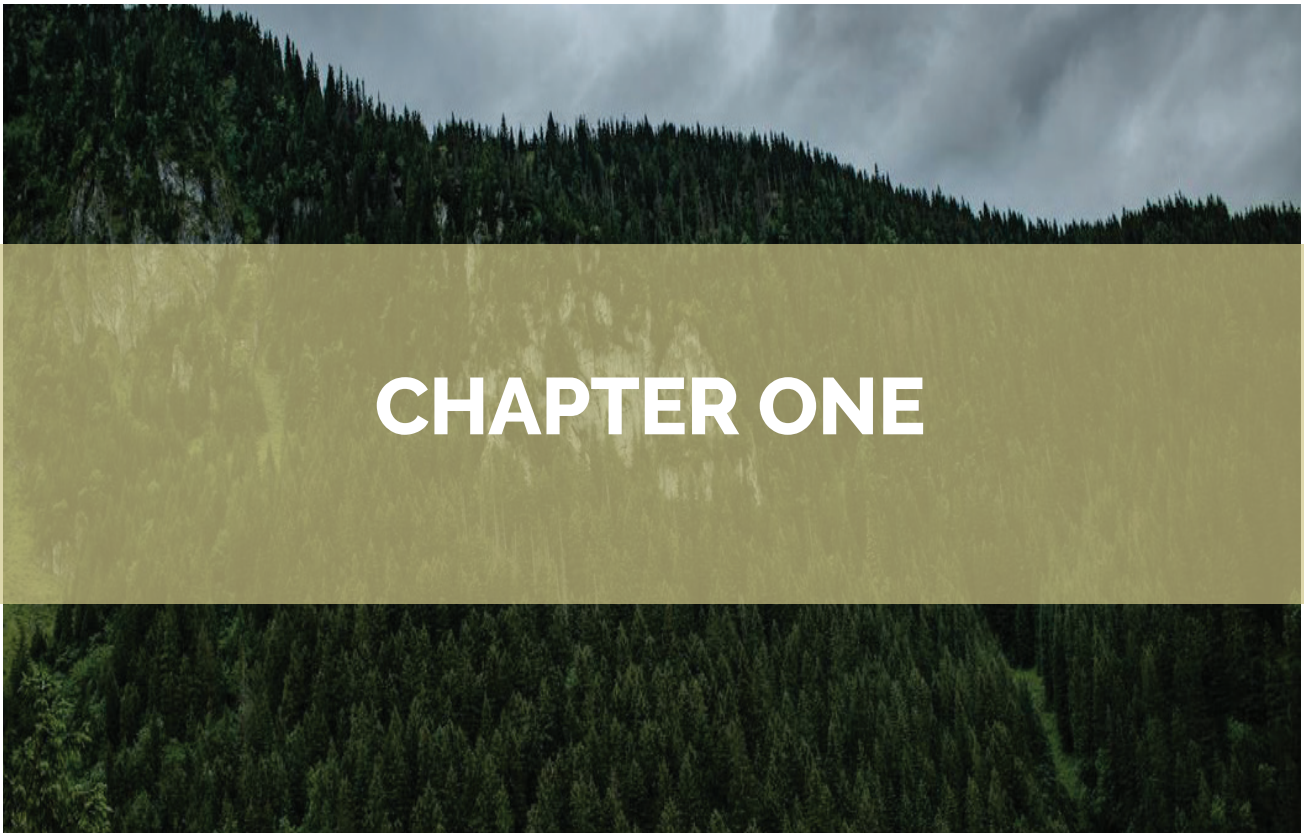
A custodial business offers to protect virtual assets within their system. The platform providing custodial cryptocurrency services can also include most exchanges and brokerage services allowing buying, selling, and storage of virtual assets in the product called 'Wallet'. A custodial wallet is a wallet in which the private keys, of the subject holding the virtual asset, are stored by a third party. This arrangement does not provide full control of virtual assets to its owner; rather the funds are held by the custodian providing the Virtual Asset Wallet Service. Coinbase is a great example of an exchange and brokerage service that also allows people to store virtual assets within their wallet system.

Fees

Institutional units that validate and confirm the transactions are called Miners. Miners are considered as book keepers / distributed ledger updaters in a Virtual asset transaction. A transaction can only be considered secure and complete once it is included in a block. Mining could be undertaken by miners individually (solo mining) or as part of a pool (pooled mining). Miners can receive a fee against the service and can also be a wallet holder.

Automated Teller Machine

A kiosk that allows a person to purchase virtual assets by using cash or debit card. Some virtual asset ATMs offer bi-directional functionality enabling both the purchase of virtual assets as well as the sale of virtual assets for cash



CHAPTER ONE

1.1 Background

In the past decade, there has been a remarkable surge in the development and adoption of digital instruments that promise to streamline global payments and transfers, offering enhanced speed, cost-efficiency, and accessibility. These digital assets, which encompass a wide and expanding range of financial instruments, are commonly referred to as VAs, digital currencies, and Virtual Assets (VAs). These terms all denote systems that store or capture value and rights in a digital format. A significant proportion of these VAs utilise new technology to secure transactions and regulate the creation of additional units, relying on distributed ledger technology (DLT) such as blockchain to maintain a decentralised ledger across a network.

The advent of Bitcoin in 2009 marked the inception of this new financial paradigm. Since then, thousands of VAs have been launched, experiencing varying levels of success. As of December 2024, VAs collectively hold a market capitalisation of approximately USD 3 trillion[1], with over a dozen assets generating daily trading volumes surpassing USD 168 billion[2]. Despite their relatively modest share of global financial markets, VAs represent a rapidly evolving sector characterized by innovative business models and new asset classes, including stablecoins, which continue to gain traction for potential mass adoption.

1 According to CoinMarketcap.com for December 2024

2 According to CoinMarketcap.com for December 2024

For the purposes of this study, and in alignment with the terminology established by the Financial Action Task Force (FATF)—the global authority on anti-money laundering (AML) and combating the financing of terrorism (CFT) standards—these instruments will be referred to as virtual assets (VAs), and the entities that facilitate their transactions will be termed Virtual Asset Service Providers (VASPs). Notably, the FATF definition excludes digital representations of fiat currencies and other assets, such as securities, that are governed by separate regulatory frameworks (FATF, 2023). Thus, while Central Bank Digital Currencies (CBDCs)[3] may share certain attributes with VAs, they are not covered under this framework.

VAs present numerous potential benefits, including faster, cheaper, and more efficient cross-border payments, with the potential to enhance financial inclusion (IMF, 2024). The underlying DLT has broader applications beyond VAs, with many countries exploring the issuance of digital currencies, such as CBDCs. As of 2024, more than 130 countries are researching or testing CBDC initiatives, with several nations, including China and the Bahamas, having already launched their own CBDCs. However, despite their promising features, VAs are also susceptible to misuse, particularly due to their inherent pseudonymity and varying levels of anonymity. These characteristics have been exploited for illegal activities such as fraud, theft, money laundering (ML), terrorist financing (TF), and other criminal endeavors. Without robust regulatory frameworks, VAs could undermine the integrity of the global financial system, presenting risks that could affect economic stability and growth.

In response to these risks, the FATF amended its global standards in June 2019 to explicitly extend AML/CFT requirements to VAs and VASPs. Subsequent reviews in June 2020 and 2021 highlighted the progress made in implementing these standards, while emphasising the need for continued efforts across both public and private sectors to address the emerging risks associated with VAs. In particular, updates such as the travel rule for VASPs were introduced to strengthen the regulatory framework. The FATF's most recent review, published in June 2023, highlighted continued progress in the adoption of AML/CFT regulations for VAs but also called for enhanced global coordination and enforcement efforts to tackle the rising threats posed by VAs in relation to money laundering, terrorist financing, and other financial crimes (FATF, 2023).

3 It is important to note that while Central Bank Digital Currencies (CBDCs) are underpinned by blockchain technology, the World Bank Money Laundering and Terrorist Financing (ML/TF) risk assessment methodology and tools used in this study do not recognise CBDCs as Virtual Assets (VAs) in line with guidance issued by the Financial Action task Force (FATF). This is because CBDCs are issued by central banks, and are backed by fiat currencies, which places them outside the scope of the FATF's definition of VAs. As such, CBDCs are not assessed in this study, as they fall outside the defined parameters for Virtual Assets and Virtual Asset Service Providers (VASPs).

1.2 introduction

This report presents the Money Laundering (ML) and terrorist financing (TF) risk assessment for the Republic of Uganda, in alignment with Financial Action Task Force (FATF) Recommendation 1 (R.1) on the risks associated with Virtual Assets[4] (VAs) and Virtual Asset Service Providers (VASPs). The assessment was carried out in accordance with the 'Guidance' and 'Tool' developed by the World Bank.

Given that the activities of VASPs and transactions involving VAs are not constrained by geographical borders, they can occur globally without any physical presence in a specific location. This unique characteristic enhances the risks associated with ML, TF, and PF. These risks pose a significant threat to Uganda's financial sector, necessitating a comprehensive assessment to understand the extent of exposure and to inform policy decisions.

This ML/TF risk assessment exercise aims to provide policymakers with strategic intelligence into the potential ML/TF/PF risks emerging from VAs and VASPs, thereby enabling the development of an effective and robust AML/CFT legislative and supervisory framework. Such a framework is essential to mitigate the identified residual risks associated with these business activities. Furthermore, it is important for ensuring that Uganda remains compliant with FATF standards, particularly, recommendations 1 and 15, safeguarding its financial sector's integrity.

Uganda has witnessed a significant rise in VA and VASP activities, driven by global trends. As a financial centre, Uganda is primarily exposed to external ML/TF threats. VA activities are conducted through service providers that fall outside the scope of current AML/CFT and tax legislation, creating challenges in areas such as the prevention and detection of ML/TF activities, investor protection, market integrity, and financial stability.

4 According to the FATF, the term 'Virtual Asset' refers to "any digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes." VAs do not include digital representations of fiat currencies, securities, and other financial assets. VAs have technological properties that enable pseudo-anonymous and anonymous transactions, fast cross-border value transfer and non-face-to-face business relationships. Those properties have the potential to improve multiple financial products and services such as trade financing, cross-border payments and financial instrument settlement.

The ML/TF risk assessment also considered the risks to consumers, such as purchasing unsuitable VAs without adequate information, falling victim to fraudulent activities, and the failings of market infrastructures and services. The authorities are fully aware of the reputational risks that may arise from fraudulent activities and operational issues stemming from unlicensed operators.

As VAs are not issued, regulated, or backed by a central authority and VASPs are not licensed in Uganda, many types of operators could exist on the market. Some are popular household names like Bitcoin and Ethereum, while many have never been heard of and are used as means of payment, investment, and funds transfer. Irrespective of their popularity, they are all convertible and provided through the centralised or decentralised system with or without an intermediary or administrator.

In light of the growing use of VAs and their potential for abuse due to the absence of a dedicated regulatory and legislative framework, the Financial Intelligence Authority on behalf of the National AML/CFT Task Force commissioned this ML/TF risk assessment exercise.

1.3 Objective of the ML/TF Risk Assessment

The general objective of undertaking the ML/TF risk assessment on VAs and VASPs is to identify, assess, and understand ML/TF risks in order to inform policy pertaining to the AML/CFT regime of Uganda. The specific objectives of the risk assessment were to;

i) Identify, understand, and assess the overall money laundering and terrorist financing (ML/TF) risks related to VA and VASP ecosystems;

ii) Identify VA and the VASP products/services/channels with high ML/TF vulnerability;

iii) Prioritize action plans to strengthen AML/CFT controls in the VA and VASP ecosystems;

iv) Apply a risk-based approach to VAs and VASPs and effectively mitigate identified risks; and

v) Build the capacity and raise awareness of competent authorities about the ML/TF risks related to VAs and VASPs, as well as strengthening the interagency cooperation among them.

CHAPTER 2

The assessment team consisted of a dedicated working group of AML/CFT practitioners in private, public sectors and academia.

2.0 Risk Assessment Methodology

2.1 The Technical Working Group

The assessment team consisted of a dedicated working group of AML/CFT practitioners in private, public sectors and academia. The WG was set up where all the sectors and institutions identified relevant for this exercise included representatives from;

i. Capital Market Authority
ii. Bank of Uganda
iii. Association of Forex Bureau and Money Remitters for Uganda
iv. Uganda Bankers' Association
v. Ministry of Finance, Planning & Economic Development
vi. Uganda Police Force, Criminal Investigations Directorate
vii. Office of the Director of Public Prosecutions
viii. Blockchain Association of Uganda
ix. Financial Technologies Service Providers Association
x. Association for Payment Service Providers
xi. Uganda Registration Services Bureau
xii. Uganda Revenue Authority
xiii. National Information Technology Authority - Uganda
xiv. Financial Intelligence Authority

2.2 Scope of the ML/TF Risk Assessment

This assessment encompassed data for the period July 1, 2020 to June 30, 2024 covering the following areas;

a) Tracing all VAs and VASPs operating in Uganda.
b) The magnitude of the threats identified
c) The vulnerability that could be exploited for ML/TF
d) Identified existing controls in place to mitigate each identified risk, with the aim of assessing their effectiveness.
e) Development of an action plan to mitigate identified risks.

2.2.1 The World Bank Tool

The ML/TF risk assessment exercise in Uganda was conducted using an analytical tool developed by the World Bank Group. This process adhered closely to the guidance, methodology, and model provided by the World Bank Group, specifically designed to assess ML/TF risks associated with VAs and VASPs. The tool is structured around interconnected Excel-based modules incorporating eight key areas, each employing

specific "input and intermediate variables" to evaluate the threats[5], vulnerabilities[6], and mitigation measures applicable to VAs and These factors, present either nationally or within specific sectors, collectively shape the overall ML/TF risk level associated with VAs or VASPs in a given jurisdiction. These measures span various levels, including government, traditional obliged entities, and VASPs.

Figure 1 : **Key Areas of the Risk Assessment Model for VA and VASP**

Source: World Bank VA/VASP Risk Assessment Tool

The World Bank Risk Assessment tool considers 07 types of VASPs, offering 12 VASP functions and 27 activities through which there could be potential interaction with different sectors in or outside Uganda. The questionnaires developed for this assessment covered any area where these 27 activities could interact with the traditional obliged entities.

It should also be noted that 06 out of these 07 types of VASPs offering 11 VASP functions were assessed leaving out Fund Management, Fund Distribution, and Compliance, Audit & Risk Management since the working group determined that these areas were not operating in Uganda, as there was no supporting information to indicate their operations at the time of the risk assessment. The types, functions and activities considered are shown in the figure below;

5 Threats pertain to the scale and characteristics of criminal proceedsor terrorism financing within a jurisdiction

6 Vulnerabilities highlight deficiencies in a jurisdiction's defenses against ML/TF activities

***Figure 2* : Types of VASP**

Types of VASPs and functions and VASPs considered for this ML/TF risk assessment			
1	Virtual Asset Wallet Providers	• Custodial Services • Non-Custodial Services	1. Hot Wallet 2. Cold Wallet
2	Virtual Asset Exchanges	• Transfer Services • Conversion Services	3. P2P; 4. P2P; 5. Virtual – Fiat; 6. Fiat – Virtual; 7. Virtual - Virtual
3	Virtual Asset Broking/ Payment Processing	• Payment Gateway	8. ATMs; 9. Merchants & 10. Cards
4	Initial Coin Offering (ICO) Providers	• Fund Raising • Investments • Other Offerings	11. Fiat – Virtual 12. Virtual – Virtual 13. Development of Products & Services 14. Security Token Offering (STO) 15. Initial Token Offering
5	Virtual Assets Investment Providers	• Trading Platform • Emerging Products	16. Platform Operators 17. Custody of Assets 18. Investment in VA related commercial activities 19. Non-Security Token/Hybrid Trading Activities 20. Stable Coins 21. VA Escrow 22. Custodian Services
6	Validators, Miners & Administrators	• Proof of Work	23. Fees 24. New Assets

2.2.2 FATF Guidance on VAs and VASPs

In June 2019, FATF revised Recommendation 15 (R.15) to incorporate obligations pertaining to VAs and VASPs. Since then, FATF has issued several guidance documents to help countries interpret these requirements, which are intended to have a broad and expansive application. These updated obligations included

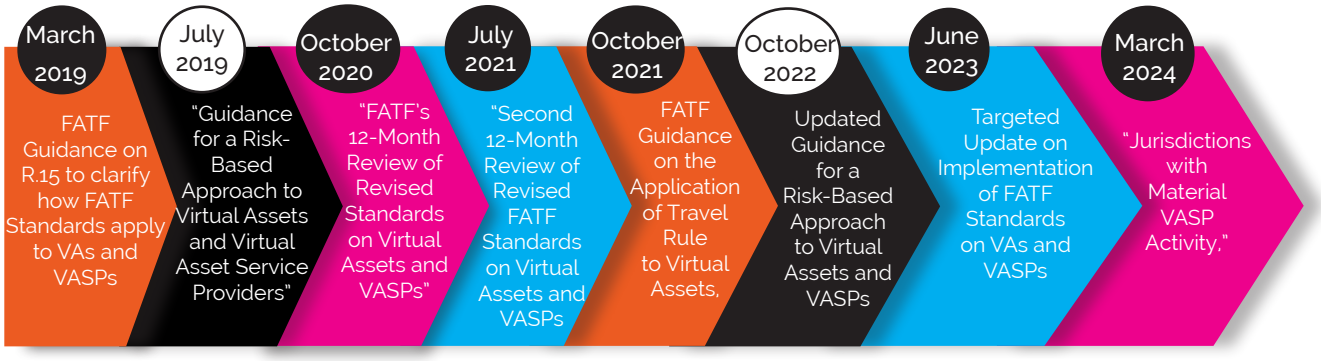
a) The identification, assessment, and understanding of ML/TF risks linked to VA activities and the operations of VASPs.
b) The licensing or registration requirements for VASPs.

c) The need for countries to apply effective, risk-based AML/CFT supervision (in-

cluding sanctions) for VASPs, under the oversight of a competent authority.

d) The enforcement of deterrent measures and fostering international cooperation related to VASPs.

Figure 3 **: FATF Publications**



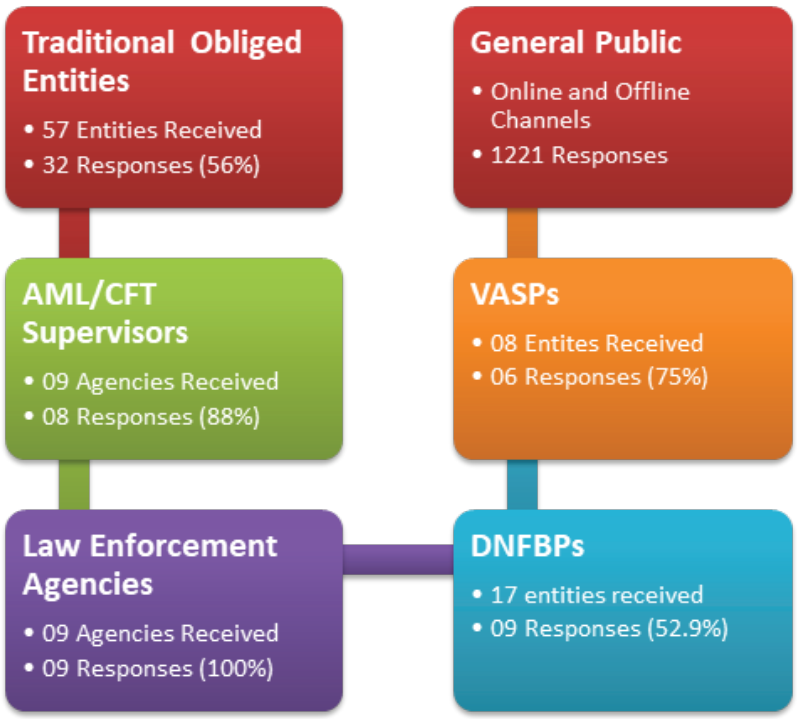
FATF has issued several guidance documents to help countries interpret these requirements, which are intended to have a broad and expansive application.

2.3 Data Collection

The working group relied on both quantitative and qualitative data in undertaking the VA & VASP risk assessment. The qualitative data included public and private sector inputs, case studies and questionnaires[7] as well as research papers and various open source information. Quantitative data was also considered from various sources including law enforcement agencies, supervisory bodies, blockchain analytical companies, among others

The assessment team distributed questionnaires through online and offline means to all 06 categories of respondents, responses were then analysed and interpreted after validation of the data accuracy. The participation rate per category of respondents is shown in the figure below;.

***Figure 4* : Survey Responses**



7 There were 06 categories of questionnaires administered through separate online links to law enforcement agencies, supervisory bodies, VASPs, traditional obliged entities, DNFBPs, and general public. Each of these questionnaires had unique areas covering issues relating to inter-alia, governance, internal controls, operations, knowledge of staff, training across the threat, vulnerability, and mitigating measures dimensions. As no official statistics on the actual level of VA and VASP activities are available in the eco-environment, the WG conducted meetings with a sample of banks, NBFIs, DNFBPs, and government ministries to understand to explain the Risk Assessment process and gather feedback on VAs and VASPs activities.

CHAPTER 3

THE VAs AND VASPs IN UGANDA

"In response to the increasing activity surrounding VAs, Bank of Uganda took a decisive action to mitigate associated risks by VAs and VASPs to the financial sector."

Uganda currently lacks a dedicated VASP licensing law, and there is no supervisory framework for VAs or VASPs. As a result, no VASPs have been licensed or regulated under the current legal framework of Uganda. However, with the inclusion of VASPs in the 2nd schedule of the Anti-Money Laundering Act (AMLA) Cap 118 as accountable persons, 16 entities have since registered with the Financial Intelligence Authority as of June 2024. Despite this registration, these entities are still not licensed in the traditional sense of prudential regulation and continue to operate without full regulatory oversight.

In response to the increasing activity surrounding VAs, Bank of Uganda took a decisive action to mitigate associated risks by VAs and VASPs to the financial sector. BoU restricted traditionally obliged entities such as financial institutions and payment system operators licenced under the Financial Institutions Act, 2004 and the National Payment Systems Act, 2020 from settling payments linked to VAs or transacting with VASPs. This action aimed at reducing the exposure of Uganda's financial system to the potential macro and micro economic risks posed by risks posed by VAs and VASPs to Regulated Financial service Providers (RFSPs)[8].

Additionally, in September 2019[9] MoFPED issued a public statement warning the public against investing in VAs as the Government of Uganda did not recognise VAs as legal tender. The public was advised to exercise caution since the sector was not regulated and lacked legal provisions for consumer protection in the event of financial loss. This was meant to address the rising incidences of fraud and threats emanating from VAs and the likely impact on the broader economy.

The ML/TF risk assessment also considered the risks to consumers, such as purchasing unsuitable VAs without adequate information, falling victim to fraudulent activities, and the failings of market infrastructures and services. The authorities are fully aware of the reputational risks that may arise from fraudulent activities and operational issues stemming from unlicensed operators.

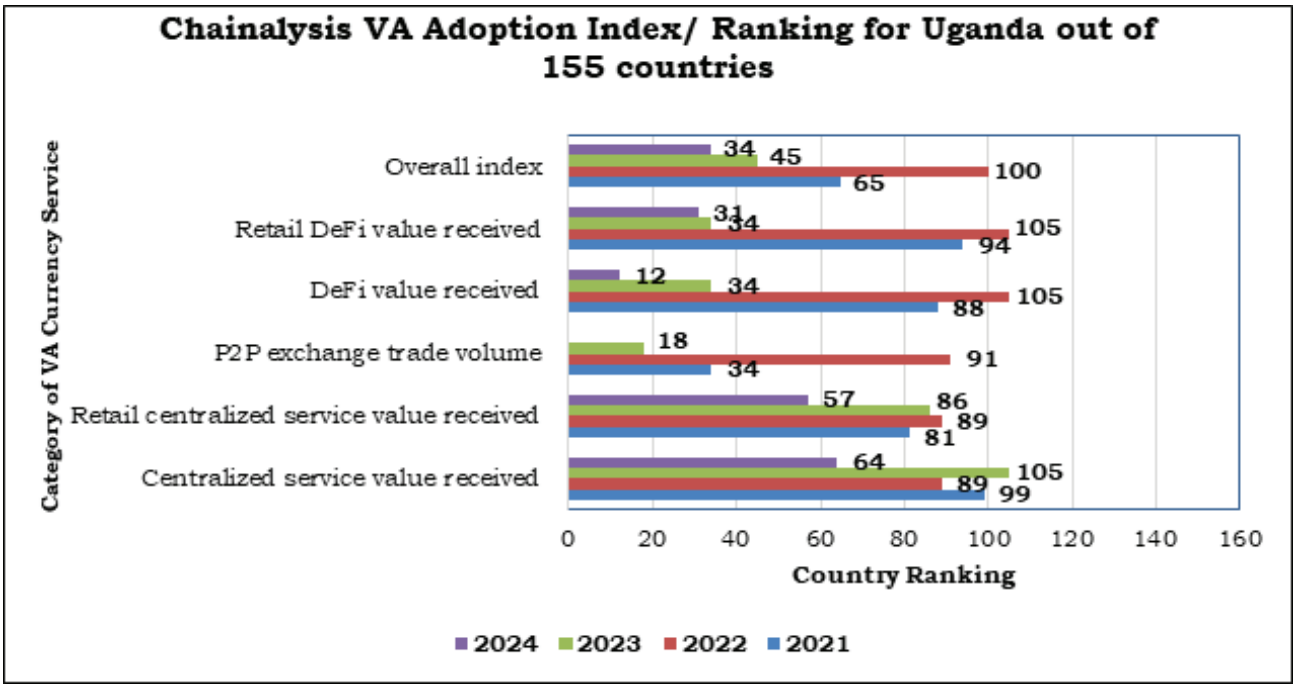
In September 2019 , MoFPED issued a public statement warning the public against investing in VAs as Government of Uganda did not recognise VAs as legal tender.

8 RFSPs include Commercial Banks, Credit Institutions, Micro-Deposit Taking Institutions, Foreign Exchange Bureaus, Money Remitters, Payment Service Provider and Operators, and Issuers of Payment Instruments.
9 https://archive.finance.go.ug/press/public-statement-cryto-currencies-minister-finance

3.2 VA Adoption Ranking for Uganda

The adoption of VAs in Uganda has been on a gradual rise over the years from July 2020 to June 2024. This can be demonstrated by the VA adoption index made up of 04 different indices each of which is based on the country usage of different categories of VA currency services as shown in the figure below;

Figure 5 : VA Adoption Ranking for Uganda



***Source:** Chainalysis Geography of VA Reports*[10]

The figure above shows significant trends in VA adoption in Uganda, with a shift from centralised services to decentralised platforms as observed below

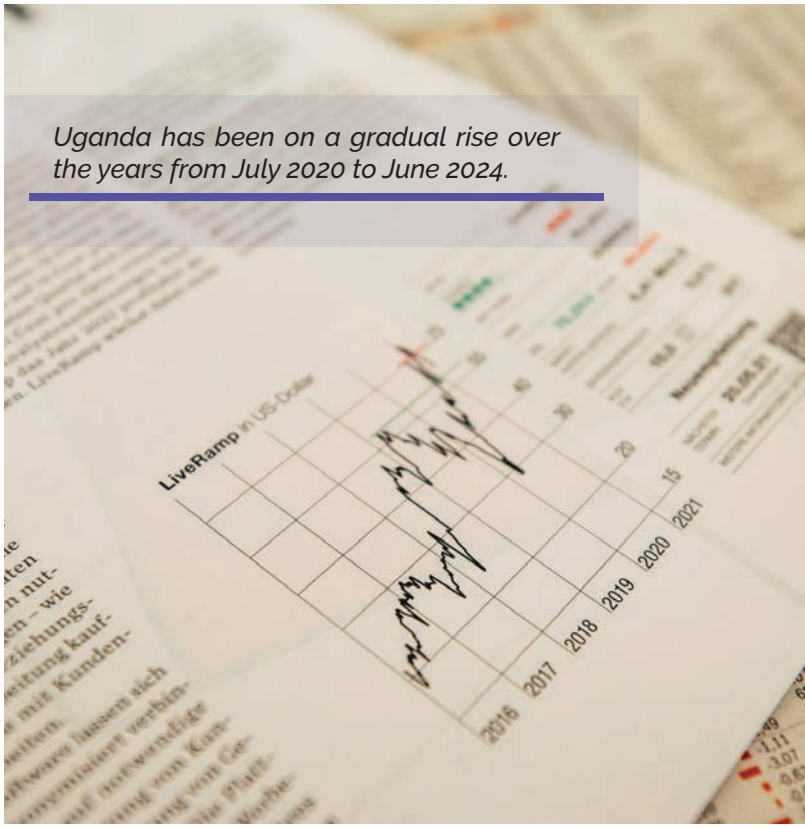
a) Centralised services, which include regulated exchanges, saw an increase in usage until 2022, before declining in 2023. This drop saw a shift by residents of Uganda towards decentralised finance (DeFi) which are less regulated across the world. The transition away from centralised exchanges may indicate a move towards platforms with fewer oversight mechanisms, which poses risks for Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) efforts. Centralised services typically have stronger Know Your Customer (KYC) and AML controls, so the shift away from these platforms could increase the likelihood of illicit financial activities, as such services are more easily exploited for Money Laundering and Terrorist Financing due to their lack of regulatory oversight.

10 The overall ranking for 2024 in the figure above is based on data from January, 2024 to April, 2024.

b) Similarly, the data on retail centralised service value received mirrors this trend, showing a fluctuating pattern over the years, but ultimately improving in 2024. The retail sector's retreat from regulated platforms further underscores a preference for more anonymous or decentralised financial solutions. While this could reflect a growing dissatisfaction with the services offered by centralised platforms, it also raises the concern of a rise in informal or unregulated VA trading. The absence of regulation in these decentralised systems allows illicit actors to easily carry out transactions without detection,increasing the risk of Money Laundering and Terrorist Financing. Therefore, the decline in retail use of centralised exchanges can be indicative of players moving towards higher-risk platforms that are less likely to monitor or report suspicious transactions.

c) P2P exchange trade volume, which increased substantially in 2022, improved sharply in 2023 and 2024[11]. In 2023, the rise in P2P exchanges indicates that users were drawn to the anonymity and flexibility they offer. P2P exchanges, by nature, allow users to trade directly with one another, often without intermediary oversight, making them susceptible to misuse for illicit activities.

d) In terms of decentralised finance (DeFi), the country ranking for value received showed a downward trend in 2022 before improving sharply in 2023 and 2024 as seen from the improved country ranking reaching 12th out of 155 countries in DeFi adoption. DeFi platforms, offering financial services without intermediaries, attract users seeking greater privacy and less regulation. However, the lack of oversight in these platforms makes them a breeding ground for Money Laundering and Terrorist Financing. The earlier surge in DeFi use suggests that Uganda saw a rise in interest in decentralised alternatives to traditional finance, which may have provided an avenue for criminals to obscure the flow of illicit funds. As DeFi services have no centralised control or regulatory compliance, the anonymity they offer can easily be exploited to facilitate illicit transactions.



Uganda has been on a gradual rise over the years from July 2020 to June 2024.

11 The Sub-index of P2P was excluded in the methodology of deriving the overall index in 2024. This was due to the shutdown of one of the largest and the most tenured P2P exchange, LocalBitcoins.com, in the previous year; leading to a substantial decrease in activity on P2P exchanges. However, basing on the overall index, it is clear that there was increased usage of P2P transactions in 2024 better than in 2023 when Uganda was ranked 18th out of 155 countries.

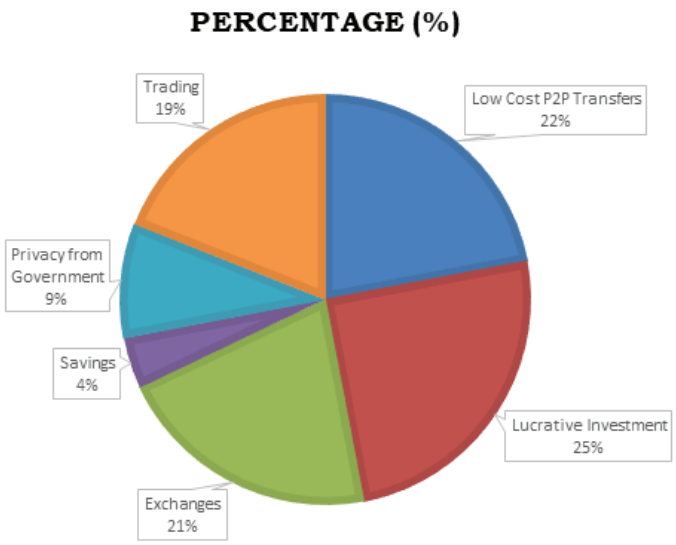
3.2.1 Factors Driving Increased Usage of VAs in Uganda

As per the Chainalysis VA adoptio reports from 2021 to 2024 mentioned in detail in Chapter 3, Uganda is among the top African countries with global rankings improving from 100th position in 2022 to 34th position in 2024. Other avaiable sources showed that between July 2020 to June 2024, Uganda registered VA inflows above the tune of USD 564,217,150 and outflows of USD 545,501,020 with the largest contribtors of this figure from VA exchanges, gambling services and P2P exchanges.Other contributors included merchant services, and fraudulent schemes.

Despite certain domestic restrictions limiting easy access to VAs, survey responses revealed a growing trend of adoption among Ugandan residents. This adoption stemmed from varied and multi-layered factors, including the increasing global shift towards digital financial solutions, the appeal of faster and more affordable cross-border transactions, and the potential for financial inclusion among the unbanked population. Additionally, some respondents cited the speculative opportunities offered by VAs, such as investment and trading prospects, while others emphasised their utility in bypassing traditional financial barriers. The main factor driving the adoption of VAs remains their potential for high returns on investment.

The chart below illustrates the reson for investing in Virtual Assets (VAs) as highlighted by respondents

Figure 6 : ***Reasons Driving Usage for VAs in Uganda***



Source: *Survey Responses*

Uganda is among the top African countries with global rankings improving from 100th position in 2022 to 34th position in 2024.

between July 2020 to June 2024, Uganda registered VA inflows above the tune of

USD 564,217,150

And Outflows of **USD 545,501,020**

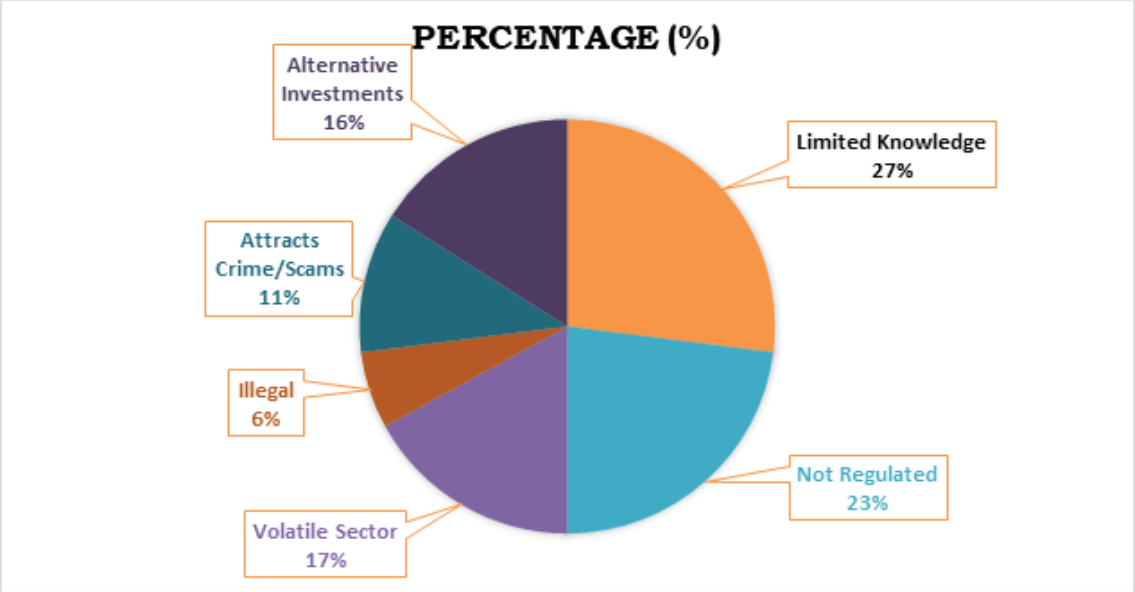
Advancements in technology and the increasing adoption of VAs have made them more accessible and appealing, particularly with the integration of bloc chain technology and smart contracts, features that resonate strongly with younger generations.

3.2.2 Factors Driving Non-Adoption of VAs in Uganda

Despite this progress, 819 out of 1,221 respondents refrained from engaging with VAs, primarily due to the lack of regulation and the cautionary messages issued by government authorities. Additionally, the absence of a comprehensive understanding of VAs has led to reluctance. Some individuals view VAs as inherenly risky or a kin to gambling schemes, making them hesitant to invest their funds. On the other hand, more financially literate individuals, who are better informed, tend to find alternative investment opportunities more attractive.

The chart below illustrates the reasons for non-adoption of VAs highlighted by respondents.

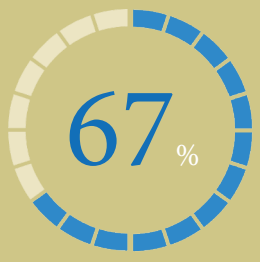
Figure 7 **: Reasons for non-adoption of VAs in Uganda**



Source: *Survey Responses*

"819 out of 1,221

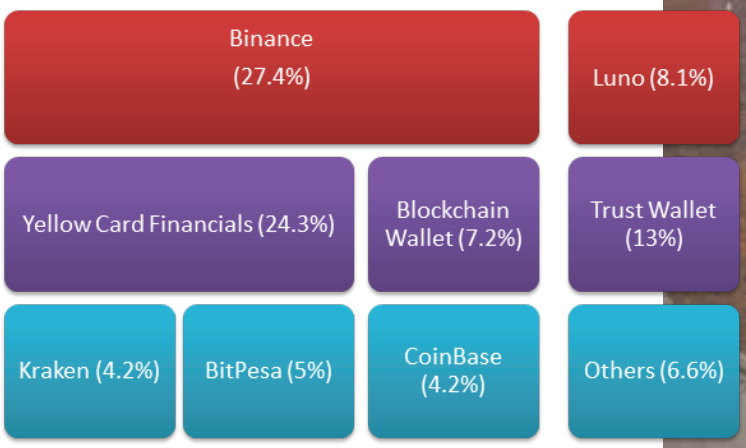
Respondents refrained from engaging with VAs, primarily due to the lack of regulation and the cautionary messages issued by government authorities."



3.2.3 Type of Centralised VASPs Operating in Uganda

Determining the exact number of centralised VA exchanges operating in Uganda is challenging due to the lackof comprehensive public data. However, the asessment team identified several centralised exchanges and a handful of decentralised exchanges known to facilitate VA trading in the country through responses from law enforcement, general public and other available sources of information as shown in the figure below;

Figure 8 **: Most Prominent VASPs Preferred in Uganda based on respondents**



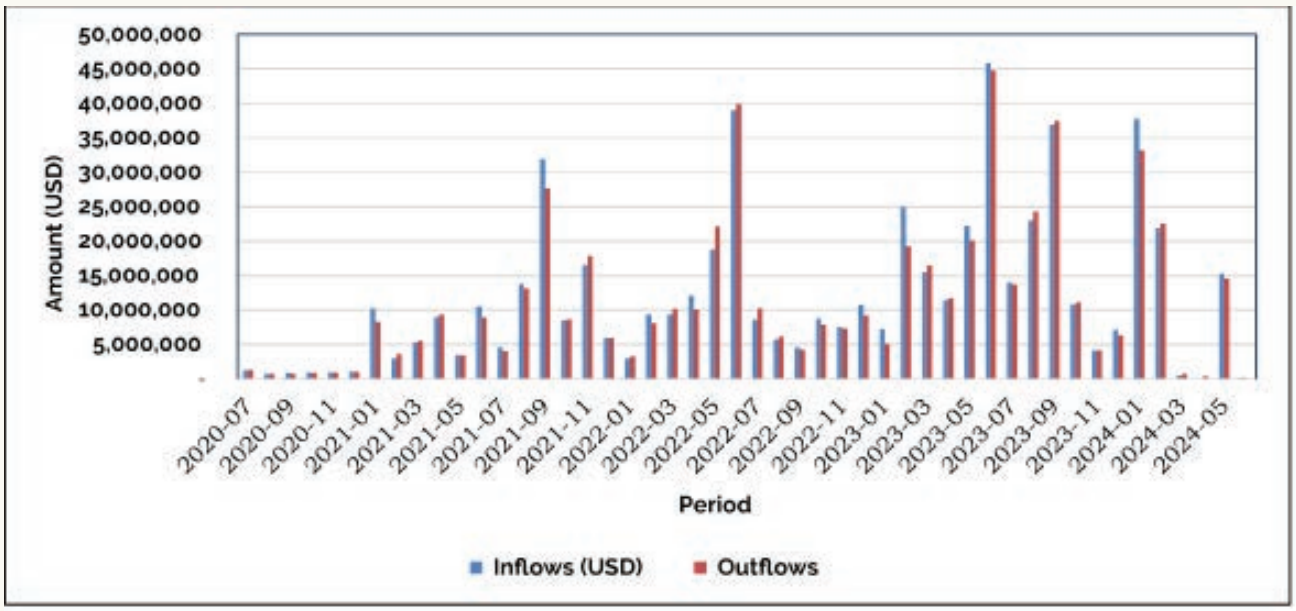
The finding that 88% of respondents emphasised that Virtual Asset Service Providers (VASPs) accessed in Uganda also operate in the East African region and multiple countries globally highlights the extensive reach and influence of these service providers. This cross-border operation means that the VASPs in Uganda are not isolated but are part of a broader regional and international ecosystem. Notably, some of the countries mentioned by respondents include neighbouring countries and other countries in Sub-Saharan Africa.

"Respondents emphasised that Virtual Asset Service providers (VASPs) accessed in Uganda also operate in the East African region and multiple countries globally highlights the extensive reach and influence of these service providers."

3.3 VA currency inflows and Outflows for Uganda

The assessment team analysed data covering the period from July 2020 to June 2024 obtained from a commercial blockchain analytics tool to gain a deeper understanding of how VA inflows and outflows have evolved over time and the factors that influenced these changes as shown in the figure below;

Figure 9 : **Trend of VA currency flows between July 2020 and June 2024**



Source: Commercial blockchain Analytics tool

The graph above shows VA inflows and outflows for Uganda from July 2020 to June 2024 revealing both a steady increase in overall flows and considerable volatility within specific months. The figures indicate a significant rise in virtual asset activity over the years, with fluctuating values in both inflows and outflows. The following observations were made;

a) The average value of VA flows was modest in the earlier months, with monthly inflows and outflows ranging from about USD 668,000 to USD 1.3 million in mid 2020. By mid-2021, the monthly average of inflows rose significantly, reaching over USD 10 million. This growth continued into 2022, where flows hit values exceeding USD 39 million in June 2022.

b) In 2023, there was a notable peak in virtual asset flows, with the highest monthly inflows and outflows recorded in June 2023 at USD 45.8 million and USD 44.7 million, respectively. These high levels of activity indicate growing interest and adoption in virtual asset transactions within Uganda.

c) There was an overall upward trend with a monthly average of inflows as follows; in 2020, there was an average monthly value of inflows totaling USD 928,000; 2021 recorded monthly average of USD 9.96 million; 2022 with a monthly average of USD 11.48 million; 2023 saw a rise to USD 18.2 million and lastly, 2024 registered a decline to USD 12.25 million.

d) It was also observed that the VA flows were highly volatile in the period reviewed which raises concerns about the nature of the transactions occurring, suggesting that they may involve speculative investments or large-scale transfers, potentially linked to illicit activities.

e) The data further indicated that the inflows are more than the outflows over the period with a marginal difference of USD 18.7 million. For example, the total inflows amounted to approximately USD 564.2 million (50.8%) and outflows totalled USD 545.5 million. This balance suggests that while the funds are entering and exiting the country in almost equal measure, there is potential for large sums of money to be transferred across borders, which can potentially be abused for ML/TF activities or other financial crimes.

"VA inflows and outflows for Uganda from July 2020 to June 2024 reveal both a steady increase in overall flows and considerable volatility within specific months"

3.4 Value of Transactions by Nature of Virtual Asset Services in Uganda

Analysis of VA transaction values by nature of service from July 2020 to June 2024 indicated a varied picture in terms of volume of transactions for both inflows and outflows as shown in the table below;

Table 1 : **Value of transactions carried out by virtual asset services**

Sn	Service	Inflows (USD)	%	Outflows (USD)	%
1.	VA Exchange	509,574,368	90.2673	489,540,928	89.8417
2.	Gambling	22,184,323	3.9331	19,461,482	3.5688
3.	P2P exchange	13,801,693	2.4467	15,684,705	2.8759
4.	Others	5,655,992	1.0024	7,015,828	1.2866
5.	Scam	3,173,079	0.5627	5,821,472	1.0678
6.	Hosted wallet	5,362,247	0.9504	3,268,877	0.5998
7.	Merchant services	2,133,580	0.3782	3,667,258	0.6726
8.	Mining pool	1,187,506	0.2106	485,278	0.0890
9.	Fraud shop[12]	567,268	0.1005	213,078	0.0391
10.	Mixing	483,387	0.0857	51,806	0.0095
11.	Infrastructure as a service	77,817	0.0138	252,895	0.0464
12.	ATM	2,003	0.0004	23,040	0.0042
13.	Online pharmacy	8,553	0.0015	9,073	0.0017
14.	NFT platform collection	3,065	0.0005	2,647	0.0005
15.	Darknet market	1,274	0.0002	1,319	0.0002
16.	OFAC Sanctioned entity	724	0.0001	1,162	0.0002
17.	Illicit actor-org	273	0.0000	171	0.0000
	Grand Total	**564,217,150**	**100.0000**	**545,501,020**	**100.0000**

Source: *Commercial Blockchain Analysis tool*

12 Fraud shops are an important part of the cybercriminal ecosystem. Typically operating on the dark web, they facilitate the sale of stolen data and personally identifiable information (PII), which in turn can be used for several different forms of cybercrime, including scamming, identity theft, and ransomware (https://www.chainalysis.com/blog/genesis-market-fraud-shop-shutdown-sanction/)

As indicated in the table above, the potential risks for ML/TF activities associated with different virtual asset services are analysed below;

a) The VA exchange service category accounted for the highest value in both inflows and outflows, with nearly USD 509.6 million in inflows and USD 489.5 million in outflows. This service represents the most significant portion of the virtual asset market in Uganda, facilitating the buying and selling of virtual assets by residents[13] in Uganda. This high transaction volume indicates a high risk for ML and TF, as exchanges are often targeted for layering illicit financial transactions.

b) Gambling services accounted for inflows of approximately USD 22.18 million, with outflows of USD 19.46 million. These values indicate that gambling activities, often associated with virtual casinos or betting platforms, are also a significant part of the virtual asset landscape in Uganda. Gambling services can be high-risk for ML and TF activities due to their nature of facilitating large sums of money being transferred quickly.

c) Peer-to-peer (P2P) exchange services had USD 13.8 million in inflows and USD 15.68 million in outflows in the reviewed period basing on available information. P2P platforms can pose higher risks compared to centralised exchanges due to their decentralised nature and lack of regulatory oversight. The disparity between inflows and outflows suggests that P2P exchanges may be facilitating cross-border transfers or enabling the transfer of funds between individuals in jurisdictions with weak or no AML/CFT regulations. P2P platforms are often used to bypass traditional financial systems, making them highly susceptible to illicit financial activities.

Scam services showed an alarming USD 3.17 million in inflows and USD 5.82 million in outflows. This category highlighted the use of fraudulent schemes to deceive individuals into investing innon-existent or illegitimate virtual assets. The disproportionate outflows in the scam category reflect the nature of scam operations that quickly convert received proceeds and move illicit funds to evade detection. Once funds are collected from victims, operators often prioritize disbursing these funds through multiple channels or to early investors to maintain the illusion of legitimacy. This pattern can indicate ponzi scheme structures, where funds are rapidly laundered, transferred to anonymous wallets, or moved to different jurisdictions with less stringent AML/CFT controls. Additionally, as scams near their collapse, operators may attempt to cash out as much as possible before being exposed, leading to higher outflows than inflows.

13 For purposes of this ML/TF National Risk Assessment for VAs and VASPs, residents refers to all natural and legal persons engaged in virtual asset transactions within the jurisdiction of Uganda at the time the transaction was initiated or terminated, regardless of whether these persons are nationals of Uganda or foreign citizens.

e) The value of transactions for hosted wallets shows a notable difference between inflows of USD 5,362,247 and outflows of USD 3,268,877, indicating a significant volume of funds flowing into these platforms compared to the outflows. Hosted wallets are often used by individuals and organisations who prefer not to manage private keys themselves, entrusting third-party service providers with their assets. The higher inflows suggest that hosted wallets are popular for storing virtual assets, likely due to the convenience they offer, particularly for users who are less experienced with managing their own wallets.

On the other hand, the lower outflows could indicate that many users are holding their assets long-term or reinvesting them within the platform, rather than transferring them out. The relatively lower outflows could also be a sign that hosted wallet services are being used as intermediaries for other transactions, such as for trading or as a storage solution before funds are moved to other, more secure platforms. This trend is consistent with the growing adoption of digital wallets for routine transactions, while also highlighting the platform's role in facilitating other virtual asset services.

f) The transaction values for merchant services reflected a disparity between inflows of USD 2,133,580 and outflows of USD 3,667,258, which indicates that while virtual assets are being accepted as payment by merchant's resident in Uganda, there was a notable movement of funds out of the platforms. Merchant services in the virtual asset ecosystem typically allow businesses to accept payments in VAs, providing a bridge between traditional commerce and the growing VA market.

The higher outflows indicate that merchants may be converting the received VAs into fiat or transferring them to other platforms for liquidity purposes, rather than holding onto the VAs themselves[14]. This is a common practice among businesses, as most prefer to manage their finances in fiat currencies to mitigate the volatility associated with VAs[15]. The relatively lower inflows could reflect the early-stage adoption of VAs as a mainstream payment method, though this could grow as more merchants integrate virtual asset payment systems.

g) Other services accounted for USD 5.66 million in inflows and USD 7.02 million in outflows. These transactions could involve various forms of virtual asset transfers not specifically categorised elsewhere, indicating diverse financial activities.

14 According to a 2021 report by Coinbase and Pymnts, businesses are increasingly adopting VA as a payment method, with 40% of merchants in the U.S. accepting virtual assets. However, many of these businesses convert the virtual assets into fiat to avoid volatility, as detailed by Forbes in a 2021 article highlighting the challenges and opportunities for businesses using VA in transactions ("VA Adoption by Merchants", Forbes, 2021).

15 The decision to convert VAs into fiat is commonly driven by concerns about volatility. As highlighted by the European Central Bank in its 2020 report on virtual currencies, the inherent price fluctuations in VAs often lead businesses to quickly liquidate digital currencies into more stable assets, which could explain the higher outflows compared to inflows in merchant services

h) The value of transactions for mining pools, with inflows of USD 1,187,506 and outflows of USD 485,278, suggests a more controlled flow of funds. Mining pools, which allow multiple participants to combine their computational resources to mine virtual assets more efficiently, typically generate revenue from successfully mining blocks and distributing the rewards to pool members. The inflows represent the total value accumulated from mining rewards, while the lower outflows may indicate that the funds are primarily retained within the pool for distribution to miners or reinvested in the mining operation itself, rather than being moved off the platform. This is common in mining pools, as the earnings are often distributed periodically, meaning funds may remain within the platform until the payout threshold is met. Additionally, the lower outflows can reflect the pool's need to maintain reserves for operational costs, such as server maintenance or electricity, which are central to sustaining the mining process.

i) The transaction values for fraud shops linked to Uganda, with inflows of USD 567,268 and outflows of USD 213,078, reflect the nature of illegal activities associated with these platforms. Fraud shops often operate in the dark web or on illicit platforms, facilitating the exchange of stolen or counterfeit goods and services. The relatively low outflows in comparison to inflows suggests funds are accumulating on the platform, potentially being used to finance further illicit activities, or are being kept within the system for fraudulent transactions. Fraud shops are used for money laundering, where illicit gains are funneled through virtual assets, converting proceeds from fraud into virtual assets before moving them to other platforms or withdrawing them in cash through peer-to-peer transactions, which is exacerbated by the cash economy of Uganda.

j) The transaction values for mixing services[16] in table above linked to Uganda, with inflows of USD 483,387 and outflows of USD 51,806, suggest a significant disparity that may be indicative of the service's role in facilitating money laundering and the anonymization of illicit funds. The high inflows reflect the volume of transactions that are being anonymized through the mixing process. The comparatively low outflows, on the other hand, indicate that the mixed funds are not immediately withdrawn or are expended elsewhere. This indicates that the coins are being held in the mixing pool for a longer period, either waiting for additional mixing rounds to enhance anonymity or being funneled to different addresses or platforms for further layering in the money laundering process.

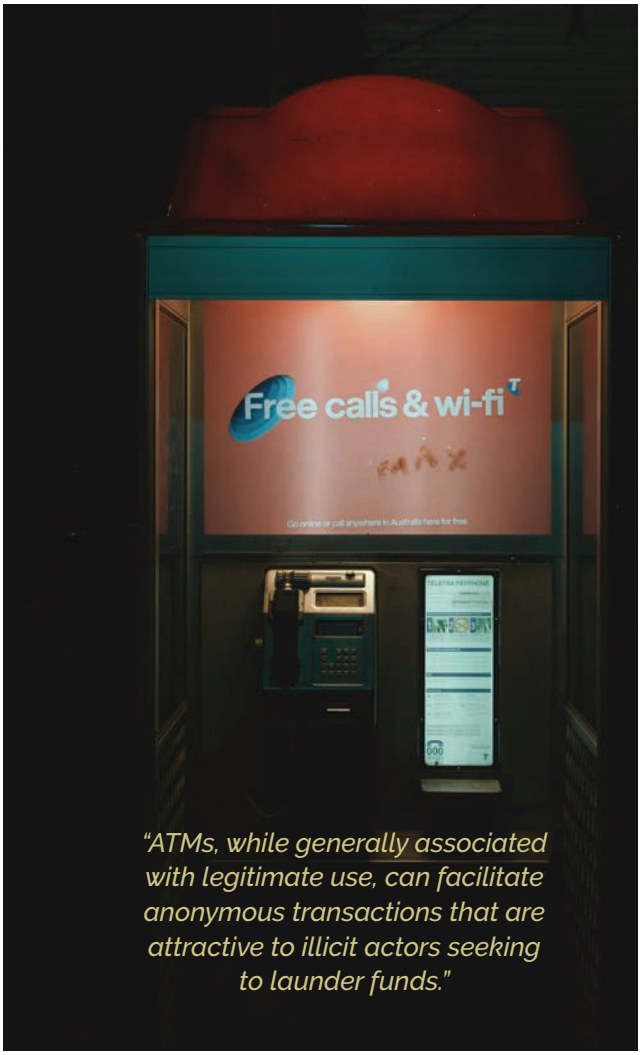
16 Mixing services, often referred to as "tumblers," are used to obfuscate the origin of VA by mixing a user's coins with others in the pool before returning them to the user, making it difficult to trace the funds.

k) The categories of ATMs, online pharmacies, NFT platforms, darknet markets, sanctioned entities, and illicit actor organisations present unique challenges for monitoring virtual asset transactions, as they typically involve lower transaction values but can still pose significant risks. ATMs, while generally associated with legitimate use, can facilitate anonymous transactions that are attractive to illicit actors seeking to launder funds. The comparatively low inflow and higher outflow in this category (USD 2,003 inflows and USD 23,040 outflows) indicates the quick movement of funds through the system, potentially obscuring the origin of illicit money.

Additionally, online pharmacies (USD 8,553 inflows and USD 9,073 outflows) are increasingly being used in unregulated markets, often associated with the sale of controlled substances. This service may overlap with illicit drug trafficking, where virtual assets are used to evade detection and regulation by Ugandan competent authorities. Similarly, NFT platforms (USD 3,065 inflows and USD 2,647 outflows) represent an emerging risk, with their ability to transfer high-value digital assets without sufficient regulatory oversight, making them a potential vehicle for money laundering.

The darknet markets linked to residents of Uganda accounted for USD 1,274 inflows and USD 1,319 outflows continued to be a hub for illegal activities, such as child pornography, sale of drugs, hire of professional mercenaries and stolen data. The use of virtual assets in these markets enables the concealment of transactions, making it difficult for competent authorities to trace illicit funds.

In addition, sanctioned entities (USD 724 inflows and USD 1,162 outflows) and illicit actor organisations (USD 273 inflows and USD 171 outflows) represented transactions that potentially breach international sanctions or involve illegal activities, highlighting the need for enhanced scrutiny of transactions linked to these actors.

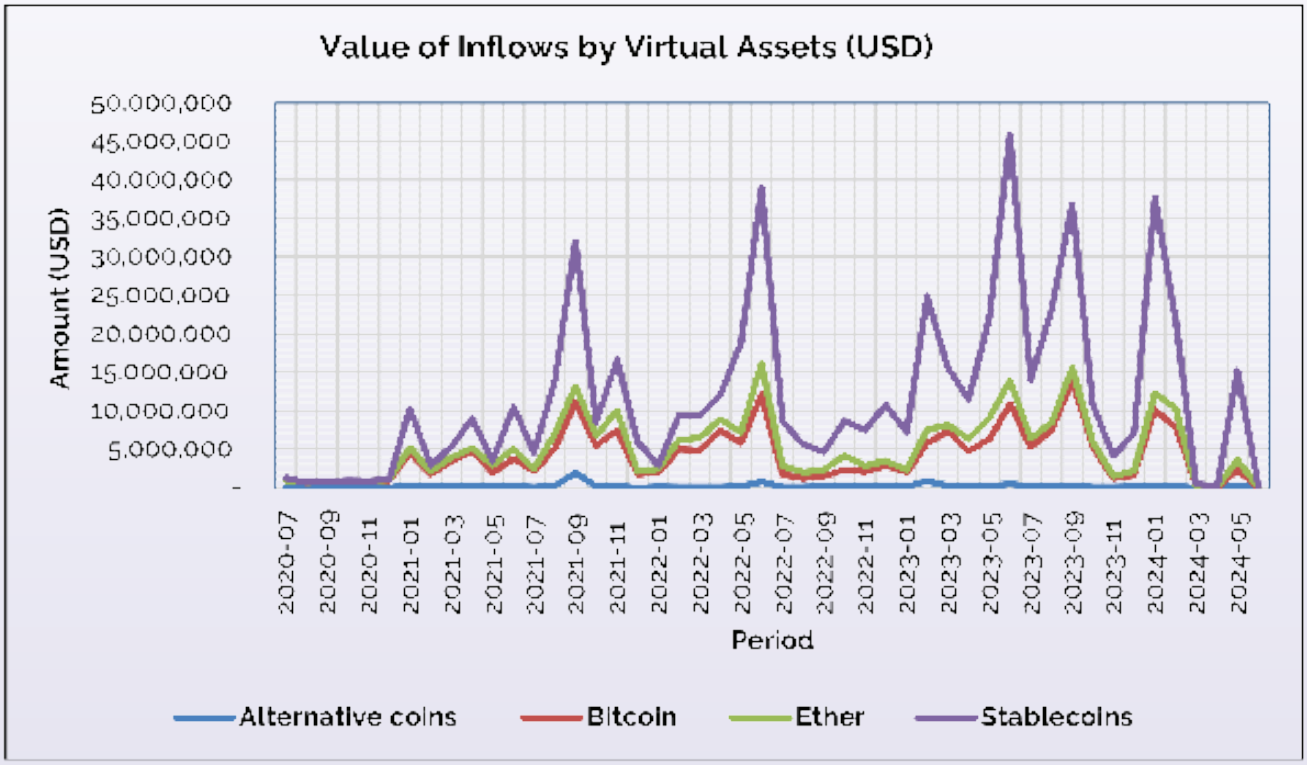


"ATMs, while generally associated with legitimate use, can facilitate anonymous transactions that are attractive to illicit actors seeking to launder funds."

3.5 Trend of Inflows by Specific Virtual Assets in Uganda

Analysis of inflows for specific VAs that are prevalent in Uganda was undertaken to determine the most traded VAs as shown in the figure below;

Figure 10 **: Trend of Inflows by Specific Virtual Assets**



Source: *Commercial Blockchain Analysis tool*

The trend analysis of inflows for VAs in four categories, namely, Alternative coins, Bitcoin, Ether, and Stablecoins from July 2020 to June 2024 indicates the following observations;

a) Stablecoins, with a total of over USD 314.5 million, show the highest total inflows with a steady rise throughout the period notably months like June 2022 (USD 22.91 million), March 2023 (USD 31.94 million), and January 2024 (USD 25.38 million) indicate their growing popularity. This available data is consistent with global trends where stablecoins are often used for large-scale, cross-border transactions due to their price stability, efficiency and accessibility. This can potentially make them attractive for illicit financial activities, including Money Laundering and Terrorist Financing particularly in jurisdictions with weak AML/CFT controls within the VA ecosystem.

b) Bitcoin shows the second highest total inflows, reaching over USD 189.8 million. The data indicates significant fluctuations in Bitcoin's monthly inflows, with large spikes in months such as January 2021 (USD 4.19 million), September 2021 (USD 9.17 million), and March 2023 (USD 13.48 million). These peaks, especially in the early and middle years, suggest high interest and active trading in Bitcoin, with the largest inflows in 2021 and 2022. Given Bitcoin's relatively high liquidity and widespread use in illicit activities, its dominance raises concerns particularly in monitoring large cross-border transactions or rapid movements between high-risk jurisdictions.

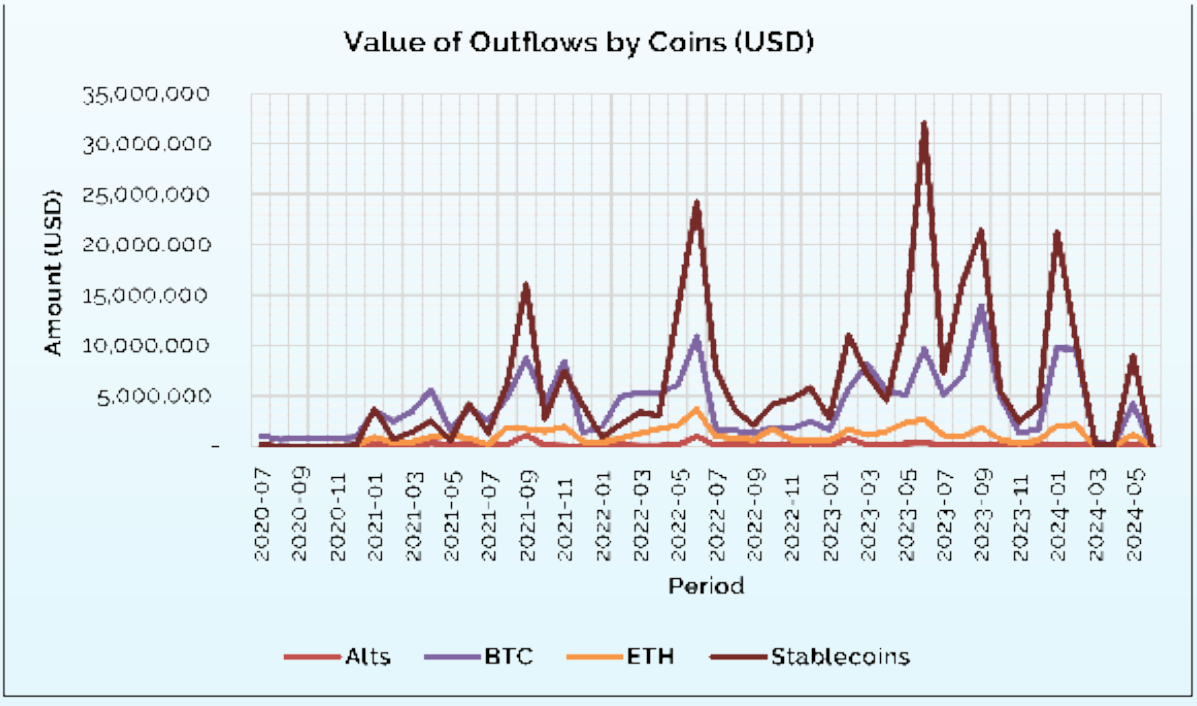
c) Ether, with a total of USD 51.06 million, shows substantial fluctuations, with large inflows in months like June 2022 (USD 4.03 million), May 2023 (USD 2.81 million) and June 2023 (USD 3.05 million). The inflows in Ether can be attributed to its strong role in decentralised finance (DeFi) platforms, which have grown in prominence. The rise of these platforms and their associated risks, such as the use of anonymous wallets or non-compliant platforms, makes DeFi a potential vehicle for illicit financial flows into and out of Uganda.

d) Alternative coins show more erratic inflows, with a total of USD 8.82 million over the period into Uganda. While the total is much lower than Bitcoin or Stablecoins, months like September 2021 (USD 1.88 million), June 2022 (USD 0.767 million) and February 2023 (USD 0.86 million) indicate occasional surges. These coins, due to their lower profile, may be used to obscure illicit activities. Their increased use could suggest that individuals or groups may be seeking to bypass traditional monitoring systems, which makes them a potential area of concern for money laundering activities.

3.6 Trend of Outflows by Specific Virtual Assets in Uganda

Analysis of outflows for specific VAs that are prevalent in Uganda was undertaken to determine the most traded VAs as shown in the figure below;

Figure 11 : Trend of outflows by coins



Source: *Commercial Blockchain Analysis tool*

Similar to the trend in VA currency inflows, the figure above shows outflow remittance transactions for Uganda from July 2020 to June 2024 with the following observations on VA categories, including Alternative coins (Alts), Bitcoin (BTC), Ethereum (ETH), and Stablecoins;

a) Between 2020 and 2024, there was a marked increase in the total volume of remittance transactions, particularly in Bitcoin (BTC) and Stablecoins. The volume for BTC, for instance, saw a notable surge, increasing from USD 1,063,015 in July 2020 to a peak of USD 13,960,547 by September 2023. Stablecoins also exhibited consistent growth, reaching a cumulative total of USD 294,425,732 in June 2024. These large increments in outflows are indicative of rising interest in virtual asset transactions driven by factors such as greater market awareness, increased investor participation, and the expanded use of virtual assets in cross-border remittances.

b) When analysing the individual VA categories, Bitcoin (BTC) consistently contributed a large portion of remittance outflows from Uganda over the reviewed period. From a volume of USD 1,063,015 in July 2020 reaching a high of USD 13,960,547 in September 2023. This growth suggests increasing use of Bitcoin for remittances and investment in Uganda. Given Bitcoin's decentralised nature and its ability to facilitate cross-border transactions, this increase raises concern about its potential use for illicit activities such as money laundering, particularly as the VA's nature such as anonymity features can complicate efforts to trace and seize proceeds of crime.

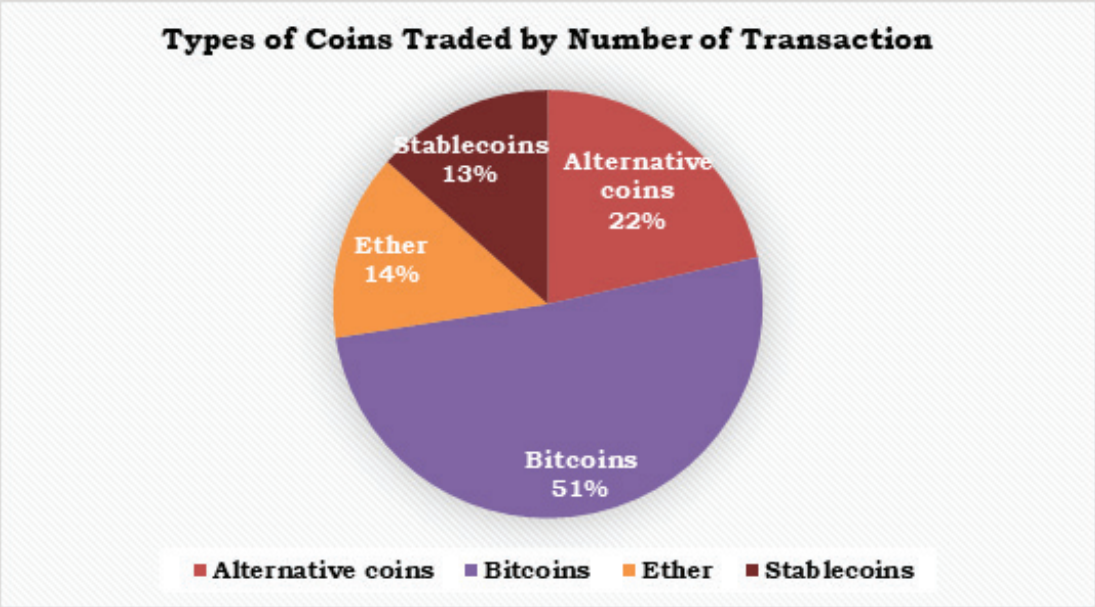
c) Ethereum (ETH) also demonstrated considerable growth, albeit at a slower rate compared to Bitcoin, with outflows increasing from USD 77,579 in July 2020 to a cumulative total of USD 48,294,607 in June 2024. As Ethereum supports various decentralised finance (DeFi) platforms and smart contracts, its rise in remittance transactions could indicate an increased use of decentralised platforms for international transactions, which may complicate AML/CFT efforts. The use of Ethereum for such activities could be particularly challenging as it operates within ecosystems that are not always subject to traditional financial regulations.

d) The consistent growth in the use of Stablecoins is of particular concern in the context of ML/TF risks. In 2020, the remittances involving Stablecoins were relatively modest at USD 129,990, but by June 2024, this had surged to a cumulative total of USD 294,425,732 reaching the highest transaction volume of USD 32,008,783 in June 2023. Stablecoins, due to their pegged value to fiat currencies like the US dollar, offer a level of price stability that is attractive for remittances. However, their increased use could present a risk if they are used to bypass regulations and facilitate untraceable transactions. The anonymity offered by some Stablecoin transactions could make it easier for illicit actors to move funds across borders without detection, thus contributing to the ML/TF risks.

The analysis of outflow remittance transactions from Uganda reveals significant and increasing activity in VAs, particularly in BTC, ETH, and stablecoins. While these assets have legitimate uses, their use in large and frequent remittance flows raises concerns about their potential misuse for illicit financial activities.

3.7 Types of Specific Virtual Assets Traded in Uganda

Figure 12 : **Types of Coins traded**



Source: *Commercial Blockchain Analysis tool*

Figure above shows the number of transactions for each type of VA traded in Uganda from July 2020 to June 2024 which further complements the previously identified trends in both inflow and outflow remittance transactions. This data offers better understanding into the volume and frequency of virtual asset transactions and can be contextualized within the broader discussion on ML/TF risks in Uganda. The following observations were made

a) Bitcoin (BTC)

With 5,011 known transactions recorded over the period representing 51% of total known VA transactions, Bitcoin stands out as one of the most frequently traded VA in Uganda after stable coins. This aligns with the earlier observation that Bitcoin had the second highest transaction volumes in terms of USD inflows and outflows, particularly in 2021. Bitcoin's dominance in the number of transactions highlights its widespread use for remittances and as a store of value.

The fact that Bitcoin continues to account for a significant proportion of transactions also suggests that it remains the preferred VA for users in Uganda, likely due to its liquidity and recognition within the broader virtual asset ecosystem. However, this high number of transactions also presents substantial ML and TF risks. Bitcoin's pseudonymous nature can make it difficult for authorities to track the flow of funds, especially when funds are transferred to or from jurisdictions with weak regulatory frameworks.

b) Alternative Coins (Alt coins)

Alternative coins accounted for 2,114 transactions representing 22% of total known VA transactions over the same period, which is a significant figure, though it was still less than Bitcoin's total. The considerable number of altcoin transactions linked to residents in Uganda demonstrates growing interest in virtual assets beyond Bitcoin and Ethereum. Given that alternative coins may have smaller market caps and potentially higher volatility compared to Bitcoin and Ethereum, their use indicates speculative trading or hedging strategies.

Altcoins are often less regulated, and their use in remittances can present challenges for monitoring,increasing the risk of misuse for illicit financial activities. The growing market for altcoins raises concern as they can be used to obscure transactions or funnel illicit funds through decentralised exchanges or peer-to-peer platforms.

c) Ethereum (ETH)

Ethereum, with 1,387 transactions, ranked third in frequency representing 14%, reflecting its important role in the virtual asset landscape, particularly in decentralised finance **(DeFi)** applications. Ethereum's infrastructure facilitates smart contracts and decentralised applications, which have become increasingly popular globally. The number of transactions recorded is consistent with the earlier observation that Ethereum transactions, while volatile, can contribute to significant financial flows.

The use of Ethereum for DeFi purposes presents unique risks, particularly as decentralised platforms may not always implement sufficient AML/CFT measures.These characteristics

make Ethereum a potential vehicle for ML/TF activities, especially if used for anonymous transfers or in jurisdictions lacking robust AML/CFT regulations.

Stablecoins represented 13% of the total known VA transactions.

d) Stablecoins

Stablecoins had 1,319 known transactions recorded during this period, representing 13% of the total known VA transactions. Despite their lower transaction count compared to Bitcoin, the substantial value of stablecoin remittances in the earlier analysis (e.g., in June 2022 with a high of USD 24,277,412 and January 2024 with a high of USD 21,198,707) suggests that stablecoins are being used for large value transfers. Based on the available data, stablecoins have become increasingly popular in Uganda given their price stability for remittances and international trade. However, their frequent use in cross-border transactions introduces significant ML/TF risks, particularly in jurisdictions where financial systems may not be fully equipped to monitor such transactions.

3.8 Transactions Conducted by Services using VAs in Uganda

Below is a detailed examination of how various types of VAs, namely Bitcoin, Ether, Stablecoins, and Alternative Coins are employed across different services in Uganda, ranging from exchanges and merchant services to scams, illicit marketplaces, and sanctioned entities. The accompanying table provides transaction counts for each service, illustrating the prevalence of Bitcoin in areas such as P2P exchanges, scams, and gambling, as well as the growing adoption of other VAs like Ether and stablecoins for more specialised activities, including NFT platforms and hedging.

Table 2 : Number of transactions conducted by Services using respective coins in Uganda

Sn	Service	Alternative Coins	Bitcoin	Ether	Stablecoins
1.	Exchange	1,342	2,334	841	882
2.	Other	163	674	103	62
3.	Scam	109	385	68	105
4.	Gambling	164	244	96	93
5.	P2P exchange	104	194	76	67
6.	Merchant services	132	162	91	55
7.	Illicit actor-org		430		
8.	Infrastructure as a service	16	337	46	23
9.	Hosted wallet	31	96	21	21
10.	Mining pool	31	59	34	4
11.	Fraud shop	15	42	1	1
12.	Darknet market	1	20		
13.	Mixing		20		
14.	ATM	2	6	2	2
15.	OFAC Sanctioned entity	4	4	2	2
16.	NFT platform - collection			6	2
17.	Online pharmacy		4		
	Grand Total	**2114**	**5011**	**1387**	**1319**

Source: *Commercial Blockchain Analysis tool*

The table above shows the volume of transactions conducted by different virtual asset services using various types of virtual assets, including Alternative coins, Bitcoin, Ether, and Stablecoins.

a) Bitcoin with 2,334 transactions remains the dominant VA used in exchanges, followed by Alternative coins at 1,342 transactions, Stablecoins (882), and Ether (841). Exchanges facilitate the highest volume of transactions, with Bitcoin being the primary asset, due to its established reputation, liquidity, and ease of conversion. The relatively high number of transactions in Alternative coins indicates that exchanges are not only catering to Bitcoin users but also to those trading altcoins, such as Ethereum, Litecoin, and others. Stablecoins, which are tied to traditional fiat currencies, are used in exchanges for hedging against volatility and as a medium of exchange for trading.

b) Scams (109 transactions for Alternative coins, 385 for Bitcoin, 68 for Ether, and 105 for Stablecoins) highlight that scammers continue to prefer Bitcoin, evidenced by the high volume of Bitcoin transactions in fraudulent activities. Bitcoin's popularity and pseudonymous nature make it a target for scam operations. Stablecoins also show a considerable number of transactions, likely due to their stable value, which can be appealing in scams, as they offer more predictable value during illicit transactions. The use of Ether and Alternative coins in scams is lower but still significant, suggesting that these coins are also being exploited in fraudulent operations, albeit at a smaller scale.

c) Gambling services (164 transactions for Alternative coins, 244 for Bitcoin, 96 for Ether, and 93 for Stablecoins) show a clear preference for Bitcoin, followed by Alternative coins, with a moderate presence of Ether and Stablecoins. Bitcoin remains the top choice in online gambling due to its widespread acceptance and anonymity, although Alternative coins and Stablecoins also have a notable presence in this space, providing alternatives for users who may want to avoid Bitcoin's more public reputation.

d) P2P exchanges (104 transactions for Alternative coins, 194 for Bitcoin, 76 for Ether, and 67 for Stablecoins) also show significant activity, with Bitcoin being the most commonly used currency. This trend mirrors the overall dominance of Bitcoin in peer-to-peer transactions, with users preferring this VA for its liquidity and reliability. Other coins like Alternative coins and Ether are also being used for P2P transactions but at a lower frequency, likely due to regional preferences or transaction fee considerations.

e) Fraud shops (15 transactions for Alternative coins, 42 for Bitcoin, 1 for Ether, and 1 for Stablecoins) focus heavily on Bitcoin, which again is linked to its use in illicit activities. Despite being a smaller category in terms of transaction volume, fraud shops continue to use Bitcoin because of its widespread recognition and ease of use in underground markets.

f) Darknet markets (1 transaction for Alternative coins, 20 for Bitcoin) show that Bitcoin remains the most prominent VA used in the purchase and sale of illicit goods. While the volume is low compared to other categories, the presence of Bitcoin as the primary VA highlights its association with illicit marketplaces. The low transaction count reflects the niche nature of the darknet economy compared to mainstream exchanges and services.

g) Mixing services (20 transactions for Bitcoin) are used to obscure the origin and destination of VA transactions. Bitcoin dominates here as well, suggesting that mixers are still most commonly used with Bitcoin to enhance user anonymity and evade detection.

h) Merchant services (132 transactions for Alternative coins, 162 for Bitcoin, 91 for Ether, and 55 for Stablecoins) show that Bitcoin and Alternative coins are most commonly used for payments in online and offline commercial services. Bitcoin's dominance suggests that many merchants still prefer it for its network effects, but Alternative coins and Ether also play a significant role in retail and service transactions. The low use of Stablecoins here may be because merchants prefer more volatile VAs for speculative purposes or are yet to adopt stablecoin payments widely.

i) Hosted wallets (31 transactions for Alternative coins, 96 for Bitcoin, 21 for Ether, and 21 for Stablecoins) indicate that Bitcoin is the most popular coin in hosted wallet services. Hosted wallets, which allow users to store and transact VA via a third-party service, see moderate usage compared to exchanges. The low transaction numbers in other categories suggest that the hosted wallet service is still emerging, with Bitcoin's dominance still evident in storage and transactions.

j) Mining pools (31 transactions for Alternative coins, 59 for Bitcoin, 34 for Ether, and 4 for Stablecoins) are primarily focused on Bitcoin, as it remains the dominant VA for mining due to its historical position as the most valuable and well-established blockchain. Although Ether is also relevant due to Ethereum's network, Bitcoin continues to attract the most mining activity due to its larger market cap and established mining infrastructure.

"Bitcoin, as it remains the dominant VA for mining due to its historical position as the most valuable and well-established blockchain."

k) Infrastructure as a service (16 transactions for Alternative coins, 337 for Bitcoin, 46 for Ether, and 23 for Stablecoins) shows Bitcoin as the most widely used currency for blockchain-related infrastructure services. The high volume of transactions for Bitcoin suggests that the underlying infrastructure for Bitcoin continues to dominate the blockchain service space, reflecting its robust and established market.

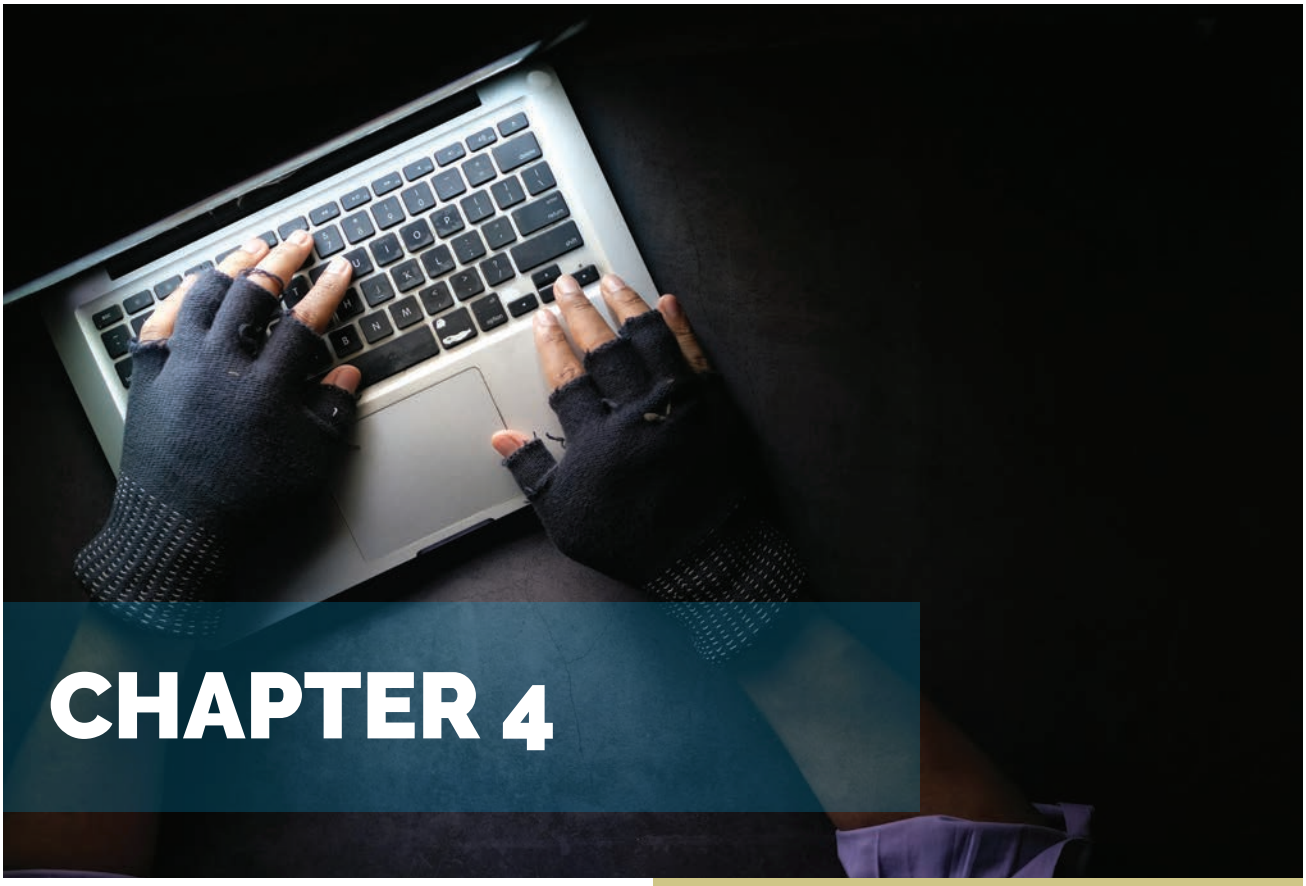
l) NFT platforms (6 transactions for Ether, 2 for stablecoins) show limited usage, but Ether and Stablecoins are the primary coins used for the purchase and sale of NFTs. The low transaction volumes suggest that NFT platforms are still developing, with Ether leading due to Ethereum's network being the dominant blockchain for NFT creation.

m) Online pharmacies (4 transactions for Bitcoin) show Bitcoin as the preferred VA in illicit and underground services, where pharmaceutical products may be sold illegally. The very low transaction numbers suggest this is a niche market, but Bitcoin continues to dominate due to its reputation and perceived anonymity.

n) Sanctioned entities (4 transactions for Bitcoin, 2 for Ether) reflect transactions involving entities that were subjected to OFAC sanctions. The limited number of transactions suggests that these entities do not conduct many transactions openly but are still active, with Bitcoin and Ether being their primary methods of exchange in Uganda.

o) Illicit actor organisations (430 Bitcoin transactions) show Bitcoin as the most widely used VA for illicit activities, reflecting its adoption by organisations involved in illegal activities. This high number suggests that Bitcoin is favored by organisations operating in illicit markets due to its widespread use and relative anonymity.

p) ATMs (2 transactions for Alternative coins, 6 for Bitcoin, 2 for Ether) show very limited activity but indicate that Bitcoin remains the most widely supported VA for use in ATMs, reflecting its ongoing dominance in the physical exchange of VA. Available information indicates that the VA ATM operated in Uganda from April 2021 to November 2022 when the authorities shut it down. However, the entity continues to operate as an OTC service provider but the VA ATM still appears on website as active, whereas not.



CHAPTER 4

> "This chapter examined the threats and vulnerabilities associated with both VAs and VASPs in Uganda"

4.1 VA AND VASP THREATS AND VULNERABILITIES

This chapter examined the threats and vulnerabilities associated with both VAs and VASPs in Uganda. It employed a distinctive and sophisticated methodology grounded in collected data, weighted averages, and integrated formulas within the assessment framework supported by the VA RA World Bank tool. The evaluation considered intermediate and input variables influencing threats and vulnerabilities from both domestic and international perspectives. It spanned a wide spectrum, from large multinational VASPs with extensive client networks to smaller VASPs and a variety of VA types operating in Uganda as clearly defined in Chapter 3 above.

4.1.1 The Overall Threat Level

The overall ML/TF threat posed by VAs and VASPs in Uganda was assessed as **High**. This was attributed to the average number of VASPs identified and the diverse range of VAs operating in the country. Many VASPs were based in other jurisdictions while extending their services to residents of Uganda. The actual number of VASPs operating in Uganda is unknown, however based on company registration records, there were 19[17] companies registered to offer services of VASPs in Uganda. However, the Blockchain Association of Uganda reported 10 registered members actively engaged in VASP-related business during the same period. Furthermore, out of the 19 VASPs registered in Uganda, 16 were registered with the Financial Intelligence Authority for compliance with AML and CFT requirements in line with the Anti-Money Laundering Act, Cap 118.

The figure below illustrates six intermediate variables representing the average threats associated with VAs and VASPs. These inherent ML/TF risks were evaluated prior to the application of any controls or mitigation measures.

Figure 13 **: Threat Levels of VAs and VASPs from a Product Perspective**

Source: *VA & VASP ML/TF Risk Assessment Tool*

The ML threat level was heightened by the absence of dedicated legislation to regulate and supervise the VA activities of these operators. The assessment team determined that the availability of clear shareholder and director information for the registered providers reduced the opacity of ownership structures among these VASPs, which is a critical factor

17 Uganda Registration Services Bureau Records as at June 30, 2024

in threat assessment. Uganda regularly updates the Beneficial Ownership (BO) register that supports the verification of true identities of all relationships and operations connected to VAs and VASPs. Currently, the law requires that sufficient information be provided on BO for each registered company, a practice that is being implemented.

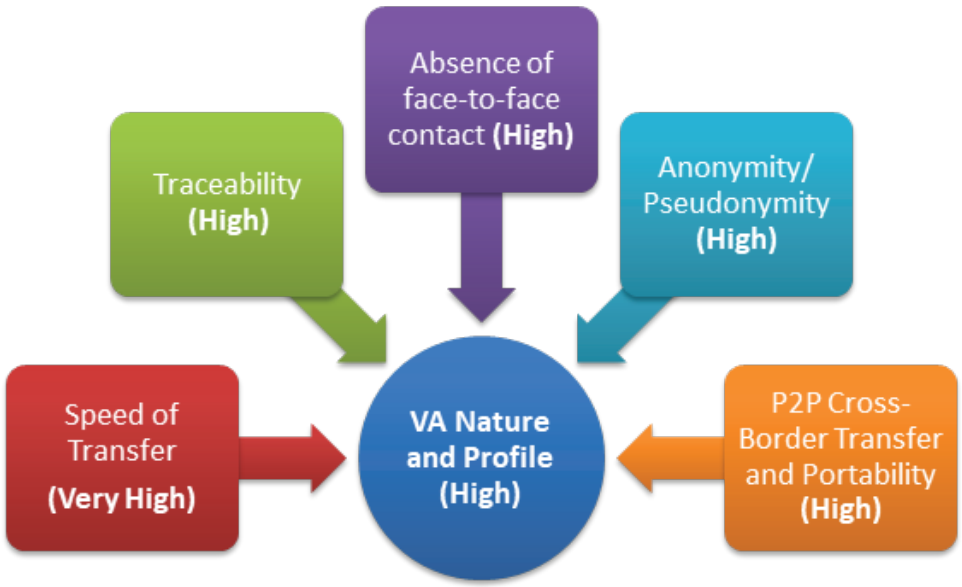
4.2 Threats Analysis

ML/TF threat for VAs and VASPs was assessed by considering input variables on the product dimension, which provides an understanding of the inherent risks before implementing any AML/CFT controls or mitigation measures. This approach focused on identifying and quantifying the risks associated with VAs and VASPs based on their nature and the broader context in which they operate.

The assessment relied on six intermediary variables of the threats in the VA-RA (Virtual Asset Risk Assessment) World Bank tool. These variables provide a framework for analysing and understanding the ML/TF risks associated with VAs and VASPs as detailed below:

4.2.1 VA Nature and Profile

Figure 14 : Summary of Risk Elements in VA Nature and Profile

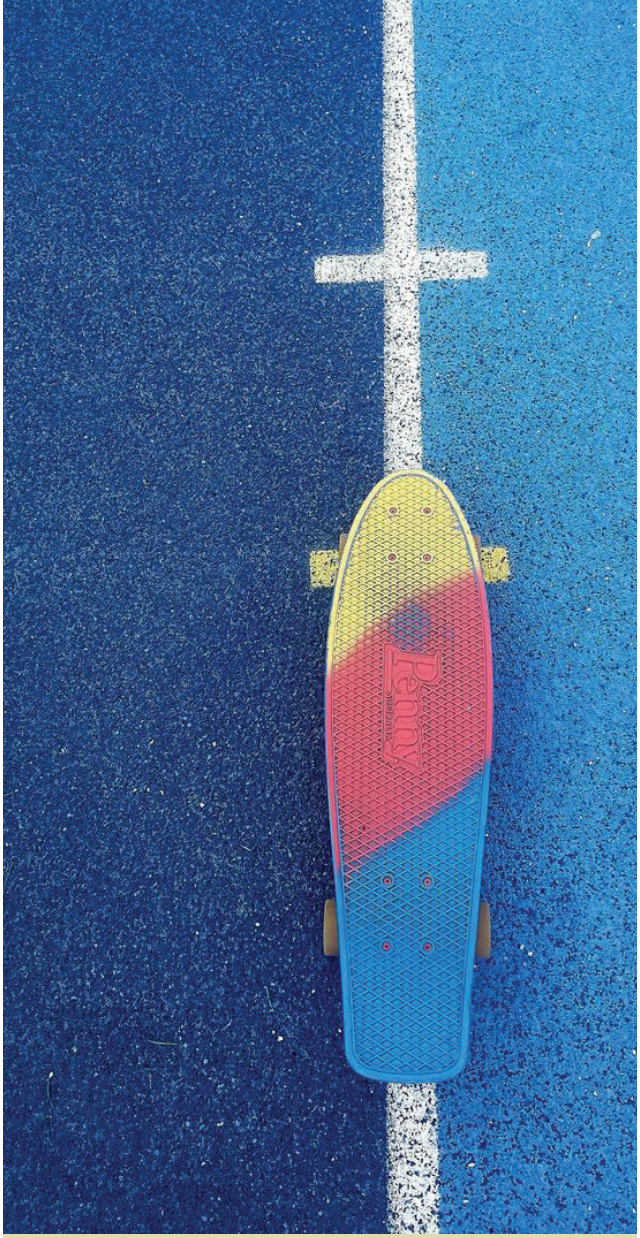


4.2.1.1 Anonymity and Pseudonymity

In Uganda, the anonymity and pseudonymity nature of VAs linked to considerable volume of transactions where it is challenging to establish the ultimate beneficial owners of certain VAs. There are many tools that enhance anonymity within the VA ecosystem such as mixers, tumblers, IP anonymisers which can obscure transactions and inhibit VASPs ability to know its customers and implement AML/CFT measures which requires prevention, detection and investigations of proceeds of crime associated with VAs leading to a **very high** ML/TF threat.

4.2.1.2 Peer-to-Peer cross-border transfer and portability

The peer-to-peer (P2P) cross-border transfer and portability nature of VAs in Uganda facilitates the decentralised and seamless movement of funds across borders without the need for traditionally known intermediaries. According to the Chainalysis VA adoption reports for 2023, Uganda was ranked 18th out of 155 countries in peer-to-peer exchange trade volumes with substantial inflows of USD 13,801,693 and outflows of USD 15,684,705 from July 2020 to June 2024. This makes VAs particularly attractive for legitimate purposes such as remittances and international payments, providing speed and convenience to users. However, these same features present significant risks, as transactions often occur outside the purview of regulated financial systems, complicating efforts to monitor or trace the flow of funds effectively resulting in **a very high ML/TF threat** associated with the portability of VAs.



Uganda was ranked 18th out of 155 countries in peer-to-peer exchange trade volumes with substantial

Inflows **USD 13,801,693**

USD 15,684,705 Outflows

From July 2020 - June 2024

4.2.1.3 Absence of face-to-face control

The absence of face-to-face controls in VA transactions in Uganda creates significant challenges for ensuring identification and verifying the identity of parties involved in transactions. Unlike traditional financial systems that rely on physical presence or robust identification processes, VA transactions are conducted entirely online, often under pseudonymous or anonymous identities that may be easily falsified. This lack of direct interaction weakens effective CDD measures, making it attractive to criminals and thus permiting anonymous funding or not revealing the identity of the parties involved in the transactions. This coupled with the peer-to- peer transferability of VAs, the degree of anonymity/ pseudonymity, and the large transaction volumes highlighted in Chapter 3, this variable poses a **high ML/TF threat** to Uganda's financial ecosystem.

4.2.1.4 Traceability

The traceability of VAs in Uganda presents a mixed picture since blockchain technology ensures that all transactions are permanently recorded on an immutable ledger, nevertheless, the use of mixers and Virtual Private Networks (VPNs) by some Ugandan residents complicates identifying transaction originators and beneficiaries. This adds an additional layer of obfuscation, making it challenging to link transactions to specific individuals, especially in the absence of robust CDD measures.

The Travel Rule in line with FATF recommendation 16 mandates the sharing of originator and beneficiary information during VA transfers, enhances traceability of VAs. However, there is limited enforcement of this rule which potentially enables individuals to conduct transactions without providing sufficient identification data. Despite these challenges, blockchain technology's inherent transparency offers significant opportunities for tracing transactions when combined with the right technical tools, signal intelligence, and human intelligence. This capability ensures that, with appropriate resources and expertise, illicit activities can be uncovered and addressed.

Given these factors, the traceability of VAs in Uganda poses a **High-level ML/TF threat** due to the balance between challenges in identification and the potential for effective monitoring through blockchain analysis and intelligence support.

4.2.1.5 Speed of Transfer

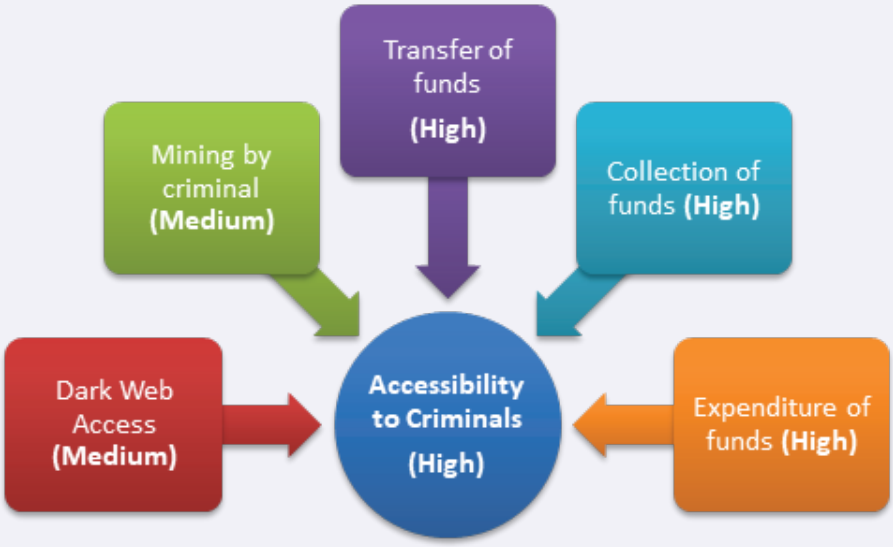
VA transactions can be processed almost instantaneously across borders, enabling rapid movement of funds at a minimal cost without the traditional delays associated with conventional banking systems. This speed, while beneficial for legitimate users, also facilitates the swift movement of illicit funds, allowing criminals to quickly transfer and launder value without sufficient time for regulatory scrutiny or intervention. The absence of real-time monitoring, compounded by weak enforcement mechanisms in Uganda, creates an environment where transactions can be completed before they are flagged or investigated.

Additionally, the ability to execute high-volume transactions within short time frames without the need for intermediaries further complicates efforts to detect and prevent illicit financial flows. The rapid movement of funds across jurisdictions, coupled with the lack of adequate oversight and controls, makes it highly challenging for authorities to track and halt these transactions in real time.

Given the speed of transfer coupled with anonymity, peer-to-peer exchanges, absence of face to face controls contributes to a very high ML/TF threat in Uganda.

4.2.2 Accessibility to Criminals

Figure 15 : Summary of Risk Elements in Accessibility to Criminals



4.2.2.1 Mining by Criminals

According to data from commercial block chain analysis tools, mining[18] pools in Uganda involve collaborative efforts by multiple miners to enhance computational efficiency and share rewards which were linked to **USD 1,187,506** in inflows and **USD 485,278** in outflows in the reviewed period. These figures demonstrate the growing activity in mining operations, even though mining infrstructure and knowledge in Uganda are relatively limited. Privacy focused VAs that can be mined further amplify these risks, as they provide greater anonymity and are harder to trace. The proliferation of unlicensed VASPs offering global mining applications poses a growing threat. These platforms often bypass existing regulations, making them an attractive option for criminals.

In Uganda, this process presents specific ML/TF threats, particularly because it allows individuals to generate anonymous and untraceable funds. Criminals can exploit mining activities, especially when mining operations are covertly managed or linked to unregistered VASPs. The absence of strict oversight coupled with limited detection increases the threat of these funds being used for illicit activities such as ML or TF.

While mining operations in Uganda are not yet widespread, the ML/TF threat was assessed **medium** reflecting the current low scale of mining but acknowledges the inherent risks and the growing presence of mining pools linked to substantial financial flows.

4.2.2.2 Collection of Funds

The collection of illicit funds through VAs presents a growing and significant threat in Uganda. Criminals leverage the anonymity, decentralisation, and cross-border reach of VAs to facilitate crimes such as online scams, human trafficking, and ransomware attacks. These transactions often bypass traditional financial institutions, making it challenging for authorities to monitor or trace their origins. Furthermore, the DeFi adoption levels of Uganda from the ranking of 105 out of 155 countries in 2022 to the current ranking of 12th in the world demonstrates that criminals may collect funds in Uganda without detection, creating new opportunities for financial abuse.

VAs have also become magnets for illicit activities such as theft and fraud, with growing concerns about their potential use in funding terrorism. According to available law enforcement data for the reviewed period, there were 06 cases of fund mobilisation by known sympathizers of the Islamic State – Central Africa Province (ISCAP), formally the Allied Democratic Forces that eventually ended in disruption by the counter terrorism intelligence agencies. This demonstrates that terrorist groups or their supporters can use VAs to collect and transfer funds through broker intermediaries or crowd funding platforms, which are convenient channels for anonymously supplying resources for attacks.

18 Mining refers to the process of validating VA transactions and creating new VAs through computational work.

Additionally, available data in the reviewed period showed that scams, fraud shops and mixing services totaling USD 4,223,734 in inflows and USD 6,086,356 in outflows also compound this ML/TF threat which was assessed High.

4.2.2.3 Transfer of Funds

The transfer of funds linked to VAs across borders presents ML/TF threats to Uganda, particularly given the decentralised and pseudonymous nature of these assets. This characteristic enables criminals to transfer illicit funds rapidly and seamlessly, bypassing traditional banking systems and evading scrutiny by financial institutions or LEAs. For terrorist groups, the ability to quickly and anonymously move funds to less developed regions where such groups may operate makes VAs an attractive medium for financing. Similarly, entities or individuals under international sanctions can exploit this system to circumvent financial restrictions and funnel funds to prohibited activities. Recent assessments further reveal financial flows associated with sanctioned entities, with USD 724 in inflows and USD 1,162 in outflows. While these figures may seem modest, they demonstrate the ease with which VAs can facilitate transactions to and from high-risk jurisdictions or entities under sanctions.

These risks are aligned with the input variables such as the 'Absence of face-to face control' and the 'Speed of transfer', which highlight the challenges in monitoring and intercepting suspicious VA transactions. Given these factors, the ML/TF threat posed by the transferability of VAs in Uganda was assessed as **high.**

4.2.2.4 Dark Web Access

The use of VAs for transactions on the dark web presents a serious threat to Uganda, particularly as it provides a platform for the trade of illegal goods and services, including drugs, weapons, and stolen data. The anonymity and decentralisation offered by VAs make them an ideal medium for conducting untraceable transactions on these illicit online marketplaces. Furthermore, the use of Virtual Private Networks (VPNs) by some Ugandan residents adds another layer of complexity in tracking these transactions, as it obscures the origin and destination of funds. This significantly hampers authorities' ability to monitor and investigate illicit activities on the dark web.

Recent data detailed in chapter 3 above revealed financial flows linked to darknet transactions worth USD 1,274 in inflows and USD 1,319 in outflows. While the use of the dark web for illicit activities in Uganda is still relatively low, due to limited technical knowledge and accessibility, its potential for expansion remains a concern. The ease with which criminals can exploit VAs to fund their activities, combined with the lack of effective monitoring tools and enforcement mechanisms, emphasises the growing ML/TF threat. Given the relatively low transaction volumes on detected on the darknet for Uganda, the

ML/TF threat from the use of VAs on the dark web in Uganda was assessed as **medium**.

4.2.2.5Expenditure of Funds

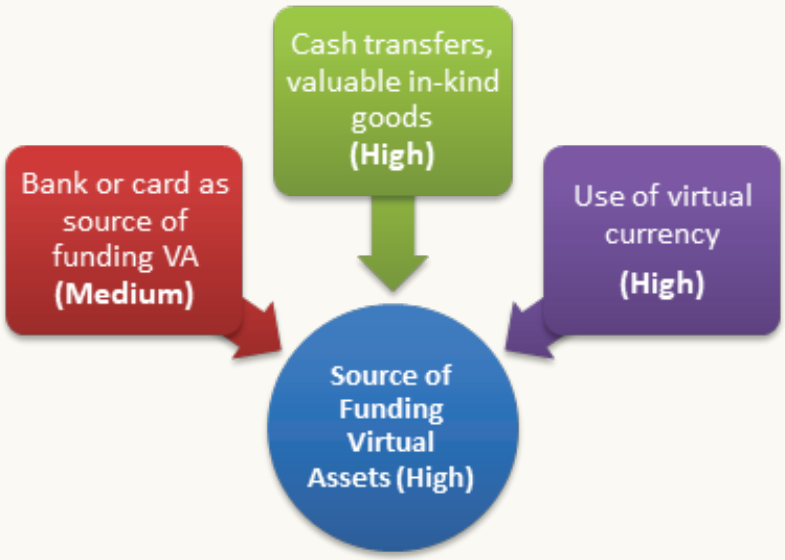
The use VAs in Uganda provides criminals with a convenient and effective method to spend illicit funds, bypassing the formal financial system. Criminals engage in online purchases, pay for illegal goods and services, and convert illicit funds into digital assets such as non-fungible tokens (NFTs), which makes it difficult for traditional financial institutions to detect and trace these transactions. Due to the pseudonymous nature of VAs, these transactions often remain outside the reach of traditional monitoring systems. Furthermore, the absence of adequate AML/CFT supervision over VASPs in Uganda enables criminals to easily convert illicit funds into fiat currency without scrutiny, further perpetuating the risk of ML or TF.

NFTs and Stablecoins as emerging technologies provide an increased ML/TF threat, with various VASPs in Uganda offering these products. Despite the lower economic impact and ease of criminality by NFTs, the same cannot be observed on Stablecoins which present a mixture of moderate to high risks, particularly related to their potential use in criminal activity, ease of criminality, and their significant economic impact measured at 82%, and ability to facilitate cross-border transactions make them vulnerable to misuse.

The high transaction volumes of stablecoins, and the ever-growing adoption of decentralised finance transactions in Uganda which are all difficult to detect by LEAs and other competent authorities pose a high ML/TF threat to the country.

4.2.3 Source of Funding Virtual Assets

Figure 16 : **Overview of Funding Sources for Virtual Assets**



4.2.3.1 Bank or card as source of funding VA

In Uganda, banks and card issuers[19] are regulated by BoU, enabling the traceability of card or bank-related transactions as potential sources of funding for VAs. BoU issued a directive[20] prohibiting all its supervised entities, including banks and card issuers, from engaging in or facilitating VA-related activities. Consequently, these entities disallowed VA-related transactions, effectively reducing the ML/TF threat of bank accounts and card schemes being used to fund VAs. This ban underscores Uganda's regulatory stance aimed at mitigating threats, both macro and micro, to the traditional financial sector.

On account of the strict enforcement of this directive, banks have identified instances of customer-driven transactions linked to VAs. In the period of July 2020 to June 2024, 6 out of 49 SARs were linked to VAs involving bank accounts or cards as funding sources for VAs or as payment channels to VASPs. These transactions occurred when customers used their accounts with commercial banks or payment system operators to facilitate VA funding or payments.

While these breaches were identified and reported by financial institutions as SARs to the Financial Intelligence Authority for further action, such transactions remain limited in scale. Criminals tend to avoid exploiting this channel due to increased detection risks, thereby reducing its potential for abuse. As a result, the ML/TF threat associated with these funding channels was assessed **medium.**

July 2020 to June 2024, 6 out of 49 SARs were linked to VAs involving bank accounts or cards as funding sources for VAs or as payment channels to VASPs.

19 As at December 2024, there were 05 card issuers licensed by Bank of Uganda - https://www.bou.or.ug/bouwebsite/bouwebsitecontent/Supervision/Supervised_Institutions/Supervision/financial_institutions/2024/List-of-licensed-licenced-Institutions-as-at-2-October-2024-003.pdf

20 In April 2022, the Bank of Uganda (BoU) issued two circulars under its mandate, barring all entities licensed under the National Payment Systems Act 2020 and the Financial Institutions Act, 2004 as amended from liquidating VAs, i.e., converting VAs into fiat accounts and vice versa.

“In Uganda, banks and card issuers are regulated by BoU, enabling the traceability of card or bank-related transactions as potential sources of funding for VAs.”

Case Study 1

Use of Bank-Issued Prepaid Card for Funding Virtual Assets

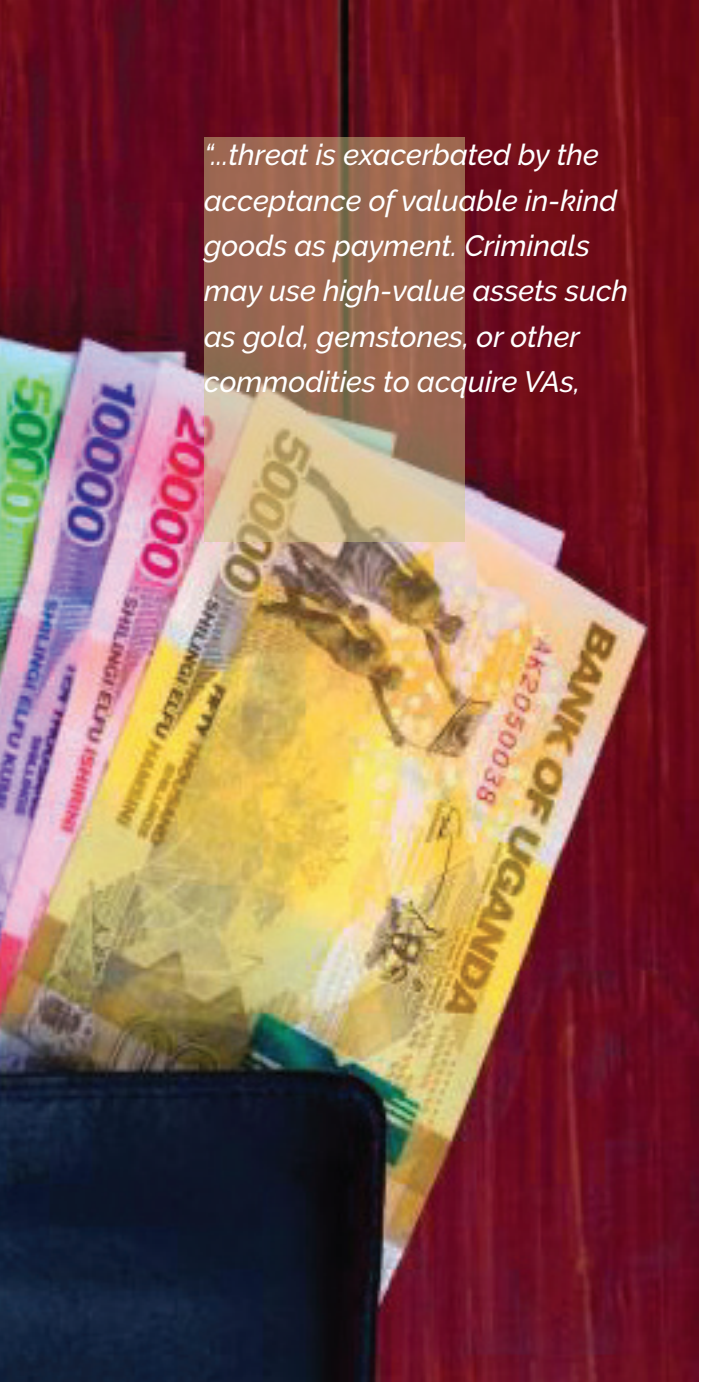
On September 13, 2022, a client acquired a USD-denominated prepaid card (Card Number: 1*********8) from Bank X. The client identified himself as the Managing Director of an international NGO and an employee of a foreign embassy in Uganda. Unlike traditional debit or credit cards, this prepaid card was reloadable and linked to a virtual account. It allowed a customer without a savings or current account to load funds directly at the bank or via mobile money and withdraw from any ATM.

The client did not hold any savings or current accounts with Bank X, and his card loads were conducted exclusively over-the-counter. On average, the client loaded approximately USD 550 per transaction and primarily used the card for Point of Sale (POS) payments.

During routine transaction monitoring, Bank X's systems flagged the client's prepaid card activity as unusual. Specifically, the customer made several payments to a prominent international VA exchange with good adoption in Uganda. The cumulative value of these payments amounted to USD 2,000. The client failed to provide supporting documentation for the nature and purpose of these transactions when requested by the bank. Despite multiple attempts, the client was uncooperative and did not furnish the requested documentation. Since VA transactions were prohibited by the banks prudential supervisor, this raised suspicions about the legitimacy of the transactions and their alignment with the sector regulatory framework.

Due to non-compliance and the suspicious nature of the transactions, the bank terminated its relationship with the client on February 1, 2023. The bank submitted a SAR to FIA in accordance with Section 10(2) of the AMLA, Cap 118. The report highlighted the potential involvement of the client in unregulated activities (Virtual assets trading) and the risk of regulatory breach.

This case demonstrates how prepaid cards, despite their convenience, can be misused as funding sources for virtual asset trading. Banks must remain vigilant and proactive in identifying and reporting suspicious activity, particularly in jurisdictions where virtual asset trading is prohibited by sector regulators. By filing an STR and exiting the client relationship, Bank X fulfilled its obligations under AML/CFT regulations and safeguarded its operations from potential regulatory or legal risks.



"...threat is exacerbated by the acceptance of valuable in-kind goods as payment. Criminals may use high-value assets such as gold, gemstones, or other commodities to acquire VAs,

4.2.3.2 Cash transfers, valuable in-kind goods

In Uganda's predominantly cash-based economy, cash transfers and valuable in-kind goods present a significant ML/TF threat for funding VAs. The extensive use of cash, coupled with informal financial practices, provides the anonymity and lack of traceability that criminals exploit for ML/TF, and other financial crimes. Over-the-counter (OTC) services offered by some VA operators and agents readily accept all forms of cash, allowing individuals to convert illicit funds into VAs with minimal detection. Notably, many of these operators impose no transaction limits and, in some cases, fail to implement CDD measures. This creates a permissive environment where high-risk individuals can anonymously fund VAs using large cash transfers or valuable in-kind goods.

The threat is exacerbated by the acceptance of valuable in-kind goods as payment. Criminals may use high-value assets such as gold, gemstones, or other commodities to acquire VAs, effectively bypassing the traditional financial sector. Once converted into VAs, these assets become significantly harder to trace, given the pseudonymity afforded by blockchain technology. Consequently, the ML/TF threat posed by these practices was assessed as **high**.

4.2.3.3 Use of virtual currency

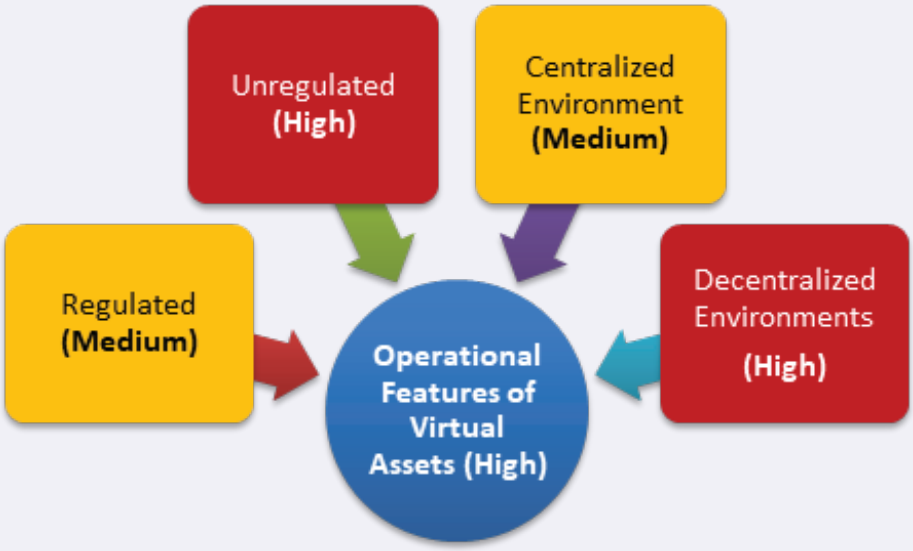
According to the Chainalysis Report for Uganda (June 2020–June 2024), the adoption of virtual currencies (VCs), including virtual assets (VAs) such as stablecoins, has grown significantly as a funding source due to their efficiency, accessibility, and decentralised nature. Peer-to-peer platforms, in particular, enable direct VC transfers without intermediaries, facilitating fast, low-cost, and cross-border transactions.

In Uganda, stablecoins have emerged as the most exchanged VA by transaction value during the review period. Unlike other volatile VAs, stablecoins offer price stability by being pegged to traditional assets such as fiat currencies. Users can maintain balances in stablecoins within their VA wallets, providing a reliable and accessible means for local

and international transactions while mitigating exposure to price fluctuations. However, while VCs such as stablecoins offer significant benefits, their pseudonymity and minimal regulatory oversight pose considerable ML/TF threats. Peer-to-peer transactions and the ability to maintain virtual balances obscure the source and destination of funds, increasing the potential for misuse in illicit activities. Consequently, the ML/TF threat VCs as a funding source was assessed as **high** driven by the prevalence of peer-to-peer transactions and the widespread adoption of stablecoins.

4.2.4 Operational Features of Virtual Assets

Figure 17 : **Summary of Operational Features of Virtual Assets**



4.2.4.1 Regulated

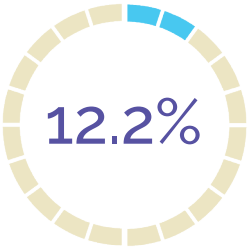
Virtual Assets possess unique operational features that have made them increasingly popular in Uganda for both legitimate and illicit activities based on the available transactional data. These features include decentralisation, borderless transferability, and the ability to facilitate peer-to-peer transactions. However, Uganda currently lacks a comprehensive legal framework specifically governing VAs and VASPs, a regulatory gap that poses significant ML/TF threats to the country. Whereas the AMLA, Cap 118 provides for VASPs as accountable persons, there is yet to be proper guidance to the sector from the Financial Intelligence Authority that is the default AML/CFT supervisor in absence of a dedicated prudential supervisor. Additionally, BoU as a regulator and AML/CFT supervisor for financial institutions and payment system operators has set regulatory standards within its supervised sectors restricting its supervised entities to conduct or interact with VAs or VASPs, a regulatory action that has curbed among others, the ML/TF threat arising from VAs and VASPs.

The majority of popular VASPs operating in Uganda are regulated in foreign jurisdictions and extend their AML/CFT standards to users in Uganda including CDD measures and

transaction monitoring protocols. However, these efforts are undermined by the fact that all prominent VAs in Uganda allow for peer-to-peer transactions, which bypass centralised oversight and regulatory scrutiny entirely. Particularly, these are conducted through non custodial wallets that do not require KYC, a practice common to some users in Uganda basing on the general public survey that indicated that 149 out of 1,221 (12.2%) respondents preferred non-custodial wallets. This capability allows bad actors to use VAs that fall outside Uganda's regulatory perimeter, thereby increasing the potential for misuse.

Given Uganda's progress requiring VASPs to comply with AML/CFT requirements, combined with BoU's directive to all supervised entities not to transact VAs or with VASPs, the ML/TF threat posed under this input variable was assessed as **medium.**

"In Ugnda, based on the general public survey 149 out of 1,221 respondents preferred non-custodial wallets.



4.2.4.2 Unregulated

The regulatory framework for VAs in Uganda is still under development, leaving significant gaps in oversight and enforcement. While most prominent VASPs, including wallet providers, are regulated in foreign jurisdictions and adhere to global AML/CFT standards, there are critical exceptions. Some wallet providers operating in Uganda are domiciled in countries with no VASP specific regulations, exposing users to risks associated with unregulated platforms. These ML/TF threats are further coupled by the decentralised nature of VAs, which allows transactions to swiftly occur across borders with limited scrutiny.

Furthermore, the large volume of VA inflows and outflows to and from high-risk jurisdictions, including some currently listed by FATF as countries under increased monitoring, highlights the threat towards Uganda's VA ecosystem. For instance, criminals may exploit the unregulated status of certain VASPs in foreign jurisdictions to launder proceeds of crime through Ugandan users. Additionally, several of these high-risk jurisdictions have general weaknesses in their AML/CFT frameworks, making them attractive for illicit financial activities.

While global VASPs operating in Uganda extend AML/CFT standards, Uganda's lack of a domestic legal framework means novel business models involving VAs, such as ICOs or DeFi, are often not captured within existing regulations. This creates challenges for consumer protection, market integrity, and financial stability, as highlighted by the InternationalMonetary Fund (IMF) in its analysis of regulatory gaps in emerging economies.[21]

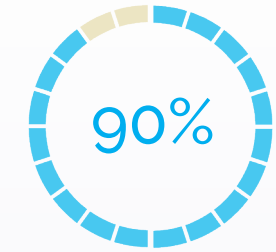
21 https://www.elibrary.imf.org/downloadpdf/book/9781513595603/ch002.xml

The nature of issuers and platforms further complicates the VA ecosystem. While some VAs are issued by regulated and identifiable entities, others are created by anonymous or unregulated entities operating outside Uganda's jurisdiction. According to Chainalysis, such entities have been linked to illicit activities, including ransomware payments and darknet transactions, in regions with weak regulatory oversight.[22] The ML/TF threat posed under this input variable was assessed as **high.**

4.2.4.3 Centralised Environment

Centralised VASPs, such as exchanges, are important in the VA ecosystem of Uganda because they offer platforms for users to buy, sell, and trade VAs. These platforms typically have stronger regulatory oversight compared to decentralised alternatives, often implementing all AML/CFT requirements. Uganda's VA adoption trend has increasingly shifted from centralised environments to decentralised environments as witnessed in the Chainalysis VA Adoption reports from 2022 to 2024.

The transition to decentralised platforms in Uganda undermines centralised VASPs' ability to enforce AML/CFT measures even where some centralised VASPs operating in Uganda are regulated in foreign jurisdictions and extend global AML/CFT standards, their capacity to track funds originating from decentralised environments is limited. According to the total VA inflows and outflows for Uganda, 90% of the transacted volumes were linked to exchanges, majority of which operate in centralised environments. Given these factors this input variable was assessed medium for ML/TF threat.



of the transacted volumes were linked to exchanges, majority of which operate in centralised environments.

4.2.4.4 Decentralised Environments

Decentralised environments, including peer-to-peer platforms and decentralised finance (DeFi) systems, have become increasingly prominent in Uganda's VA ecosystem. Unlike centralised exchanges, these platforms operate without intermediaries, enabling users to transact directly with one another. While this decentralised nature offers benefits such as lower costs and greater autonomy, it also poses significant ML/TF threats to the country due to the lack of oversight and regulatory controls.

Uganda has seen a growing trend towards P2P transactions, driven by the accessibility and convenience of decentralised platforms. Many of these platforms allow users to bypass traditional financial systems and centralised VASPs, offering anonymity and enabling transactions without formal identification or scrutiny. This trend is further reflected in Uganda's ranking as 12th out of 155 countries globally for DeFi adoption, according to data

22 The Chainalysis VA Crime Report," Chainalysis, 2023

from Chainalysis.

Additionally, the emerging use of non-fungible tokens (NFTs) in Uganda illustrates the ML/TF threats posed by decentralised systems. During the review period, NFT platforms recorded inflows of USD 3,065 and outflows of USD 2,647. NFTs, which represent unique digital assets used for trading collectibles, art, and virtual real estate, are increasingly being exploited for laundering illicit funds. A typical scheme involves criminals purchasing NFTs with illicit funds and subsequently selling them to legitimate buyers, effectively integrating illegal proceeds into the financial system. The use of smart contracts[23] in NFT transactions adds another layer of complexity, as these contracts can execute trades autonomously, leaving minimal traceability.

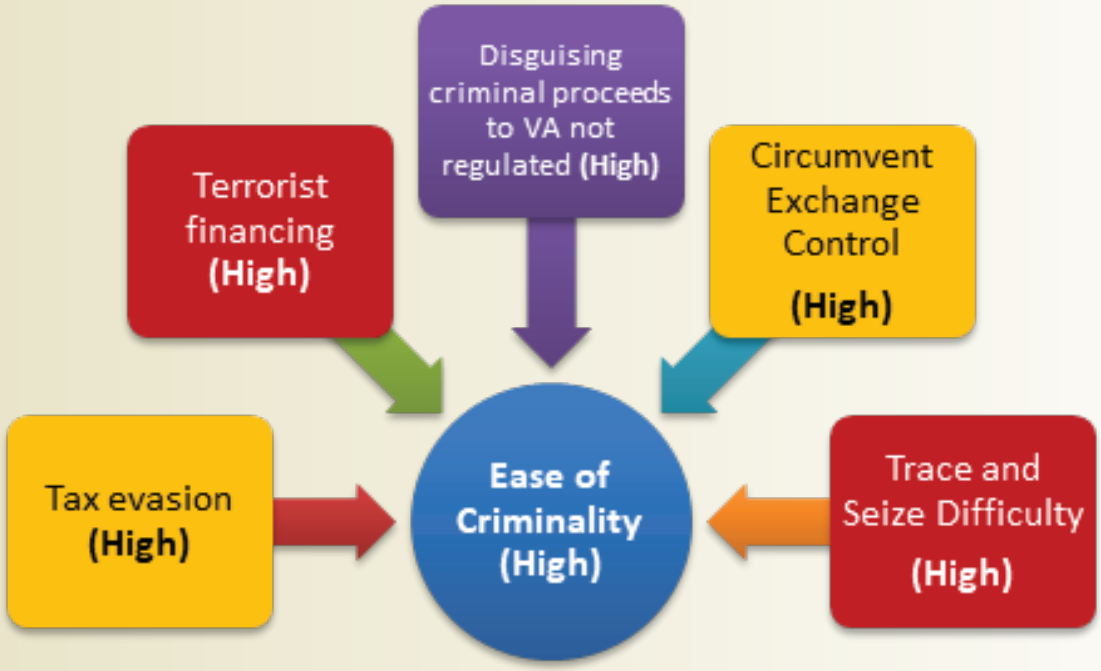
The widespread adoption of decentralised platforms, high volumes of P2P transactions, and Uganda's strong DeFi adoption ranking collectively led to this input variable being assessed as **high** for ML/TF threats.

4.2.5 Ease of Criminality

Virtual Assets in Uganda provide unique opportunities for both legitimate use and exploitation by criminals. The following assessment evaluates the ease with which specific criminal activities can be conducted using VAs in Uganda, including tax evasion, terrorist financing, disguising criminal proceeds, trace and seize difficulties, and circumventing exchange controls.

23 A smart contract is a self-executing piece of code stored on a blockchain, with the terms of the agreement directly embedded in the code. These contracts are foundational to many decentralised platforms, enhancing efficiency and transparency. However, their ability to enable complex and automated transactions can also make them appealing to illicit actors, as they can be challenging to monitor.

Figure 18 : **Summary of Ease of Criminality**



4.2.5.1 Tax Evasion

Given that VAs provide a decentralised and pseudonymous mechanism for individuals and businesses to evade taxes, particularly in Uganda's predominantly cash-based economy. In the absence of comprehensive VA specific regulations, income or gains derived from VAs often go unreported, creating a significant loophole for tax evasion. For instance, individuals can convert fiat currency into VAs through peer-to-peer transactions, bypassing traditional banking systems where tax reporting and enforcement are more robust.

The Chainalysis 2022 Global VA Adoption Index highlighted significant P2P activity in Uganda,underscoring the potential for underreporting of VA-related earnings. Additionally, the high volume of stablecoin transactions for inflows and outflows indicates that some businesses have shifted away from traditional banking systems, which are subject to audits and tax return filing requirements. Transactions conducted through stablecoins often remain unreported by the users to the URA as part of their tax obligation, thereby facilitating tax evasion.

The growing adoption of decentralised finance (DeFi) in Uganda further exacerbates this issue. DeFi platforms allow businesses to operate in decentralised environments with minimal AML/CFT requirements, reducing the visibility of transactions. This, coupled with the operation of some VASPs in unregulated jurisdictions, means cross-border transactions often escape local tax laws.

The lack of automated tools and mechanisms for URA to track VA transactions significantly complicates enforcement efforts. Consequently, tax evasion through VAs has been assessed as a **high** ML/TF threat due to the prevalence of unregulated transactions, insufficient monitoring tools, and the absence of mandatory reporting mechanisms for VA-related income.

4.2.5.2 Terrorist Financing

In Uganda, virtual assets pose a significant risk for terrorist financing due to their anonymity, borderless nature, and peer-to-peer transfer capabilities, which make them especially appealing to terrorist groups and sympathizers seeking to raise and move funds undetected. This threat is further heightened by the presence of active terrorist organisations in neighbouring regions, including ISCAP in the Democratic Republic of Congo and Al-Shabaab in Somalia, which maintains cells in a neighbouring country. Uganda's counter-terrorism intelligence agencies have already disrupted six incidents involving local supporters of these groups who attempted to employ virtual assets for terror-related funding, with some transactions traced to two other African countries within the ESAAMLG region. When combined with regulatory gaps and the availability of unregulated peer-to-peer platforms, these factors contributed to a **high** ML/TF threat level for this input variable.

4.2.5.3 Disguising criminal proceeds to VA not regulated

The use of unregulated VAs to disguise criminal proceeds poses a significant ML/TF threat in Uganda. Criminals exploit decentralised platforms, unregulated VASPs, and anonymity enhancing technologies such as mixers to obscure the origins of illicit funds. These methods enable the conversion of proceeds from activities like corruption, fraud, and drug trafficking into VAs, which can then be laundered and reintegrated into the formal financial system. Mixers, which obscure the traceability of transactions by pooling and redistributing funds, are increasingly being exploited to launder illicit funds in Uganda. Available information from July 2020 to June 2024 indicates inflows of USD 483,387 and outflows of USD 51,806 linked to mixers.

For instance, 01 SAR submitted in the review period flagged the activities of a public official who attempted to launder proceeds of illicit enrichment through VAs. The individual used decentralised platforms to transfer funds derived from unexplained wealth into unregulated VAs eventually funneling the funds through a known PSO in Uganda that detected several transactions linked to unregulated VAs. This case highlights the ML/TF threat in Uganda's VA ecosystem, where unregulated platforms and mixers provide an avenue for laundering proceeds of corruption and other illicit activities. The lack of domestic regulation and oversight in Uganda also encourages the use of decentralised wallets and privacy-enhancing technologies. Criminals can store and transfer illicit funds without leaving a traceable footprint, making it difficult for law enforcement to intervene

effectively. In light of this, the assessment team assessed a **high** ML/TF threat for this input variable.

4.2.5.4 Trace and Seize Difficulty

The difficulty in tracing and seizing VAs presents a significant challenge for Uganda in combating ML/TF. The decentralised and pseudonymous nature of VAs, coupled with the use of advanced privacy technologies such as mixers, makes it increasingly difficult for competent authorities to identify, freeze, or confiscate VA-related property linked to criminal activities. Despite Uganda being partially compliant with FATF recommendation 30, which requires competent authorities to have the responsibility and capacity to expeditiously identify, trace, freeze, and seize property linked to proceeds of crime, the same is yet to be implemented on VAs.

> *The difficulty in tracing and seizing VAs presents a significant challenge for Uganda in combating ML/TF.*

Currently, Uganda lacks a comprehensive legal framework for VAs, creating ambiguities in how they are classified under property laws.Without a clear legal foundation, even when suspicious transactions are identified, initiating asset seizure becomes a lengthy and cumbersome process. This legal gap further complicates the ability of LEAs to take swift action to confiscate VA-related assets suspected of being used for criminal activities.

"Without a clear legal foundation, even when suspicious transactions are identified, initiating asset seizure becomes a lengthy and cumbersome process."

The borderless nature of VAs further complicates tracing and seizing efforts as criminals often transfer illicit funds to jurisdictions with weak AML/CFT frameworks, taking advantage of the lack of international cooperation, an area Uganda is still improving with existing challenges in the mutual legal assistance provisions.

The combination of technical and legal barriers, coupled with insufficient implementation of FATF Recommendation 30, places Uganda at a significant disadvantage in addressing trace and seize difficulties related to VAs. Given these factors, the ML/TF threat level was assessed as **high.**

4.2.5.5 Circumvent Exchange Control

Uganda exchange control regulations are primarily governed by the Foreign Exchange Act 2004 as amended which mandates under section 9 (2) and (3) that all payments in foreign currency within Uganda, to or from Uganda, between residents and non-residents or between non-residents, shall be made through an entity licensed by the Bank of Uganda. It further states that every transfer of foreign exchange to or from Uganda shall be through a person licensed to carry out the business of money transfers.

The decentralised and borderless nature of VAs enables individuals and entities to bypass exchange control regulations, posing a significant challenge to Uganda's financial regulatory system. Exchange controls, which are intended to monitor and regulate the flow of capital across borders, are rendered ineffective when transactions are conducted using VAs which can be exploited by criminals internationally without detection.

One of the primary mechanisms for circumventing exchange controls is the use of VASPs that operate outside of Uganda's regulatory framework. This was noted in the survey which indicated that 94% of respondents were using services of different VASPs that were all based outside Uganda with exception of 01 foreign VASP registered with URSB as a company limited by shares.

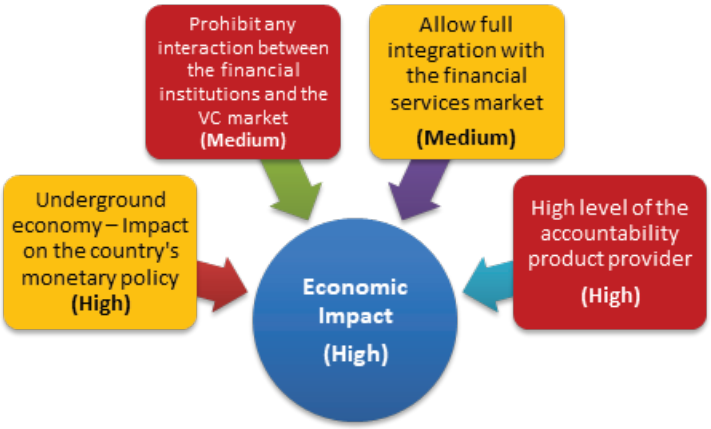
For instance, the significant inflows and outflows of Bitcoin and stablecoins amounting to over USD 504 million and USD 489 million respectively highlighted the scale of VA activity in Uganda. Much of this activity involved transactions to and from jurisdictions with limited AML/CFT enforcement, including those listed by FATF as countries under increased monitoring. The ability to circumvent exchange controls through VAs posed a **high** ML/TF threat to Uganda.

"One of the primary mechanisms for circumventing exchange controls is the use of VASPs that operate outside of Uganda's regulatory framework"

4.2.6 Economic Impact

Virtual Assets present both opportunities and threats for Uganda's economy. While they offer avenues for financial innovation and inclusion, their unregulated nature and inherent characteristics also pose significant

Figure 19 **: Summary of Economic Impact**



4.2.6.1 Underground Economy – Impact on Uganda's Monetary Policy

The increasing adoption of VAs in Uganda over the last three years, particularly stablecoins, is significantly impacting the underground economy and posing challenges to the country's monetary policy. Stablecoins, which are pegged to fiat currencies, have gained popularity due to their price stability and ability to facilitate seamless peer-to-peer exchanges outside the traditional financial system. Recent data, as discussed in Chapter 3, shows that stablecoin transactions in Uganda have nearly doubled in value from July 2020 to June 2024 compared to Bitcoin, despite fewer transactions, indicating their growing use for high-value transfers.

In April 2022, BoU issued two circulars under its mandate, barring all entities licensed under the National Payment Systems Act 2020 and the Financial Institutions Act, 2004 from liquidating VAs, i.e., converting VAs into fiat accounts and vice versa. This directive was aimed at mitigating threats associated with VAs including ML/TF threats, and financial instability. While this action was within the BoU's regulatory functions, it has had unintended consequences for Uganda's economy. For instance, the data shows that before the ban, stablecoin inflows were; USD 502,321 (Half-Year) in 2020 to USD 56,948,446 in 2021, and after the ban, stable coins increased to USD 72,460,648 in 2022, USD 135,577,969 in 2023, a clear reflection of increased usage and adoption.

By restricting the interaction between financial institutions and VAs, BoU effectively limited the integration of VAs into the regulated financial services sector driving VA activities further into the underground economy, where transactions occur through unregulated platforms, making it harder for authorities to monitor or control. The prohibition also

fueled the rise of decentralised platforms as preferred alternatives for users seeking financial autonomy supported by the value in transaction volumes extensively explained in chapter 3.

When comparing VA market capitalisation to Uganda's banking sector, it is notable that financial institutions assets, according to recent Bank of Uganda financial stability report, stood at approximately UGX 53.9 trillion (around USD 14.4 billion[24]), in June 2024. Although the total value of Ugandan VA holdings and trading activity falls between USD 73 million and USD 200 million, its rapid growth and relative opacity emphasise the need for closer regulatory scrutiny and improved data collection. The partially regulated nature of VA transactions introduces risks linked to capital flight and illicit financial flows, as virtual assets enable swift cross-border transfers that can circumvent traditional controls, and if Ugandan consumers and businesses increasingly adopt virtual assets, authorities could experience challenges monitoring liquidity and credit risks, particularly since VAs typically remain outside conventional measures such as currency in circulation and formal sector deposits.

For instance, Bank of Uganda officials rely on conventional indicators such as currency in circulation (M1), the broader money supply (M2), and formal sector deposits for determining liquidity and credit risks. If consumers and businesses increasingly move part of their savings and transactions into virtual assets such as stablecoins[25] as cited in this report, official data could systematically underestimate actual liquidity conditions and overes mate the effectiveness of monetary policy measures.This mismatch between official statistics and real-world capital flows may become more pronounced if VA-based remittances gain further traction.Uganda's significant diaspora often sends funds through established channels, which are monitored for balance of payments calculations and AML/CFT compliance. Should more remittances occur via virtual assets, the Bank of Uganda may find it increasingly difficult to capture the true magnitude of foreign exchange inflows in its official records. Such a gap can impede accurate macroeconomic forecasting and disrupt the planning of monetary policy tools, including open market operations and interest rate adjustments.

Actions by BoU inadvertently highlighted the absence of regulatory measures that should foster safe integration of VAs into the formal financial sector. Without mechanisms to regulate DLT applications, the VA ecosystem has shifted toward a largely unregulated cyber underground economy which attracts both legitimate users seeking alternatives to traditional financial systems and criminals exploiting the anonymity and ease of stablecoin transactions for illicit activities such as ML/TF and tax evasion.

24 According to Bank of Uganda, in June 2024, the Ugandan Shilling traded at an average mid-rate of UGX 3,747.19/USD
25 Since stablecoins operate independently from formal banking systems, their widespread use erodes the central bank's influence over monetary supply and capital controls.

4.2.6.2 Allow full integration with the financial services market

The Bank of Uganda's directive, which barred RSFPs from conducting VA transactions, has significantly shaped how VAs could be integrated into Uganda's banking and payment markets. This stance, introduced to reduce exposure of VAs to the conventional financial system was to maintain the integrity of Uganda's monetary policy, protect consumers from unregulated emerging financial markets that could erode confidence in the formal financial sector thereby limiting the formal adoption of VAs among RSFPs but also insulated the sector from unregulated VA activities. Under this restriction, VAs remain largely outside traditional financial channels, lowering the risk of systemic misuse by illicit actors.

Although the directive curbed mainstream VA usage, financial institutions that have encountered VA-related transactions reported them to FIA as STRs or SARs that subsequently analysed them, taking into account possible ML/TF indicators and sharing relevant findings with competent authorities including BoU. The directive's influence is evident in the relatively low number of VA transactions within the formal sector, thereby minimizing institutional exposure to illicit financial flows and contributing a medium ML/TF threat level assessment for this input variable.

4.2.6.3 Prohibit any Interaction between the Financial Institutions and the VA Market

In Uganda, BoU prohibited interactions between RFSPs, and the VA market to safeguard the traditional financial sector from the threats associated with unregulated VAs, including ML/TF, and financial instability. This regulatory stance reflects efforts to shield the formal financial system from the potential exposure posed by the broader VA ecosystem.

The prohibition has effectively reduced the direct threat of ML/TF within Uganda's formal financial system by restricting RSFPs from engaging in VA-related activities. However, this measure has not eliminated the threats entirely, as VA activities continue to flourish wit in the country bypassing formal financial channels. For instance, available data indicates that stablecoin inflows have continued to rise from USD 56,948,446 in 2021, to USD 135,577,969 in 2023. These transactions indicate rising usage of VAs within the broader economy which heightens the ML/TF threat level to.

4.2.6.4 High Level of the Accountability Product Provider

The accountability of VA service providers in Uganda is heavily influenced by the regulatory environments in which they operate. Over 90% of the popular VASPs accessible to Ugandans are based in jurisdictions with weak or nonexistent AML/CFT frameworks. These jurisdictions often lack robust preventive measures,creating gaps in oversight and enabling bad actors to exploit these platforms for illicit purposes as some of these

transactions are peer-to-peer and decentralised which makes it difficult for LEAs to obtain client data, to support investigations. For instance, one of the largest VASPs widely used in Uganda has faced multiple sanctions for ML, with its founder prosecuted and convicted for ML albeit the VASP continues to facilitate transactions in Uganda with the highlighted AML/CFT deficiencies.

Unlike centralised payment systems, where central authorities assume the risk of failed transactions, decentralised VA platforms place the burden of transaction failures on individual users. This fundamental difference exposes Ugandan users to the risks associated with unregulated platforms, such as fraud, loss of funds, and the inability to trace illicit transactions. Currently, Uganda lacks a comprehensive regulatory framework to ensure accountability in decentralised systems, including provisions for freezing assets and confiscating illicit funds.

The absence of enforceable regulations in Uganda has allowed decentralised platforms to expand their operations without adequate oversight, leaving users vulnerable and increasing the country's exposure to ML/TF threats which is demonstrated by the Chainalysis VA adoption ranking for Uganda at 12th out of 155 countries for DeFi services. The combination of weak external regulatory frameworks, decentralised governance structures, and the lack of domestic oversight led to a high ML/TF threat for this input variable.

4.3 The Overall Vulnerability Level

Assessing ML/TF vulnerabilities related to VAs and VASPs allows the country to understand the potential weaknesses in the AML/CFT systems to inform the development of appropriate regulatory frameworks, and equip competent authorities with the appropriate mitigation strategies to address identified risks effectively. VAs have become particularly attractive to criminal actors due to their ability to bypass traditional banking systems, facilitate rapid and borderless transactions, and obscure the origins of funds. In the absence of robust oversight mechanisms, the risks of VAs being used to finance criminal networks, fund terrorist activities, or evade taxes are significantly heightened. These vulnerabilities are amplified by the pseudonymous nature of VAs, the decentralised governance structures of many platforms, and the absence of acomprehensive regulatory framework for VASPs in Uganda. The overall national vulnerability for Uganda was rated as **"High"**, reflecting significant systemic weaknesses.

The two primary factors that emerged as significant contributors to the overall vulnerability include;

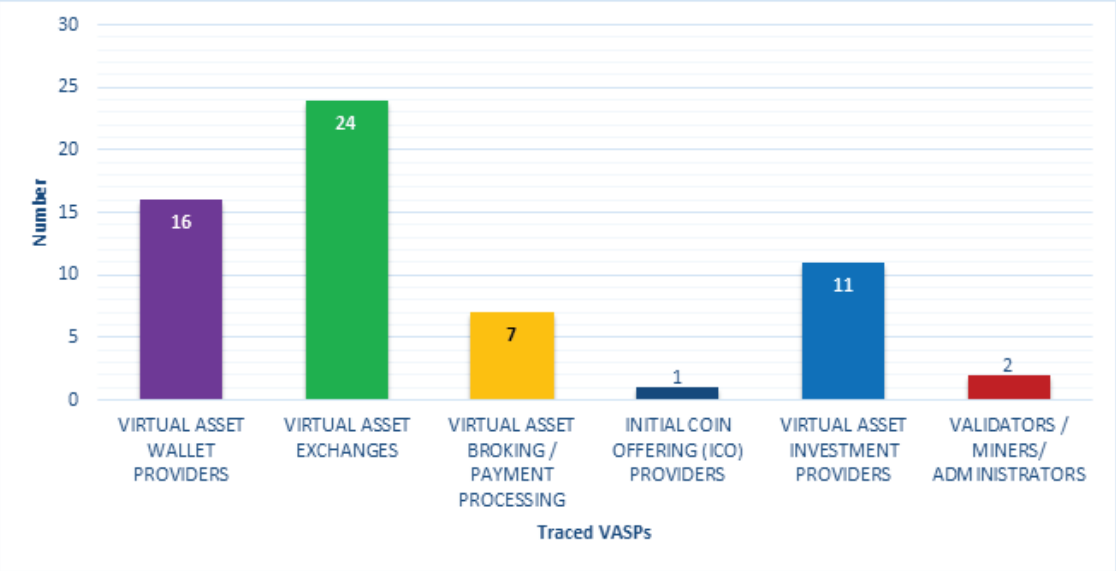
a) The nature of VA services offered by providers as part of the global financial system; and

b) The interaction between VA and VASP activities and traditional AML/CFT obligated entities in Uganda and other countries, particularly those with weak AML/CFT frameworks.

4.3.1 Traced entities operating as VASPs in Uganda

According to available data from respondents, a total of 61 VASPs were identified to be operating in Uganda as shown in the chart below;

Figure 20 : **Traced entities operating as VASPs in Uganda**



Source: Survey Data

4.3.2 Assessing VASPs (Intermediate and Input Variables)

The assessment focused exclusively on transactions facilitated by VASPs as Non-VASP transactions, such as peer-to-peer transfers, are not directly included. According to the FATF Standards, specifically the revised Interpretive Note to Recommendation 15, P2P transfers of VAs conducted without the involvement of a VASP or financial institution are not explicitly subject to AML/CFT obligations.

Nevertheless, the FATF emphasises the importance of countries assessing and understanding the ML/TF risks associated with such transactions. Countries were also encouraged to implement appropriate measures to mitigate these risks. Regulatory efforts, however, primarily target VASPs and other intermediaries that facilitate VA transactions.

Figure 21 : **Summary of Overall Vulnerabilities Exposure of VASPs**

OVERALL VASP VULNERABILITIES		
Products & services provided, and the types of VASPs	Licensed in the country or abroad	High Risk
	Nature, size and complexity of business	High Risk
	Products/services	High Risk
	Methods of delivery of products/ services	High Risk
	Customer types	High Risk
	Country risk	High Risk
	Institutions dealing with VASP	High Risk
	VA (Anonymity/pseudonymity)	High Risk
	Rapid transaction settlement	Very High Risk
	Dealing with unregistered VASPs from overseas	High Risk

4.3.2.1 Licensed in the Country or Abroad

Most VASPs accessible to Ugandan users are licensed in foreign jurisdictions with varying degrees of regulatory oversight with some jurisdictions implementing robust AML/CFT measures while others lack comprehensive frameworks, creating opportunities for exploitation. Uganda currently has no domestically licensed VASPs, limiting the country's ability to enforce compliance and monitor transactions effectively. The country's existing laws neither clearly identify all types of VASPs nor provide specific entry controls to assess the fitness and propriety of applicants, including transparency in corporate structures and shareholding. This gap allows for the participation of unlicensed or poorly regulated VASPs, both domestically and internationally, increasing exposure to ML/TF risks. The absence of detailed guidance on VASP licensing and registration further complicates oversight, particularly for cross-border transactions and emerging technologies like decentralised finance (DeFi) platforms and stablecoins.Combined with limited resources and insufficient technical capacity for supervision, this regulatory vacuum leaves Ugandan authorities with minimal control over VASP activities. These deficiencies are compounded by the global nature of virtual asset transactions, which often involve jurisdictions with weak AML/CFT regimes. Given these challenges, the ML/TF vulnerability rating for this input variable was assessed

as **high.**

4.3.2.2 Nature, Size, and Complexity of Business

The nature, size, and complexity of VASPs in Uganda present significant challenges for effective oversight and regulation. Most VASPs accessible to Ugandan users facilitate the rapid transfer of value with minimal oversight, which inherently increases exposure to ML/TF risks. The business complexity of VASPs varies widely, as some platforms offer only a limited selection of VAs and exclude fiat currency transactions, while others provide a broader range of services, including decentralised finance (DeFi) products and cross-border transactions, making the sector difficult to monitor comprehensively.

The absence of a robust legal framework to regulate the role and exposure of various participants in VA ecosystems further compounds these vulnerabilities.For example, while stablecoin administrators and other participants in stablecoin arrangements are expected to comply with AML/CFT regulations and register or be licensed as financial institutions or VASPs depending on their activities, Uganda lacks the mechanisms to enforce these requirements. Additionally, the global and internet-based nature of VASPs allows them to interact with jurisdictions that have weak or no AML/CFT measures, thereby amplifying risks. Combined with the lack of tailored risk-based controls, minimal supervision, and the inherent complexity of VASP operations, these factors justify a **high** ML/TF vulnerability rating for this input variable.

4.3.2.3 Products/Services

The products and services offered by VASPs in Uganda contribute significantly to its ML/TF vulnerability. The VASPs accessible to Ugandan users typically offer a range of VAs, including mixers, stablecoins, anonymity enhanced VAs, tokens, and decentralised finance (DeFi) products, which are delivered through online platforms. These products often feature characteristics such as pseudonymity, rapid transaction settlement, and global accessibility, which complicate the implementation of effective AML/CFT measures. Additionally, certain VA tokens and services are designed to obscure transactions, undermining VASPs' ability to comply with AML/CFT requirements and further heightening risks. Furthermore, the lack of a structured regulatory framework in Uganda increases these vulnerabilities, as there are no mechanisms to assess the risks associated with specific products or delivery channels effectively. Given these factors, the ML/TF vulnerability level for this input variable was assessed as **high**, reflecting the limited oversight of VASP products and services and the inherent risks associated with their operations.

4.3.2.4 Methods of Delivery of Products/Services

All the VASPs facilitating services in Uganda operate through online platforms that allow pseudonymous or, in some cases, anonymous transactions, enabling users to transact

without face -to- face interactions or verifiable identity checks. Non-face -to- face business relationships and payments received from unknown third parties further complicate the implementation of effective AML/CFT measures, making these delivery channels inherently higher risk. The lack of a regulatory framework in Uganda increases these vulnerabilities, as there are no mandatory requirements for VASPs to adopt enhanced due diligence (EDD) measures to mitigate risks associated with their delivery mechanisms.In the absence of robust oversight, VASPs often fail to implement key EDD measures, such as corroborating customer identity information through national identity databases, tracing customers' IP addresses, or verifying transactional consistency with a customer's profile. These gaps create opportunities for terrorists and other criminals to exploit VAs for illicit purposes, including electronically facilitated funds transfers.

Whereas Uganda is compliant in enforcement of FATF recommendation 16, intended to prevent unfettered access to electronic fund transfers, there is no implementation of this recommendation by VASPs in Uganda which increases the exposure to ML/TF risks. Given the widespread use of pseudonymous delivery channels and the absence of controls to mitigate their associated risks, the ML/TF vulnerability level for this input variable was assessed as **high.**

4.3.2.5 Customer Types

The customer types interacting with VASPs accessible to Ugandan users contribute significantly to ML/TF vulnerabilities due to the inherent challenges in verifying customer identities and monitoring beneficial ownership. Many of the VASPs in Uganda lack the robust risk management systems necessary to identify foreign politically exposed persons (PEPs) or those connected to them, as required under FATF Recommendation 12. Without adequate measures to identify PEPs or their associates, including verifying the source of funds and applying enhanced scrutiny, these platforms remain susceptible to exploitation by high-risk individuals and entities. Furthermore, all VASPs in Uganda are not implementing the travel rule, which is critical for ensuring the traceability of transactions across jurisdictions and preventing obscuring of customer identities.

VASPs also face challenges in detecting and mitigating risks related to customers from high-risk jurisdictions known for inadequate AML/CFT measures, including weak CDD measures. Customers from such jurisdictions may exploit VASPs to transact back to their home countries, using layering and complex ownership structures to conceal beneficial ownership information. Additionally, the lack of controls to identify customers who use intermediaries, proxies, or third parties to manage transactions further amplifies these risks. Many VASPs accessible to Ugandan users are domiciled in jurisdictions with weak CDD requirements, which undermines their ability to detect suspicious activities effectively. Given these factors, the ML/TF vulnerability level for this input variable was assessed as High.

4.3.2.6 Country Risk

Country risk can be relied on to determine the ML/TF vulnerabilities associated with VASPs accessible to Ugandan users, as their operations often involve jurisdictions with varying levels of risk. 88% of respondents engaged in VA transactions mentioned different countries with which they transact and some are listed by FATF as high-risk jurisdictions. Some of these countries host designated terrorist organisations, or exhibit weak AML/CFT regimes. Additionally, jurisdictions known for high levels of organised crime,corruption, or as source/ transit points for illegal activities such as drug trafficking, human trafficking, and smuggling, further elevate the risks when VASPs interact with clients or transactions originating from these regions.

VASPs often fail to adequately consider or mitigate the risks associated with country specific factors, such as the geographic origin of customers, the nature of transactions, or the delivery channels used. Many VASPs accessible in Uganda are unable to identify or analyse the risk posed by non-resident clients, including the types of VAs or products they use, which creates gaps in their respective risk assessment. Furthermore, the global reach of VASPs facilitates cross-border movement of funds, particularly from anonymous or pseudonymous transactions, and business relationships involving customers from geographic areas of concern. As a result, the ML/TF vulnerability level for this input variable was assessed as **high.**

"Country risk can be relied on to determine the ML/TF vulnerabilities associated with VASPs accessible to Ugandan users, as their operations often involve jurisdictions with varying levels of risk."

4.3.2.7 Institutions dealing with VASP

VASPs have exposure to other VASPs such as exchanges and wallet providers, which may have insufficient AML/CFT controls in place. These institutions interacting with VASPs accessible in Uganda face significant ML/TF vulnerabilities, particularly due to the inherent risks associated with the specific types of VAs and technologies offered. Many VASPs provide products such as anonymity-enhanced VAs (AECs), embedded mixers, tumblers, and other mechanisms that obfuscate the identity of senders, recipients, holders, or beneficial owners. This is demonstrated by the different VA transactions in Uganda linked to mixers, darknet markets, among others. These features undermine the ability of VASP institutions to implement effective CDD measures and other AML/CFT measures, leaving transactions highly susceptible to abuse by illicit actors. Furthermore, the lack of a comprehensive framework to address these technologies amplifies the risks associated with VASP institutions dealing with such VASPs.

Additionally, VASPs licensed abroad or operating without registration in Uganda often engage in activities involving non-registered actors and anonymity-enhancing technologies, making risk management and mitigation challenging for domestic institutions. Without robust oversight, these institutions struggle to ensure that their interactions with VASPs comply with AML/CFT standards, especially in cases involving technologies that obscure transaction details. The inability to identify the beneficial owners or trace the flow of funds increases exposure to ML/TF risks. Given the reliance on VASPs offering products with these high-risk features and the lack of measures to address the associated vulnerabilities, the input variable was assessed as **High.**

4.3.2.8 VA (Anonymity/pseudonymity)

The pseudonymous and anonymity-enhanced features of VAs accessible through VASPs in Uganda present significant ML/TF risks, particularly as these characteristics inhibit the identification of beneficiaries and complicate transaction traceability. The cross-border nature of VAs amplifies these risks, as customer identification and verification measures employed by many VASPs are often insufficient to address the challenges posed by enhanced anonymity. This deficiency allows illicit actors to exploit gaps in the system, using VAs to conduct obscured transactions that bypass traditional financial oversight mechanisms.

VASPs operating in or accessible to Ugandan users often leverage technologies and platforms that enable transaction obfuscation, and reduced transparency which further undermine their ability to conduct effective AML/CFT measures or CDD. These technologies, including mixers, tumblers, and certain VA designs, facilitate the concealment of the origin and destination of funds, posing a higher risk for financial conduct associated with ML/TF activities. Without a robust framework to enforce transparency

and implement stringent verification and monitoring measures, the risks associated with VAs offering pseudonymity or enhanced anonymity remain unaddressed. Consequently, the ML/TF vulnerability level for this input variable was assessed as **High**

4.3.2.9 Rapid Transaction Settlement

The ability of VASPs accessible to Ugandan users to facilitate rapid transaction settlements poses an increasing ML/TF vulnerability, given the inherent risks associated with such processes. VAs enable near-instantaneous cross-border transfers without reliance on traditional financial institutions, bypassing the checks and balances typically conducted by intermediaries in the correspondent banking system. This rapid settlement capability reduces the traceability of funds and allows illicit actors to quickly move large sums across jurisdictions, evading regulatory scrutiny and creating significant challenges for AML/CFT compliance.

Moreover, the peer-to-peer nature of many VA transactions, coupled with features like enhanced anonymity and obscured transaction flows, makes it difficult for VASPs to implement robust CDD measures or effectively monitor transaction patterns. Policies to track fiat-to-VA and VA-to-fiat conversions, as well as transactions involving privacy coins, are either non-existent or poorly enforced, further increasing the risk of misuse by criminals, money launderers, and terrorist financiers. Additionally, the absence of CDD measures during the conversion of one VA to another or to privacy-focused assets intensifies vulnerabilities, as these exchanges often occur without verifiable information about the transacting parties leading to a very high vulnerability rating for this input variable.

4.3.2.10 Dealing with unregistered VASP from overseas

The engagement of Ugandan users with unregistered or unlicensed VASPs operating overseas makes Uganda vulnerable to ML/TF due to the lack of mechanisms to identify, monitor, or sanction such entities. Uganda currently lacks robust tools and resources, such as web-scraping technologies or advanced blockchain analysis tools, to detect unregistered VASPs soliciting business online or through industry channels.

Additionally, there is limited coordination among national authorities involved in the regulation and oversight of VASPs, which weakens efforts to share information or develop a unified approach to managing the risks posed by unregistered overseas entities. Uganda does not have a designated authority or an established framework to investigate and sanction unlicensed VASPs engaging in VA activities, making it difficult to hold such entities accountable. This regulatory gap allows criminals and other illicit actors to exploit unregistered VASPs for ML/TF purposes, taking advantage of the lack of scrutiny and enforcement. Given these systemic weaknesses, the vulnerability level for this input variable was assessed as very high, highlighting the urgent need for enhanced monitoring,coordination, and enforcement mechanisms to address the risks posed by

CHAPTER 5

MITIGATION MEASURES

5.1 ML/TF Mitigation Measures for VAs/VASPs

This chapter examined the adequacy and effectiveness of Uganda's current AML/CFT framework in mitigating ML/TF threats and vulnerabilities associated with VAs and VASPs. It focused on the roles and responsibilities of the government, VASPs, and traditionally obliged entities such as financial institutions and DNFBPs assessing how well these entities address the identified threats and vulnerabilities.

Figure 22 : **Summary of Government mitigation measures**

5.1.1 Overall Mitigation Measures

The assessment of Uganda's overall effectiveness in mitigating ML/TF threats and vulnerabilities associated with VAs and VASPs involved an evaluation of its legal, financial, and human resource frameworks to identify factors that make the country attractive to such ML/TF activities.

The analysis identified two primary factors influencing the national effectiveness outcome; these included, the robustness of Uganda's legislative framework to combat ML/TF and its implementation to address vulnerabilities across various sectors. The legislative framework revealed gaps and weaknesses that limit the country's capacity to detect, prevent, and respond to ML/TF risks linked to VAs and VASPs. Sectoral vulnerabilities, on the other hand, highlighted specific features of financial products, services, and industries

that allow VASPs to exploit the regulated sector and launder proceeds of crime, often without regulatory oversight.

Uganda's effectiveness in mitigating ML/TF risks was rated Very Low. This low effectiveness arose from the limited capacity to investigate and prosecute financial crimes involving VAs/VASPs, and the lack of a comprehensive regulatory framework for licensing, monitoring, and supervising VASP activities.

5.2 Government Mitigation Measures

5.2.1 Comprehensiveness of the AML/CFT Legal Framework

While VASPs were included in the AMLA, Cap 118 as accountable persons, the country still lacks specific legislation governing VAs/VASPs. VAs are not recognised as "property," "funds," or "proceeds" under current laws, meaning ML/TF requirements do not apply effectively to their use. There are no mandates requiring VASPs to identify or assess ML/TF risks related to their operations, products, or services. Additionally, the absence of licensing or registration requirements allows unregulated entities to operate freely, heightening exposure to misuse by criminals.

Despite Uganda having legal provisions to impose sanctions on VASPs for AML/CFT non-compliance through FIA, the AML/CFT supervisor for VASPs, there have been no imposed sanctions, on VASPs that are in breach of AML/CFT requirements. This coupled by the lack of alignment between AML/CFT requirements for VASPs and broader regulatory measures, such as consumer protection, network security, tax compliance, and prudential safety, undermines a holistic response to ML/TF risks. This disconnect leaves Uganda's VA ecosystem susceptible to abuse, particularly by unregulated entities operating in decentralised networks. As a result of these regulatory gaps, the mitigation measures for this input variable was assessed **very low.**

5.2.2 Availability and Effectiveness of Entry Controls

Uganda does not have a legal framework requiring VASPs to register, obtain a license, or otherwise secure authorization to operate. This regulatory gap leaves the VA sector largely unregulated, with no formal entry controls to mitigate ML/TF risks. The absence of such controls exposes the country to significant vulnerabilities, as entities can operate without scrutiny or accountability. For instance, there are no provisions to prevent criminals or their associates from holding ownership or management roles in VASPs. Similarly, there are no mandates for fit-and-proper tests, which are critical for vetting shareholders, beneficial owners, or administrators to ensure their integrity and compliance with AML/CFT measures. Without these measures, there is little to prevent bad actors from exploiting the VA eco-system for illicit purposes in the country.

Uganda also lacks a competent authority tasked with overseeing VASPs' entry into the market, conduct due diligence on VASP applicants, verifying beneficial ownership structures, or monitoring compliance with AML/CFT requirements. This gap means there is no enforcement mechanism to ensure VASPs comply with national or international standards, nor are there sanctions for entities that fail to register, report changes in ownership, or maintain proper AML/CFT controls.

The lack of a framework for licensing or registration also limits the government's ability to build trust in the VA ecosystem. By failing to establish entry controls, the country misses out on an opportunity to create a regulated environment that encourages compliance and deters criminal exploitation. As a result of these highlighted gaps, the mitigation measure for this input variable was assessed **Does-Not-Exist.**

5.2.3 Adequate Supervision & Monitoring Mechanism

Uganda has taken initial steps to address supervision and monitoring of VASPs by designating FIA as the AML/CFT supervisor for the sector, a legal requirement in the AMLA, Cap 118 that covers all accountable persons that do not have a prudential supervisor. A total of 16 VASPs were registered with FIA by end of June 2024 to comply with AML/CFT provisions, marking progress toward bringing some VASPs under regulatory oversight. However, the supervisory and monitoring mechanism remains inadequate to effectively mitigate ML/TF risks.

While the designation of VASPs as accountable persons establishes a legal basis for AML/CFT supervision, significant gaps remain in implementation. The FIA, as the designated supervisor, is tasked with monitoring VASPs for compliance with AML/CFT requirements, including customer due diligence (CDD), recordkeeping, and suspicious transaction reporting. Despite this mandate, AML/CFT inspections of the registered VASPs have not yet been conducted. This limits the FIA's ability to assess VASPs' compliance or identify gaps in their AML/CFT measures.

Additionally, FIA faces several challenges in carrying out its supervisory duties effectively which include limited resources, limited technical expertise, and a lack of a risk-based supervisory framework tailored to the unique characteristics of VASPs and VAs. Additionally, FIA has not yet put in place a mechanism to conduct on-site or off-site inspections or impose sanctions for non-compliance, this was because, the country needed to first conduct an ML/TF risk assessment on VAs and VASPs and once the risk have been established, then a mechanism would be put in place following FATF principles of a risk-based approach.

The growing use of stablecoins for high-value transactions in Uganda presents an additional supervisory challenge. Supervisors must oversee not only stablecoin issuers but

also mechanisms for their distribution, trading, and conversion into fiat currency. The FIA has not yet established guidelines or supervisory practices for these activities, further increasing the sector's vulnerability to ML/TF risks. As a result of these highlighted gaps, the mitigation measure for this input variable was assessed **Very Low.**

5.2.4 Regulation for CDD and source of funds & Availability of Reliable Identification Infrastructure

In Uganda, VASPs are recognised as accountable persons under the AMLA, Cap 118 and are therefore required to comply with all AML/CFT requirements, including CDD measures which align with FATF Recommendations 10 and 15. However, despite these legal obligations, the implementation of these requirements by VASPs remains minimal creating significant ML/TF risks.

Additionally, VASPs are required to conduct ongoing due diligence, monitor transactions, and report suspicious activities to FIA. However, in practice, these requirements are not being effectively implemented. According to the VASP industry tailored questionnaire, all 07 VASP entities reported that they were waiting for FIA to issue guidance on how they can file STRs and the industry specific red flags that are applicable to their business.

VASPs are also expected to conduct counterparty due diligence to determine whether VA transfers involve other VASPs or unhosted wallets. This obligation is critical to ensuring the traceability of transactions and mitigating ML/TF risks. Available information indicated that counterparty due diligence was being systematically carried out by VASPs, but there was no indication this was happening in peer-to-peer platforms and decentralised networks, where the identities of counterparties often remain obscured. As a result of these highlighted gaps, the mitigation measure for this input variable was assessed **Low.**

5.2.5 Availability of Reliable Identification Infrastructure

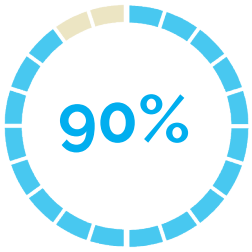
Uganda has a national identification system that provides a foundation for verifying customer identities, which has been integrated with some commercial CDD providers[26] that operate in Uganda and around the world. It is these commercial CDD providers that provide access to majority of the centralised VASPs operating in Uganda. However, there remains a significant number of foreign VASPs providing services to Ugandan users who do not enforce CDD measures and therefore do not utilise reliable and independent identification sources when conducting CDD. As a result of these highlighted mitigation measures, this input variable was assessed **Medium.**

26 https://usesmileid.com/company/about-us

5.2.6 Financial and Human Resource Capacity of Law Enforcement Authoities to Investigate, Trace, Seize and Secure Virtual Assets

While Uganda has a comprehensive legal framework that provides LEAs with the explicit authority to investigate, trace, seize, and secure proceeds of crimes, the same does not include provisions specific to VAs, such as enabling LEAs to access wallets, obtain passcodes or private keys, or trace transactions across blockchain networks. Additionally, there are no established procedures for handling seized VAs, such as creating secure vaults or leveraging technologies like Faraday bags to prevent tampering with confiscated devices.

Uganda has made significant progress in building the capacity of its LEAs showing that between July 2020 and June 2024, 23 staff members from FIA participated in 16 training sessions on VAs and VASPs. These sessions, delivered by reputable organisations such as the OECD, ECOFEL under the Egmont Group, UNODC, GCCS, IMF, and ESAAMLG, covered advanced financial investigations and forensic analysis. Furthermore, over 90% of FIA technical staff have obtained professional certifications through ACAMS (Association of Certified Anti-Money Laundering Specialists) and CFCS (Certified Financial Crime Specialist) programs. These specialised trainings equip them with the expertise to manage AML/CFT risks effectively. Furthermore, FIA has conducted 02 public awareness workshops about ML/TF risks associated with VAs and VASPs in which members of the public engaged in VASPs could be educated on VAs.



FIA technical staff have obtained professional certifications through ACAMS (Association of Certified Anti-Money Laundering Specialists) and CFCS (Certified Financial Crime Specialist) programs

Training has also extended beyond FIA to other competent authorities such as cybercrime unit under CID, IG and ODPP wherein a total of 36 officers were trained on conducting financial investigation associated with VAs and VASPs. These initiatives have enhanced inter-agency capacity and coordination, although the scope of training remains limited in addressing advanced technological needs.

Despite advancements in training, LEAs in Uganda face significant challenges due to a lack of technological tools. Essential capabilities such as blockchain analysis, wallet clustering, transaction de-anonymization, and identifying mixers are not available to law enforcement. Without these tools, LEAs rely on manual and less effective methods to trace and investigate VA transactions. The absence of a secure system to store and manage confiscated VAs further complicates enforcement.

FIA also received 49 SARs and 07 STRs related to VAs and VASPs during the same period. These reports were analysed, resulting in 6 intelligence reports disseminated to relevant LEAs for investigation. Additionally, the goAML system, an ICT system used by FIA to receive all reports from Accountable Persons was upgraded to cater for the tailored reporting of VASPs whose business processes and reported data is different from other accountable persons. Despite this upgrade, VASPs are yet to use the platform to file SARs, STRs, among others.

As a result of the above highlighted mitigation measures that demonstrate progress for the country, this input variable was assessed **Medium.**

5.2.7 Effectiveness of International Cooperation

The transnational nature of VAs and VASPs necessitates robust international cooperation to address ML and TF risks effectively. Uganda's current framework for international cooperation demonstrates progress but remains inadequate in certain critical areas, limiting its ability to engage comprehensively with other jurisdictions in VA-related cases.

Uganda is a member of several international frameworks that facilitate cooperation in addressing ML/TF risks, including INTERPOL, Egmont Group of Financial Intelligence Units and the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG). Through these memberships, Ugandan competent authorities can exchange information with their counterparts globally, enabling the sharing of intelligence on suspicious transactions and VA-related activities.

Between July 2020 and June 2024, FIA made a total of 05 formal requests to foreign jurisdictions for information related to VA cases, primarily focusing on tracing transactions and identifying counter parties. While some responses were received, delays and incomplete information hindered the timely resolution of cases. Additionally, Uganda

received 03 requests for international cooperation with 01 spontaneous dissemination about VAs during the same period. The FIA responded to these requests by analysing blockchain transactions after sending requests to blockchain analysis companies, and receiving responses that were shared with requesting jurisdictions. Although this demonstrates Uganda's willingness to cooperate, the lack of advanced tools for blockchain analysis and data verification limits the quality of intelligence shared linked to VAs and VASPs.

As a result of the above highlighted mitigation measures that demonstrate progress for the country, this input variable was assessed **High**.

5.2.8 Effectiveness of Domestic Cooperation

Uganda has established mechanisms to promote domestic coordination and cooperation on AML/CFT policies in line with FATF recommendations. The FIA serves as the lead agency in interagency coordination related to VAs and VASPs. Additionally, the National AML/CFT Coordination Task Force includes representatives from law enforcement, regulatory authorities, intelligence agencies, private sector and the judiciary, provides a platform for developing and implementing policies to address ML/TF risks in the country including about the VA sector.

Uganda has demonstrated a level of domestic cooperation among LEAs in handling VA-related cases. Between July 2020 and June 2024, FIA received 17 formal domestic requests for information related to VAs andVASPs. Of these, 12 were from Uganda Police, 03 from the Inspectorate of Government, and 02 from intelligence agencies. Additionally, the country formed a Blockchain Technical Working Group under BoU with membership including MoFPED, FIA, Blockchain Association of Uganda, FITSPA, Financial Sector Deepening, NITA-U, UCC, among others which discusses DLT including VAs and VASPs.

As a result of the above highlighted mitigation measures that demonstrate progress for the country, this input variable was assessed **Medium.**

5.2.9 Quality of Guidance issued to VASPs and Engagement with VASPs

Uganda, through FIA, has not yet issued specific guidance to VASPs on key reporting requirements, including the identification and filing of STRs, SARs, LCTRs, ALCTRs, IWTRs. Additionally, there is no guidance on how VASPs can identify suspicious activities, form suspicions, and report them effectively which increased the risk of non-compliance and misuse of VAs for ML/TF. The absence of detailed guidance extends to critical areas such as understanding the ML/TF risks associated with VAs, including anonymous peer-to-peer transactions, stablecoins, and decentralised networks. While VASPs are designated as accountable persons under the AMLA, Cap 118, they have not been equipped with tools or frameworks to meet these obligations. Measures like the Travel Rule, which requires

the collection and transfer of originator and beneficiary information for VA transactions, remain unimplemented due to the lack of specific directives.

Furthermore, there is no structured framework to guide VASPs in establishing internal control systems such as guidance on appointing qualified Compliance Officers, conducting risk assessments, maintaining robust compliance programs, or implementing onging training. This leaves VASPs without the institutional capacity to identify, manage, or mitigate risks associated with their operations effectively. While some VASPs have registered with FIA as required by AMLA, Cap 118 there is no continuous or structured engagement to share emerging typologies, explain compliance expectations, or collaborate on addressing sector-specific challenges. As a result of these highlighted gaps, the mitigation measure for this input variable was assessed **Does-Not-Exist.**

5.3 VASP Mitigation Measures

5.3.1 Transparency of shareholder Structure of VASP

Transparency in the shareholder, ownership, and control structure of VASPs is critical for mitigating ML/TF risks. However, in Uganda, the level of transparency among VASPs (facilitating transactions of Ugandans but not incorporated or registered in Uganda) remains low due to the absence of a comprehensive legal framework requiring the disclosure of such information. Without such mechanisms, it is challenging to detect whether criminals or their associates hold controlling interests and senior management positions in these entities. Furthermore, some of the VASPs are registered abroad in jurisdictions with weak AML/CFT frameworks, making it difficult for Ugandan authorities to access or verify critical information about their shareholders, investors, and administrators. As a result of the above highlighted mitigation measures that demonstrate limited proress by VASPs this input variable was assessed **very low**.

5.3.2 Quality of Governance Structure and Level of Accountability of VASP

The governance structures of VASPs in Uganda lack consistency and alignment with international standards. Distributed Ledger Technology (DLT) solutions, which form the backbone of VA systems, provide inherent benefits such as traceability and auditable transactions. However, these technologicalcapabilities are not fully leveraged due to the absence of a regulatory framework that mandates their integration into governance structures. VASPs operating within Uganda have not established institutional frameworks or oversight mechanisms to ensure accountability over their operations. For instance, there is no uniform governance model to oversee decentralised systems or ensure accountability within P2P networks. This gap leaves the VA ecosystem vulnerable to misuse, as technological governance structures that could promote legitimacy and accountability are absent.

Additionally, VASPs in Uganda vary significantly in their levels of accountability. Larger VASPs tend to adopt prudent business practices and implement AML/CFT measures, including the appointment of AML/CFT Compliance Officers and conducting regular internal audits. However, smaller operators often lack the resources and expertise to establish robust accountability mechanisms, leaving them more exposed to risks such as corruption, money laundering, and terrorist financing. Whereas the survey responses indicate that 6 out of the 7 VASPs that participated were aware of their AML/CFT obligations, and implemented these measures, records at FIA showed no records of LCTRs, ALCTRs, SAR, STRs submitted by VASPs, and therefore the survey results could not be conclusive.

There were no instances of willful blindness identified in the VASPs facilitating transactions in Uganda, however there was 01 case where the shareholder and founder of a major VASP in Uganda was charged and convicted for Money Laundering which points to integrity failures of the VASP. As a result of the above the mitigation measure for this input variable was assessed **Medium**

5.3.3 Effectiveness of Compliance Function and Internal Controls

The compliance function and internal control mechanisms among VASPs in Uganda exhibit significant disparities, primarily due to differences in resources, expertise, and adherence to international AML/CFT standards.

The 7 VASPs, also members of BAU that participated in the survey had established AML/CFT compliance functions, and applied internal controls as required under the law. However, the survey established that there were over 61 VASPs currently operating in Uganda whose status in terms of having compliance functions and internal control mechanisms could not be verified. Available information from FIA indicated that there were no AML/CFT reports which cast doubt on the effectiveness of the compliance function and internal control mechanism of the VASPs. Therefore, the rating for this input variable was assessed **very low.**

5.3.4 AML/ CFT Knowledge of VASP Staff

The 7 VASPs (members of the blockchain association) that participated in the survey indicated that the AML/CFT knowledge were adequate as they included familiarity with risks tied to specific services, products, and transaction types, as well as customer and geographic risks. Some staff have been trained to identify red flags such as the use of anonymizing tools like Internet Protocol (IP) anonymizers and mixers, which hinder efforts for CDD measures. However, the survey established that there were over 61 VASPs currently operating in Uganda whose staff knowledge in AML/CFT is unknown.

It was further noted that the VASP staff who responded to the survey were aware of the legal consequences of AML/CFT compliance breaches, including potential penalties for failing to implement effective controls. This awareness is more pronounced among the 07 surveyed VASPs, which typically have dedicated compliance teams responsible for ensuring adherence to national and international AML/CFT requirements. However, this understanding is uneven across the sector, with 02 smaller VASPs lacking the resources to train their teams effectively. Therefore, the rating for this input variable was assessed **very low.**

5.4 Traditional Obliged Entities Mitigation Measures

5.4.1 Risk assessment and Risk Mitigation measures by TOEs (Financial Institutions (FIs) and DNFBPs)

a) *New products, services, and delivery mechanisms*

According to sections 7(2)(a) and (b) of the AMLA, Cap 118, accountable persons are required to identify, assess and take appropriate measure to manage and mitigate ML/TF and PF risks that may arise in relation to the development of new products and new business practices including, new delivery mechanisms and the use of new or developing technologies for both new and pre-existing products. In addition to the issues discussed in threat and vulnerability above, TOEs under the regulatory purview of Bank of Uganda are prohibited from interacting in VAs and VASPs, as a result, their subsequent risk assessments during introduction of new products, services, and delivery mechanisms will not involve VAs or interactions with VASPs while simultaneously identifying and mitigating indirect risks arising from client interactions with VAs or VASPs. However, this prohibition did not extend to other financial sector players like in investment, securities, insurance and DNFBPs like casinos, lawyers, accountants and real estate sector with possibility of linking VAs and VASPs. Through survey responses, 87% of the TOEs with exception to RFSPs reported that there were no risk assessments or risk mitigation measures conducted on new products, channels to consider ML/TF risks for VAs/VASPs as interaction with VAs or VASPs was limited. The mitigation measure for this input variable was assessed Medium.

a) *Existing Products, Business Practices, Services, and Delivery Mechanisms*

For existing services and delivery channels, TOEs must adopt a continuous approach to identify, assess, and mitigate ML/TF risks. This involves closely monitoring pre-existing products and customer behaviours, especially when such offerings interact with VAs or VASPs. Similar to the variable above, this mitigation measure was assessed **Medium.**

5.4.2 Effectiveness of Compliance Function and Internal Control Mechanisms

To address risks associated with VAs and VASPs effectively, TOEs ensured that the compliance function and internal control mechanisms were robust and tailored to meet FATF standards. The respective compliance functions in RFSPs, other financial sector players had the capacity to oversee VA-related services, with staff adequately trained to understand and respond to unique risks posed by VAs. However, majority of entities in the DNFBP sector did not have capacity to effectively apply compliance and internal controls to respond to the risks posed by VAs including clear policies for risk assessment, strong monitoring and reporting protocols, and mechanisms for sanction screening.

For RFSPs, these internal controls incorporated mechanisms to enforce compliance with the prohibition on VA-related activities in their respective sectors. This included implementing systems to detect and prevent transactions that contravened the prohibition, enhancing employee training on regulatory restrictions, and maintaining clear policies to manage indirect exposures. The mitigation measure for this input variable was assessed **Low.**

CHAPTER 06

VA AND VASP INTERACTION WITH TRADITIONAL OBLIGED ENTITIES

6.1 VA AND VASP INTERACTION WITH TRADITIONAL OBLIGED ENTITIES

The interaction of VAs and VASPs with various sectors presents a range of ML/TF risks, ranging from low (where regulatory prohibitions exist) to high (in sectors like gambling, real estate, and DPMS). The pseudo-anonymous nature of VAs and the evolving regulatory landscape significantly elevate ML/TF risks in sectors with high transaction volumes or high-value transactions.

6.1.1 Banking Sector, Payment System Operators, Forex Bureaus, and Money Remitters

The prudential regulator in Uganda imposed a blanket prohibition on banking sector, payment system operators, forex bureaus, and money remitters from engaging with VAs or VASPs. This regulatory measure ensured that these entities are not directly exposed to VA-related ML/TF risks. However, this restriction did not eliminate the broader systemic risks posed by the informal use of VAs. For instance, individuals and businesses may bypass the formal financial system to engage in peer-to-peer transactions or use offshore VA wallets, creating significant blind spots for regulatory oversight. Despite efforts to minimize interaction, available data indicates that VA-related transactions continue to trickle through these regulated entities, often under the registered legal names of prominent VASPs rather than their more familiar trading or brand names. Several instances have been identified where virtual assets have been settled into customers' accounts, with the sender captured as a registered PLC, Pte, or similar entity, names that AML/CFT compliance officers are less likely to associate with VA services. As a result, these transactions have bypassed the scrutiny that would typically apply if the well-known brand names were used. This has enabled significant amounts in billions of Uganda shillings to be processed undetected through local banks and payment system operators. The ML/TF risk for these interactions was assessed **Medium.**

"Several instances have been identified where virtual assets have been settled into customers' accounts, with the sender captured as a registered PLC, Pte, or similar entity, names that AML/CFT compliance officers are less likely to associate with VA services."

"A property purchased using VAs can later be resold for fiat currency, further obscuring the origin of funds."

6.1.2 Real Estate

The real estate sector remains highly vulnerable to VA misuse in Uganda as it remains largely unregulated. VAs can be used to purchase properties, either directly or through intermediaries such as brokers and agents. These transactions often bypass conventional financial institutions, making it difficult to trace the origin of funds. Additionally, property developers may unknowingly receive payments derived from illicit VA transactions coupled with cross-border VA transactions that may pose additional ML/TF risk, as they allow international buyers to acquire high-value properties without triggering local reporting requirements.

Real estate also presents opportunities for layering illicit funds by converting VAs into tangible assets. For example, a property purchased using VAs can later be resold for fiat currency, further obscuring the origin of funds. The anonymity and global nature of VAs make it challenging to enforce effective CDD measures in this sector coupled with the high ML/TF risk identified in the national ML/TF risk assessment. The ML/TF risk for this interaction was assessed **High.**

6.1.3 Lawyers and Accountants

Lawyers and accountants are inherently high-risk gatekeepers in financial transactions and advisory roles, making them susceptible to VA-related ML/TF risks. There have been several reports in adverse media and through questionnaire responses that lawyers and

accountants in Uganda are engaged in VA transactions, demonstrated by law enforcement data as well as several accounting and law firms and partners that have published guidance on how to set up VASPs in Uganda. Available information further indicates some lawyers and accountants have provided escrow services for VA-based transactions or have assisted clients in structuring complex deals involving VAs. Additionally, they can be involved in creating offshore entities or VA accounts that can obscure the true ownership of assets.

The professions' fiduciary nature often places lawyers and accountants in positions where they can inadvertently facilitate the transfer of illicit funds including VAs. The ML/TF risk for this interaction was assessed **High.**

6.1.4 Gambling

The gambling sector is particularly exposed to VA misuse due to the high volume of inflows and outflows it processes as evidenced in the ML/TF threat analysis data that VA deposits and withdrawals are increasingly common in online gambling platforms, allowing individuals to bypass traditional financial systems. High-value betting activities funded by VAs make it difficult to distinguish legitimate winnings from laundered funds.

Additionally, gambling platforms provide opportunities for layering illicit funds. A typical scenario involves an individual depositing VAs into a gambling account, betting small amounts to establish legitimacy, and then withdrawing the remaining balance as "clean" winnings. The ML/TF risk for this interaction is **High.**

> **"Gambling sector is exposed due to high volume Inflows and Outflows. This allows individuals bypass traditional financial systems."**

6.1.5 Capital Markets

Capital markets are experiencing growing interaction with VAs, particularly in the form of tokenised securities, VAs, and VA-backed investment schemes. These instruments provide an avenue for both legitimate investment and ML/TF activities. The cross-border nature of VAs makes it easier for bad actors to move funds into brokerage accounts for speculative trading, potentially laundering money in the process.

Another risk arises from the lack of comprehensive regulation in the VA space. Investors may use VAs to bypass traditional financial controls, such as CDD and reporting requirements, when entering capital markets. This creates a vulnerability in detecting and preventing illicit activity. The ML/TF risk for this interaction is **Medium.**

6.1.6 Insurance

While the insurance sector's interaction with VAs is limited, it presents specific ML/TF risks. For example, individuals may use illicit VAs to fund premium payments for high-value policies, such as life insurance or property insurance. These policies can later be redeemed or used as collateral for loans, effectively laundering the proceeds of crime.

The anonymity of VAs complicates the identification of beneficial owners, particularly in cases where VAs are used as underlying assets for policy claims. Additionally, some insurers are beginning to offer coverage for cybercrimes, which could inadvertently provide a veneer of legitimacy to VA holdings of dubious origin. The ML/TF risk for this interaction is **Medium.**

6.1.7 Dealers in Precious Metals and Stones

Dealers in precious metals and stones (DPMS) face a high risk of VA-related ML/TF activities due to the high-value, low volume nature of their transactions. The pseudo-anonymity of VAs makes it easier for individuals to purchase gold, diamonds, or other precious items without disclosing their true identity or the source of funds.

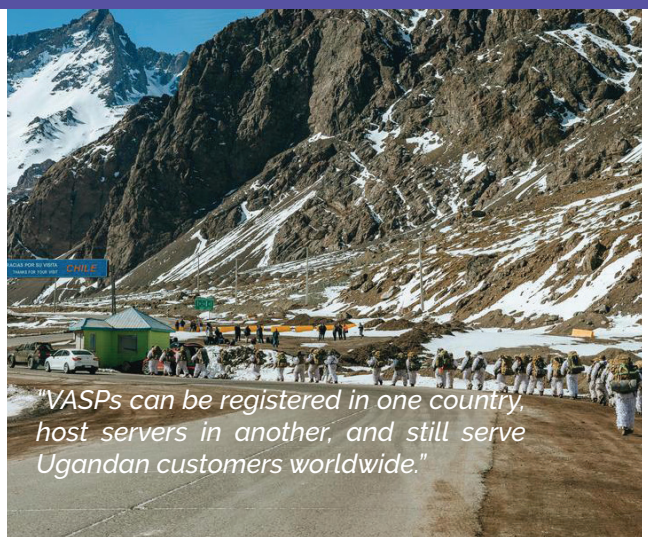
Once acquired, these items can be resold for fiat currency, completing the money laundering cycle. Cross-border trade in precious metals and stones further complicates regulatory oversight, as VAs can be used to settle transactions between international buyers and sellers. The ML/TF risk for this interaction is **High**.

CHAPTER 7

KEY FINDINGS

Uganda faces a **high overall exposure** to ML/TF risks from VAs and VASPs with the ML/TF threat level at High and the overall vulnerability at High. These elevated risks stem from the presence of numerous VASPs, many of which are operating from abroad and a wide range of VAs in use domestically. In contrast, the effectiveness of current controls was very low, Uganda's ability to mitigate VA/VASP risks was Very Low which indicates serious deficiencies in the country's AML/CFT framework for VAs, leaving significant systemic weaknesses.

A major exposure factor is regulatory gaps in Uganda's framework relative to FATF standards. Uganda lacks specific laws for VAs/VASPs, falling short of FATF Recommendation 15 and 16 requirements While VASPs are nominally recognised as "accountable persons" under the AMLA Act Cap 118, there is no dedicated VASP licensing or supervision regime. VAs are not legally defined as money or property, meaning AML/CFT obligations are not effectively applied to them. Additionally, the "Travel Rule" under FATF Rec. 16 requiring originator/beneficiary information on VA transfers is not enforced in Uganda, undermining traceability.



7.1.1 Inherent Cross-Border Risk

Uganda exhibits high inherent cross-border ML/TF risk in the VA/VASP sector in absence of domestic regulations as Uganda-based or global VASPs with Ugandan clients freely provide services globally. VASPs can be registered in one country, host servers in another, and still serve Ugandan customers worldwide. As established, **88% of surveyed Ugandan users indicated the VASPs they use operate in multiple countries** (e.g. Kenya, Nigeria, South Africa, Tanzania), showing that Ugandan VA activity is interconnected with a broad international ecosystem. This global reach, absent local oversight, means illicit actors can exploit Ugandan channels to move funds across borders with little friction. Criminals take advantage of inconsistent international regulations – a form of regulatory arbitrage – by routing activities through jurisdictions like Uganda that have minimal or nascent VA controls. This creates a significant risk of undetected cross-border value transfers, as evidenced by Uganda's VA inflows/outflows which indicate large sums moving transnationally that could be abused for money laundering and other illicit financial flows.

The nature of emerging VA technologies such as increased use of DeFi platforms heightens cross-border vulnerabilities as these allow users worldwide to transact without a central intermediary, which appeals to those seeking less oversight including criminals. Uganda's DeFi usage spiked as the adoption ranking improved to 12th out of 155 countries by 2023. While this signifies growing usage of innovative services, it also means transactions are happening on global decentralised networks beyond regulators' and LEAs reach. DeFi's anonymity and lack of KYC make it a potential haven for laundering funds. NFTs and other novel assets present new cross-border risks as well though these in Uganda are still in a nascent stage (only about USD 3,065 in inflows and USD 2,647 outflows recorded), they enable high-value digital asset transfers with minimal oversight. A criminal can purchase an NFT with dirty money and later sell it to a legitimate buyer, thus laundering the funds, a method made easier by the pseudonymous, borderless nature of blockchain transactions. Similarly, stablecoins are heavily used for cross-border transfers in Uganda as they accounted for the largest share of inflows and outflows from 2020 – 2024. Stablecoins facilitate fast, low-cost cross-border payments but with pseudonymity, posing considerable ML/TF threats.

7.1.2 Camouflaged VASPs with Concerns

Uganda's VA ecosystem includes unlicensed VASPs that have raised red flags in media and law enforcement reports. Without any licensing regime, a variety of entities offer VA services, and some have been implicated in scams or fraudulent schemes. Notorious examples include Ponzi-style investment programs such as OneCoin – a pseudo-VA scam that Ugandan authorities openly warned the public about . Beyond OneCoin, domestic scams such as pyramid investment clubs and fake "VA trading" companies have also targeted Ugandans. For instance, analysis of blockchain data identified "scam services" with about USD 3.17 million inflows and USD 5.82 million outflows linked to Uganda. These schemes typically lure victims to invest in non-existent assets, then rapidly siphon the funds out. The outflows often exceed inflows as perpetrators cash out and launder victims' money, a pattern consistent with ponzi schemes where early investors are paid with money from new victims. Adverse media coverage has highlighted how such fraudulent VASPs vanish with customer funds or collapse, leaving investors with losses and tainting the sector's reputation.

Other camouflaged VASP types of concern include services that directly facilitate criminal activity. Mixing services (tumblers) operating in or accessible from Uganda have been noted for their misuse in laundering proceeds of crime about USD 483,000 entered mixers versus only USD 52,000 leaving, suggesting criminals are pooling illicit VA in mixers for anonymity. Darknet market facilitators are another risky category although usage was not widespread, blockchain tracing showed Ugandan-linked addresses transacting on darknet markets, ndicating involvement in illicit trade for instance drugs, stolen data via unlicensed platforms.

Even seemingly legitimate service types can carry risks if unregulated. Online peer-to-peer exchanges are widely used as well and are inherently unlicensed and they allow individuals to trade VAs directly for cash or mobile money. These P2P platforms, by bypassing regulated intermediaries, can become conduits for moving funds between jurisdictions with weak controls.

7.1.3 Regulatory Arbitrage

Uganda's underdeveloped regulatory framework has made it an attractive venue for regulatory arbitrage in the VA space with no licensing, registration or prudential requirements for VASPs, bad actors can exploit Uganda as a base of operations or target market with minimal fear of enforcement. As noted by the assessment team, many countries are still implementing VA standards, creating gaps that criminals exploit by operating in jurisdictions with nonexistent or lax regulations. Uganda exemplifies this vulnerability as its lack of comprehensive VA laws provides an opening for VASPs to skirt stricter regimes elsewhere. For example, a VASP barred or heavily regulated in one country can simply serve Ugandan users online, or even incorporate in Uganda, to enjoy a light-touch environment. The absence of entry controls since there are no fit-and-proper tests for directors and shareholders, no checks on criminal backgrounds means there is little to prevent criminals or sanctioned persons from owning or operating a Ugandan VASP. This weak oversight invites overseas illicit funds and operators to pass through Uganda in order to avoid detection in more vigilant jurisdictions, consequently, this raises reputational risks for Uganda.

Domestic authorities are aware that unchecked VA activity especially frauds and failures by unlicensed operators can tarnish the country's financial integrity as the country can be seen internationally as a "safe haven" for VA laundering or scam projects, undermining its standing in AML/CFT compliance. Indeed, until February 2024, Uganda was on the FATF "grey list" partly due to deficiencies in supervising new technologies such as VAs, lack of transparency requirements such as no mandated disclosure of VASP beneficial owners further compounds this risk. Some Ugandan VASPs are registered abroad in secrecy havens, making it difficult for competent authorities to obtain ownership information. Such gaps enable regulatory arbitrageurs to hide their identities and move funds through Uganda's VA sector with impunity. For instance, during 2020 – 2024 multiple SARs identified a politically exposed person attempting to launder illicit wealth via unregulated VAs and a local payment systems operator highlighting how criminals leverage Uganda's weaker controls to arbitrage against stricter formal financial rules.

7.1.4 High-Risk Virtual Assets

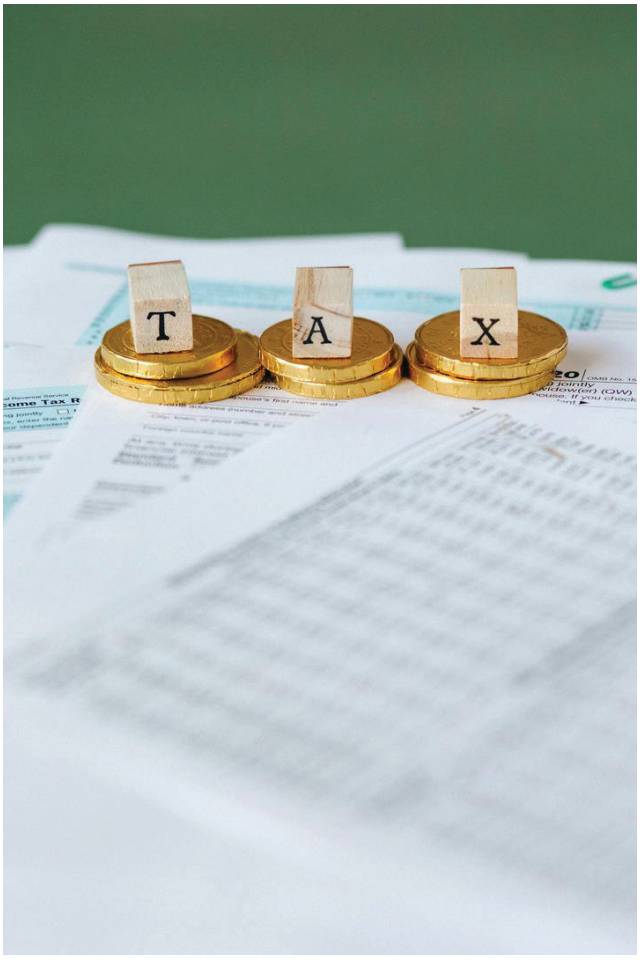
The presence of unlicensed VASPs offering high-anonymity services in Uganda elevates the risk profile of certain VAs. In the current unregulated environment, several VASPs provide or enable privacy-enhancing features whether intentionally or as a by-product of the products they offer. For example, mixers/tumblers accessible in Uganda allow users to commingle VAs funds and redistribute them, severing the audit trail and traceability. As noted, substantial amounts flowed into mixers from Ugandan-linked wallets with only a fraction exiting, indicating illicit funds likely being laundered and held in anonymity pools. Similarly, privacy-focused VAs are in use and pose extreme tracing difficulties. DEXs and non-custodial wallet services used by Ugandans also qualify as high-anonymity facilities, since they enable peer-to-peer transfers without any CDD measures. The proliferation of such unregulated, anonymity granting VASPs is a growing threat since their offerings attract users specifically looking to hide transaction sources, making Uganda's VA ecosystem risky from an AML/CFT perspective.

These VASPs employ various obfuscation techniques that significantly increase ML/TF risks, a common tactic in Uganda is the use of VPNs and TOR networks by local VA users, which masks their IP addresses and geographic location. The assessment found that some Ugandans leverage VPNs in tandem with mixers, adding "additional layers of obfuscation" that frustrate tracing of transaction originators and beneficiaries.Chain-hopping, rapidly converting one VA into another such as Bitcoin to Monero to Ethereum is another technique to break the transaction trail, often facilitated by services that support many types of VAs. LEAs in Uganda struggle to trace or seize VA assets under these conditions since existing laws do not even clearly recognise VAs as property, and advanced privacy tech (mixers, encrypted wallets) hampers efforts to freeze illicit VAs. In one case, a public official used decentralised platforms and mixers to launder proceeds of corruption, successfully obscuring the trail until a local payment provider noticed unusual transactions and filed an STR. Such instances show that high-anonymity VASPs provide criminals a potent tool to conceal their activities, significantly elevating ML/TF risk levels.

7.1.5 The Legality of Virtual Assets

Uganda's official stance on VAs is one of non-recognition (and caution) rather than outright prohibition. There is no law in Uganda that explicitly bans owning or trading virtual assets, but VAs are not legal tender and not legally recognised as a form of payment. In September 2019, the Ministry of Finance publicly warned that the government "does not recognise VAs as legal tender" and advised the public to exercise caution, since the sector was unregulated and lacked consumer protection. This means one cannot discharge a debt or pay taxes in Bitcoin or other VAs, and merchants accepting VAs do so at their own risk. Moreover, existing laws do not clearly define VAs as an asset class neither as currency, securities, commodities, nor property under established definitions. The risk assessment explicitly notes that VAs are not categorised as "property," "funds," or "proceeds" under the existing law, which in practice excludes them from many AML/CFT provisions. This means, when a crime is committed involving VAs, there is ambiguity about how to treat the VA itself such as whether it can be seized as proceeds of crime, undermining enforcement and oversight.

September **2019,** the Ministry of Finance publicly warned that the government "does not recognise VAs as legal tender" - Advised the public to exercise caution, since the sector was **unregulated** and **lacked** consumer protection.



7.1.5.1 Tax Matters

Additionally, because VAs are not formally recognised in law, there are no specific tax guidelines on VAs in Uganda. Income or capital gains from virtual asset trading often go unreported to the Uganda Revenue Authority. The predominantly cash-based economy and absence of VA tax rules create a loophole easily exploited for tax evasion. For instance, an individual can convert fiat money into VA, trade or invest abroad, and later convert back to fiat without those transactions ever being declared for tax effectively bypassing tax reporting systems. The National Budget does not explicitly account for revenue from VA activities, and the URA has yet to issue any notice on taxing VA gains. As a result, tax evasion via VAs was assessed high risk by the assessment team.

7.1.5.2 Legal Recognition as Payment or Store of Value

Uganda does not recognise Virtual Assets (VAs) as an official means of payment, as demonstrated by the BoU, which has emphasised that VAs are not backed by any government guarantee and are not accepted as currency in Uganda's economy. This stance was upheld by the High Court in Kayondo v Bank of Uganda (Miscellaneous Cause No. 109 of 2022) 2023 UGHCCD 113 (24 April 2023), where the Court affirmed the BoU's authority to direct its licensees to refrain from facilitating VA or cryptocurrency transactions, thereby reiterating that VAs lie outside Uganda's recognised payment systems. There was also no legal status for VAs as a store of value, as they fall outside BoU's legal mandate covering fiat currency and licensed financial instruments. Additionally, since VAs are not officially classified, no licenses or regulatory guidelines have been issued by key authorities (such as BoU or the CMA) for their operation.

7.1.6 High-Risk VASPs

Several high-risk VASP business models are active or accessible in Uganda, each posing challenges to AML/CFT controls. One such model is the peer-to-peer service where rather than using a traditional exchange, many Ugandans trade VA directly with each other often facilitated by websites or mobile apps that match buyers and sellers. P2P exchanges have no central intermediary holding customer funds and typically impose minimal or no CDD requirements. This model is popular in Uganda since it was ranked 18th globally in P2P trade volume according to Chainalysis Crypto Adoption Report, with significant inflows/outflows via P2P channels making it high-risk since it bypasses regulated financial institutions. The lack of any intermediary oversight on P2P trades means there are no systematic customer verification or transaction monitoring, severely undermining AML/CFT controls. Criminals can exploit P2P networks to move funds between fiat and VA or across borders with little chance of detection.

Another high-risk model present is the use of decentralised exchanges and DeFi protocols. These platforms such as allow users in Uganda to swap VAs using automated smart contracts, with no centralised entity collecting CDD information. DeFi platforms have grown in prominence in Uganda as users shift away from more transparent centralised exchanges. The decentralised nature offers benefits like direct custody and lower fees, but from an AML/CFT perspective, this poses challenges since transactions on DEXs are pseudonymous and often untraceable to real identities. Moreover, DeFi often enables advanced techniques like liquidity pooling and yield farming, which can commingle funds from thousands of users globally, making illicit funds harder to pinpoint. The impact is that standard AML/CFT measures cannot be readily applied, giving criminals a channel to launder money or finance terrorism covertly.

Mixing and tumbling services represent another business model considered extremely high-risk. These are services sometimes integrated into wallets or offered by standalone websites accept users' VA and return different VAs after mixing them with others' funds. As noted earlier, mixers tied to Uganda have seen heavy use for anonymization linked to VPNs and TOR networks which undermines traceability and aggravates AML/CFT efforts. FATF considers such services as VASPs in some cases, subject to regulation, but Uganda does not currently regulate or sanction them.

Additionally, foreign-based exchanges with weak AML/CFT controls operate in Uganda's market and are de facto part of the high-risk segment. Survey data showed **94% of Ugandan respondents** use VASPs based outside Uganda with only one foreign VASP having a local company registration. Some of these offshore exchanges are domiciled in jurisdictions with no specific VA regulations or lax enforcement, and thus may not rigorously enforce CDD measures on Ugandan clients. For example, a Ugandan can easily sign up on

an overseas platform that only does basic email registration. These exchanges also offer high-risk products like margin trading, VA swapping, or support for privacy coins without oversight, allowing users to obscure sources of funds. The business complexity and variety from simple trading apps to multi-service platforms offering everything from NFTs to VA loans further complicates the risk profile. Some VASPs intentionally exclude fiat entirely catering for VA-to-VA conversions to stay outside traditional AML/CFT regulations, while others engage in cross-border remittance-like services using stablecoins. As a result, these business models collectively contribute to a High risk rating signifying that without new controls, they pose substantial increase for ML/TF.

7.1.7 Business Model

The dominant VASP business models in Uganda reflect the lack of local regulated options and the community's adaptation to that void. Foreign centralised exchanges effectively serve as the primary on/off ramps for Ugandans such as Binance, Kraken, and OKX are among the commonly used exchanges available in Uganda according to industry listings. These large exchanges are not Ugandan-incorporated[27] , yet they handle the bulk of Ugandan VA volume. Users deposit via mobile money or informal agents and trade on these exchanges – meaning that while these businesses have robust AML/CFT programs internationally, Ugandan regulators have no direct oversight over their operations. This model has mixed implications, on one hand, top-tier global exchanges do perform CDD measures, transaction monitoring, and have compliance teams; on the other, any compliance is offshore and Ugandan authorities must rely on foreign cooperation to obtain information. For instance, If a Ugandan uses an exchange registered in the EU, any suspicious activity reporting happens to EU authorities, not Uganda's FIA creating a gap in local financial disclosures. Thus, while foreign centralised exchanges are dominant and somewhat safer than unregulated platforms, they still pose regulatory challenges due to jurisdictional disconnect.

In parallel, peer-to-peer and decentralised models are increasingly prevalent, which further undermines regulatory oversight. As noted, users have been shifting from CeFI services to DeFi finance in recent years driven by convenience and perhaps necessity since RFSPs cannot facilitate VAs, users resort to P2P trading in cash. With DeFi exchanges, regulators cannot easily impose reporting obligations, there's no centralised entity to report suspicious transactions or implement counterparty verifications. This means a whole class of VA transactions goes unmonitored. Peer-to-peer exchanges similarly erode the CDD measures even if popular exchanges enforce KYC, once VA is withdrawn, users can trade it P2P without any trace. Ugandan competent authorities currently do not have measures to address P2P beyond general public warnings. Each peer-to-peer trade is essentially an unregulated money value transfer, raising the risk that criminals use these avenues to launder money or move terrorism financing with impunity.

27 Binance had a short-lived Uganda branch, but mostly Ugandans use the global site

7.1.8 Lack of Customer Due Diligence Measures

Significant gaps in CDD practices exist in Uganda's VA sector, both among the service providers themselves and the supporting financial infrastructure (fiduciary and capital providers). Because there is no mandated licensing regime for VASPs, many VASPs in Uganda are not performing robust KYC on their customers. Whereas VASPs are listed on the second schedule of the AMLA Cap 118 and are required to implement AML/CFT requirements including CDD measures, this is currently not being enforced in Uganda and no sanctions have been imposed on those found in breach. In practice, this means a Ugandan VASP such as a trading app or OTC broker could onboard customers without any KYC documents or risk assessment, since no regulator is checking compliance. Some VASPs may voluntarily implement KYC, but many likely do the bare minimum, especially if they are small start-ups or P2P platforms. Additionally, the lack of reliable identification infrastructure usage is also an issue, while Uganda has a national ID system, there is no integration of that with all VA platforms, and no requirement that VASPs verify users against it. This CDD gap leaves VASPs open to abuse by criminals using fake names or proxies.

RFSPs in Uganda are restricted from dealing with VA directly, so their exposure is limited. However, if a customer tries to use a bank account or card to fund a VA purchase or receive proceeds), the banks have occasionally detected and reported it as suspicious demonstrated by the 6 STRs and 49 SARs filed with FIA from 2020 – 2024. This number is low, suggesting either few attempts or possibly that banks miss many cases. It also indicates that while banks might flag an obvious VA transfer due to BoU directives, they do not examine the ultimate counterparties, that is, the VASP or the beneficiary of the VA.

The Travel Rule, which would require transmitting originator/beneficiary data with VA transfers, remains unimplemented, meaning even when VASPs send VA to each other, they do not include identifying info. This omission is a critical data gap that authorities cannot readily link transactions to specific individuals without painstaking blockchain analysis. VASPs have not been issued detailed guidance on reporting suspicious transactions or maintaining records. As a result, many VASPs may be unaware of how to detect and document suspicious activity, leading to under or non-reporting. This creates a fertile ground for illicit actors to operate with anonymity or false identities.

7.1.9 Limited Understanding in the Private Sector

There is a limited level of AML/CFT knowledge and experience related to VAs/VASPs in Uganda's private sector. VA is a relatively new domain, and many traditional financial institutions, as well as the emerging VASP industry, are still climbing the learning curve on how to manage associated risks. The assessment highlighted that specific guidance or training for VASPs has not been provided by financial regulators for instance, FIA has not issued instructions to financial institutions on how to identify and file STRs or red flags unique to VA transactions. Consequently, VASPs who have registered with FIA are not necessarily equipped with the practical knowledge to implement effective AML/CFT programs. Most of the 16 entities registered as VASPs are start-ups or fintech firms that lack dedicated AML/CFT compliance staff. The assessment found no structured framework for some VASPs to appoint qualified compliance officers, conduct risk assessments, or implement ongoing AML/CFT training. This indicates a gap in institutional capacity many VASPs likely do not have personnel who deeply understand AML/CFT regulations or VA-typologies, and they have not been receiving sector-specific guidance from authorities. In the broader private sector financial institutions, forex bureaus and money remittance companies, PSOs, auditors among others, awareness and engagement on VA risks is also nascent.

Additionally, there is limited public-private dialogue specific to VAs compared to more mature jurisdictions where regulators and exchanges might meet regularly, none-the less the Blockchain Association of Uganda with 10 active members as of the assessment period can assist share knowledge among industry players.

7.1.10 Exposure to Unsafe VASPs

Ugandan users are currently exposed to a number of unsafe or high-risk VASPs, as evidenced by third-party risk ratings. In fact, available information on global VA regulations assigned Uganda one of the lowest "safety ranks" in the world – just 0.4 out of 10. This exceptionally low score where a higher number would indicate a safer, more regulated environment demonstrates the country's unprotected status, warning that engaging in VA in Uganda carries high risk. The low safety rank correlates with factors like lack of legal protections, prevalence of scams, and absence of regulatory oversight. Another metric of risk is the number of projects barring Ugandan participation with 25 ICOs geofencing Uganda which implies many operators view Ugandan investors as high-risk due to high fraud rates or compliance issues[28]

28 trading-education.com

Bitrawr, which ranks exchanges available in each country by security and reliability, shows that only a handful of trusted exchanges operate in Uganda all of which are large international ones. Bitrawr's methodology gives preference to exchanges with strong security records and those specifically serving the country. The fact that just four exchanges make the list suggests that beyond those, the other platforms Ugandans might be accessing are less reputable or outright unsafe. Indeed, many Ugandans resort to peer-to-peer on platforms that do not guarantee fund safety – leaving them vulnerable to hacks or exit scams. There have been instances of obscure exchanges or wallet providers that disappeared with client funds, which reinforces the "unsafe" character of much of the market.

7.1.11 Lack of a Position on VA Activities

Unlike some countries that have imposed strict licensing conditions or bans, Uganda has not placed explicit restrictions on most VA activities for the general public, instead, the sector operates in a regulatory vacuum. Since there is no licensing regime, there are no license conditions or limits such as caps on transactions, specific reporting thresholds beyond generic AML/CFT rules, among others. Anyone in Uganda can technically buy, sell, or use VA, as there is no law forbidding individuals or non-RFSP businesses from doing so. The only notable restriction comes indirectly via BoU's stance toward TOEs, which prevents RFSPs from getting involved. But outside the regulated financial sector, VA activities have not been curtailed by law. For instance, the Uganda Communications Commission or other bodies have not blocked VA websites.

However, Uganda has used existing financial regulations in limited ways to indirectly influence VA activity. Notably, the Foreign Exchange Act requires all cross-border payments in foreign currency to go through authorized dealers, financial institutions. VA transactions inherently sidestep this, meaning they violate the spirit of exchange control regulations. Yet Uganda has not updated the law to explicitly include or forbid VAs as a means of evading capital controls. So while on paper all forex flows should be via financial institutions, in reality VA provides a route to bypass that, a gap acknowledged by the assessment.

7.1.12 Implicit Ban by Bank of Uganda

Bank of Uganda has taken an implicit but significant step to limit VA activity it banned all RFSPs from facilitating VA transactions. In essence, BoU's stance is "VA should remain outside the formal financial system." ***In 2022, BoU issued a directive restricting its supervised entities from directly or indirectly dealing in VAs*** which meant, for example, commercial banks must not open accounts for VA exchanges, process purchases of VA with credit/debit cards, or settle payments to or from VASP businesses. Similarly, PSOs and other payment companies licensed under the National Payment Systems Act 2020 were instructed not to transfer funds related to VA trades. BoU's rationale was to "mitigate

risks to the financial sector" by cordoning off VA, they aimed to prevent potential contagion or abuse of the formal payment network. This policy, while it does not criminalize VA for the public, it cuts off the bridge between VA and the mainstream financial infrastructure. It sends a clear signal that BoU does not endorse or permit its licensees to interact with VAs.

This proactive stance limits the conversion of VAs into Ugandan shillings through official channels, reducing the likelihood of fraudulent activities and money laundering within regulated entities; however, it simultaneously forced VA trading into less visible, informal networks where transactions occur via cash, foreign accounts, or stablecoins. This redirection has not only undermined the growth of legitimate VA ventures as witnessed with the closure of some internationally affiliated VASPs that were based in Uganda but also fostered a black-market dynamic that remains largely beyond the reach of conventional regulatory oversight.

7.1.13 Facilitating Unlicensed Money Services Businesses

The VA ecosystem in Uganda has inadvertently paved the way for unlicensed money service businesses by enabling channels that transfer funds outside the formal financial system, allowing informal VASPs to mimic the functions of traditional remittance or currency exchange operators without any regulatory oversight. For instance, an individual acting as a local VA agent in Kampala might collect shillings from customers and remit equivalent VAs such as Stablecoins to relatives abroad, operating in a manner similar to a licensed money transfer service yet completely bypassing BoU's controls. The borderless and rapidly convertible nature of VAs, such as USDT and USDC, facilitates near-instantaneous cross-border transfers that circumvent the requirements of Uganda's Foreign Exchange Act, which mandates that all such transactions go through authorized financial institutions. This has given rise to a parallel remittance system where neither the sender nor the intermediary is licensed, a practice that not only undermines regulatory control but also heightens the risk of ML/TF by allowing criminals to shift illicit funds without reporting obligations.

Furthermore, many of these operations are intertwined with fraudulent investment schemes and unsanctioned financial services, where deceptive ventures like VA investment clubs, coin networks, or mining schemes solicit fiat money, convert it into VAs, and transfer it abroad under the guise of legitimate business, as seen in cases like OneCoin and Dunamiscoins ponzi schemes. With terrorists and corrupt officials also exploiting these channels to launder money and fund illegal activities through anonymous online campaigns and unregulated intermediaries, a significant portion of Uganda's financial activity now occurs off the books, highlighting a critical vulnerability in its financial crime defenses that demands stringent regulatory intervention to either integrate these entities into the formal system or eliminate their operations entirely.

7.1.14 Cybercrime

> "Hackers demand payment in Bitcoin or other VAs, along with phishing and fraud schemes that trick individuals into surrendering wallet keys.
>
> ***Ransomware attacks***

Cyber-attacks targeting VASPs and VA users in Uganda introduce an additional layer of ML/TF risk by generating illicit proceeds that are then funneled through sophisticated laundering mechanisms. Although Uganda has not witnessed a breach on the scale seen in larger markets, many local VASPs operate with limited cybersecurity measures, rendering them susceptible to hacks that can result in substantial theft of VAs. Once stolen, these assets are rapidly moved through mixers, multiple addresses, and privacy coins to obscure their origins, effectively transforming a cyber breach into a complex laundering operation on the blockchain.

Ransomware attacks, where hackers demand payment in Bitcoin or other VAs, along with phishing and fraud schemes that trick individuals into surrendering wallet keys, further consolidate these funds into untraceable sums, which may circulate through both domestic and international unregulated channels. Moreover, even when global exchange hacks indirectly affect Ugandan users, the tainted VAs often find their way into the local market, implicating unwitting traders in the laundering process. The link between cybercrime and financial fraud shows that Uganda must improve its cybersecurity, strengthen its ability to track and respond to incidents, and put in place strong rules to stop criminals from using the country to conceal proceeds from cybercrime.

7.1.15 Increased Adoption of DeFi Products

Uganda's rapid adoption of DeFi platforms evidenced by a leap in global rankings from 105th to 12th has seen a significant shift in VA activity into decentralised channels that offer access to global liquidity, higher yield opportunities, and financial services unburdened by traditional gatekeepers, yet this evolution comes with heightened ML/TF risks. The inherently pseudonymous and borderless nature of these platforms, which require nothing more than a VA wallet for access, facilitates the obfuscation of illicit fund flows, enabling criminals to, for example, swap USDT for various tokens on a DEX, distribute assets across multiple wallets, and blend them within liquidity pools to disguise their origins. This risk is compounded by the susceptibility of DeFi platforms to hacks and "rug pulls," where fraudulent schemes not only lead to substantial losses but also generate large volumes of tainted funds that must be laundered through domestic P2P networks. Moreover, the absence of conventional CDD procedures and regulatory oversight creates fertile ground for activities ranging from investment frauds to money laundering connected with drug trafficking, trafficking in persons or wildlife, and even online pharmacies evading detection by quickly swapping stablecoins. Terror groups,

too, can exploit these decentralised systems, raising and distributing funds across borders with minimal oversight. Consequently, while the surge in DeFi adoption among Ugandans reflects an increasingly tech-savvy populace, it also significantly magnifies the potential for undetected illicit finance, challenging authorities to develop innovative strategies such as tightening on/off ramps and enhancing blockchain analytics to effectively counter fraud, money laundering, and other criminal misuses that thrive in this unregulated environment.trafficking in persons or wildlife, and even online pharmacies evading detection by quickly swapping stablecoins. Terror groups, too, can exploit these decentralised systems, raising and distributing funds across borders with minimal oversight. Consequently, while the surge in DeFi adoption among Ugandans reflects an increasingly tech-savvy populace, it also significantly magnifies the potential for undetected illicit finance, challenging authorities to develop innovative strategies such as tightening on/off ramps and enhancing blockchain analytics to effectively counter fraud, money laundering, and other criminal misuses that thrive in this unregulated environment.

Category	Sub-Saharan Region	Uganda	Global
DeFi	34.3%	84.5%	34.9%
Centralised Exchange	63.8%	15.5%	62.4%
Others	1.9%	0.0%	2.1%

Source: *Blockchain Analysis Company - 2024*

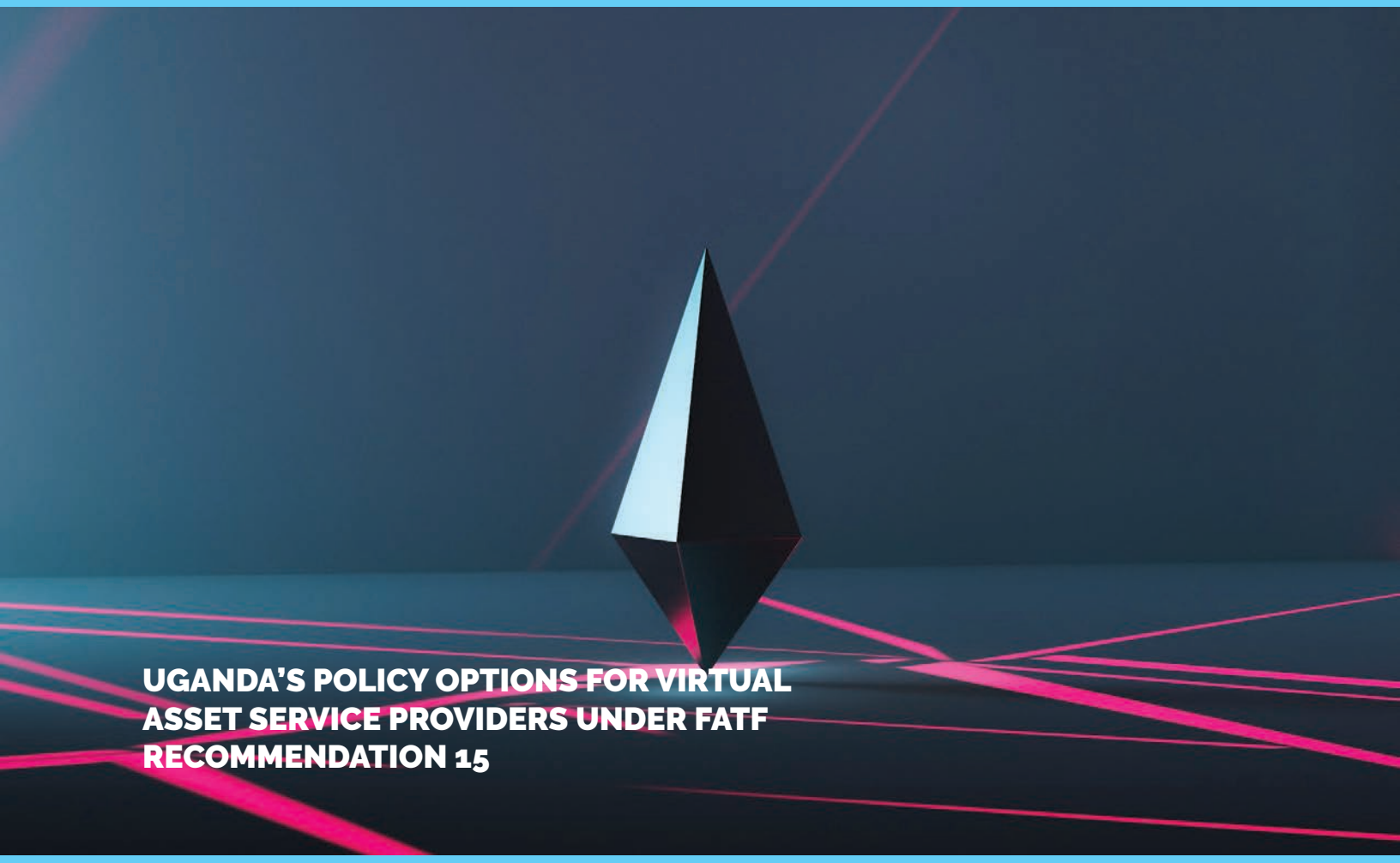
The table above illustrates that Uganda **relies** heavily on DeFi platforms, with **84.5%** of transactions happening through DeFi, much higher than the 34.3% in the Sub-Saharan region and 34.9% global average. In contrast, Uganda has a very low usage of CEX at only 15.5%, while the Sub-Saharan region stands at 63.8% and the global average is 62.4%. This indicates a serious lack of CDD measures on VAs and VASPs. DeFi platforms usually allow users to transact without revealing their identities, making it easy to avoid KYC checks. Since Uganda has very low use of CEXs, which have stronger AML/CFT controls, it means that most transactions are happening without proper regulatory oversight.

7.1.16 NFT and Stablecoins

NFTs and stablecoins have emerged as notable elements of Uganda's VA landscape, each characterized by distinct usage patterns and risks that highlight the evolving challenges in this sector. Although the NFT market remains in its infancy reflected by only a handful of transactions totaling modest values, its capacity to facilitate high-value single transactions poses a money laundering risk. Criminals can purchase NFTs with illicit funds and later resell them in unregulated, peer-to-peer marketplaces to "clean" their proceeds. In contrast, stablecoins such as USDT and USDC have become central to Uganda's VA economy, evidenced by high value inflows and outflows, and serve as a digital substitute for fiat in remittances and trading; their fast, low-fee transactions and inherent pseudonymity enable not only legitimate cross-border transfers but also illicit financial flows that circumvent traditional exchange controls, thereby elevating risks related to money laundering, sanctions evasion, and unrecorded capital flight. Moreover, the unregulated nature of these assets could attract foreign operators seeking jurisdictions with lax oversight, further complicating consumer protection and regulatory enforcement.

NFTs and stablecoins have emerged as notable elements of Uganda's VA landscape,

CHAPTER 8



UGANDA'S POLICY OPTIONS FOR VIRTUAL ASSET SERVICE PROVIDERS UNDER FATF RECOMMENDATION 15

This section provides guidance on two possible policy directions for Uganda regarding Virtual Asset Service Providers. It is based on the Financial Action Task Force (FATF) Recommendation 15, which addresses new technologies and specifically covers virtual assets and VASPs. Uganda can consider either banning VASP operations in the country or regulating VASP operations through a licensing or registration regime. Each choice entails different requirements and consequences for Uganda's AML/CFT framework. This report aims to explain, in clear terms, the key actions that Uganda would need to take under each scenario and highlights the possible outcomes. It is intended to assist policymakers, law enforcement agencies, regulators, financial institutions, and the general public in understanding the ramifications of each approach.

8.1 Scenario 1: Banning VASP Operations

If Uganda decides to prohibit or ban all VASP activities, the country must still comply with certain aspects of FATF Recommendation 15 that revolve around identifying and assessing the risks posed by new technologies and taking action against any VASPs that operate illegally. The following key requirements and actions would be taken;

8.1.1 Identify and Assess Risks (Criteria 15.1 & 15.2)

Uganda would continue to research and understand the ML/TF risks linked to VAs and VASPs, even if they are officially banned. In practice, it would be essential to maintain and update risk assessments regularly, since some individuals might resort to using virtual assets through foreign platforms or informal networks. Achieving this goal would require a dedicated team within the Financial Intelligence Authority or a similar body that focuses on emerging illicit trends involving virtual assets including the Uganda Police Force. Furthermore,

"Investigators and supervisors would need specialised training to recognise the techniques that criminals use to conceal transactions"

and the country would benefit from acquiring software capable of monitoring suspicious or high-risk transactions. Clear guidelines for financial institutions, stipulating how they should spot and report potentially illicit virtual asset activities, would also help Uganda stay vigilant.

8.1.2 Risk-Based Approach (Criteria 15.3(a) & 15.3(b))

Competent Authorities in Uganda would have to remain alert to the ways in which banned or illegal VASP operations might infiltrate the Ugandan market, possibly through cross-border activity or underground trading platforms. In response, they should allocate resources according to the level of risk that these illegal operations pose. To accomplish this, Uganda could include banned VASP activities in its broader ML/TF National Risk Assessment, thereby ensuring that relevant competent authorities share intelligence and coordinate their efforts. Moreover, sustained investments in specialised cybercrime and financial crime units would enable Uganda to detect and investigate suspicious online forums or hidden VA platforms. Public awareness campaigns can also bolster these measures, encouraging

citizens to report any suspected illegal VASP operations.

8.1.3 Action Against Unlicensed VASPs (Criterion 15.5)

If Uganda bans VASPs, it requires legislation that unequivocally outlaws VASP operations and grants law enforcement the power to take down illegal platforms. Such laws should define VASP activities clearly, list punitive measures, and ensure there are meaningful sanctions for anyone contravening the ban. To enforce these rules, Uganda would profit from equipping its authorities with secure "government seizure wallets" and establishing asset recovery procedures that allow them to freeze and confiscate any seized virtual assets. Investigators would need robust legal powers to request data from internet providers and to cooperate with foreign VASPs such as exchanges whenever they uncover illegal VASP operators. The penalties, which could include fines, license revocations (if any supervised financial sector players are involved), and even criminal prosecutions, must be substantial enough to deter ongoing or future violations.

8.1.4 International Cooperation (Criterion 15.11)

Although VASP operations may be banned in Uganda, foreign-based entities can still facilitate illicit activities across borders. Uganda must therefore remain capable of exchanging information and collaborating with international partners to halt or investigate the criminal misuse of virtual assets. This process includes strengthening Mutual Legal Assistance Treaties and other legal instruments that facilitate cross-border inquiries. It also requires specialised training for law enforcement, FIA analysts or prosecutors in crypto-forensics and digital evidence collection. Working closely with international authorities, whether through Interpol, the Egmont Group, or bilateral arrangements, would help ensure effective asset tracing and freezing whenever illegal VA funds flow in or out of Uganda.

8.1.5 Consequences of Banning VASP Operations

Banning VASPs may reduce direct local activity in virtual assets, but risks pushing potential users to underground or offshore platforms, which might be harder to monitor. It also limits fintech innovations and reduces potential benefits linked to faster, cheaper cross-border payments. Enforcement is likely to be a challenge, as authorities must invest in technological infrastructure and train personnel to detect covert digital transactions and take regulatory action fast enough before detection. Certain international stakeholders might view the ban as evidence of a strong approach to mitigating ML/TF risks, whereas others could see it as stifling technological growth.

8.2 Scenario 2: Regulating VASP Operations

Should Uganda opt to permit and regulate VASPs, it must take steps to comply with all of FATF Recommendation 15's requirements in order to be considered technically compliant. This approach would involve creating or refining legal frameworks to license or register VASPs, supervising them adequately, and ensuring they implement the usual AML/CFT procedures required of other financial institutions. The following key requirements and actions would be taken;

8.2.1 Risk Assessments for New Technologies (Criteria 15.1 & 15.2)

Uganda should mandate thorough risk assessments for new virtual asset products or services prior to their launch. VASPs and financial institutions must carefully analyse the potential ML, TF, or PF vulnerabilities associated with their products and take appropriate measures such as enhanced due diligence or transaction monitoring to reduce the identified risks. Specialised training for AML/CFT supervisors would be essential to equip them with the knowledge to identify red flags and enforce compliance. Additionally, official guidance on high-risk virtual asset activities, such as privacy-enhancing cryptocurrencies, can help direct firms toward enhanced safeguards.

8.2.2 National-Level VA/VASP Risk Assessment (Criteria 15.3(a) & 15.3(b))

Virtual assets should be integrated into Uganda's overall AML/CFT risk analysis so that policy makers can allocate resources where they are most needed. By incorporating VASP operations into the National Risk Assessment, Uganda's authorities can build a comprehensive understanding of how domestic and international VASP activities intersect with the country's traditional financial system. This process calls for coordinated efforts among government agencies, private-sector stakeholders, and law enforcement to compile and analyse data on suspicious activity. It also necessitates investing in specialised training for those investigating virtual asset crimes so they can recognize higher-risk areas and respond effectively.

8.2.3 VASP Requirements to Manage Risks (Criterion 15.3(c))

VASPs should conduct their own ML/TF/PF risk assessments and be prepared to demonstrate how they plan to mitigate identified risks. Activities or customers identified

as being higher risk for ML/TF must be subject to enhanced AML/CFT measures. To achieve this, Uganda competent authorities could publish detailed guidelines that explain how to gauge virtual asset risks, taking into account transaction volumes, customer profiles, geographic exposures, and specific VA features. VASPs would also need compliance officers who are adept at detecting and reporting suspicious activity. In addition, supervisory authorities could encourage the use of blockchain analytics software to trace complex or obfuscated transaction patterns within their respective systems.

8.2.4 Licensing or Registration of VASPs (Criterion 15.4)

Under a regulated environment, Uganda must enact legislation making it compulsory for all VASPs to apply for either a license or registration. To prevent criminals or their associates from owning or controlling these services, fit-and-proper tests should be established. These measures can involve background checks, screening for prior financial crimes, and verifying that managerial staff have the requisite expertise. A publicly accessible register of licensed VASPs would not only offer transparency to consumers but also deter unscrupulous operators who may seek to remain clandestine.

8.2.5 Preventing and Punishing Unlicensed VASPs (Criterion 15.5)

A licensing regime does not fully eliminate unregistered or unauthorized platforms, so Uganda must maintain procedures for detecting and dismantling illegal VASP operations. This endeavour would benefit from ongoing collaboration among the FIA, the national police, telecommunications companies, and commercial banks. Swift penalties for violators, such as financial penalties, business closures, or criminal charges for deliberate non-compliance, would reinforce the seriousness of Uganda's regulatory stance.

8.2.6 Risk-Based Supervision (Criterion 15.6)

To ensure VASPs follow AML/CFT obligations, Uganda should appoint a suitable supervisory authority or authorities with a clear mandate to oversee VASP activity. Regular inspections, both on-site and off-site, allow supervisors to examine customer data and transaction logs while verifying adherence to AML/CFT requirements. VASPs presenting higher risks may be subject to more frequent or thorough reviews. Regulators also stand to gain from adopting cutting-edge reguratory technology solutions capable of analysing large volumes of data and spotting anomalies in real time.

8.2.7 Guidelines and Feedback (Criterion 15.7)

Regulators must issue written instructions explaining precisely how VASPs can comply with AML/CFT rules, including requirements such as customer due diligence, suspicious transaction reporting, and record-keeping. Periodic updates are crucial because the virtual asset industry evolves rapidly. It would be prudent to establish feedback loops through workshops, official notices, or forums so that VASPs can learn from typology reports and receive suggestions for improving their compliance programs.

8.2.8 Sanctions for Non-Compliance (Criterion 15.8)

Uganda should offer a broad spectrum of sanctions ranging from administrative fines and reprimands to severe criminal penalties for VASPs and their managers who breach AML/CFT obligations. To maintain transparency, regulators might publish enforcement actions and outcomes. This system not only deters future transgressions but also reassures investors and the international community that Uganda takes compliance seriously.

8.2.9 Preventive Measures (Criterion 15.9, including Criterion 15.10)

In line with other financial institutions, VASPs must implement standard preventive measures such as customer due diligence (CDD), record retention, and suspicious transaction reporting. For transfers exceeding USD/EUR 1,000, VASPs should obtain and share details regarding the originator and beneficiary ("the travel rule"). It is equally important that VASPs be able to comply with targeted financial sanctions, freezing or blocking assets tied to persons or entities designated by the United Nations or other international bodies. Achieving this compliance often involves equipping VASPs with advanced screening tools that can automatically flag blacklisted wallet addresses.

8.2.10 International Cooperation (Criterion 15.11)

Given the global nature of virtual assets, Uganda's ability to cooperate with foreign counterparts is paramount. Domestic law should permit regulators to exchange information on licensing, ownership, and compliance with foreign authorities. By engaging in joint investigations or asset-tracing exercises, Uganda can better respond to cross-border ML/TF cases involving virtual assets. Membership in international networks such as the Egmont Group or active participation in FATF-style regional bodies can significantly improve Uganda's knowledge base, strengthen relationships with foreign officials, and enhance the country's capacity to detect, freeze, and recover illicitly obtained virtual assets.

For transfers exceeding USD/EUR

1,000,

"VASPs must implement standard preventive measures such as customer due diligence (CDD), ...

8.2.11 Consequences of Regulating VASP Operations

A regulated environment promotes greater transparency by compelling VASPs to maintain proper customer records and send timely suspicious transaction reports. It can also improve Uganda's international reputation and attract investment, as compliance with FATF standards often reassures global partners. Nevertheless, regulators and law enforcement agencies will require additional funding, training, and technical solutions to supervise VASPs effectively. Permitting the development of VASP services could foster innovation, reduce remittance costs, and expand financial inclusion, yet Uganda must carefully strike a balance in order to avoid overly lax or excessively restrictive rules that might facilitate regulatory arbitrage.

8.3 Benchmark on Kenya's Proposed Regulatory Framework for Virtual Assets and Virtual Asset Service Providers

Kenya's Virtual Asset Service Providers Bill, 2025 provides a comprehensive legal structure for regulating VAs and VASPs. It seeks to foster innovation while curbing risks associated with money laundering, terrorism financing, and other forms of financial crime. The Bill ensures that entities engaging in virtual asset activities meet licensing and prudential requirements set by relevant regulatory bodies. Its core intentions focus on consumer protection, market stability, and the transparent operation of virtual asset businesses.

8.3.1 Legislative Overview

a) The Bill places emphasis on licensing all VASPs operating "in or from" Kenya and proposes strict conditions for eligibility indicating only locally incorporated companies or foreign companies with certificates of compliance would qualify to seek a license. The scope of the Bill primarily covers assets or tokens with a clear monetary or investment function and excludes those used in purely closed-loop environments or limited to non-financial uses, such as some non-fungible tokens (NFTs). This distinction ensures that the highest-risk activities remain under the authorities' supervision while allowing innovation to continue unencumbered in less risky domains.

b) Under the Bill, the Capital Markets Authority (CMA) of Kenya and the Central Bank of Kenya (CBK) share oversight responsibilities. Their mandate includes assessing license applications, monitoring compliance with anti-money laundering obligations, and approving any entity that issues virtual assets to the public. This dual-regulator model recognises that certain VAs resemble payment instruments, while others more closely resemble securities or investment products. Segmenting oversight allows each regulator to focus on its specific area of expertise, although collaboration remains necessary where payment and securities characteristics overlap. The Bill provides wide enforcement powers to these two regulators, allowing them to investigate VASPs, examine business

records, and impose penalties or sanctions where noncompliance occurs.

c) A key element of the Bill involves AML/CFT requirements by designating VASPs as reporting entities integrating their operations within existing financial intelligence mechanisms. These provisions enable Kenyan regulators to demand transaction data and enforce robust controls that curtail illicit use of VAs, and violations attract administrative, civil, or criminal penalties.

d) The legislation also addresses the issuance of virtual assets through a formal approval process that requires disclosure of risks, token characteristics, and ongoing updates should the nature of the offering change. This mechanism includes a prohibition on natural persons promoting or issuing initial virtual asset offerings (IVOs) to the public, meaning these offerings must be organised by registered companies. Alongside safeguarding retail investors from dubious schemes, these obligations strengthen market transparency and reinforce consumer confidence.

8.3.2 Lessons and Guidance for Uganda from Kenya's Approach

Kenya's Bill offers a detailed model that Uganda can adapt to its own jurisdictional context by introducing a dedicated virtual asset regulatory framework. Under Uganda's existing laws, VAs or VASPs are not specifically addressed, so clear definitions and coverage are advisable to reduce legal uncertainty. The following considerations were noted to assist Uganda in creating an effective regulatory environment for VAs and VASPs;

a) Uganda could benefit from clearly defining "virtual assets" and "virtual asset service providers," following Kenya's approach. Clear definitions make it easier to determine which activities fall under regulation and which are exempt (such as closed-loop tokens or NFTs used for non-financial purposes).

b) Policymakers including MoFPED, MoJCA, Parliament of Uganda, among others could consider whether to adopt a single regulator model, whereby one body regulates all VASPs, or a multi-agency model based on the nature of each virtual asset (for example, payments under the Bank of Uganda and investments under the Capital Markets Authority). If a dual-regulator approach is chosen, Uganda could establish clear coordination mechanisms between regulatory authorities, similar to the Kenyan model involving the CMA and the CBK.

c) Kenya's Bill stipulates local incorporation or compliance certificates for foreign entities and mandates that VASPs meet strict fit-and-proper standards and have adequate capital before market entry. Such measures can assist Uganda ensure that only legitimate, financially sound operators enter its digital asset market. Uganda might also require that prospective licensees disclose their business

models, technology infrastructure, and risk management policies to allow regulators to assess their readiness.

d) The examination of directors, principal officers, and beneficial owners helps eliminate operators with links to criminal networks. Uganda's framework could provide for detailed due diligence, including background checks for criminal or insolvency records. This process reduces the likelihood of fraudulent enterprises exploiting the sector.

e) Uganda could adopt Kenya's emphasis on segregating client assets from the VASP's corporate funds. This requirement would reduce client exposure in the event of insolvency or mismanagement. For additional consumer protection, Uganda's framework might also require clear disclosures of risks, fees, and obligations that apply to both the VASP and the client.

f) Integrating virtual assets into Uganda's existing AML/CFT regime would make it difficult for illicit actors to abuse VAs. Kenya's Bill designates VASPs as reporting entities, obliging them to implement transaction monitoring, know-your-customer (KYC) protocols, and suspicious transaction reporting. This is similar to Uganda having included VASPs in the 2nd schedule of the AMLA Cap118 as accountable persons requiring them to comply with all AML/CFT obligations.

g) Uganda may consider requiring a formal approval process for entities wishing to issue new virtual assets. Kenya's Bill bars individuals from promoting offerings and requires the involvement of corporate entities, which must adhere to transparency and disclosure guidelines. This safeguard helps deter fraudulent tokens from saturating the market and provides investors with clear information.

h) Kenya's approach highlights the importance of enforcement powers, including administrative penalties, license revocations, and, where necessary, criminal liability. A similar set of options would allow Ugandan regulators to tailor sanctions to the severity of any violation. This helps deter wrongdoing, reassure investors, and maintain trust in the VA sector.

i) Regulators in Uganda would need continuous training to keep up with the rapidly evolving nature of the VA sector. Close collaboration with Kenyan regulators and other international standard-setting bodies could accelerate the process of knowledge-sharing. It would also help ensure that Uganda's framework remains relevant and effective as new token models or blockchain technologies emerge.

8.4 Benchmark on Namibia's Regulatory Framework for Virtual Assets and Virtual Asset Service Providers

The Namibia Virtual Assets Act, 2023 (Act No. 10 of 2023) represents a significant advancement in regulating the evolving virtual asset market in Namibia, as it aims to create a secure and robust framework that promotes innovation in digital finance while ensuring comprehensive consumer protection, preventing market abuses, and mitigating risks associated with money laundering and terrorism financing. The Act outlines the responsibilities and obligations of businesses providing virtual asset services and clarifies the extensive powers granted to the regulatory authority, thereby establishing a harmonised environment for both market participants and investors. The Act is applicable to all persons or entities that, by way of business, provide virtual asset services, which encompasses activities such as the exchange, transfer, custody, and safekeeping of digital representations of value using distributed ledger technology. It is important to note that the Act exclusively focuses on these digital representations, deliberately excluding traditional fiat currencies and regulated financial securities, thus ensuring that its provisions address only the innovative sectors of digital finance.

8.4.1 Legislative Overview

a) Under the Act, the Minister of Finance is entrusted with designating oneor more entities as the Regulatory Authority, and at present the Central Bank of Namibia has been given this designation. In addition to overseeing the licensing, supervision, and enforcement responsibilities defined by the Act, the Central Bank of Namibia has actively demonstrated its commitment to establishing a robust regulatory environment by issuing provisional licences to two entities, thereby ensuring that only qualified and properly regulated virtual asset service providers operate within the Namibian market.

b) The Regulatory Authority is endowed with extensive powers that include the review of applications, the granting of licences, and the supervision of ongoing operations to ascertain compliance with the Act, as well as the authority to conduct inspections and investigations when necessary. Furthermore, it is empowered to issue directives, formulate rules and guidelines, and impose administrative sanctions, while also collaborating with domestic and international regulatory counterparts; such a coordinated approach is critical for maintaining market integrity and safeguarding financial stability.

c) The Act mandates that any entity offering virtual asset services must obtain a licence, and applicants are required to provide extensive documentation demonstrating local incorporation, technological capability, robust internal controls, and a viable business plan. VASPs are expected to maintain a physical presence in Namibia, segregate client funds from their own operational finances, and implement rigorous record-keeping and cybersecurity measures. Moreover, the framework distinguishes between different classes of licences tailored to the specific services offered, such as asset custody, token issuance, or exchange operations, and it outlines strict requirements for conducting initial token offerings, including the preparation, publication, and continuous update of detailed prospectuses.

d) Furthermore, the Act imposes robust financial and governance standards by requiring minimum capital maintenance, the submission of annual audited financial statements, and strict criteria concerning changes in ownership or control.

e) The Regulatory Authority is empowered to conduct regular inspections, investigations, and audits to ensure VASPs' adherence to the Act, and it has the authority to suspend, cancel, or amend licences in cases of non-compliance. Stringent penalties including fines of up to **N$10,000,000 (UGX 2,003,430,198** and **imprisonment** for up to **10 years** are stipulated for infractions such as operating without a licence, misappropriating client assets, or failing to meet disclosure obligations, thereby ensuring that investor interests are rigorously protected and that market integrity is preserved.

8.5 Benchmark on others ESAAMLG Members with Existing Regulatory Frameworks for Virtual Asset Service Providers

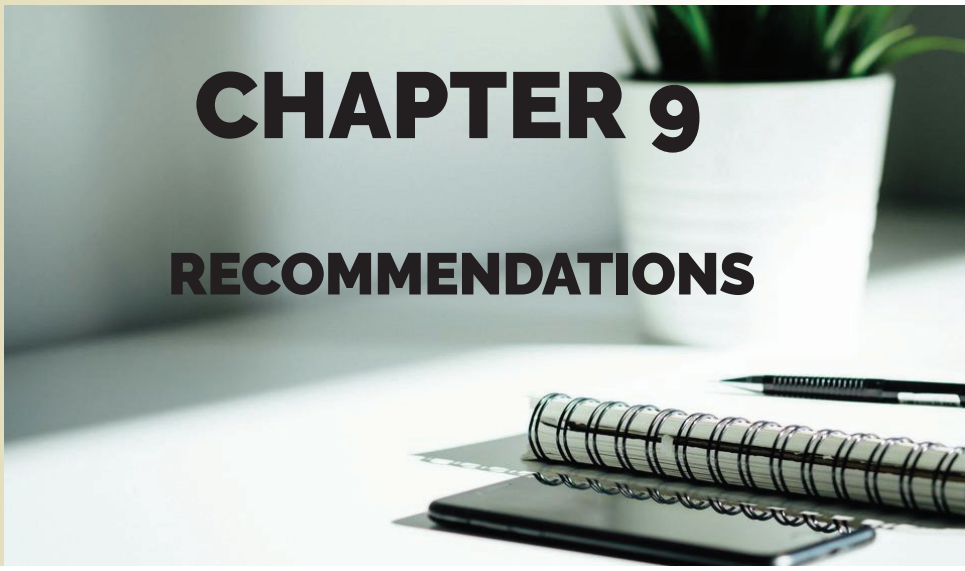
Several African nations have taken the lead in establishing formal regulatory frameworks for digital assets. These jurisdictions have enacted specific laws or amended existing financial regulations to bring Virtual Asset Service Providers (VASPs) under oversight. Their approaches typically include licensing regimes, compliance standards, investor protection mechanisms, and the enforcement of anti-money laundering and counter-terrorism financing (AML/CFT) measures. The table below shows the regulatory status of VASPs across majority of ESAAMLG member countries.

Country	Legislation (Existing / Proposed)	Primary Regulatory Authority/ Proposed Regulator	Status
Botswana	Virtual Assets Act, 2025	Non-Bank Financial Institutions Regulatory Authority (NBFIRA)	Active licensing regime; six VASP licences issued.
Namibia	Virtual Assets Act (Namibia VA Act), draft bill published Mar 2025	Bank of Namibia (BoN)	Draft framework under parliamentary review; two entities provisionally authorised pending full licences.
Mauritius	Virtual Asset and Initial Token Offering Services (VAITOS) Act, 2022; security tokens under the Securities Act	Financial Services Commission (FSC) / Bank of Mauritius (guidelines)	Operational licensing framework Six VASP licences Bankingaccess challenges persist for VASPs
South Africa	Financial Advisory and Intermediary Services (FAIS) Act – crypto assets classified as financial products (2022)	Financial Sector Conduct Authority (FSCA)	Crypto intermediaries require an FSP licence; 248 approvals have been obtained as of December 2024; phased processing continues.
Seychelles	Virtual Asset Service Providers (VASP) Act, 2024	Financial Services Authority (FSA)	A licensing regime has been established, with substance requirements in place; however, no licenses have been issued yet.

Ethiopia	Amendment to the National Bank of Ethiopia Establishment Proclamation for digitalasset oversight	National Bank of Ethiopia (NBE)	In June 2022, the National Bank of Ethiopia (NBE) warned the public against using digital assets. In August 2022, the Information Network Security Agency (INSA) issued a directive requiring all parties involved in cryptocurrency mining to register with them. In December 2024, Ethiopia passed a legal amendment allowing the National Bank of Ethiopia to regulate digital assets. However, it clarified that cryptocurrency would not be legalised as tender anytime soon.
Kenya	Draft Virtual Asset Service Providers Bill, gazetted 17 Mar 2025	Central Bank of Kenya (CBK) & Capital Markets Authority (CMA)	The National Treasury published a draft national policy and the Virtual Asset Service Providers (VASP) Bill, which was gazetted on 17 March 2025. The bill proposes licensing for VASPs and recognises digital assets and stablecoins as payment instruments. It identifies CBK and CMA as regulators. Despite historical warnings by CBK and CMA, both regulators now support the bill for sector oversight.
Rwanda	Draft Law on Virtual Asset Business (Mar 2025)	Capital Market Authority (CMA) in coordination with National Bank of Rwanda (BNR)	The Capital Market Authority (CMA) published a draft law on 'virtual assets business' currently under public consultation. The law proposes licensing for a wide range of activities such as trading, issuance, custody, matching platforms, wallets, escrow services, cross-border transfers, and tokenization.

Tanzania	No legislation on VASPs. Fintech Sandbox Regulations 2024 (under National Payment Systems Act)	Bank of Tanzania (BoT)	The Bank of Tanzania has historically cautioned the public that virtual currencies are not legal tender. In June 2021, the President urged the BoT to prepare for the adoption of digital assets. A High Court ruling clarified that digital asset trading is not illegal. In July 2024, Fintech Sandbox Regulations were enacted under the National Payment Systems Act. These allow unregulated products, including those using distributed ledger technology, to be tested over a 12-month period. Admissions began in January 2025.
Zambia	Draft BoZ Directive on Virtual Assets & Stablecoins (Mar 2025) under the National Payment Systems Act	Bank of Zambia (BoZ)	In March 2025, the Bank of Zambia (BoZ) issued a circular requesting feedback on draft directives under the National Payment Systems Act aimed at regulating virtual assets and stablecoins. The framework proposes licensing for governance, capital adequacy, cybersecurity, anti-money laundering (AML), and consumer protection. Only licensed entities are permitted to operate, and existing operators have six months to comply. BoZ expects to finalise the directive within 12 months. It has previously demonstrated openness to innovation through its regulatory sandbox, which has been run jointly with the Securities and Exchange Commission since 2021.

Angola	Law No. 3/24 (10 Apr 2024) – Prohibition of Cryptocurrency Mining & Virtual Assets	Banco Nacional de Angola (BNA)	Mining banned; broader virtualasset regulatory instruments anticipated.
Comoros	No dedicated crypto legislation (as of 2024)	Central Bank of Comoros (CBC)	CBC issues risk advisories; activity operates in a legal grey area.
Eswatini	National Payment System Act, 2023 (crypto regulations in draft)	Central Bank of Eswatini (CBE)	CBE drafting secondary regulations to operationalise Act; no VASP licences yet.
Lesotho	No specific VASP law; existing AML & Capital Market Regulations apply	Central Bank of Lesotho (CBL)	CBL states cryptocurrencies outside its regulatory scope; sector unregulated.
Malawi	None; RBM exploring CBDC options	Reserve Bank of Malawi (RBM)	RBM warns crypto not legal tender; no VASP framework.
Mozambique	Notice No. 4/GBM/2023 (rules for VASP registration)	Bank of Mozambique	Registration regime effective 14 Nov 2023; VASPs must register before operating.
South Sudan	No law	Bank of South Sudan	Central bank cautions public; crypto activity not explicitly banned but unregulated.
Zimbabwe	No law	Reserve Bank of Zimbabwe (RBZ) & Financial Intelligence Unit (FIU)	No licensing regime; the RBZ is reviewing policy options following the 2024 risk assessment.
Democratic Republic of Congo	Draft DigitalAsset Bill (target enactment end2025)	Banque Centrale du Congo (BCC)	The draft bill envisions BCC licensing of VASPs; currently, there is no dedicated framework.



CHAPTER 9

RECOMMENDATIONS

9.0 RECOMMENDATIONS

It is recommended that a comprehensive Regulatory Impact Assessment (RIA) on virtual assets be undertaken as a first step toward establishing an effective legal and regulatory framework. This process should be led by the Ministry of Justice and Constitutional Affairs in collaboration with the Ministry of Finance, Planning and Economic Development, and should actively involve all relevant public and private sector stakeholders. Broad-based consultations with the general public should also form part of this exercise to ensure inclusive input and transparency. The findings of the RIA will serve as the foundation for determining the most appropriate regulatory and policy actions to be pursued by the Government of Uganda.

To operationalize the outcomes of the proposed Regulatory Impact Assessment and address the key ML/TF risks identified in this study, a series of targeted recommendations have been developed in line with FATF Guidance. These recommendations are organized by thematic areas to provide a structured and actionable roadmap for strengthening Uganda's regulatory and institutional response to virtual assets. The first set of recommendations focuses on the legal and regulatory framework, beginning with the licensing and regulation of Virtual Asset Service Providers (VASPs), which is critical for establishing supervisory oversight and promoting responsible participation in the virtual asset ecosystem.

The recommendations below are structured by thematic areas; that is, regulatory framework, supervision and compliance, capacity building, technological infrastructure, and public awareness, to provide clear and practical steps for mitigation. The ultimate goal is to strengthen Uganda's resilience against VA-related ML/TF threats while enabling responsible innovation in the VA ecosystem. In light of the above, the following recommendations were made by the assessment team;

9.1 Legal and Regulatory Framework

9.1.1 Licensing and Regulation of VASPs

To effectively regulate VASPs, Uganda's policymakers should enact a consolidated Virtual Asset Service Providers (VASP) law that clearly defines virtual assets, VASPs, and permissible activities; mandates local incorporation or an authorized local presence; requires tiered licensing based on the nature, scale, and risk profile of the VASP; and includes robust fit-and proper tests for major shareholders and directors, minimum capital requirements, and strict client asset supervision. The framework should also allow regulators to bar criminals from owning or managing VASPs,demand robust risk management and cybersecurity standards, and ensure that licensed VASPs comply with prudential and market conduct rules as well as AML/CFT requirements, including periodic reporting to relevant authorities.

9.1.2 Risk-Based Approach to VASP Supervision

The law should be consistent with the AMLA Cap 118 in implementing proportional regulation for VASPs, with stricter requirements for high-risk services such as privacy focused VAs and decentralised finance (DeFi) platforms. Require VASPs to conduct comprehensive risk assessments and implement AML/CFT controls commensurate with their risk profiles. Additionally, the law should impose civil, administrative, and criminal penalties for unlicensed operations, non-compliance with AML/CFT laws, and fraudulent activities.

9.1.3 Secure Virtual Asset Restraining and Seizure Infrastructure

In anticipation of more frequent investigations and enforcement actions involving VAs, Uganda must establish a secure infrastructure for seizing, storing, and managing VAs that are confiscated. To implement this, law enforcement agencies should develop standard operating procedures for VA seizure beginning with a core element of creation of Government VA Custody Wallet essentially, an official wallet or set of wallets where seized VAs can be transferred and held under government control. International practice shows that agencies often pre-create storage wallets specifically for holding seized VA, and transfer confiscated funds into those wallets as soon as they obtain the private keys or the cooperation of exchanges. Uganda may consider the same, ensuring these government wallets are multi-signature to prevent single-point fraud, offline/hardware-based for security, and thoroughly documented for audit trails.

Additionally, competent authorities need protocols for managing and possibly liquidating seized assets, for example, deciding whether to convert VA to fiat immediately to avoid market volatility, or holding until court adjudication, among others. The transparency and security of this process are paramount, clear record-keeping of seizure amounts, secure handling of keys perhaps with court oversight, and periodic audits will build confidence that seized VAs are not misappropriated. Implementing these measures in Uganda would require technical guidelines for handling private keys, chain-of-custody procedures for digital evidence, and possibly partnerships with experienced custodians. Establishing clear asset forfeiture provisions for VAs aligned with FATF Recommendation 4 on confiscation and Recommendation 30 on law enforcement powers will ensure criminals cannot easily retain illicit VA profits and enable competent authorities to recover value from crime facilitated by VAs.

9.1.4 Alignment with FATF Recommendations 15 & 16

The proposed VA regulatory framework should align with FATF standards for VAs, particularly, the "Travel Rule" as per FATF Recommendation 16, which requires VASPs to obtain, verify, and share originator and beneficiary information for VA transfers. At present, no VASP in Uganda implements the travel rule, undermining cross-border transaction traceability. Regulations should mandate that VASPs include required sender/receiver data with VA transfers and respond to information requests from authorities, just as financial institutions do for domestic and international wire transfers. This will close the

gap where pseudonymous VA transfers could occur without oversight.

Additionally, FATF Recommendation 15 on new technologies calls for VASP licensing and risk assessment, measures that Uganda's framework should adopt fully. All VASPs should be required to perform risk-based CDD, keep records, and report suspicious transactions, with explicit coverage of peer-to-peer transactions where feasible. Although purely peer-to-peer VA transfers are not directly subject to AML/CFT laws under FATF standards authorities are encouraged to understand and mitigate those risks. Uganda's laws and guidelines should therefore also address P2P risks (for instance, by focusing on points where VAs convert to cash or by raising public awareness of P2P dangers. Aligning domestic regulations with FATF 15 and 16 will not only improve Uganda's compliance ratings but also strengthen international cooperation, since foreign VASPs will more readily share information if Uganda has equivalent rules in place.

All VASPs should be required to perform risk-based CDD, keep records, and report suspicious transactions, .

9.1.5 Regulatory Sandboxes for Innovation

To balance risk mitigation with fintech innovation, Uganda should introduce or enhance regulatory sandbox programs specifically for VA and blockchain-based services. A regulatory sandbox allows select innovators to pilot new products under the supervision of regulators, within controlled parameters. Uganda has already taken steps in this direction through BoU which launched a RegulatorySandbox in 2021, and in 2022 it indicated openness to admitting VA firms into the sandbox framework.[29]

This approach should be formalised and expanded to include key Government Ministries, Departments and Agencies to establish a VA Innovation Sandbox tracking mechanism. VASP start-ups and other VA-related service providers would apply to this sandbox to test their business models for a limited period, with exemptions from full licensing requirements but under controlled oversight. During sandbox testing, firms would have to implement basic consumer safeguards and AML/CFT controls, and regulators would closely monitor outcomes. This initiative would serve two purposes, encourage responsible innovation by giving entrepreneurs a way to work with regulators early, rather than operate unregulated, and also assist regulators learn about new VA technologies in a low-risk environment. Ultimately, successful sandbox tests can inform the development of permanent regulations, while any risks observed can be addressed before wider roll-out.

29 Bank of UG Accepts Crypto In Its Regulatory Sandbox | CIO Africa

9.1.6 AML/CFT Guidelines for VASPs

Uganda Competent Authorities responsible for the AML/CFT supervision should promptly issue detailed guidelines on AML/CFT compliance for VASPs. Although VASPs are recognized as accountable persons under the AMLA, many are unsure of how to effectively implement AML/CFT measures in practice. To address this, these guidelines should cover all key obligations, including among others customer due diligence tailored to VA services, ongoing transaction monitoring expectations including how to handle blockchain analytics and identify unusual on-chain patterns, reporting procedures for suspicious transactions or activity involving VAs, and record-keeping standards. The guidelines should emphasize a risk-based approach, acknowledging that not all VASPs present equal risk – for example, a large exchange with global operations may require more stringent controls than a small startup with limited services.

9.2 Capacity Building and Institutional Strengthening

Uganda should invest in comprehensive training programs for all stakeholders involved in VA oversight including policy makers to craft informed legislation, law enforcement agencies to investigate and prosecute VA-related crimes, financial regulators to supervise compliance, and members of the judiciary to adjudicate cases involving VAs. The risk assessment noted that Uganda has begun efforts in this area: for instance, FIA and other authorities participated in specialised training sessions on VA investigations provided by international bodies like the OECD, UNODC, and ESAAMLG. While these initiatives have enhanced foundational knowledge, the scope of training remains limited, especially on advanced technological aspects.

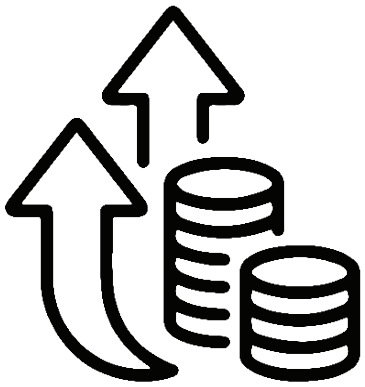
A structured capacity-building plan should be rolled out to cover among others blockchain technology basics, VA-tracing techniques, the legal framework for VAs, investigative best practices for tracking illegal transactions, prosecutorial strategies for VA cases, and international cooperation mechanisms. Law enforcement for instance Uganda Police Force, Inspectorate of Government, Uganda Revenue Authority, Uganda Wildlife Authority, Intelligence Services and Financial Intelligence Authority would benefit from hands-on workshops in using blockchain analytics tools and understanding VA seizure procedures. Judges and prosecutors might need seminars on handling VA evidence and interpreting new VA laws.

.

9.3 Public Financial Literacy Programs

As part of capacity building, it is important to enhance the knowledge of the general public regarding VAs. Many Ugandans may be attracted to investing in VAs or tokens due to promises of high returns, but lack an understanding of the associated risks, a gap often exploited by fraudsters running Ponzi schemes or false coin offerings.

Therefore, competent authorities led by financial regulators and consumer protection agencies should develop structured financial literacy and awareness programs focused on VAs. These programs can take the form of workshops, informational campaigns, inclusion in school curricula, or partnerships with media and fintech associations to spread key messages. Content should cover the basics of how VAs work, the legal status of VAs in Uganda, red flags of common scams, and tips for safe usage such as using licensed platforms once they are available, safeguarding one's wallet credentials, among others. These efforts should be significantly expanded into a nationwide campaign. Possible initiatives include: radio and TV infomercials in multiple languages; collaboration with local influencers or community leaders to disseminate information; setting up a public website or helpdesk for queries about VA investments; and leveraging International Consumer Protection Day or Financial Literacy weeks to highlight VA issues.



it is important to enhance the knowledge of the general public regarding VAs.

Hence Capacity building

9.4 Blockchain Analytics and Monitoring Tools

To effectively monitor the VA sector, Ugandan competent authorities must acquire modern blockchain analytics tools and establish technical infrastructure for monitoring VA transactions. Traditional financial surveillance systems are not sufficient for the pseudonymous and transnational nature of VAs as has been explained extensively in this risk assessment. Currently, FIA and law enforcement agencies in Uganda lack dedicated tools for analysing blockchain

"high priority recommendation is to procure specialised blockchain analysis software for use by the FIA, Uganda Police Force under the anti-cybercrime unit, and Uganda Revenue Authority for tax monitoring and compliance.

data, essential capabilities like wallet clustering, transaction graph analysis, and identification of mixers/tumblers are not available to analysts, investigators which leaves these agencies reliant on foreign assistance or basic methods, which are untenable as VA usage grows.

Therefore, a high priority recommendation is to procure specialised blockchain analysis software for use by the FIA, Uganda Police Force under the anti-cybercrime unit, and Uganda Revenue Authority for tax monitoring and compliance. These tools provide user-friendly interfaces to trace VA flows, identify suspicious addresses, and even flag transactions in real time based on risk scoring. Deploying such technology will significantly improve the ability to track and link illicit VA activities, as has been demonstrated in other jurisdictions where billions in illicit VA have been successfully traced and seized using blockchain analytics.

9.4.1 Real-Time VA Transaction Monitoring Tools

Beyond investigative tracing, competent authorities such as FIA should implement real-time monitoring and risk assessment systems for VA transactions. Blockchain Reactor Tools can be used not only for post -incident analysis but also for continuous monitoring of the blockchain for red-flag indicators to detect ML/TF linked to VAs. FIA should seek to integrate such solutions with its goAML analysis system to receive real-time feeds or notifications when a suspicious VA movement is detected such as transfer from a wallet known to be associated with darknet markets to a Uganda-linked wallet. This early intervention mechanism enables FIA to alert exchanges, RFSPs or other financial technology companies to freeze related funds, or warn law enforcement of an ongoing illicit operation. Additionally, regulators could use this real time technology to ensure VASPs themselves are following rules for example, checking if VASPs are blocking transactions with sanctioned addresses. As cross-border VA transactions are a major concern, having real-time risk assessment tools is particularly useful in detecting transactions that involve foreign high-risk exchanges or mixers before those funds dissipate beyond reach. This technological vigilance acts as a force multiplier for the relatively small enforcement teams on the ground.

9.5 Collaboration with Financial Sector Umbrella Bodies

Virtual Assets do not exist in isolation as they intersect with the broader financial system and economy. Therefore, it is important that Uganda's mainstream financial sector and other related sectors are aware of VA risks and involved in mitigation efforts. Financial sector regulators should collaborate with umbrella organisations such as the Uganda Bankers' Association, Financial Technology Service Providers Association of Uganda, Payments Service Providers Association, Forex Bureaus and Money Remitters Association, and other financial sector associations. Similarly, professional bodies for accountants, lawyers, and auditors can be engaged to sensitize their members on VA-related red flags since professionals may unknowingly facilitate VA transactions if they are not vigilant. The insurance sector, securities brokers, and other financial intermediaries should also be brought into the conversation, as they might encounter clients with VA holdings or businesses that deal in VA. Moreover, these traditional sectors can assist amplify public education for example, RFSPs could distribute pamphlets or SMS alerts about VA fraud to their customers. Collaboration across sectors ensures consistent messaging, policy application and also signals that the country as a whole, not just the government, is taking the challenges and opportunities of VAs seriously and responsibly.

9.6 Regional & International Cooperation

Uganda should enhance its cooperation with regional and international organisations to address ML/TF and prudential risks related to VAs and VASPs working closely with regional groups such as the East African Community and ESAAMLG to benefit from shared intelligence and harmonised regulatory approaches. In addition, collaborating with international law enforcement bodies like INTERPOL and financial intelligence networks such as the Egmont Group will improve information exchange on cross-border virtual asset transactions. Aligning with the Automatic Exchange of Information (AEOI) standards will help to ensure that tax and financial data are shared seamlessly, further reducing opportunities for money laundering and terrorist financing.

Furthermore, Uganda should engage with other key international regulatory bodies and forums. Participation in IOSCO meetings will allow Uganda to stay informed of global best practices, while collaboration with central banks and insurance regulators can help integrate monetary and financial oversight into its broader regulatory framework. Regional platforms like LATF and ARINSA offer tailored support in combating AML/CFT risks, and working with these organisations will strengthen Uganda's ability to monitor and control illicit activities in the VA sector.

,

IMPLEMENTATION TIMELINE AND PRIORITY ACTIONS

To effectively roll out the above recommendations, below is a suggested action plan table covering each recommendation, key action steps, responsible entities, and indicative timelines (short-term, medium-term, long-term).

Table 3 : Action Plan

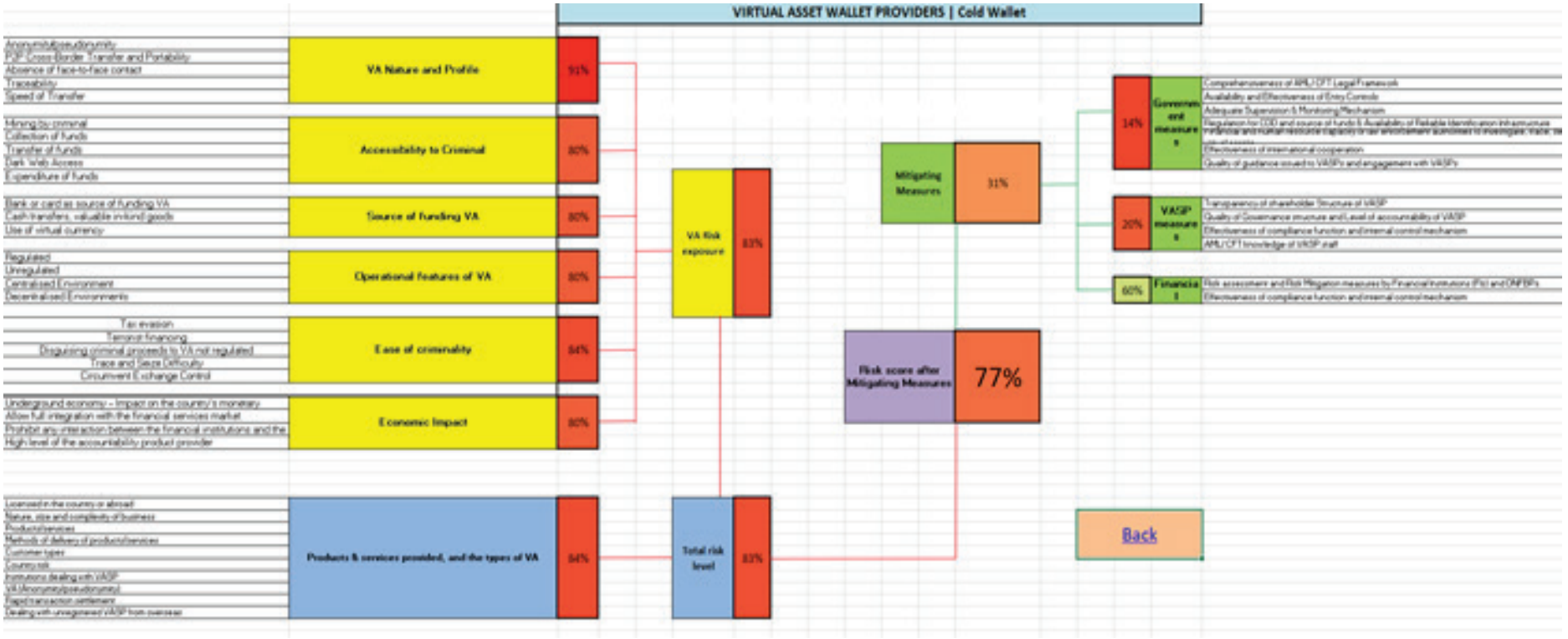
Recommendation	Key Action Steps	Responsible Entities	Timeline
9.1.1 Licensing & Regulation of VASPs	1. Draft and propose a VA and VASP law for Uganda providing for a comprehensive legal framework for all players and clear roles for competent authorities.	• Attorney General's Chambers • Ministry of Finance (MoFPED) • Parliament of Uganda • BoU, CMA,LGRB, IRA, UMRA, URSB, FIA,	
9.1.2 Risk-Based Approach to VASP Supervision	1. Align with AMLA Cap 118 for proportional regulation of high-risk VASPs such as privacy coins, DeFi). 2. Require VASPs to conduct risk assessments & enhanced AML/CFT controls. 3. Impose penalties for unlicensed operations & non-compliance.	• FIA (AML/CFT over sight) • BoU, CMA, LGRB, IRA, UMRA (sector-specific super vision) • Law Enforcement Agencies (LEAs)	
9.1.3 Secure VA Restraining & Seizure Infrastructure	1. Establish a government-managed multi-signature custody wallet for seized VAs. 2. Develop SOPs for seizure, secure storage, and liquidation of illicit VAs. 3. Enact asset forfeiture provisions aligned with FATF standards.	• LEAs (UPF, IG, URA,etc.) • Judiciary (oversight of seizure/legal processes) • Ministry of Internal Af fairs	

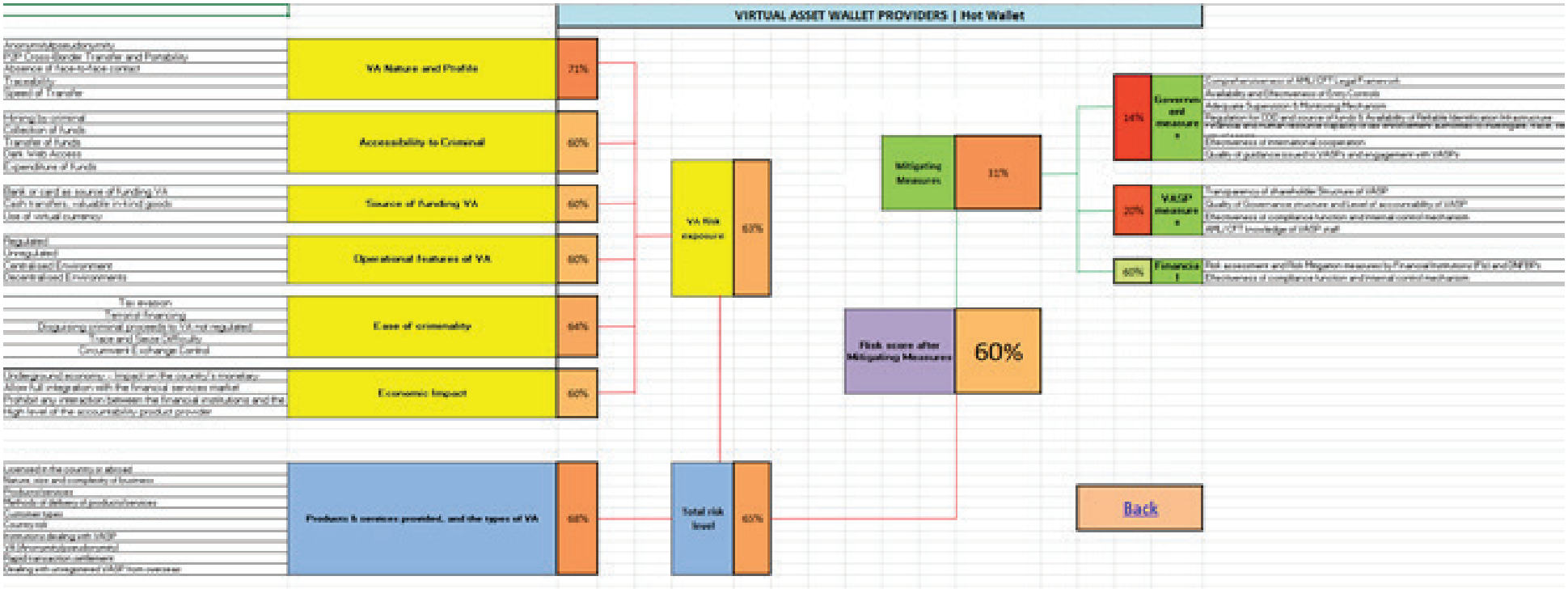
9.1.4 Alignment with FATF	1. Enforce "Travel Rule" for VASPs (collect/share originator & beneficiary info). 2. Require VASP licensing & risk-based CDD/STR reporting. 3. Address P2P transaction risks by focusing on cash-out points & public awareness.	• FIA (AML/CFT compliance) • BoU, CMA, LGRB, IRA, UMRA • VASPs	
9.1.5 Regulatory Sandboxes for Innovation	1. Formalize/regulate BoU's sandbox & expand it to VA and blockchain-based services. 2. Include key MDAs in sandbox tracking (MoFPED, ICT Ministry, NITA-U FIA). 3. Allow start-ups to pilot products under limited exemptions but strict safeguards.	• BoU (existing sand box host) • Ministry of Finance, ICT • FIA, CMA, URSB	
9.1.6 AML/CFT Guidelines for VASPs	1. FIA to issue detailed AML/CFT guidelines for VASPs (CDD, transaction monitoring, STR reporting). 2. Emphasise a risk based approach & use of blockchain analytics. 3. Provide practical examples of VA-specific red flags & record-keeping standards.	• FIA for lead guidance) • BoU, CMA, UMRA, IRA, LGRB for sector-specific input	

9.2 Capacity Building & Institutional Strengthening	1. Develop comprehensive training modules on blockchain, AML/CFT, VA-tracing, & seizure procedures. 2. Conduct regular workshops for policymakers, regulators, law enforcement, judiciary. 3. Incorporate advanced analytics and investigative tools into trainings.	• FIA, BoU, CMA, URSB UPF, Judiciary, URA, IG, Intelligence Services • Regional & international partners (OECD, UNODC, ESAAMLG)	
9.3 Public Financial Literacy Programs	1. Implement nationwide VA awareness campaigns on risks, scams, safe usage. 2. Collaborate with media, community leaders, schools for outreach. 3. Provide resources (hotlines, brochures, websites) on VA investment scams and consumer protection.	• BoU, FIA, CMA, Consumer Protection Agencies • Civil society, media houses, fintech associations	
9.4 Blockchain Analytics & Monitoring Tools	1. Procure blockchain analysis software (wallet clustering, risk scoring). 2. Train FIA, Police, URA in using these tools for investigations. 3. Establish procedures for exchanging analytics results among competent authorities.	• FIA (lead on analytics) • UPF (Anti-Cybercrime Unit), URA, other LEAs	

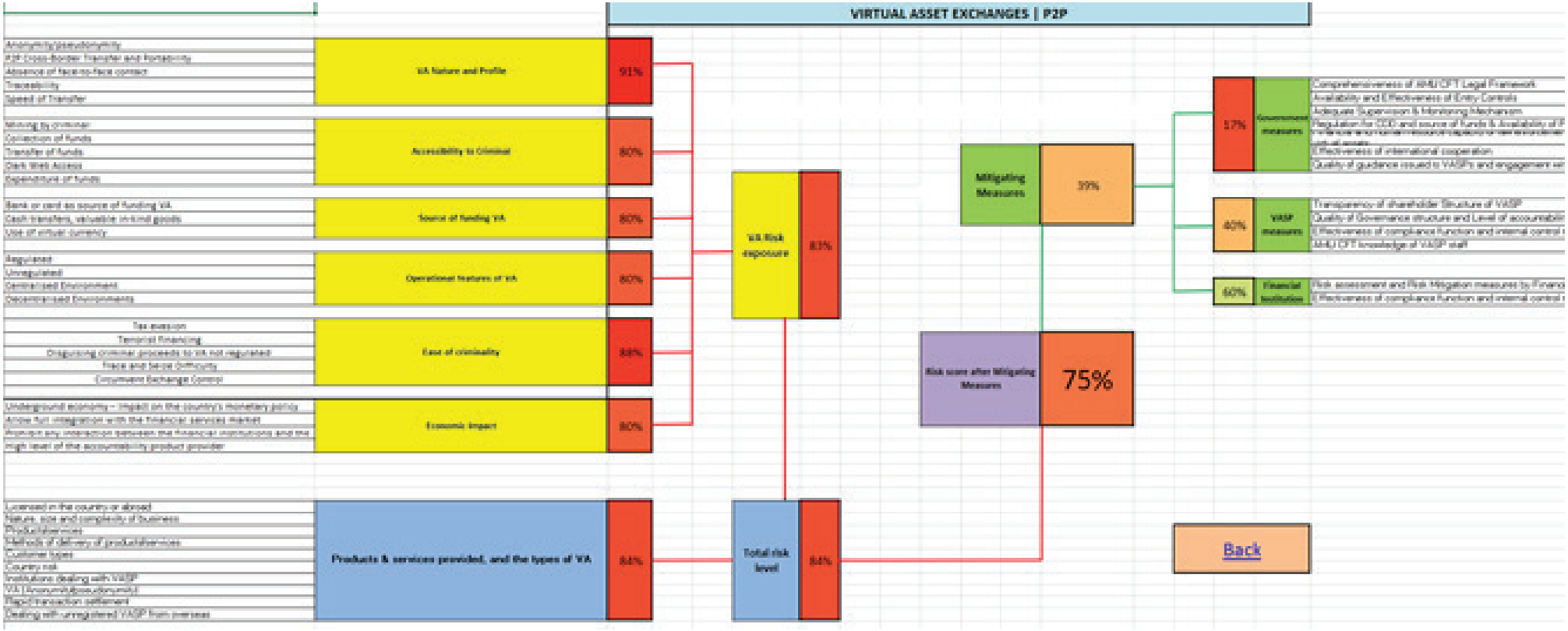
9.4.1 Real-Time VA Transaction Monitoring Tools	1. Integrate real-time blockchain monitoring with goAML or similar intelligence systems. 2. Use automated alerts for high-risk or sanctioned wallet addresses. 3. Enable early intervention (freezing or blocking suspicious assets).	• FIA (system integration) • BoU, UPF, VASPs (cooperation & data sharing)	
9.5 Collaboration with Financial Sector Umbrella Bodies	1. Engage Uganda Bankers' Association, Fintech associations, Forex bureaus, insurance associations to disseminate VA-related red flags. 2. Encourage mainstream FIs to incorporate VA risk checks in KYC/CDD processes. 3. Share best practices across sectors.	• BoU, FIA, CMA, URSB, IRA • Industry associations (UBA, FITSPA,PSP Association, Forex Bureaus & Money Remitters, Insurers)	
9.6 Regional & International Cooperation	1. Strengthen ties with ESAAMLG, ARINSA, Egmont Group for shared intelligence on VA ML/TF. 2. Participate in EAC/regional frameworks for harmonised VA regulations. 3. Sign MoUs with INTERPOL & other global bodies for cross-border VA crime enforcement.	• MoFPED, FIA, BoU • Ministry of Foreign Affairs • Regional & global partners	

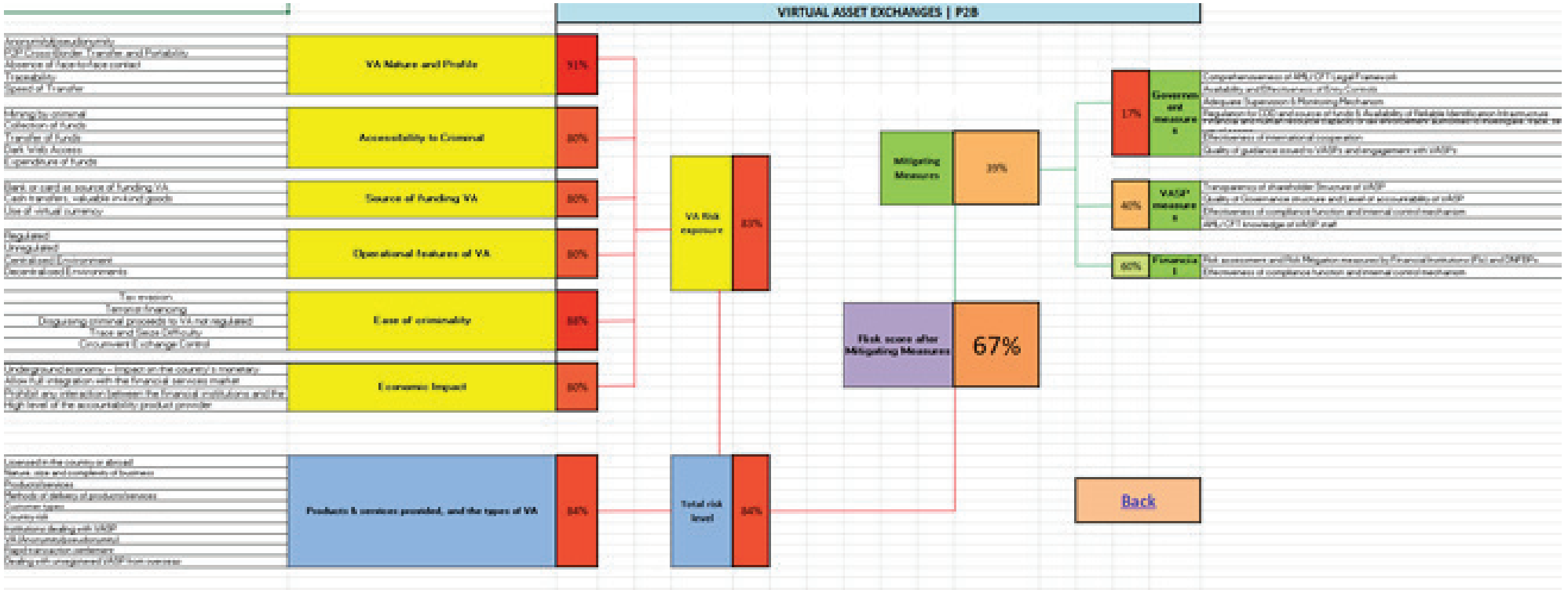
Integrate real-time blockchain monitoring

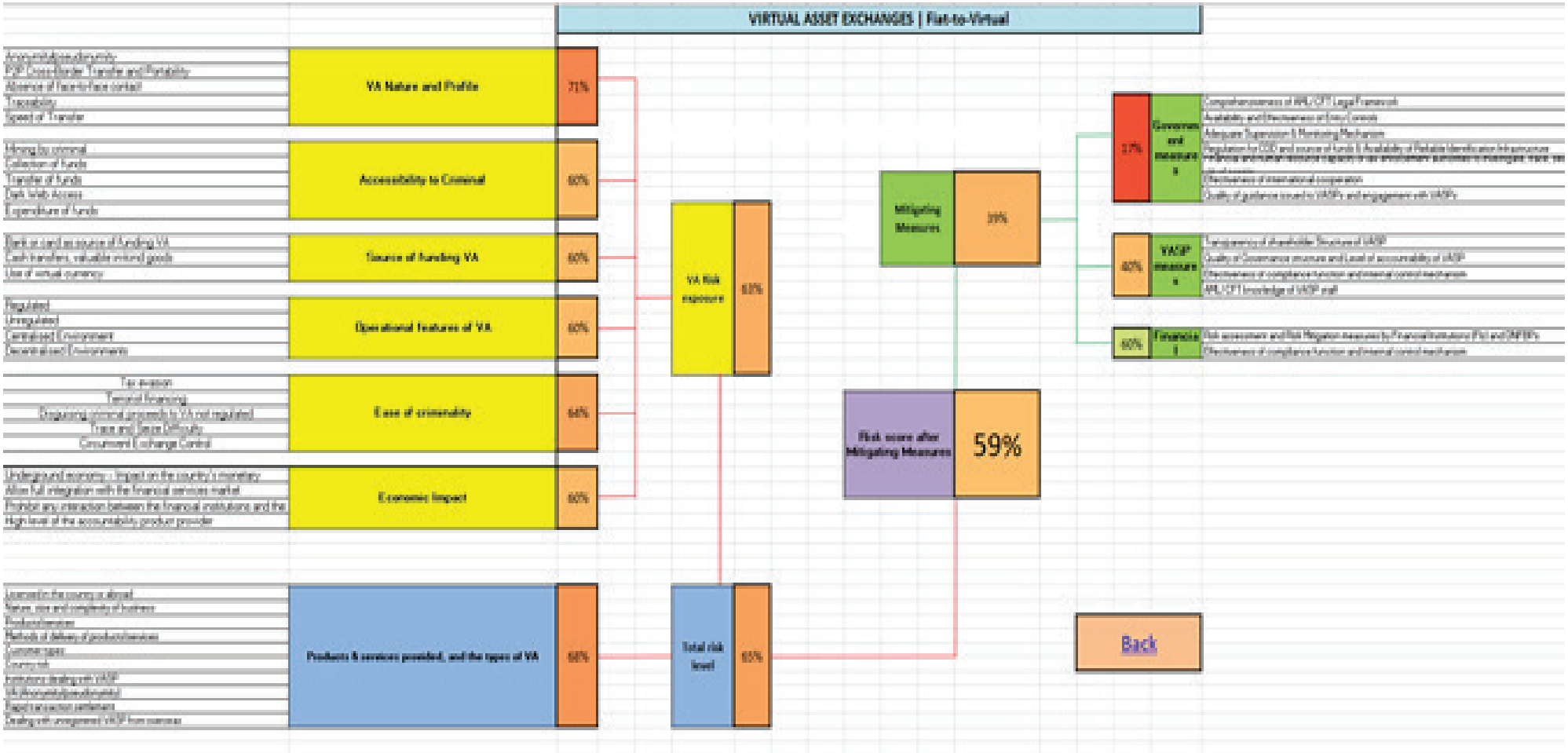

VIRTUAL ASSET WALLET PROVIDERS | Cold Wallet
VA Nature and Profile
91%
Accessibility to Criminal
80%
Source of funding VA
80%
Operational features of VA
80%
Ease of criminality
84%
Economic Impact
80%
Products & services provided, and the types of VA
84%
VA Risk exposure
83%
Total risk level
83%
Mitigating Measures
31%
Risk score after Mitigating Measures
77%
14%
Governance measures
20%
VASP measures
60%
Financial
Back

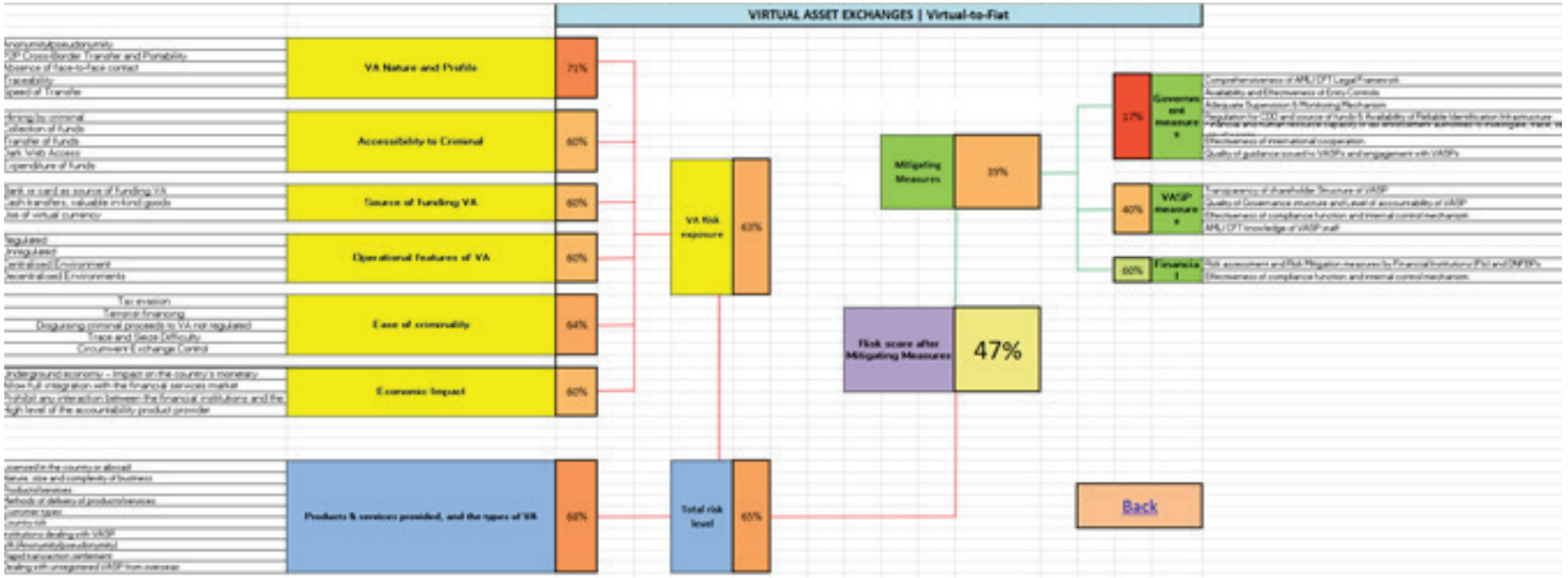

VIRTUAL ASSET WALLET PROVIDERS | Hot Wallet
VA Nature and Profile
71%
Accessibility to Criminal
60%
Source of funding VA
60%
Operational features of VA
60%
Ease of criminality
64%
Economic Impact
60%
Products & services provided, and the types of VA
68%
VA Risk exposure
63%
Total risk level
65%
Mitigating Measures
31%
Risk score after Mitigating Measures
60%
14%
Governance measures
20%
VASP measures
60%
Financial
Back

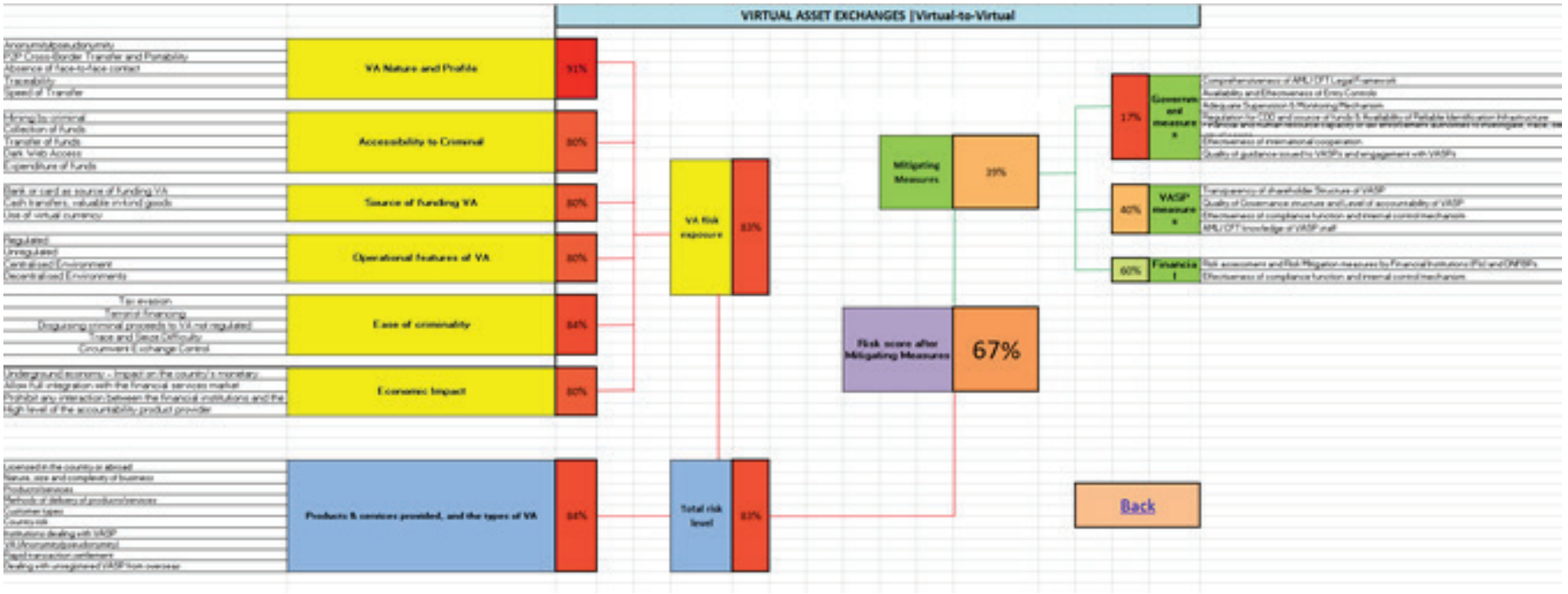
Annexures

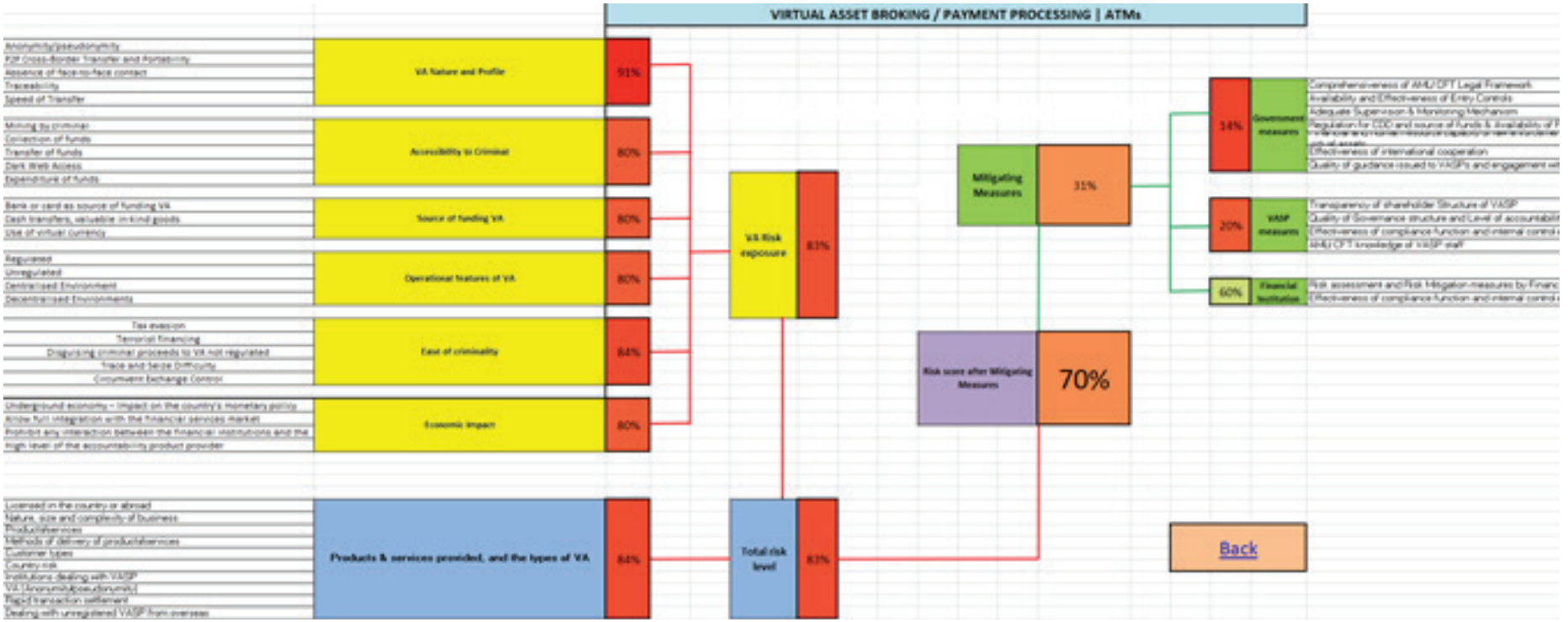

VIRTUAL ASSET EXCHANGES | P2P
VA Nature and Profile
91%
Accessibility to Criminal
80%
Source of funding VA
80%
Operational features of VA
80%
Ease of criminality
88%
Economic impact
80%
Products & services provided, and the types of VA
84%
VA Risk exposure
83%
Total risk level
84%
Mitigating Measures
39%
Risk score after Mitigating Measures
75%
17%
40%
60%
Back

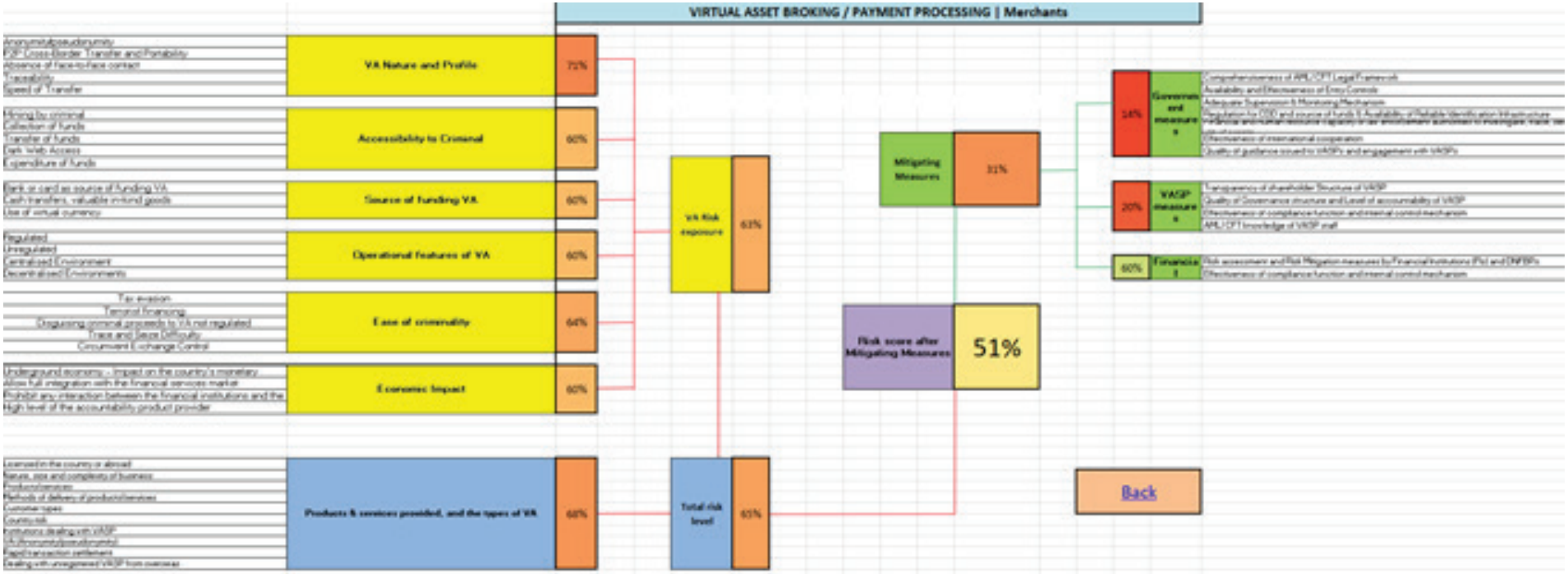

VIRTUAL ASSET EXCHANGES | P2B
VA Nature and Profile
91%
Accessability to Criminal
80%
Source of Funding VA
80%
Operational features of VA
80%
Ease of criminality
80%
Economic Impact
80%
Products & services provided, and the types of VA
84%
VA Risk exposure
83%
Total risk level
84%
Mitigating Measures
39%
Risk score after Mitigating Measures
67%
17%
Governance and measure
40%
VASP measure
60%
Finance
Back

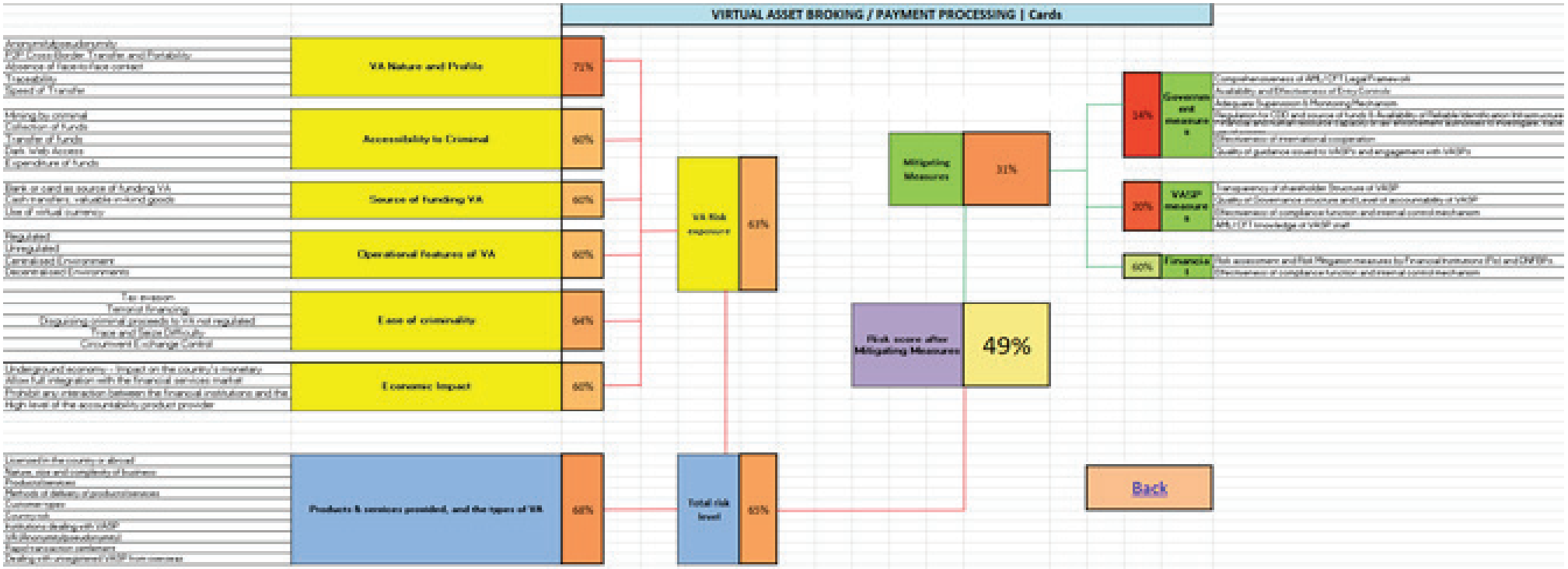

VIRTUAL ASSET EXCHANGES | Fiat-to-Virtual
VA Nature and Profile
71%
Accessibility to Criminal
60%
Source of funding VA
60%
Operational features of VA
60%
Ease of criminality
64%
Economic Impact
60%
Products & services provided, and the types of VA
68%
VA Risk exposure
63%
Total risk level
65%
Mitigating Measures
39%
Risk score after Mitigating Measures
59%
17%
Governance and measures
40%
VASP measures
60%
Financial
Back

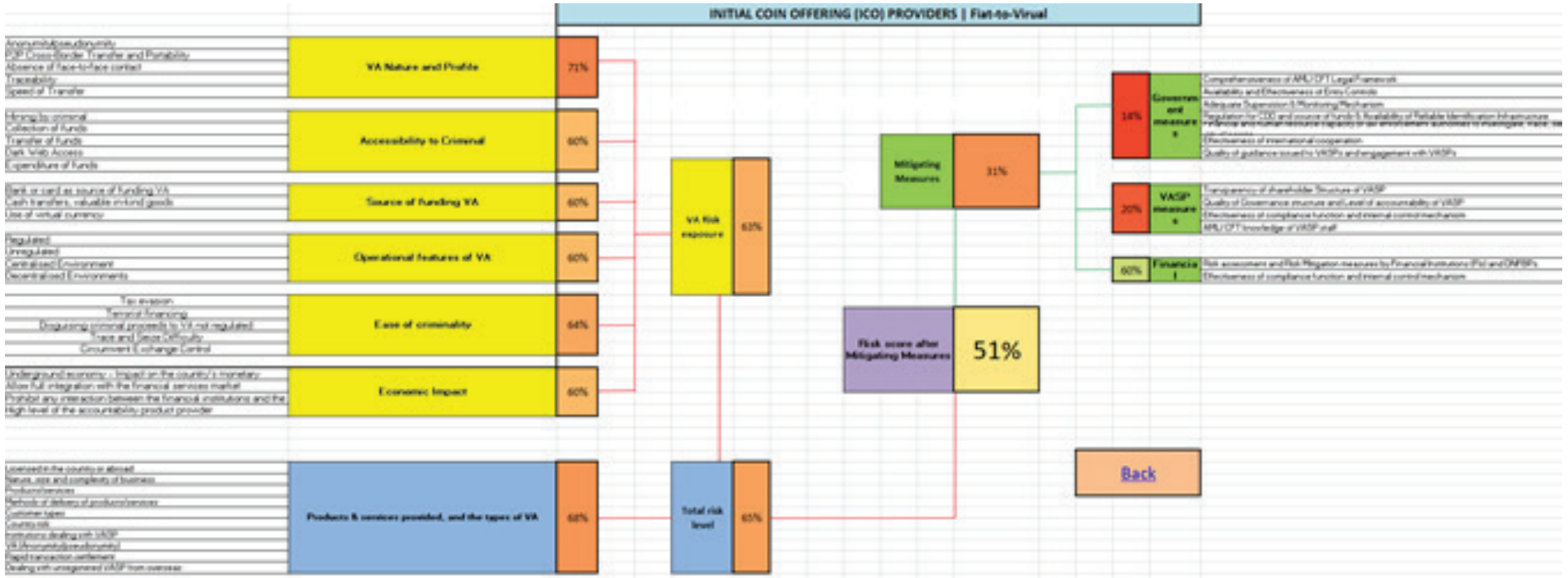

VIRTUAL ASSET EXCHANGES | Virtual-to-Fiat
VA Nature and Profile
71%
Accessibility to Criminal
60%
Source of funding VA
60%
Operational features of VA
60%
Ease of criminality
64%
Economic Impact
60%
Products & services provided, and the types of VA
68%
VA Risk exposure
63%
Total risk level
65%
Mitigating Measures
39%
Risk score after Mitigating Measures
47%
17%
40%
60%
Back

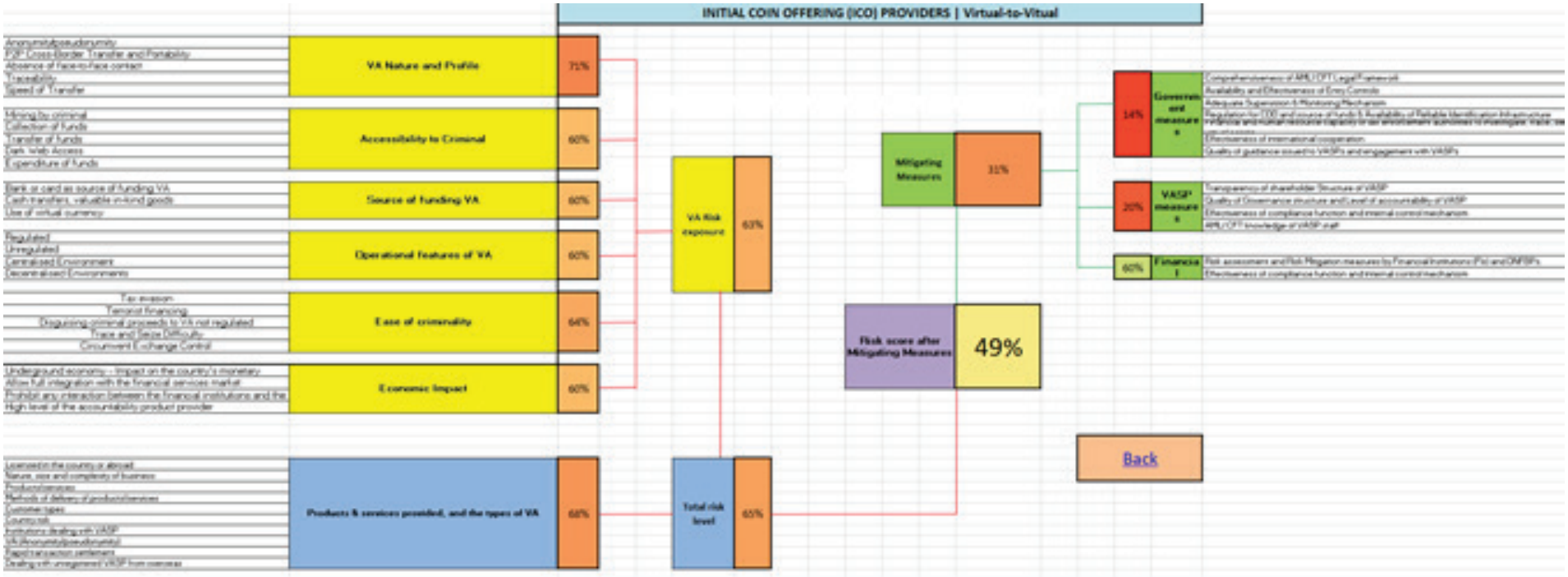

VIRTUAL ASSET EXCHANGES |Virtual-to-Virtual
VA Nature and Profile
91%
Accessibility to Criminal
80%
Source of funding VA
80%
Operational features of VA
80%
Ease of criminality
84%
Economic Impact
80%
Products & services provided, and the types of VA
84%
VA Risk exposure
83%
Total risk level
83%
Mitigating Measures
39%
Risk score after Mitigating Measures
67%
17%
40%
60%
Back

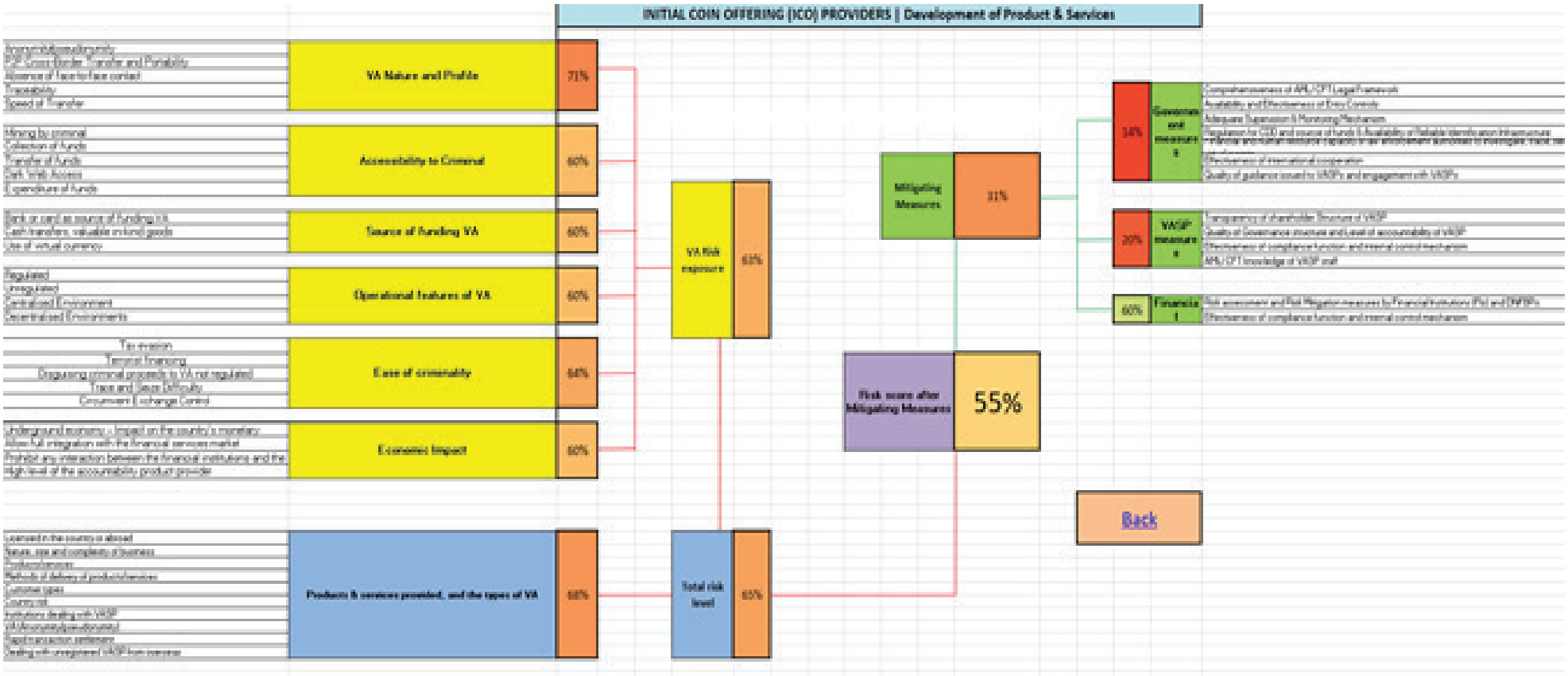

VIRTUAL ASSET BROKING / PAYMENT PROCESSING | ATMs
Anonymity/pseudonymity
P2P Cross-Border Transfer and Portability
Absence of face-to-face contact
Traceability
Speed of Transfer
VA Nature and Profile
91%
Mining by criminal
Collection of funds
Transfer of funds
Dark Web Access
Expenditure of funds
Accessibility to Criminal
80%
Bank or card as source of funding VA
Cash transfers, valuable in-kind goods
Use of virtual currency
Source of funding VA
80%
Regulated
Unregulated
Centralized Environment
Decentralized Environments
Operational features of VA
80%
Tax evasion
Terrorist financing
Disguising criminal proceeds to VA not regulated
Trace and Seize Difficulty
Circumvent Exchange Control
Ease of criminality
84%
Underground economy – Impact on the country's monetary policy
Allow full integration with the financial services market
Prohibit any interaction between the financial institutions and the
High level of the accountability product provider
Economic Impact
80%
VA Risk exposure
83%
Licensed in the country or abroad
Nature, size and complexity of business
Product/services
Methods of delivery of product/services
Customer types
Country risk
Institutions dealing with VASP
VA (Anonymity/pseudonymity)
Rapid transaction settlement
Dealing with unregistered VASP from overseas
Products & services provided, and the types of VA
84%
Total risk level
83%
Mitigating Measures
31%
Risk score after Mitigating Measures
70%
14%
Government measures
Comprehensiveness of AML/CFT Legal Framework
Availability and Effectiveness of Entry Controls
Adequate Supervision & Monitoring Mechanism
Effectiveness of international cooperation
20%
VASP measures
Transparency of shareholder Structure of VASP
Quality of Governance structure and Level of accountabili
Effectiveness of compliance function and internal contro
AML/CFT knowledge of VASP staff
60%
Financial Institution
Risk assessment and Risk Mitigation measures by Financ
Effectiveness of compliance function and internal contro
Back

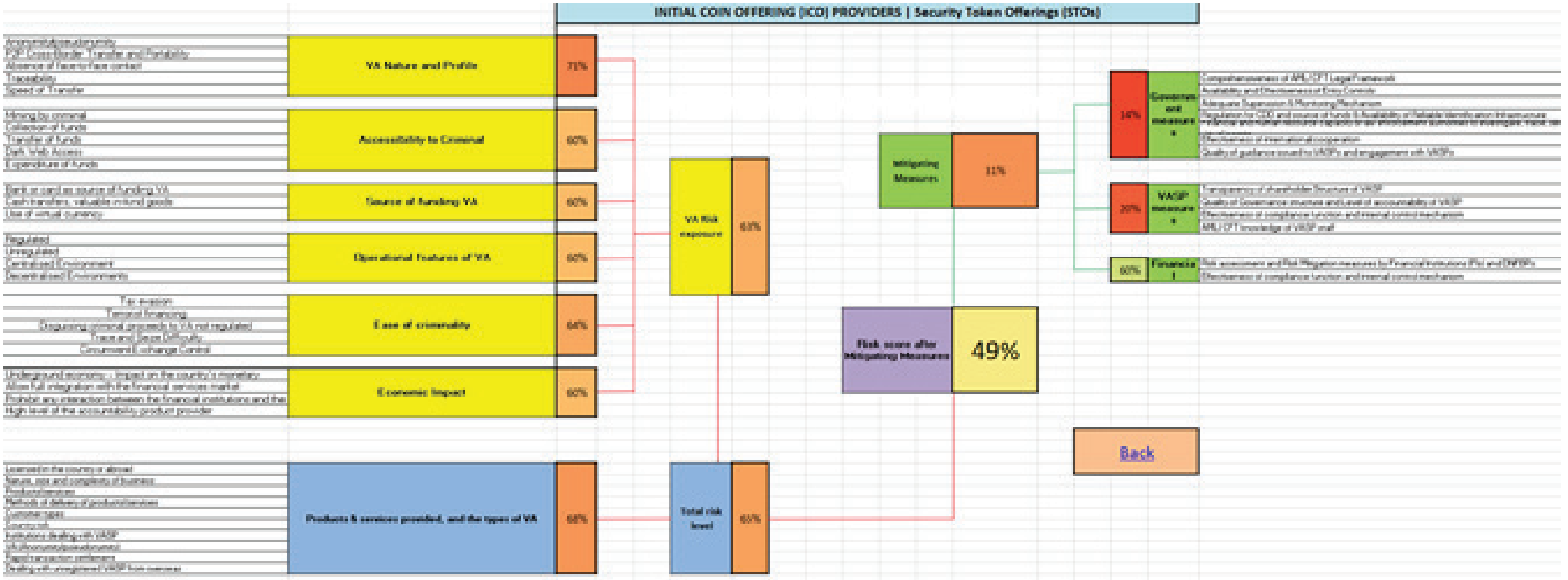

VIRTUAL ASSET BROKING / PAYMENT PROCESSING | Merchants
Anonymity/pseudonymity
P2P Cross-Border Transfer and Portability
Absence of face-to-face contact
Traceability
Speed of Transfer
VA Nature and Profile
72%
Mining by criminal
Collection of funds
Transfer of funds
Dark Web Access
Expenditure of funds
Accessibility to Criminal
60%
Bank or card as source of funding VA
Cash transfers, valuable in-kind goods
Use of virtual currency
Source of funding VA
60%
Regulated
Unregulated
Centralized Environment
Decentralized Environments
Operational features of VA
60%
Tax evasion
Terrorist financing
Disguising criminal proceeds to VA not regulated
Trace and Seize Difficulty
Circumvent Exchange Control
Ease of criminality
64%
Underground economy – Impact on the country's monetary
Allow full integration with the financial services market
Prohibit any interaction between the financial institutions and the
High level of the accountability product provider
Economic Impact
60%
VA Risk exposure
63%
Licensed in the country or abroad
Nature, size and complexity of business
Product/services
Methods of delivery of product/services
Customer types
Country risk
Institutions dealing with VASP
VA (Anonymity/pseudonymity)
Rapid transaction settlement
Dealing with unregistered VASP from overseas
Products & services provided, and the types of VA
68%
Total risk level
63%
Mitigating Measures
31%
Risk score after Mitigating Measures
51%
14%
Government measures
Comprehensiveness of AML/CFT Legal Framework
Availability and Effectiveness of Entry Controls
Adequate Supervision & Monitoring Mechanism
Effectiveness of international cooperation
Quality of guidance issued to VASPs and engagement with VASPs
20%
VASP measures
Transparency of shareholder Structure of VASP
Quality of Governance structure and Level of accountability of VASP
Effectiveness of compliance function and internal control mechanism
AML/CFT knowledge of VASP staff
60%
Financial
Risk assessment and Risk Mitigation measures by Financial Institutions (FIs) and DNFBPs
Effectiveness of compliance function and internal control mechanism
Back

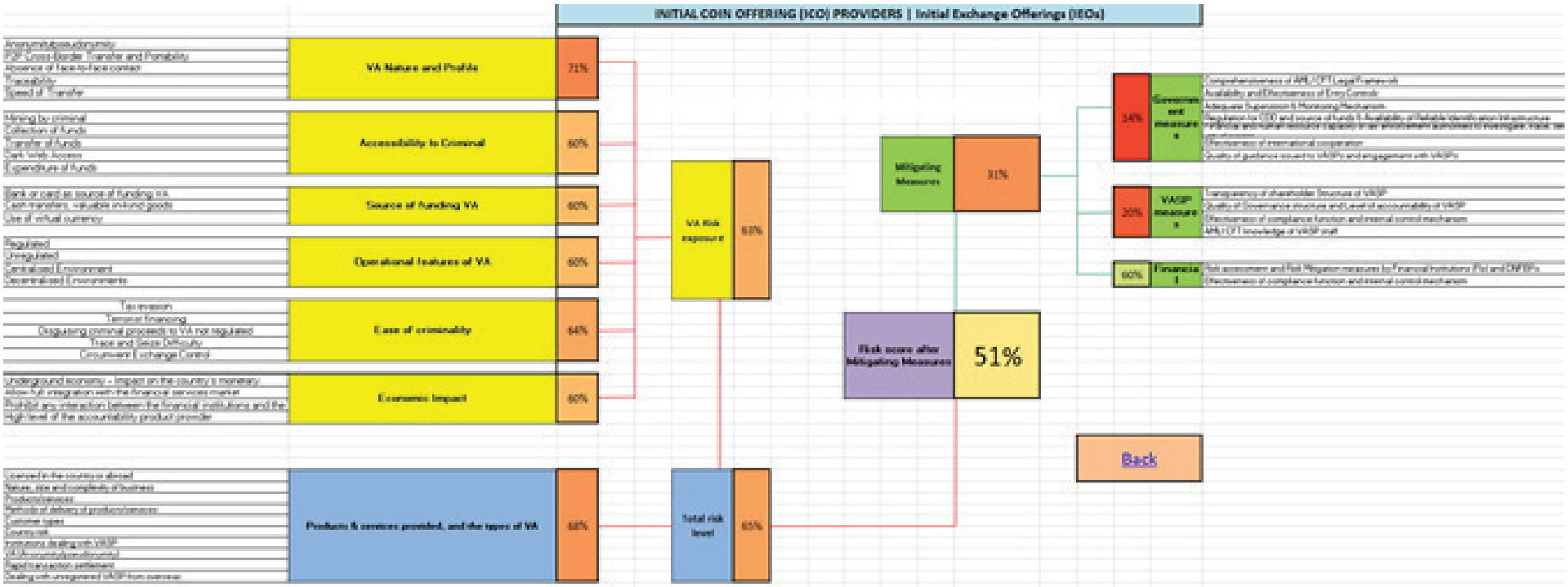

VIRTUAL ASSET BROKING / PAYMENT PROCESSING | Cards
VA Nature and Profile
72%
Accessibility to Criminal
60%
Source of funding VA
60%
Operational features of VA
60%
Ease of criminality
64%
Economic Impact
60%
Products & services provided, and the types of VA
68%
VA Risk exposure
63%
Total risk level
65%
Mitigating Measures
31%
Risk score after Mitigating Measures
49%
34%
Governance and measures
20%
VASP measures
60%
Finances
Back

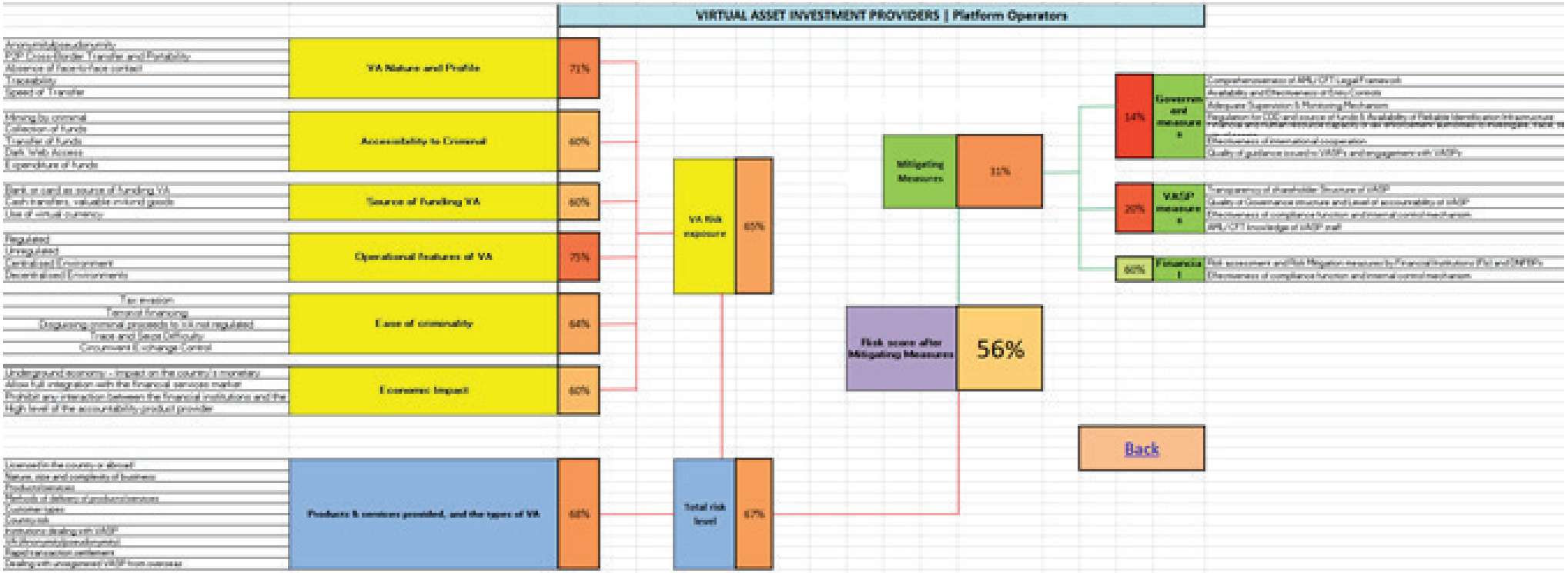

INITIAL COIN OFFERING (ICO) PROVIDERS | Fiat-to-Virtual
Anonymity/pseudonymity
P2P Cross-Border Transfer and Portability
Absence of face-to-face contact
Traceability
Speed of Transfer
VA Nature and Profile
71%
Mixing by criminal
Collection of funds
Transfer of funds
Dark Web Access
Expenditure of funds
Accessibility to Criminal
60%
Bank or card as source of funding VA
Cash transfers, valuable in-kind goods
Use of virtual currency
Source of funding VA
60%
Regulated
Unregulated
Centralised Environment
Decentralised Environments
Operational features of VA
60%
Tax evasion
Terrorist financing
Disguising criminal proceeds by VA not regulated
Trace and Seize Difficulty
Circumvent Exchange Control
Ease of criminality
64%
Underground economy - Impact on the country's monetary
Allow full integration with the financial services market
Prohibit any interaction between the financial institutions and the
High level of the accountability product provider
Economic Impact
60%
Licensed in the country or abroad
Nature, size and complexity of business
Products/services
Methods of delivery of products/services
Customer types
country risk
Institutions dealing with VASP
VA (Anonymity/pseudonymity)
Rapid transaction settlement
Dealing with unregistered VASP from overseas
Products & services provided, and the types of VA
68%
VA Risk exposure
63%
Total risk level
65%
Mitigating Measures
31%
Risk score after Mitigating Measures
51%
14%
Governance and measures
Comprehensiveness of AML/CFT Legal Framework
Availability and Effectiveness of Entry Controls
Adequate Supervision & Monitoring Mechanism
Regulation for CDD and source of funds & Availability of Reliable Identification Infrastructure
Effectiveness of international cooperation
Quality of guidance issued to VASPs and engagement with VASPs
20%
VASP measures
Transparency of shareholder Structure of VASP
Quality of Governance structure and Level of accountability of VASP
Effectiveness of compliance function and internal control mechanism
AML/CFT knowledge of VASP staff
60%
Financial
Risk assessment and Risk Mitigation measures by Financial Institutions (FIs) and DNFBPs
Effectiveness of compliance function and internal control mechanism
Back

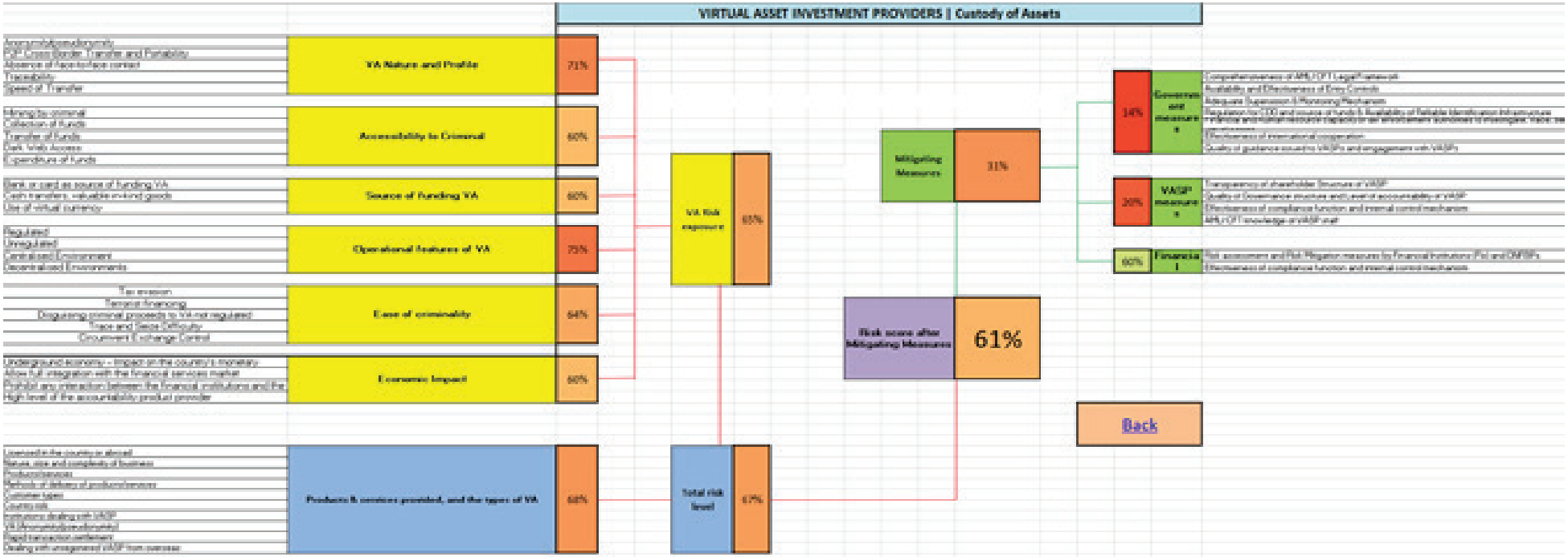

INITIAL COIN OFFERING (ICO) PROVIDERS | Virtual-to-Virtual
Anonymity/pseudonymity
P2P Cross-Border Transfer and Portability
Absence of face-to-face contact
Traceability
Speed of Transfer
VA Nature and Profile
71%
Mixing by criminal
Collection of funds
Transfer of funds
Dark Web Access
Expenditure of funds
Accessibility to Criminal
60%
Bank or card as source of funding VA
Cash transfers, valuable in-kind goods
Use of virtual currency
Source of funding VA
60%
Regulated
Unregulated
Centralised Environment
Decentralised Environments
Operational features of VA
60%
Tax evasion
Terrorist financing
Disguising criminal proceeds by VA not regulated
Trace and Seize Difficulty
Circumvent Exchange Control
Ease of criminality
64%
Underground economy - Impact on the country's monetary
Allow full integration with the financial services market
Prohibit any interaction between the financial institutions and the
High level of the accountability product provider
Economic Impact
60%
Licensed in the country or abroad
Nature, size and complexity of business
Products/services
Methods of delivery of products/services
Customer types
country risk
Institutions dealing with VASP
VA (Anonymity/pseudonymity)
Rapid transaction settlement
Dealing with unregistered VASP from overseas
Products & services provided, and the types of VA
68%
VA Risk exposure
63%
Total risk level
65%
Mitigating Measures
31%
Risk score after Mitigating Measures
49%
14%
Governance and measures
Comprehensiveness of AML/CFT Legal Framework
Availability and Effectiveness of Entry Controls
Adequate Supervision & Monitoring Mechanism
Regulation for CDD and source of funds & Availability of Reliable Identification Infrastructure
Effectiveness of international cooperation
Quality of guidance issued to VASPs and engagement with VASPs
20%
VASP measures
Transparency of shareholder Structure of VASP
Quality of Governance structure and Level of accountability of VASP
Effectiveness of compliance function and internal control mechanism
AML/CFT knowledge of VASP staff
60%
Financial
Risk assessment and Risk Mitigation measures by Financial Institutions (FIs) and DNFBPs
Effectiveness of compliance function and internal control mechanism
Back

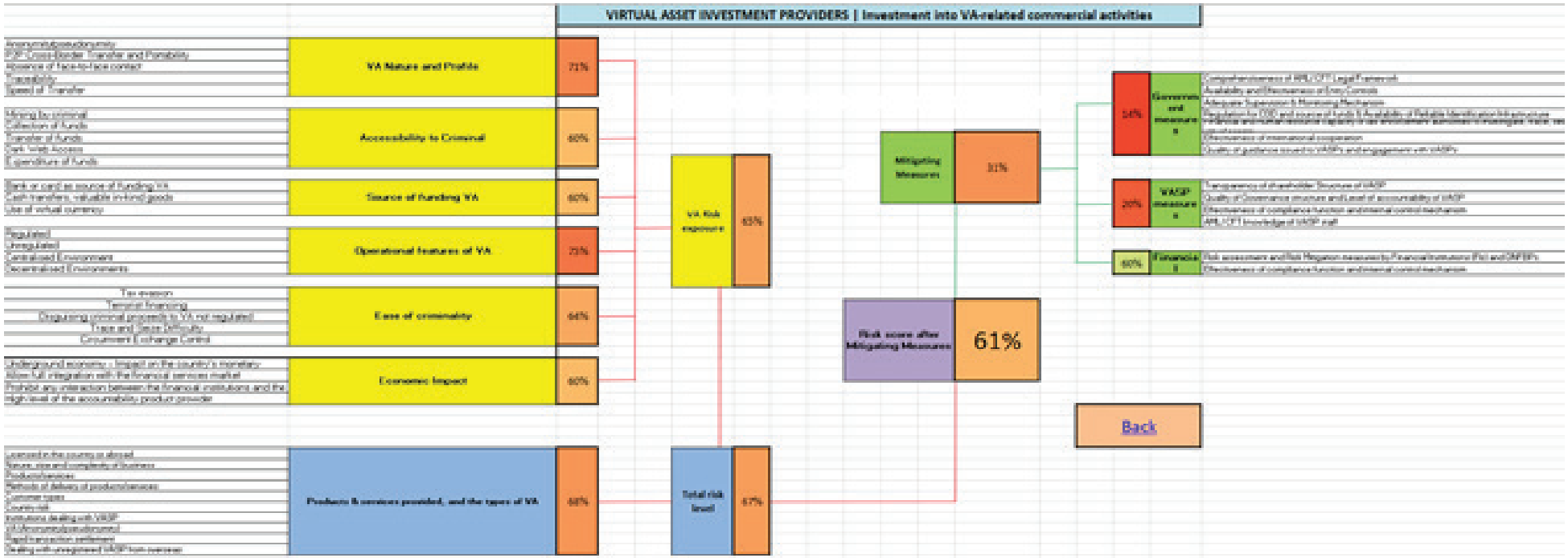

INITIAL COIN OFFERING (ICO) PROVIDERS | Development of Product & Services
VA Nature and Profile
71%
Accessibility to Criminal
60%
Source of funding VA
60%
Operational features of VA
60%
Ease of criminality
64%
Economic Impact
60%
Products & services provided, and the types of VA
68%
VA Risk exposure
63%
Total risk level
65%
Mitigating Measures
31%
Risk score after Mitigating Measures
55%
14%
Governance and measures
20%
VASP measures
60%
Finance
Back

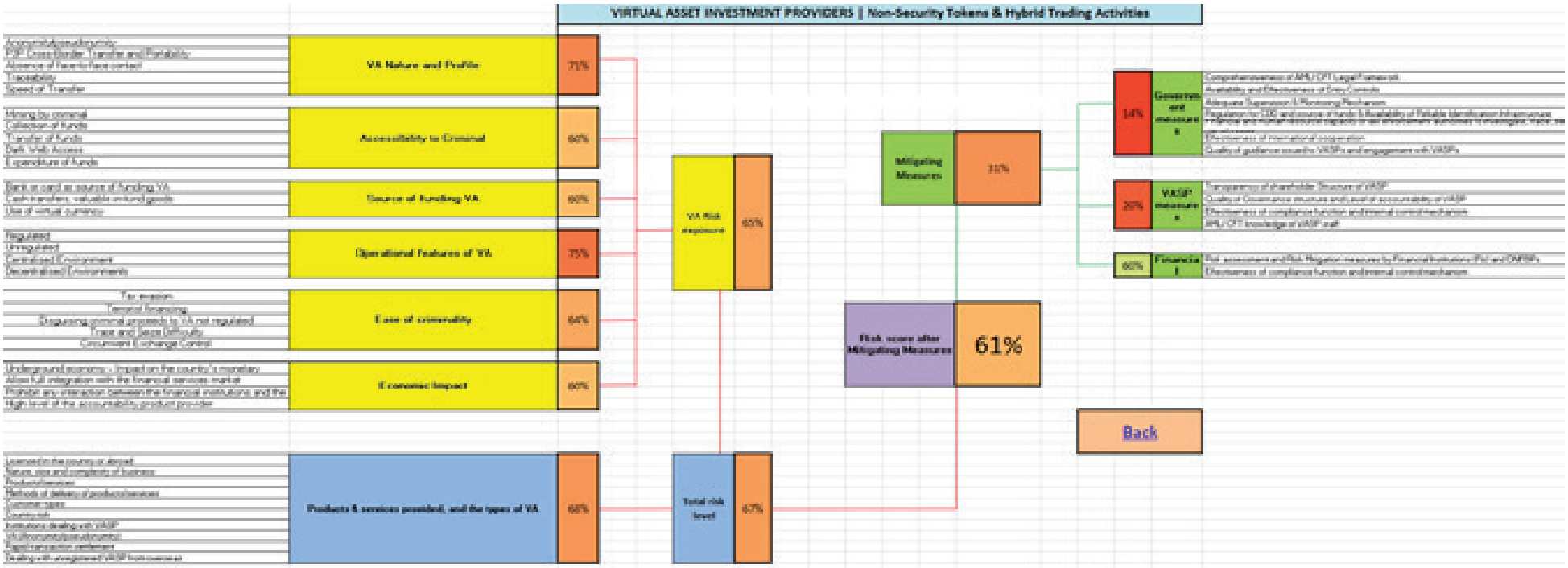

INITIAL COIN OFFERING (ICO) PROVIDERS | Security Token Offerings (STOs)
VA Nature and Profile
71%
Accessibility to Criminal
60%
Source of funding VA
60%
Operational features of VA
60%
Ease of criminality
64%
Economic Impact
60%
Products & services provided, and the types of VA
68%
VA Risk exposure
63%
Total risk level
65%
Mitigating Measures
31%
14%
Governance and measures
20%
VASP measures
60%
Financial
Risk score after Mitigating Measures
49%
Back

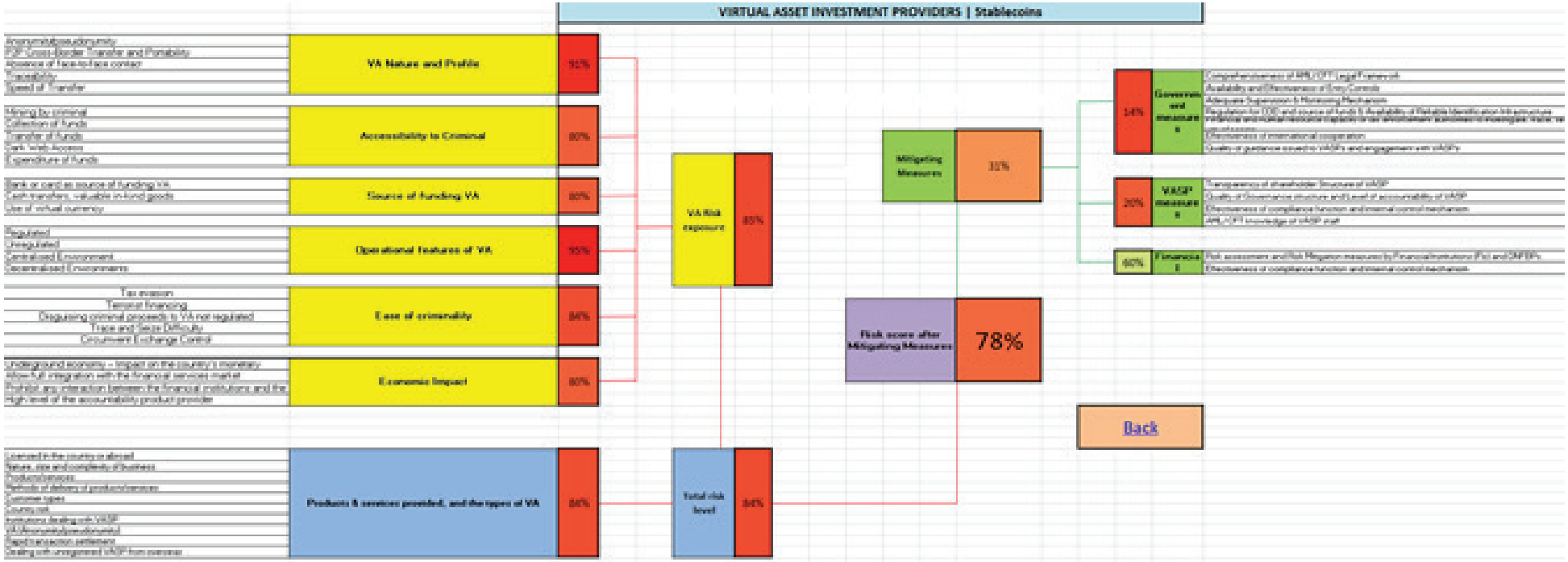

INITIAL COIN OFFERING (ICO) PROVIDERS | Initial Exchange Offerings (IEOs)
VA Nature and Profile
71%
Accessibility to Criminal
60%
Source of funding VA
60%
Operational features of VA
60%
Ease of criminality
64%
Economic Impact
60%
Products & services provided, and the types of VA
68%
VA Risk exposure
63%
Total risk level
65%
Mitigating Measures
31%
14%
Governance and measures
20%
VASP measures
60%
Financial
Risk score after Mitigating Measures
51%
Back

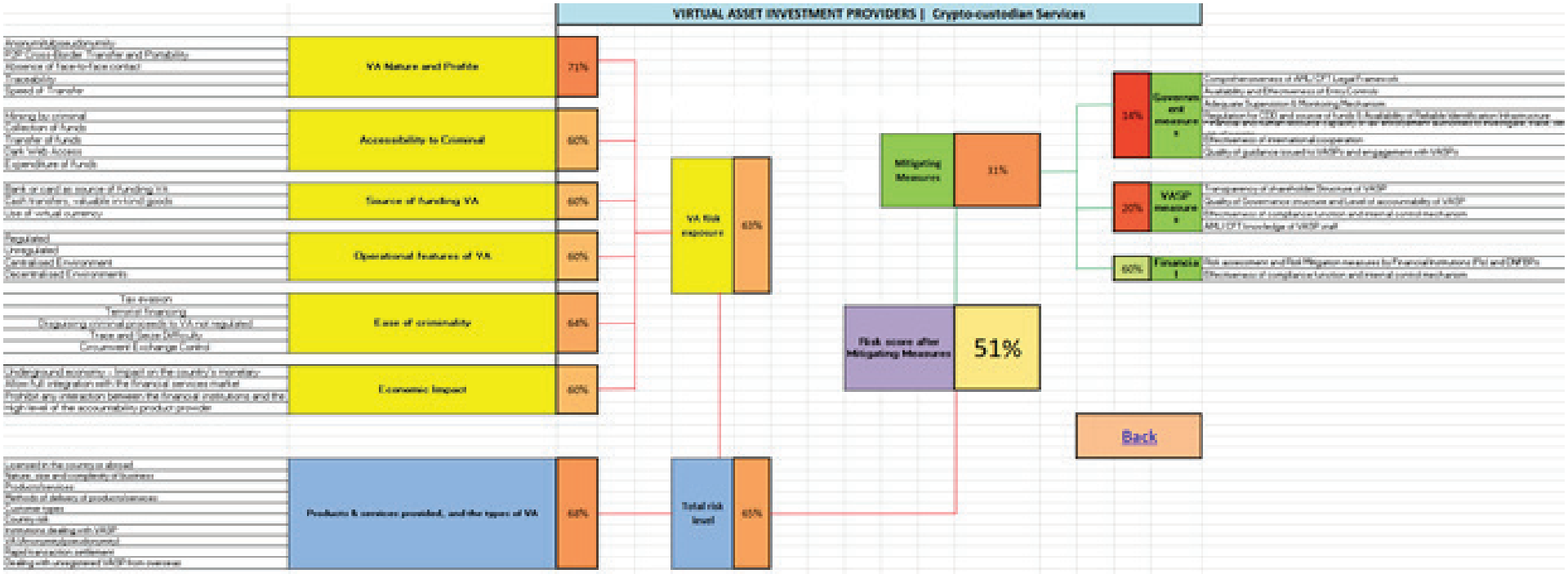

VIRTUAL ASSET INVESTMENT PROVIDERS | Platform Operators
VA Nature and Profile
71%
Accessibility to Criminal
60%
Source of Funding VA
60%
Operational features of VA
75%
Ease of criminality
64%
Economic Impact
60%
Products & services provided, and the types of VA
60%
VA Risk exposure
65%
Total risk level
67%
Mitigating Measures
31%
Risk score after Mitigating Measures
56%
14%
Governance and measures
20%
VASP measures
60%
Financial
Back

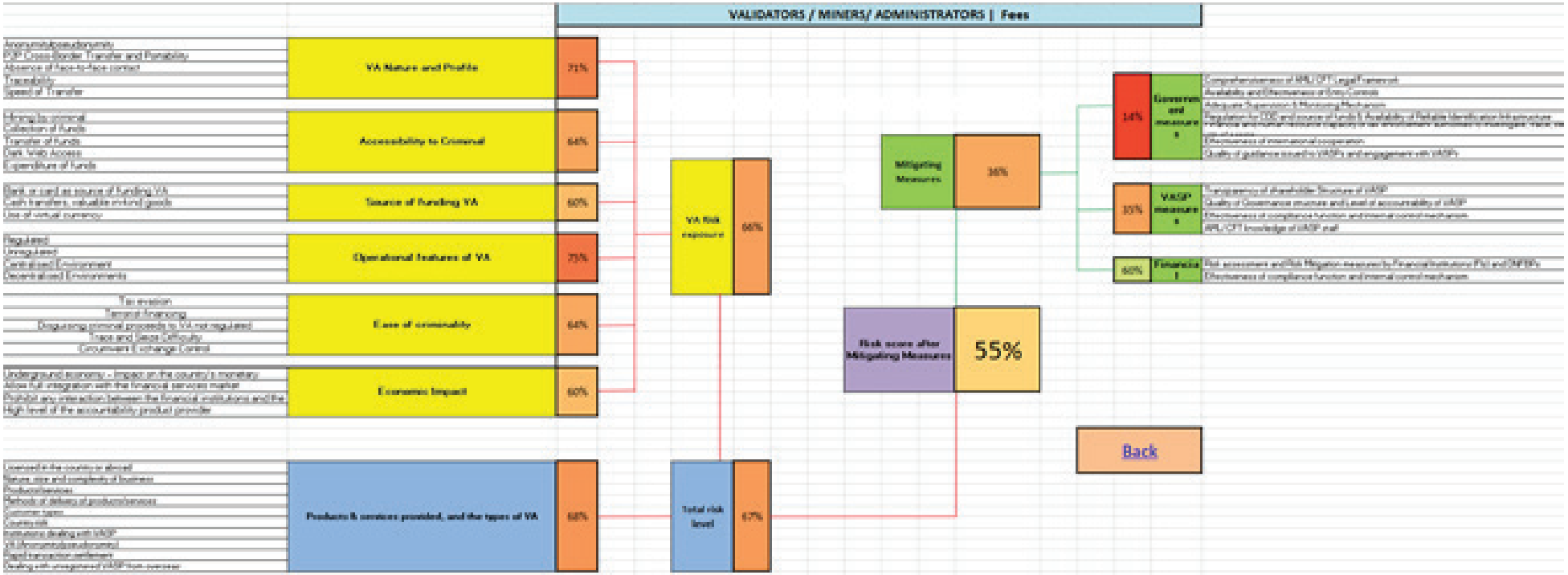

VIRTUAL ASSET INVESTMENT PROVIDERS | Custody of Assets
VA Nature and Profile
71%
Accessibility to Criminal
60%
Source of Funding VA
60%
Operational features of VA
75%
Ease of criminality
64%
Economic Impact
60%
Products & services provided, and the types of VA
68%
VA Risk exposure
65%
Total risk level
67%
Mitigating Measures
31%
14%
Governance and measures
20%
VASP measures
60%
Financial
Risk score after Mitigating Measures
61%
Back

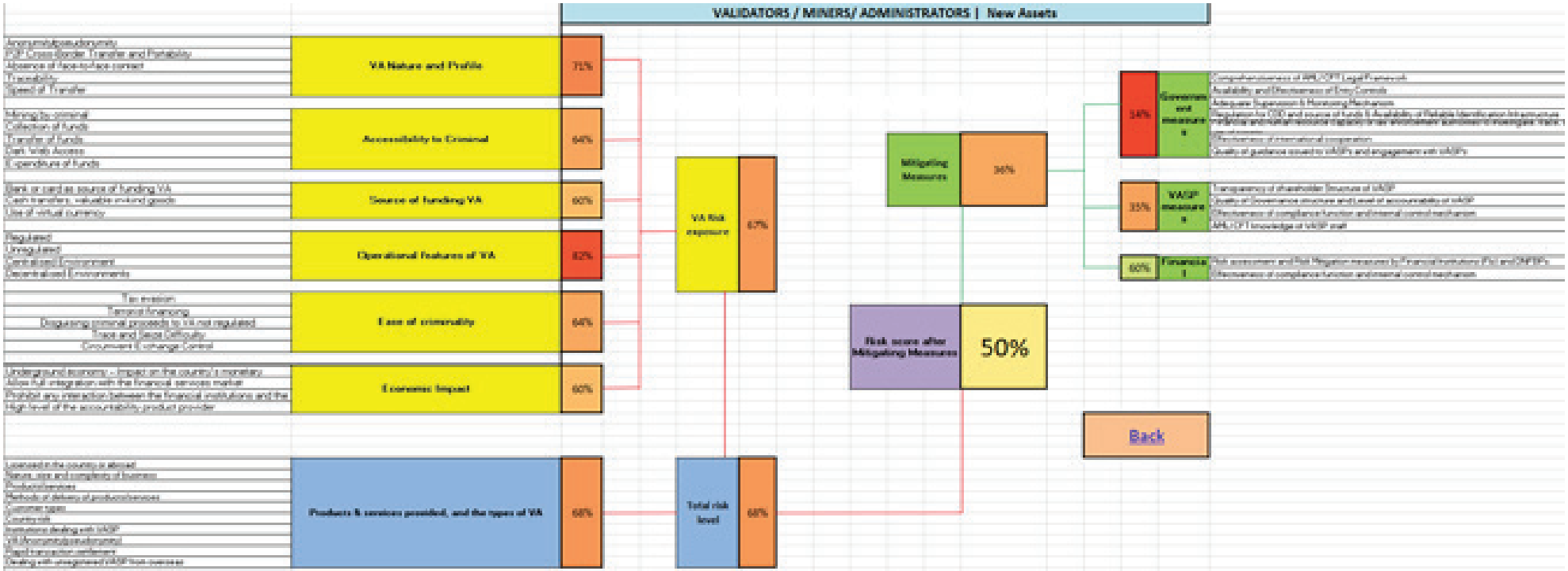

VIRTUAL ASSET INVESTMENT PROVIDERS | Investment into VA-related commercial activities
VA Nature and Profile
71%
Accessibility to Criminal
60%
Source of Funding VA
60%
Operational features of VA
75%
Ease of criminality
64%
Economic Impact
60%
Products & services provided, and the types of VA
68%
VA Risk exposure
65%
Total risk level
67%
Mitigating Measures
31%
14%
Governance and measures
20%
VASP measures
60%
Financial
Risk score after Mitigating Measures
61%
Back


VIRTUAL ASSET INVESTMENT PROVIDERS | Non-Security Tokens & Hybrid Trading Activities
VA Nature and Profile
71%
Accessibility to Criminal
60%
Source of funding VA
60%
Operational features of VA
75%
Ease of criminality
60%
Economic Impact
60%
Products & services provided, and the types of VA
60%
VA Risk exposure
65%
Total risk level
67%
Mitigating Measures
31%
14%
Governance measures
20%
VASP measures
60%
Financial
Risk score after Mitigating Measures
61%
Back


VIRTUAL ASSET INVESTMENT PROVIDERS | Stablecoins
VA Nature and Profile
91%
Accessibility to Criminal
80%
Source of funding VA
80%
Operational features of VA
95%
Ease of criminality
84%
Economic Impact
80%
Products & services provided, and the types of VA
88%
VA Risk exposure
85%
Total risk level
84%
Mitigating Measures
31%
Risk score after Mitigating Measures
78%
14%
Governance and measures
20%
VASP measures
60%
Finance I
Back


VIRTUAL ASSET INVESTMENT PROVIDERS | Crypto-custodian Services
VA Nature and Profile
71%
Accessibility to Criminal
60%
Source of funding VA
60%
Operational features of VA
60%
Ease of criminality
64%
Economic Impact
60%
Products & services provided, and the types of VA
68%
VA Risk exposure
65%
Total risk level
65%
Mitigating Measures
31%
Risk score after Mitigating Measures
51%
14%
Governance and measures
20%
VASP measures
60%
Finance I
Back


VALIDATORS / MINERS/ ADMINISTRATORS | Fees
VA Nature and Profile
71%
Accessibility to Criminal
64%
Source of funding VA
60%
Operational features of VA
75%
Ease of criminality
64%
Economic Impact
60%
Products & services provided, and the types of VA
68%
VA Risk exposure
66%
Total risk level
67%
Mitigating Measures
36%
14%
Governance measures
35%
VASP measures
60%
Finance
Risk score after Mitigating Measures
55%
Back


VALIDATORS / MINERS/ ADMINISTRATORS | New Assets
VA Nature and Profile
71%
Accessibility to Criminal
64%
Source of funding VA
60%
Operational features of VA
82%
Ease of criminality
64%
Economic Impact
60%
Products & services provided, and the types of VA
68%
VA Risk exposure
67%
Total risk level
68%
Mitigating Measures
36%
14%
Governance measures
35%
VASP measures
60%
Finance
Risk score after Mitigating Measures
50%
Back

FINANCIAL INTELLIGENCE AUTHORITY
Rwenzori Towers (Wing B) 4th Floor, Plot 6, Nakasero Road
P. O. Box 9853, Kampala, Republic of Uganda
Tel: 256 414 231556
E-mail: -fia@fia.go.ug
website: www.fia.go.ug