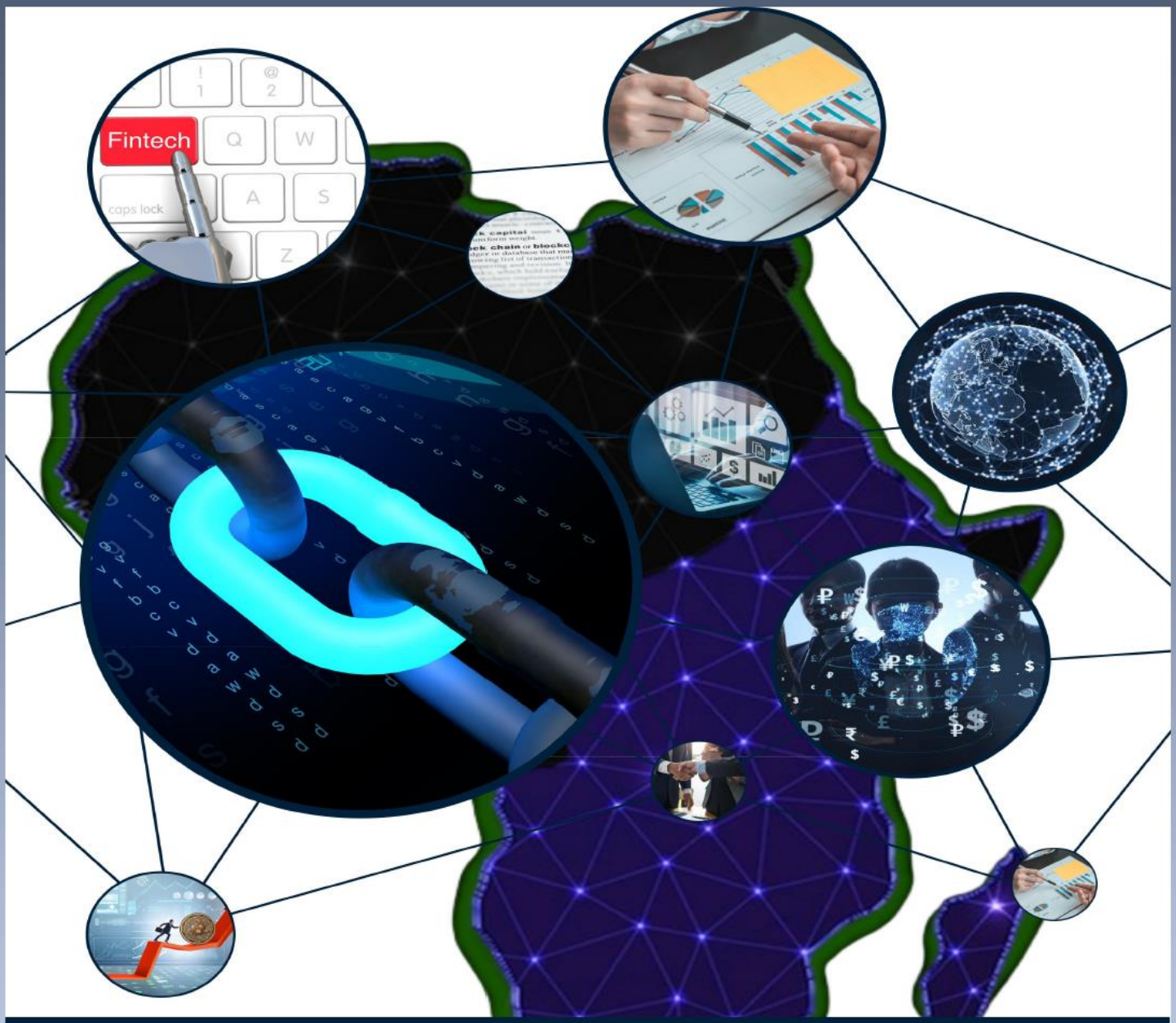
ESAAMLG REPORT

JUNE 2024



The Opportunities and Challenges Posed by Virtual Assets (VAs) and Virtual Assets Service Providers (VASPs) in the Eastern and Southern Africa Anti-Money Laundering (ESAAMLG) Region

Table of Contents

LIST OF ACRONYMS

AML/CFT	Anti-Money Laundering and Combating Financing of Terrorism
BCBS	Basel Committee on Banking Supervision's
BO	Beneficial Ownership
CBDC	Central Bank Digital Currencies
CDD	Customer Due Diligence
CPMI	Committee on Payments and Market Infrastructures
DeFi	Decentralised Finance
DLT	Distributed Ledger Technology
E-KYC	Electronic Know Your Customer
ESAAMLG	Eastern and Southern Africa Anti-Money Laundering Group
FATF	Financial Action Task Force
FIC	Financial Intelligence Centre
FIU	Financial Intelligence Unit
FinTech	Financial Technology
IMF	International Monetary Fund
KYC	Know your customer
LEAs	Law Enforcement Agencies
ML/ TF	Money Laundering / Terrorist Financing
Recs.	FATF Recommendations
SADC	Southern African Development Community
UNODC	United Nations Office on Drugs and Crime
UNSC	United Nations Security Council
VASPs	Virtual Asset Service Providers
VAs	Virtual Assets

GLOSSARY

Fund Management of Virtual Assets	Covers all aspects of fund management in relation to VAs such as investing within the mandate, best execution, order allocation, participation in initial offerings, transactions with connected persons, house accounts, risk management, disclosure of leverage and liquidity management.
Fund Distributors of Virtual Assets	Fund Distributors of Virtual Assets are entities which distribute funds to invest (wholly or partially) in Virtual Assets.
Financial Technology	Technologically enabled innovation in financial services that could result in new business models, applications, processes or products with an associated material effect on financial markets and institutions and the provision of financial services[1].
Initial Coin / Token Offering	An Initial Coin Offering is a fundraising transaction from the investing public carried out through a distributed register system (or "blockchain") and resulting in a token issue.[2]
Mining	Mining is the process that generate new VAs and verify new transactions. It involves vast, decentralized networks of computers around the world that verify and secure blockchains – the virtual ledgers that document VA transactions.[3]
Non-Fungible Tokens	Non-Fungible Tokens (NFTs) are unique VAs that cannot be copied and are recorded on a blockchain to verify authenticity and ownership. An NFT is digitally sourced or created and recorded to a blockchain, and an owner's claim to the NFT can be verified by associating the asset to an address on a blockchain.[4]
Stablecoins	Stablecoins[5] are a type of VA that aims to maintain a stable value relative to a specified asset, or a pool or basket of assets to other assets. A reference asset can be fiat money, exchange-traded commodities (such as precious metals), or a VA.[5]
Virtual Asset	A Virtual Asset is a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes. Virtual Assets do not include digital representations of fiat currencies, securities, and other financial assets that are already covered elsewhere in the FATF Recommendations.[6]
Virtual Asset Automated Teller Machine	Virtual Asset Automated Teller Machine are kiosks that allows a person to purchase VAs by using cash or cards. Some VA ATMs offer bi-directional functionality enabling both the purchase of VA as well as the sale of VA for cash.[6]

[1] Financial Stability Board: https://www.fsb.org/work-of-the-fsb/financial-innovation-and-structural-change/fintech.
[2] https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-VASP.pdf
[3] https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf.coredownload.pdf
[4] https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2023.html
[5] Note: The FATF considers that the term "stablecoin" is not a clear legal or technical category but is primarily a marketing term used by promoters of such coins. To reflect the common usage of the term, the FATF refers to them as stablecoins, but this does not represent an endorsement of their claims.
[6] https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-VASP.pdf

Virtual Asset Custody services provider	Virtual Asset Custody Services Provider is a service provider that stores VAs on behalf of customers using clearly defined features and controls to provide certainty over the safekeeping of the VA. [6]
Virtual Asset Exchanges	Virtual Asset Exchanges generally provide third-party services that enable their customers to buy and sell virtual assets in exchange for traditional fiat currency, another virtual asset, or other assets or commodities. These can be "traditional" virtual asset exchanges or virtual asset transfer services. [6]
Virtual Asset Merchants/ Brokers	Virtual Asset Merchants provide the service of arranging transactions involving VAs and fiat currency. [6]
Virtual Asset Service Provider	Virtual Asset Service Provider means any natural or legal person who is not covered elsewhere under the FATF Recommendations. and as a business, conduct 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[7] 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 virtual asset. [6]
Virtual Asset Wallet Provider	A Virtual Asset Wallet Provider provides storage for virtual assets or fiat currency on behalf of others. It then facilitates exchanges or transfers between one or more virtual assets, or between virtual assets and fiat currency. There are custodial wallets, non-custodial wallets, hot wallets, and cold wallets (3 common being hardware wallet, USB Wallet, and paper wallet). [6]

[7] In this context of virtual assets, transfer means to conduct a transaction on behalf of another natural or legal person that moves a virtual asset from one virtual asset address or account to another.

EXECUTIVE SUMMARY

In the last decade, the world of financial technology (fintech) has seen a phenomenal increase in the number of new digital instruments promising easier, faster, and cheaper global payments and transactions. The Financial Action Task Force (FATF), an intergovernmental body that sets global standards for AML/CFT/CPF, refers to some of these new instruments among others as Virtual Assets (VAs) and those who provide VA-related services as Virtual Asset Service Providers (VASPs). VAs and VASPs markets are growing rapidly in the region despite limited or no regulatory oversight. To this effect, the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG)'s Working Group on Risk, Compliance, and Financial Inclusion (WG-RCFI) agreed during the April 2022 Task Force meetings in Arusha, Tanzania to conduct a survey into the opportunities and threats posed by FinTech products, in particular, VAs and VASPs in the ESAAMLG region and their resultant effect on inclusive financial integrity. The research is intended to promote a shared understanding of the challenges and opportunities of the VA landscape among ESAAMLG member countries and guide the development of appropriate policy and regulatory responses to enhance financial integrity and stability among member countries. ESAAMLG member countries rely on FATF Standards, as well as guidance from FSB, IMF, and other organisations, as well as experts from domestic, regional, and international forums, to enhance their understanding of VAs and VASPs and inform their policy and regulatory responses.

The study was carried out through survey of the 20 ESAAMLG member countries and the project team received an overall 90 percent response rate on the nature, scope and effect of VAs and VASPs in the region. A structured questionnaire instrument was administered by means of email and respondents were given enough time to provide feedback. This method was selected to enable generalisation of the findings across the ESAAMLG region.

This survey outlines the trends, use cases, opportunities, challenges and risks of VAs and VASPs within the ESAAMLG region. The survey highlights the existing regulatory, supervisory, and monitoring approaches, and recommends international best practices, cooperation tools and mechanisms to be adopted by the region to tackle the risks posed by VAs and VASPs in the member countries.

The survey revealed that, while VAs and VASPs are still in their infancy in the ESAAMLG region, there is little or no interconnectedness between the VAs sector and the financial sector due to the relatively low exposure of the banking, insurance, securities, and DNFBP sectors to VAs. Key opportunities presented by VAs and VASPs include enhanced financial services and products, economic growth and development,

regulatory advancements, financial innovation, financial inclusion, technological innovation, and potential sources of funding, most of which are yet to be realised.

Although the majority of members have conducted ML/TF National Risk Assessments (NRAs) and/or Sectoral Risk Assessments (SRAs) these assessments did not specifically include the risk exposure associated with VAs and VASPs. However, ESAAMLG member countries through public discourses and other private -publicly available researchers have identified numerous challenges and risks posed by VAs and VASPs. The major challenge is the lack of regulatory framework compounded by lack of knowledge by competent authorities, which makes VAs and VASPs attractive for ML, TF, PF and other illicit activities. This is further worsened by that VAs in their nature are characterised by high volatility, lack of data, lack of consumer protection, lack of traceability or transactions due to anonymity and pseudonymity. These have also exacerbated fraud, cyber risks, financial loss, and tax avoidance. Lack of regulatory frameworks, capacity, and skills in identifying, investigating, and prosecuting VA -related cases are some of the issues that were raised as challenges by competent authorities. The report advocates for prudent utilisation of VAs and VASPs opportunities and benefits while mitigating risks.

The survey's key recommendations are that member countries that should incorporate VAs and VASPs in their NRAs or other risk assessments, should do so in order to gain a better understanding of the risks and opportunities posed by these technologies. Additionally, national authorities must develop skills to comprehend the underlying technology of VAs, to respond appropriately through establishing effective legal, regulatory, institutional, and supervisory frameworks while service providers must comprehend and implement FATF Standards pertaining to VAs and VASPs. Furthermore, authorities in member countries should also have experts in the use of technologies such as machine learning, distributed ledger technology, natural language processing and soft computing techniques, and application of programming interfaces to assist in the implementation of AML, CFT and CPF measures in the VAs sector. Moreover, the VAs sector should ensure that their underlying technology meets FATF requirements, particularly the 'travel rule,' which requires securely collecting and transmitting originator and beneficiary information.

The survey further, revealed that a majority of the ESAAMLG member countries implicitly allow the use of VAs and VASPs in their jurisdictions despite lacking the appropriate legal and regulatory frameworks. As of the close of this current survey, 17% of member countries have enacted bespoke VA and VASP legislations. The remaining countries have either incorporated VAs and VASPs into their existing sectoral, AML/CFT/PF, and/or taxation legal frameworks or do not have legal frameworks.

Moreover, the survey recommendations emphasize the importance of international best practices, standards, and cooperation in improving a common understanding of VAs and VASPs landscape and ensuring coordinated and consistent regulation and supervision of VASPs.

1. INTRODUCTION AND BACKGROUND

1.1. Fintech is changing the delivery of financial services, products, and investment management processes. The VAs and VASPs have proliferated in this Fintech global spectrum. They present new opportunities in financial inclusion, innovation and economic growth. However, they have to some extent been misused for illicit activities, thus posing challenges to Anti-money laundering and counter terrorism financing and counter proliferation financing (AML/CFT/CPF) efforts.

1.2. Globally, there is consensus among different authorities and standard setting bodies on the upsurge in VAs and VASPs activities. The International Monetary Fund (IMF), Financial Stability Board (FSB), World Bank, G20, and G7, amongst others, have called for a responsible, balanced approach to VAs that enables the legitimate use of VAs and fosters innovation while mitigating the associated risks.

1.3. As with traditional assets, the mitigation of ML/TF/PF risks emerging from VAs requires several steps, starting with a risk assessment and commensurate tailoring of the existing legal and institutional frameworks. Mitigation also requires the active, ongoing participation of the private sector and a range of governmental agencies (e.g., policymakers, regulators, supervisors, financial intelligence units, and law enforcement agencies). Finally, considering the cross-border nature of both legitimate and criminal VA-related activities, mitigation necessitates extensive dialogue, cooperation, and information sharing with foreign counterparts.

1.4. This study aims to contribute to the work on VA and VASP regulation in the ESAAMLG region and this report outlines the findings of the study and proposes the way forward for the region and the membership.

FATF RECOMMENDATIONS AND FRAMEWORK FOR VAs AND VASPs

1.5. The work of this study is guided by FATF Recommendation 15 (Rec 15) on New Technologies. Countries are required to identify and assess the ML and TF risks emerging from virtual asset activities and the activities or operations of VASPs. Based on their understanding of their risks, countries should apply a risk-based approach to ensure that measures to prevent or mitigate ML and TF are commensurate with the risks identified. Countries should further require VASPs to take appropriate steps to identify, assess, understand, and mitigate their ML and TF risks, as required by criteria 1.10 and 1.11 of the FATF Methodology.

1.6. Virtual Assets and Virtual Asset Service Providers fit squarely into this definition. In fact, FATF adopted an Interpretive Note (INR.15) to Recommendation 15 to further clarify how the FATF requirements should apply in relation to VAs and VASPs. These revisions extended to require VASPs to be licensed or registered and subject to an effective system of monitoring or supervision for AML/CFT/CPF purposes.

1.7. In addition, the FATF's Recommendation 16 urges countries to ensure that originating VASPs obtain, and hold required and accurate originator information and required beneficiary information on virtual asset transfers, and beneficiary VASPs, to obtain and hold required originator information; and required and accurate beneficiary information (referred to as personally identifiable information or PII). Countries are encouraged to adopt a *de minimis* threshold for transactions of USD 1,000. The FATF Travel Rule requires both the originating and beneficiary VASPs to make the required information available to appropriate authorities upon request and freeze or stop transactions related to ML, TF, sanctions evasion, and other illicit activities.

1.8. In October 2021, FATF updated it's FATF 2019 VA Guidance as part of its ongoing monitoring of the VA and VASP sector. The 2021 update essentially assists countries and VASPs to understand their AML/CFT/CPF obligations, and effectively implement the FATF requirements applicable to VAs and VASPs. Six key focus areas of the updated Guidance include clarification of the definition of VAs and VASPs, guidance on the applicability of FATF Standards to stablecoins, the risks and tools available to countries to address the ML/TF risks for peer-to-peer transactions, licensing and registration of VASPs, implementation of the 'travel rule' by the public and private sectors and principles of information sharing and co-operation among VASP Supervisors.

1.9. In addition, FATF issued a *Targeted update on implementation of its Standards on Virtual Assets and Virtual Asset Service Providers* in June 2022, specifically focused on the FATF's travel rule. The targeted update provided a short update on the country's compliance with FATF Recommendation 15 and its Interpretative Note, and relevant emerging risks and market developments, including Decentralised Finance (DeFi), NFTs, and un-hosted wallets.

1.10. To date, some jurisdictions are already implementing the FATF Recommendations to regulate VAs and VASPs for AML/CFT/CPF, while others are in the process of doing so. ESAAMLG has taken a mixed approach to the regulation of this sector as found in the study. The following sections discuss the purpose of the study, the project team, and the methodology. This is followed by

the main findings of the study, including VAs and VASPs Landscape, Regulatory Landscape, and the Risk Landscape.

2. PURPOSE AND OBJECTIVES

2.1. The objective of the study was to determine opportunities and challenges posed by VAs and VASPs in the ESAAMLG Region. In April 2022, the Task Force Plenary approved the conduct of the project based on a recommendation from the WG - RCFI to assess if jurisdictions have regulatory frameworks in place and further identify specific gaps in existing regulatory frameworks.

2.2. The purpose was mainly aimed at enhancing the ESAAMLG region financial regulators and authorities' understanding of the functioning of the VAs and VASPs ecosystem. This would enable the implementation of regulatory and supervisory frameworks for VAs and VASPs and foster financial stability, integrity, and inclusion in the region.

2.3. The specific objectives of the study include:

Primary Objectives:

i. To explore the nature of virtual assets. The study aimed to provide a comprehensive understanding of virtual assets, including their definition, types, characteristics, and the underlying technologies;

ii. To identify the potential opportunities and threats offered by VAs and VASPs. The study explores the potential benefits of virtual assets, such as increased financial inclusion, decentralized finance, and innovation in business models as well as threats such as money laundering, terrorist financing, tax evasion, and other cybercrimes;

iii. To assess regulatory challenges posed by virtual assets. The study aimed to assess the challenges posed by existing regulations and the need for regulatory clarity. This involves analysing the legal frameworks, compliance requirements, anti-money laundering (AML) and know-your-customer (KYC) regulations, consumer protection, taxation, and cross-border implications;

Sub-objectives:

iv. To investigate the forms of VAs and VASPs operating in the ESAAMLG region;

v. To establish laws, rules, regulations, and guidelines that enforce risk mitigation and management of VAs and VASPs in the ESAAMLG region;

vi. To examine trends and utilisation level of VAs in the ESAAMLG region;

vii. To identify international best practices and experiences in regulation, and supervision of VAs and VASPs in the ESAAMLG region; and

viii. To identify, assess, and understand the emerging ML/TF/PF risks from VAs activities, and operations of VASPs in the ESAAMLG region.

PROJECT AND PROJECT TEAM

2.4. The ESAAMLG Council of Ministers tasked the WG – RCFI to constitute a project team to conduct the survey in Arusha, Tanzania during the April 2022 meeting.

2.5. Consequently, a project team was constituted for this purpose, which developed a survey questionnaire and circulated the questionnaire to twenty (20) ESAAMLG member countries.

2.6. A Project Team comprising experts from Botswana, Kenya, South Africa, Eswatini, Malawi, Mauritius, Namibia, Rwanda, Uganda, and Zimbabwe was constituted to conduct the survey, co-chaired by Kenya and Zimbabwe. A questionnaire covering the period January -December 2022, was developed and circulated to all 20 ESAAMLG member countries in December 2022.

2.7. Eighteen (18) countries responded to the questionnaire representing 90% and all responses were considered for data analysis. Two countries did not give their responses neither their reasons for not responding.

2.8. As an addendum to this report, the project team decided it was appropriate to provide an update on the developments in 2023 based on the findings of the 2022 questionnaire. As such, the addendum is attached (ANNEX: ONE) to this report.

VIRTUAL ASSETS AND VIRTUAL ASSETS SERVICE PROVIDERS

2.9. Virtual asset is any digital representation of value that can be digitally traded or transferred and can be used for payment or investment purpose.

2.10. Virtual Asset Service Providers are entities or individuals that provide services related to virtual assets.

2.11. In relation to AML/CFT/CPF efforts VAs and VASPs have gained attention due to their potential vulnerabilities to illicit activities. The anonymity and borderless nature of virtual assets can be exploited for money laundering, terrorist financing, proliferation financing, fraud, tax evasion, and other illicit purposes. To address these concerns, regulatory authorities, and international bodies have been working to establish AML/CFT/CPF regulations and guidelines for VAs and VASPs.

2.12. The Financial Action Task Force (FATF) issued the revised Recommendation 15 and the revised Interpretative Note to Recommendation 15 in 2018 and 2019 respectively, and the Guidance Note on the Risked-based approach to VAs and VASPs (Guidance) in 2019 and the updated Guidance in 2021. The revisions imposed a set of recommendations known as the "Travel Rule" on VAs and VASPs. The Travel Rule requires VASPs to collect and transmit customer information during virtual asset transfers to ensure proper identification and verification of the parties involved. This helps prevent anonymous transactions and enhances the traceability of funds.

2.13. Furthermore, with the assistance of ESAAMLG, member countries are beginning to implement regulatory frameworks to comply with AML/CFT/CPF obligations related to VAs and VASPs. These regulations typically include customer due diligence (CDD) requirements, suspicious transaction reporting, record-keeping, and reporting obligations to the relevant regulatory authorities.

2.14. The objective of AML/CFT/CPF measures in relation to VAs and VASPs is to mitigate the risks associated with money laundering, terrorist financing, proliferation financing, and other illicit activities. By subjecting VASPs to AML/CFT/CPF obligations, ESAAMLG aims to ensure that virtual asset transactions are conducted in a transparent and accountable manner, similar to traditional financial transactions. This helps protect the integrity of the financial system, prevent criminal activities, and maintain public trust in virtual assets.

METHODOLOGY

2.15. The study utilised a survey approach. This method was selected to enable generalisation of the findings across ESAAMLG jurisdictions. A structured questionnaire instrument was administered by means of email on the 13th December 2022 and respondents were given one month to provide feedback. The questionnaire was designed to provide insight into different cross-cutting areas within the VA focal area. The questionnaire was intended to establish the existence of laws, rules, regulations, and guidelines that enforce risk mitigation and management of VAs and VASPs in the ESAAMLG region.

2.16. The target population was the 20 ESAAMLG member countries, with no other specific sampling technique being used. Eighteen (18) ESAAMLG members responded to the survey and these include:

1. Angola
2. Botswana
3. Eswatini
4. Ethiopia
5. Eritrea
6. Kenya
7. Lesotho
8. Madagascar
9. Malawi
10. Mauritius
11. Namibia
12. Rwanda
13. South Africa
14. Seychelles
15. Tanzania
16. Uganda
17. Zambia
18. Zimbabwe

2.17. Mozambique and South Sudan did not submit their responses.

2.18. The respondents comprised of fintech experts, VASPs; such as VA Exchanges and VA custodians, qualified and experienced consultants in VAs, law enforcement authorities, judicial authorities, financial intelligence units (FIUs),

supervisory authorities, regulatory authorities, data protection authorities, financial inclusion experts and other AML/CFT/CPF policy makers.

2.19. The following sections cover the findings of the study in terms of the VA and VASP Landscape in the ESAAMLG region, the Regulatory Framework setting, and the Risk environment. Finally, the report closes with a conclusion and set of recommendations for ESAAMLG and its membership.

ANALYSIS OF THE FINDINGS

3. VAs AND VASPs LANDSCAPE

3.1. The analysis of the VAs and VASPs landscape in the ESAAMLG region aims to identify the prevalence, types, use, cases, and trends of VAs and VASPs in the region.

3.2. VAs and VASPs are increasingly becoming prevalent in the ESAAMLG region, with the majority of ESAAMLG members having indicated some presence of VAs use in their respective jurisdictions. 56% of the jurisdictions reported one or more use of VAs in their respective jurisdictions with 50% of the jurisdictions reporting 'cryptocurrency' as the dominant form of VA in use.

3.3. Of the countries that reported 'cryptocurrency' 22% highlighted Bitcoin as the most prevalent. Some of the other VAs prevalent include Ethereum, Ripple, Tron, Litecoin, LEO coin, EOS, Tether, One Coin, and Stellar.

3.4. It was further indicated by 28% of the respondents that other forms and names of VAs in use remain unknown. This shows that the actual prevalence of VAs in the region may be higher than the 50% of the jurisdictions that expressly indicated the existence of such.

3.5. Analysis of the use of VAs shows that 61% of the countries use VAs for trading. VAs are also used for payment for goods & services, investment purposes, overseas transfers, and donations, though to a lesser extent. Table 1 indicates the uses of VAs. None of the countries have designated VAs as legal tender.

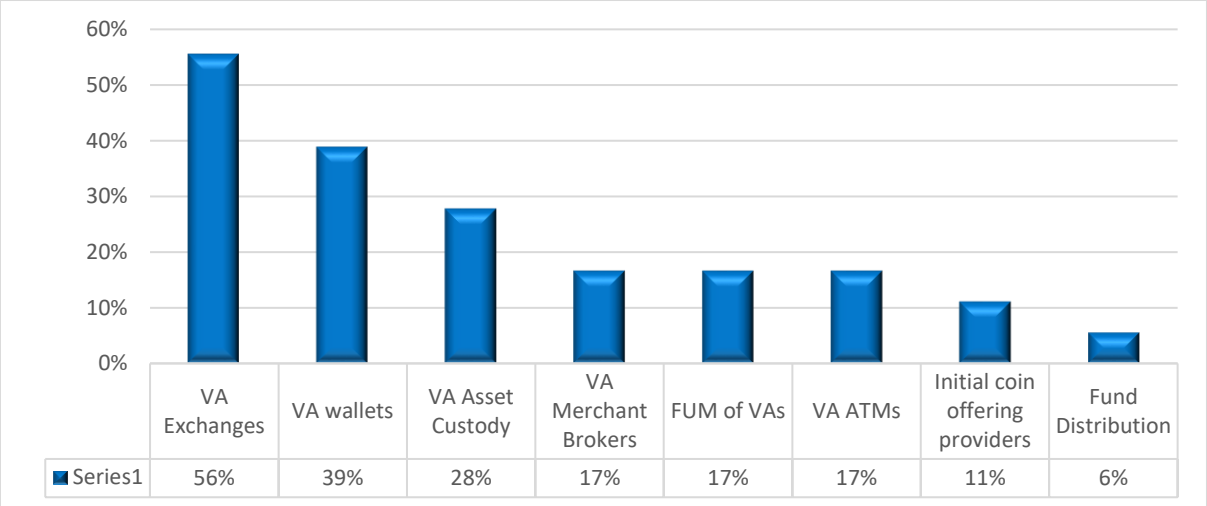
Table 1 Use of VAs

Uses of VAs	Number of Countries	Expressed as a %
Trading	11	61%
Payment for Goods & Services	9	50%
Investment Purposes	9	50%
Overseas Transfer	9	50%
Donations	3	17%

3.6. Twenty – two (22%) of the respondents' reported presence of mining operations in their jurisdictions.

3.7. In terms of VASPs, the region has at least eight types of VASPs conducting operations. The survey showed a high presence of VA Exchanges and Wallet providers. Thirty-three percent (33%) of respondents reported the non-existence of VASPs in the respective countries. Figure 1 shows the types of VASPs operating in the region.

Figure 2 Types of VASPs Operating In ESAAMLG



3.8. Despite the possibility of a higher prevalence of VAs and VASPs in the ESAAMLG region, 100% of the countries indicated a lack of information and/ or statistics on the volume, quantity, and/or value of VAs. While some countries attributed the lack of such information to failure to conduct any risk assessment on the use of VAs and VASPs, Mauritius, which had conducted a risk assessment at the time, also reported a scarcity of such information.

Banking Sector

3.9. Eighty percent (80%) of ESAAMLG countries indicated that the banks in their jurisdictions do not offer VA related products while 20% did not respond. Some of the countries indicated that their banks have been indirectly involved in VA activities since their customers have been using some of their banking products, such as bank accounts, debit, and credit cards to transact in VAs via online platforms. Sixteen percent (16%) of the countries indicated that banks are aware of customers using wire transfers for VA-related investments while 64% said they are not aware. Botswana indicated that two banks have on-boarded one client each in the past 3 years, which was a VA exchange and a VA wallet provider, respectively.

3.10. Twenty- four percent (24%) of countries indicated that banks have automated systems to monitor their clients who use banking products and services to transact in VAs such as the use of specific key words to flag inward and outward transactions that relate to VAs. Twenty-nine percent (29%) indicated that they do not have any systems, 26% indicated not applicable and 21% did not respond.

Securities Sector

3.11. Apart from Seychelles, all countries do not have entities in the securities sector operating as VASPs. Seychelles has 27 security dealers licensed under the Securities Act which provide functions that fall within the VASP functional definition of the FATF:

- Virtual Asset Wallet Service Providers
- Virtual Asset Exchanges
- Virtual Asset Broker and Payment Processing
- Virtual Management Providers
- Initial Coin Offering (ICO) Providers; and
- Mixers

Insurance Sector

3.12. Insurance companies in three countries; namely Mauritius, Seychelles, and Lesotho indicated that they are offering cyber liability and cyber insurance while two of them are also offering digital assets insurance. Cyber insurance in Lesotho is offered by regulated reinsurance counterparts normally from overseas where it is regulated.

3.13. In Seychelles there is a non-domestic insurance company licensed under the insurance legislation which offers a policy for crypto exchanges to safeguard against employee-assisted hacking. It also offers businesses an end-to-end risk management solution to mitigate the risk of cyber-attacks and safeguard against computer hacking, employee theft of data, and privacy breaches.

3.14. On the other hand, insurance companies licensed and regulated in Mauritius indicated that there has been an increasing trend in cyber liability and cyber insurance over the past three years. The volume of transactions has doubled from 2020 to reach approximately USD 1.6M (MUR 75,236,299) in 2022.

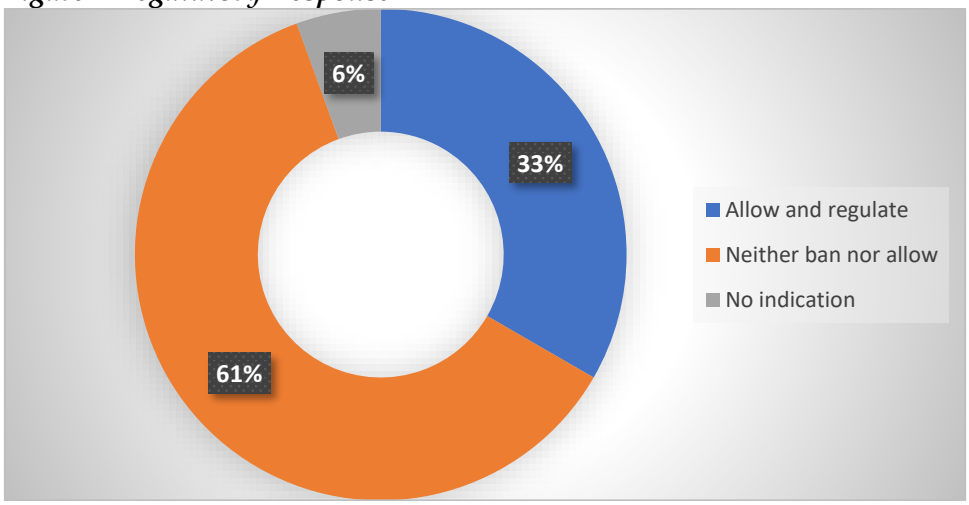
DNFBP Sector

3.15. The majority of the countries indicated that there are no interactions between the DNFBPs and VAs/VASPs in their jurisdictions. Six (6) countries did not provide any response.

4. REGULATORY LANDSCAPE

4.1. There is diverse regulatory response to VAs and VASPs in the region. 56% of the respondents (i.e., Ethiopia, Kenya, Lesotho, Madagascar, Malawi, Namibia, Rwanda, Tanzania, Uganda, Eritrea and Zimbabwe) indicated that they do not ban or allow VAs and VASPs, while 33% of the respondents (i.e., Botswana, Eswatini, Mauritius, South Africa, Angola and Zambia) indicated that they either regulate and allow VAs and VASPs or consider VASPs as accountable institutions. Seychelles did not indicate its regulatory approach with regards to VAs and VASPs.

Figure 2 Regulatory Response



4.2. In the countries with VA or VASP frameworks, the supervisory authorities are non-bank regulators as well as Financial Intelligence Centers/Authorities/Units. These authorities have the power to apply administrative or criminal penalties on unregistered VASPs.

4.3. While the majority of countries do not have a legal framework as yet, about 35% of respondents indicated that there are plans to carry out a National Risk Assessment that will include VAs and VASPs issues.

4.4. Countries reported the following challenges being faced in developing the legal framework or regulatory response to VA activities and VASP operations in their respective countries;

(i) Legislative framework requires conceptualisation, which is a cumbersome process involving other regulatory and supervisory authorities, and law-making, and enforcement agencies.

(ii) Lack of national risk assessment leading to low levels of understanding of the risks involved impeding taking of appropriate measures, including the establishment of a legal framework and designation of authorities.

(iii) Resource constraints with respect to both skills and people.

(iv) Limited awareness of authorities on the importance of legal provisions governing VAs.

(v) Stakeholder agreement/buy-in on the required legal framework.

Licensing and Registration

4.5. Botswana, Mauritius, and South Africa reported that they have designated authorities with responsibility for licensing VASPs. Mauritius and Botswana reported that they have created a new licensing regime for VASPs. In South Africa, the Financial Sector Conduct Authority (FSCA) has commenced the process to license VASPs in terms of the Financial Advisory and Intermediary Services Act (FAIS Act), although no license has been issued yet at the time of this survey. In addition, following the classification of VASPs as accountable institutions in terms of the Financial Intelligence Centre Act, VASPs are required to be registered with the Financial Intelligence Centre. In Uganda, Eswatini, and Zambia, VASPs are required to register with the relevant registration authorities under the AML/CFT/CPF laws.

4.6. The survey results indicated that currently only Botswana and Mauritius, have the bespoke VAs and VASPs legislation in place to ensure compliance with the VAs and the VASPs, as outlined below:

- Mauritius – In December 2021, the Virtual Assets and Initial Token Offering Services (VAITOS) Act was enacted. The VAITOS Act, together with other AML/CFT/CPF legislation, mandates VASPs to comply with AML/CFT/CPF requirements. The Financial Services Commission has been designated as the supervisor of this sector.
- Botswana - In February 2022, the Virtual Assets Act was promulgated and the Non-Bank Financial Institution Regulatory Authority (NBFIRA) was designated as the Regulator and Supervisor of VASPs and VAs. The Virtual Assets Act subjects VASPs as regulated entities to the ML/TF/PF supervision under the Financial Intelligence Act 2022.

4.7. Some of the jurisdictions without the bespoke VA legislation, have enabling provisions in their existing legislation or regulations that apply to VAs and VASPs. These vary from AML/CFT/PF legislation to existing financial sector legislation.

- South Africa, has through a ministerial declaration of 2022, declared VAs as financial products under the FAIS Act and the FSCA is the Supervisor of the financial services providers regulated under the FAIS Act. Similarly, VASPs are classified as accountable institutions in terms of item 22 of Schedule 1 to the Financial Intelligence Centre Act, 2001 (FIC Act) with effect from 19 December 2022, and the FIC is the Supervisor of these VASPs. Arrangements are being implemented between the FSCA and FIC to facilitate joint supervision of VASPs to avoid duplication of efforts.
- Eswatini promulgated an amendment to the Eswatini Money Laundering and Terrorism Financing (Prevention) Act, 2011 (as amended) on 26th of August 2022 to include VASPs as accountable institutions under Schedule 3 of the Act.

4.8. Angola, Uganda, and Zambia reported that they have subjected VASPs to existing AML/CFT/CPF regulation and risk-based supervision.

4.9. Angola, Botswana, Mauritius, South Africa, and Zambia, reported that they have AML/CFT/CPF Guidelines issued or established by responsible authorities that assist VASPs in applying national measures to combat ML/ TF/PF.

Travel Rule

4.10. The majority of the countries, except for Mauritius, indicated that the VASPs do not have the obligation to share the originator and beneficiary information on VAs with counterparties or authorities.

4.11. In Mauritius, the VAITOS Act imposes on originating VASPs the obligation to obtain and hold accurate originator information and beneficiary information on transfers of VAs. The VASPs are required to immediately and securely submit the information obtained and held to the beneficiary VASP or any other financial institution. Similarly, the beneficiary VASP should obtain and hold originator information and accurate beneficiary information on the transfer. Furthermore, the information obtained and held by the originating and beneficiary VASPs shall be kept in a manner that they are immediately made available to the supervisory authority in Mauritius or, upon request, to any other relevant competent authority. The supervisory authority may also exchange information with law enforcement agencies, investigatory authorities, other supervisory authorities, regulatory bodies, FIU, public sector agencies, and comparable overseas entities under section 42 of the VAITOS ACT.

Screening of customers and parties to transactions, and associated wallets

4.12. The majority of countries indicated that the market players screen customers and parties to transactions, and associated wallets against Sanction lists while other countries did not respond to this question or indicated that the question was not applicable.

Sanction regime on non-compliant VASPs

4.13. Botswana, Mauritius, and South Africa have pronounced sanction regimes with a range of proportionate and dissuasive sanctions, criminal, civil, or administrative, available to deal with VASPs that fail to comply with AML/CFT/CPF requirements.

Law Enforcement Agencies (LEAs)

4.14. The survey demonstrated that most of the LEAs in the region are not able to investigate and prosecute VA or VASP- related cases. The reason raised for this was that the sector is nascent and requires specialised expertise and skills. Generally, most of the LEAs in the region do not have reported cases related to VAs and/or VASPs being misused for ML/TF/PF, or other financial crimes, except for Lesotho, Mauritius, and Seychelles.

4.15. In Mauritius, between 2021 and 2023, there were 20 cases of VA- related frauds (such as bogus VA investment schemes) affecting individuals in Mauritius. For Seychelles, cases brought to court have been linked to VASP registered in Seychelles as offshore companies. Even where the criminal conduct itself occurs outside Seychelles; the country has helped in a few international cases through the confiscation of VAs under the Proceeds of Crime Act (POCA).

4.16. In Lesotho, people have complained of losing funds through platforms, in one case, it was reported that two persons who were investing through MEDIA COIN, had their money withdrawn by an unknown person and the investigations were still ongoing.

4.17. Botswana indicated that the VA phenomenon is a relatively new concept in the country and more training and resources are needed. Mauritius, Tanzania, and Zambia indicated that training has been availed to LEAs and that they are able to trace VAs and identify illegal activities to some extent. Mauritius has acquired blockchain analytical tools/ software to be able to trace, identify, and monitor VA transactions.

4.18. The inability to identify and investigate VA and VASP- related crimes in most countries poses a risk to financial integrity as perpetrators of illegal or criminal activities surrounding VAs will go unpunished, thus perpetuating criminality using VAs. However, some countries in the region have succeeded in investigating VAs and VASPs. For example, in 2017, South Africa's Financial Intelligence Centre (FIC) referred a case to Namibia's National Prosecutions Authority's Asset Forfeiture Unit (NPA:AFU). The NPA:AFU, through preservation and forfeiture orders eventually recovered R961 654 ($65 400)[8].

Obligations for VASPs to declare their activities to the Tax Authorities

4.19. Despite the revenue that VAs is said to generate, there are no express legal provisions on collection of tax from the VASPs. Instead, they are general collection provisions in the Income Tax Act and Value Added Tax (VAT Acts) on businesses operating in the countries requiring the VASPs to make the necessary returns to the Tax Authorities, as demonstrated below:

[8] Mutual Evaluation Report of South Africa dated October 2021 and available via https://www.fatf-gafi.org/content/dam/fatf-gafi/mer/Mutual-Evaluation-Report-South-Africa.pdf.coredownload.inline.pdf

4.20. In Botswana, income deemed to be from a source within Botswana is taxable. In terms of Section 12 of the Income Tax Act, the taxable income of any person shall be charged to tax in the name of that person. The Income Tax Act defines a "person" as an individual, a trustee, the estate of a deceased person, a company, whether incorporated or unincorporated, a partnership, and every other juridical person.

4.21. For Mauritius, the relevant provision is Section 112 of the Income Tax Act, requiring every person deriving income to submit a return of income to the Mauritius Revenue Authority (MRA). Further, under section 116 of the Income Tax Act, every company, non-resident Société, cell of a protected cell company, Foundation, trust other than a trust to which section 46(3) or trustee of a unit trust scheme, whether or not it is a taxpayer, is required to submit to the MRA, not later than six months from the end of the month in which its accounting period ends, a return of all income derived by it during the preceding income year and at the same time pay any tax payable in accordance with its return. Additionally, every person who, in the course or furtherance of his business, makes taxable supplies; and whose turnover of taxable supplies exceeds or is likely to exceed MUR 6 million (USD 134,000), shall apply to the MRA for compulsory registration as a registered person under section 15 of the VAT Act and is required to submit monthly/quarterly VAT returns as per Section 22 of the VAT Act.

4.22. Accordingly, VASPs are also governed by the above-mentioned provisions in the Income Tax Act and VAT Act thus, required to make the necessary returns to the MRA.

4.23. In South Africa, the South African Revenue Service (SARS) has a wide range of collection and reporting powers in terms of the Tax Administration Act, No. 28 of 2011 (the TA Act), including provisions that enable SARS to acquire data from third parties, which would include VASPs. Currently, there is no automatic requirement on VASPs to provide third-party data on their clients, but subject to possible amendments by way of public notice (section 26 of the TA Act), VASPs can be included as automatic third-party data providers. However, currently, SARS obtains third-party data information from VASPs on an *ad hoc* basis (section 46 of the TA Act).

4.24. Zambia indicated that the obligations have been provided for as per the Zambia Revenue Authorities Law under the general provisions of all the entities that are subject to tax.

4.25. Some countries, like Botswana, are currently working on reviewing their statutes, the Value Added Tax Act to incorporate the taxation of the digital economy. Botswana's second draft of the VAT Bill refers to digital currency (has since been proposed that the term "Digital Currency" be replaced with "Virtual Asset" to align with the Virtual Assets Act of 2022). Some of the countries are working on their laws as regards VAs.

5. OPPORTUNITIES PRESENTED BY VAs AND VASPs IN THE ESAAMLG REGION

5.1. Some ESAAMLG member countries view VAs as opportunities to boost economic performance and financial inclusion, while others highlight the need for comprehensive analysis and regulatory oversight to address the corresponding challenges.

5.2. 65% of ESAAMLG member countries recognised the potential benefits of VAs and VASPs. The overall responses reflected a positive outlook on the potential of VAs and VASPs to boost economic and financial investments in their jurisdictions.

5.3. The main opportunities and benefits are summarised as follows:

- Technological and Financial Innovation
  Virtual asset technology has the capacity to transform financial innovation. This, in turn, brings about new business models, applications, processes, or products that have a significant impact on financial markets, institutions, and the provision of financial services.[9]

- Financial Inclusion
  Virtual assets possess the capacity to furnish unbanked and underbanked populations with access to financial services, especially in developing nations. Cryptocurrencies, for example, can be accessed with just an internet connection and a smartphone, making them particularly accessible to populations in developing countries or regions with limited banking infrastructure.

[9] FSB

- Reduced Transaction Costs
  Virtual assets have the potential to lower transaction costs by eliminating intermediaries and automating processes, which includes broker and legal fees.

- Access to Global Markets
  Virtual assets enable cross-border transactions with reduced fees and intermediaries through their ability to connect asset owners directly to execute transactions without the assistance of centralised institutions or governments.

- Improved Efficiency and Accessibility
  Virtual assets can streamline financial transactions by eliminating intermediaries, reducing settlement times, and lowering costs.

5.4. Reduced transactions costs were ranked high followed by financial inclusion whilst access to global markets was lowest among the opportunities and benefits.

6. RISK LANDSCAPE: ML/TF/PF RISKS

6.1. Most of the ESAAMLG countries highlighted various ML/TF/PF risks related to the VA activities and operations of VASPs in the ESAAMLG region. Concerns were expressed that the risks posed by VAs could lead to systemic and financial impacts on the integrity, inclusion, stability, and consumer protection endeavours in the region.

6.2. The most prevalent risks identified by the ESAAMLG members are outlined in Table 2 below, most of which overlap with the challenges outlined above. The risks identified emanate from countries that conducted NRAs of VAs and VASPs and countries that are yet to conduct NRAs.

Table 2: Risks identified in the key major sectors.

VA risks identified in the key sectors		
Banking sector	**Securities and insurance**	**DNFBPs**
• Anonymity • Illicit flows • Inability to conduct Customer Due Diligence (CDD) • Cybersecurity • Misuse • Lack of traceability • Fast and instant transaction	• Anonymity • Pseudonymity • Fast and instant transaction • Inability to conduct CDD • Cybersecurity • Traceability • Illicit flows	• High volatility • False valuation • Conversion of illegal proceeds into VAs • Traceability • Illicit flows • Anonymity – false identity and illegal source of funding not easily detectable • Lack of awareness • Lack of capacity • Easily conversion from one VA to another • Allows market participation of unlicensed players that pose risks to the market. • Transnational transactions

i. **Consumer Protection**:

6.3. Consumer protection is a critical aspect of financial inclusion. Tanzania mentioned that there is need for caution when considering financial inclusion through VA activities. This may be due to VAs and VASPs lacking the same level of consumer protection measures as traditional financial institutions.

ii. **Taxation**:

6.4. Eswatini mentioned that VAs increase a massive outflow of funds and hinder taxation. The following challenges posed by VAs and VASPs for taxation were highlighted:

- ***Classification and Recognition***: Determining the appropriate classification of VAs for tax purposes can be challenging and difficult to establish consistent rules.

- ***Valuation***: Valuing VAs for tax purposes can be complex. VAs are highly volatile and can experience significant price fluctuations, making it difficult to calculate tax liabilities.

iii. Anonymity

6.5. VA transactions prelude ease of identification and traceability of the ultimate beneficial owner. 67.% of respondents indicated anonymity as a technical challenge posed by VAs and VASPs in their jurisdictions. However, 33% of respondents indicated that they are not aware of the same.

iv. Data Privacy

6.6. 10.5% of respondents believed data privacy is another technical challenge - which requires using advanced technologies and techniques to protect personal and sensitive information from unauthorized access, theft, and corruption.

v. Cybersecurity

6.7. Altogether 14.6 % of the respondents identified cybersecurity as a technical challenge posed by VAs and VASPs, as cybercriminals continually develop new techniques to bypass security measures. As such potential VA & VASP regulators in ESAAMLG should be required to be sufficiently resourced with cybersecurity professionals to keep up with these new threats and adapt their defences accordingly.

vi. Working with third-party platforms

6.8. VAs rely on third party servers and systems and hence prone to be misused or shared with other parties without the consent of the owner.

vii. Pseudonymity

6.9. Due to the difficulties in tracing the BOs with VAs, VAs might open up avenues for ML, TF, and other financial crimes.

viii. Decentralisation

6.10. VAs and related technology raise regulatory and oversight challenges as they operate across various jurisdictions, and lack centralised authority, thus making jurisdictional ownership a challenge.

ix. Peer-to-peer (P2P) cross border transfer

6.11. Peer-to-peer cross-border transactions reduce transaction transparency and complicate transaction monitoring by regulatory authorities.

x. Traceability

6.12. The anonymous nature of the transactions makes traceability of beneficial owners challenging.

xi. Transaction Reporting and Accounting Framework

6.13. The complexity of the accounting framework for VAs can hinder financial inclusion efforts, as particularly mentioned by South Africa, where the technological integrity of VA platforms is not guaranteed. This lack of assurance opens up the possibility of fraudulent and opaque functionalities that could facilitate payments-off the blockchain. The complexity can make it challenging to properly account for and report these transactions within existing frameworks.

xii. Financial Exclusion

6.14. Financial exclusion challenges could result from the majority of ESAAMLG member countries' lack of appetite for VAs. Exclusion proved to be the major risk as most of the VASPs could be operating in the ESAAMLG region unregulated and unlicensed.

xiii. Investigations and prosecutions of VAs and VASPs.

6.15. The ESAAMLG region decries the lack of expertise in monitoring, investigation, prosecutions, and recovering/seizing and confiscating VAs. Some countries indicated that they lack a centralised VA/VASP control system and have limited awareness of this sector. The very nature of VAs renders the investigation more challenging. The challenges identified include, amongst others, identifying the owners of the VAs and tracing transactions from end to end, especially where the recipients are in foreign jurisdictions.

6.16. Across most of the ESAAMLG countries, there is a lack of expertise within LEAs to investigate VA cases. LEAs do not have access to VA investigative tools and are unable to trace transactions and identify potential suspects through wallet addresses. More training and tools are needed to acquire the knowledge and skills necessary to better equip the officers to use the latest investigation tools and software to trace VA-related crimes.

6.17. Furthermore, the cross-border nature of VA flows, makes it challenging to identify jurisdictions in which relevant VASPs are situated. Various VASPs indicate the method that they wish to be contacted by LEAs and in certain instances require subpoenas or similar legal documentation before providing information. Formal international channels need to be utilised to approach authorities in the identified jurisdictions for assistance. Given that the space is unregulated for most of the countries, it is difficult for LEAs and Tax Authorities to properly investigate this area.

VAs and VASPs Threats and Vulnerabilities

Risks

6.18. Most of the ESAAMLG countries indicated that the anonymity, lack of traceability, and rapid global reach features of VAs propel ML/TF/PF risks in the region. These features make VAs attractive to criminals who want to launder funds, provide funds to terrorists, and also fund proliferation. VAs are attractive to money launderers, and terrorist financiers, as well as the proliferation of weapons of mass destruction as they allow for anonymity, they can be easily and rapidly moved across borders and are not subject to the same regulatory controls as traditional financial systems.

6.19. VASPs may provide a means for criminals to convert illicit funds into VAs making it more difficult for law enforcement to trace the source of the funds. The risk is compounded by the fact that VAs can be remotely accessed, promoting non-face-to-face transactions that cannot be interrogated by the legal officers. Moreover, VA funds can be moved rapidly changing identity quickly thus further inhibiting law enforcers from tracing the funds/transaction.

6.20. With regards to TF, countries indicated that VAs are said to be attractive as they can be used to transfer funds across borders and can be difficult to trace. VASPs provide a means for terrorists to convert funds into VAs which can then be used to purchase terrorist property, providing a source of financing for terrorist activities.

6.21. VAs further pose cybersecurity risk due to the complexity of the technology used by VAs and VASPs where a financial service provider may fail to have up-to-date technology and mitigation measures to cope with cybersecurity risk.

7. INTERNATIONAL BEST PRACTICES AND EXPERIENCES IN REGULATION, AND SUPERVISION OF VAs AND VASPs IN THE ESAAMLG REGION.

(a) FATF works on VAs and VASPs consultation by ESAAMLG member countries to inform regulatory strategy.

7.1. The survey results revealed a significant appreciation of FATF Standards on VAs and VASPs by member states. The FATF has been closely monitoring developments in the crypto sphere and has issued global, binding standards to prevent the misuse of VAs for ML and TF. All ESAAMLG member countries that

responded to the questionnaire are aware that they must comply with Recommendation 15.3 - 15.11. Member countries indicated that FATF Standards are assisting them in understanding the ML and TF risks posed by VAs and VASPs; deciding whether to license, register, or ban VASPs in their respective countries, and the steps required to supervise the VAs and VASPs sector.

7.2. The findings suggested that the FATF Guidance for RBA to VAs and VASPs is assisting ESAAMLG supervisory authorities in deciding how to supervise VAs and VASPs. The Guidance emphasizes the importance of conducting a coordinated NRA, including on VAs and VASPs to understand the risks posed by VAs and VASPs in each country. By completing an NRA, member countries that do not yet have a strategy will be able to select a strategy to manage the risks posed by VAs and VASPs in their countries.

7.3. However, survey results revealed that regulating VASPs remains difficult for the majority of ESAAMLG member countries. Most member countries are concerned about the sector's rapid evolution and risk mutation levels, which has left many of them without a strategy to deal with VAs and VASPs. Many member countries are simply unsure where to begin in terms of regulating the sector and detecting illicit activity in virtual asset transactions.

(b) Experiences gained for regulation and supervision of VAs and VASPs

(i) Participation in the VA/RegTech forums

7.4. The findings of the survey revealed that the majority of national authorities participated in VA-related forums at the national and/or international levels. The 2022 ESAAMLG Public-Private Sector Dialogue in Livingstone, Zambia, and the 2023 UNODC workshop on VAs are among the forums mentioned by the majority of member countries.

(ii) Experience gained from other countries

7.5. Member countries reported receiving learning experiences from other jurisdictions, with the majority of ESAAMLG member countries reporting that the learning experience was beneficial. Some ESAAMLG member countries that were exposed to VAs' experience have developed their own regulations. Member countries believed that the commitment demonstrated in other jurisdictions could be used as a benchmark to initiate regulation and supervision of VASPs in countries that had not yet started implementing supervisory approaches to the VAs and or /VASPs sector.

(iii) Secondments related to VAs and VASPs

7.6. According to the survey results, eighteen (18) ESAAMLG member countries did not have personnel seconded to another country to learn about VAs and VASPs. These member countries did not provide any explanations for the lack of secondments related to VAs and VASPs.

(c) Exploring Regulatory Technology (RegTech)

7.7. The majority of ESAAMLG member countries are yet to explore RegTech (modern regulatory and supervisory technology solutions). However, there are a few countries in the region that have taken the initiative to explore RegTech services. In order to improve its supervisory and enforcement capabilities, the FSC in Mauritius, for example, purchased a Blockchain Analytics tool from a leading global firm.

(d) International Cooperation

7.8. According to the findings of the survey, the majority of member countries lack a legal framework that directly regulates VAs and VASPs. As a result, there are no legal provisions in place for Mutual Legal Assistance among the majority of member countries in relation to VAs and VASPs. Mauritius, on the other hand, is an exception, as Section 42 of their VAITOS Act allows for the exchange of information and mutual legal assistance in the case of VAs and VASPs.

(e) Public/private sector discussion and engagements on VAs

7.9. Despite the region's low level of VA and VASP regulation development, the survey found that most member countries have put in place mechanisms to engage with private players in this technological space. The Regulatory Sandbox is the most visible form of engagement with the private sector operating VAs. Other member countries pointed out that their engagement with the private sector occurred during their NRAs on VAs and VASPs.

7.10. There was also evidence of engagement in the form of joint subcommittees formed with key private sector representatives. Other member countries have hosted Public Private Sector Dialogue workshops to discuss the best approach to dealing with VASPs in their countries. The study discovered that, while VAs and VASPs have many benefits, they are also vulnerable to criminal abuse which cannot be dealt with by individual country authorities but requires collaboration between national authorities and the private sector.

8. RECOMMENDATIONS

8.1. In view of the findings and conclusions drawn from the analysis, the following measures are recommended:

i. Member countries that have not yet conducted a national risk assessment on VAs and VASPs should do so to better understand the contexts, risks, and opportunities presented by the VAs and VASPs in their respective jurisdictions.

ii. National authorities must develop skills to understand the underlying technology of VAs, while service providers (VASPs) must understand and apply FATF standards related to VAs and VASPs.

iii. Authorities in member countries should have information technology experts in areas such as machine learning, distributed ledger technology, natural language processing and soft computing techniques, and application programming interfaces to help implement AML and CFT measures in the VAs sector.

iv. The VAs sector should ensure their underlying technology meets the FATF's requirements, particularly when it comes to the 'travel rule', which requires securely collecting and transmitting originator and beneficiary information.

v. Member countries are encouraged to engage intensively with VASPs in order to build partnerships and gain a holistic understanding of VAs by hosting VA/RegTech forums amongst other options.

vi. ESAAMLG member states should ensure that the operations of VAs/VASPs in their countries reflect both threats and opportunities and that the technology used is compatible with international data protection, privacy, and cybersecurity standards.

vii. Members should strive towards reaching a consensus in approaching VAs and VASPs regulation in the ESAAMLG region, to ensure harmonised and consistent regulation of VAs and VASPs within the region.

viii. Based on FATF requirements, the ESAAMLG member countries are encouraged to expeditiously take the necessary steps to comply with the applicable recommendations and guidelines on VAs and VASPs.

ix. ESAAMLG member countries should consider seeking technical assistance in the supervisory, legal framework, and law enforcement to ensure effective implementation of the FATF Recommendations, including effective implementation of the travel rule by VASPs.

x. Authorities should ensure that VASPs possess the requisite tools for ongoing monitoring of transactions for the purpose of sanction screening and reporting of terrorist-link transactions.

xi. Promote evidence-based polices and regulatory frameworks in VAs and VASPs to avoid regulatory failure.

9. CONCLUSION

9.1. VAs and VASPs are increasingly becoming prevalent within the ESAAMLG region. Member countries presented differing perspectives on how to approach VAs and VASPs identification, understanding, and regulation in the ESAAMLG region. Members are of the view that harmonised regulation will facilitate the effective implementation of AML/CFT/CPF frameworks for mitigating ML/TF/PF risks associated with VAs and VASPs. It is critical to establish a foundation and basis for clearly delineating the type of regulation, oversight, and supervision to be accorded to the various categories of VAs and VASPs. Some countries believed that a base legal framework for VAs and VASPs should be established, with member countries tailoring the requirements based on their idiosyncratic risks with the intention of protecting investors' interests.

9.2. Furthermore, while leveraging the opportunities and benefits of VAs and VASPs, member countries must comply with FATF Standards, facilitate the smooth regulation of VAs and VASPs, and reduce the risk of criminal misuse of VAs and VASPs in the ESAAMLG region. Information exchange should be encouraged and facilitated, especially in relation to cross-border criminal activities. The countries in the ESAAMLG region must all have a shared understanding of VAs and VASPs in terms of mechanisms and threats which should undoubtedly result in fewer delays in the exchange of relevant information. The Fintech space is highly dynamic and complex, with rapid innovation. As a result, it is critical for regulators to cooperate and collaborate to promote greater financial integrity and stability in the region.

9.3. However, due to regional knowledge parity, some member countries believe it may be too early to reach a consensus on the best approach to VAs and VASPs. Before an agreement can be reached, member countries must first consider the scarcity of expertise, the region's limited resources, the ML/TF/PF risk of this technology, and the availability of a mitigation method. More consultations and technical training for individual member countries and within the region are required for the region to reach a consensus due to varying levels of technological and infrastructural advancement.

9.4. Consistent, proportionate, activity-based, and risk- based regulatory approach is necessary to regulate VAs and VASPs in the ESAAMLG region. However, this regulatory approach may not be immediately possible due to the various factors influencing different jurisdictions, such as the size, scale, complexity of the VA sphere, the threats and vulnerabilities of exploitation of the VAs/VASPs sphere, industry role players, and so on. To ensure that the region remains internationally consistent, the approach used in ESAAMLG must be aligned with standards, principles, and recommendations communicated by international standard - setting bodies, particularly FATF.

REFERENCE

1. Financial Action Task Force (2021). Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, FATF, Paris.
2. Financial Stability Board (2020). Financial innovation and structural change-FinTech. https://www.fsb.org/work-of-the-fsb/financial-innovation-and-structural-change/fintech/
3. Financial Action Task Force (2021). Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. FATF. Paris.
4. International Monetary Fund (2021). Virtual Assets and Anti-Money Laundering and Combating the Financing of Terrorism: Some Legal and Practical Considerations. FINTECH NOTE/2021/002.
5. Intergovernmental Fintech Working Group. (2021). Position Paper on Crypto Assets. https://www.ifwg.co.za/Pages/About-Us.aspx
6. Mauritius Money Laundering/Terrorist Financing Risk Assessment of Virtual Assets and Virtual Asset Service Providers. (2022). Public Report.
7. Financial Action Task Force (2021). Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, FATF, Paris.
8. Financial Intelligence Centre (2020). Virtual assets and Virtual Assets Service Providers (VASPs): from the Zambian perspective.
9. Financial Action Task Force (2013). Methodology for Assessing Technical Compliance with the FATF Recommendations and The Effectiveness of AML/CFT Systems. FATF/OECD.
10. International Monetary Fund (2021). Virtual Assets and Anti-Money Laundering and Combating the Financing of Terrorism: Some Legal and Practical Considerations. FINTECH NOTE/2021/002.
11. KPMG International Cooperative (2019). Regulation and supervision of fintech: Ever-expanding expectations.

ANNEX: ONE. ADDENDUM:

Preamble

This report has been prepared to provide a consolidation of further technical information to support the survey into the opportunities and threats posed by FinTech product projects. Consequently, the current document should be read in conjunction with the survey report on the opportunities and challenges posed by virtual assets (VAS) and virtual assets service providers (VASPS) in the Eastern and Southern Africa Anti-Money Laundering (ESAAMLG) Region covering up to 31 December 2022.

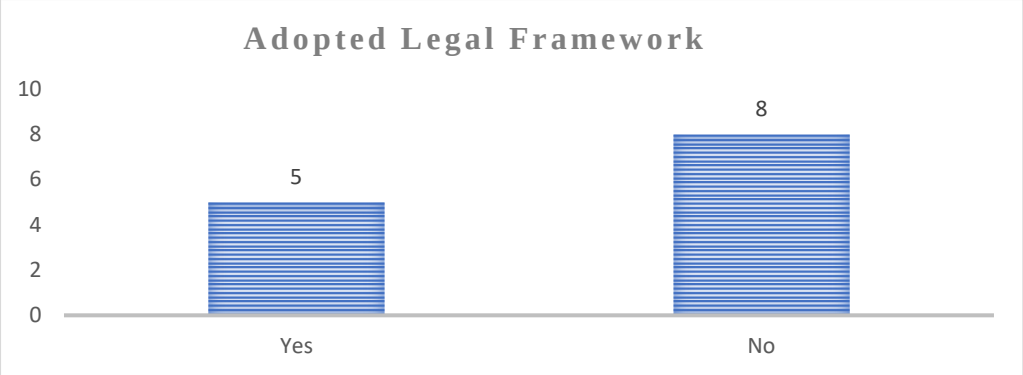
Developments in the region's VAs and VASPs landscape: January - December 2023

Given that some countries may have made progress in the VAs and VASPs landscape in 2023 while the study scope covers the year 2022, the project team believes it is important to note developments from 01 January to 31 December 2023. A supplemental questionnaire, as well as a draft report, were distributed to member countries for feedback. Thirteen (13) countries responded to the supplementary questionnaire. These countries are Angola, Botswana, Eswatini, Ethiopia, Kenya, Lesotho, Malawi, Mauritius, Namibia, Rwanda, South Africa, Uganda, and Zimbabwe, with a 65% response rate.

1. Legal frameworks:

Botswana, Mauritius, and South Africa [10]had already put in place legal frameworks before 2023. Namibia's Parliament passed the **Virtual Assets Act No. 10 of 2023** on 21 July 2023, which took effect on 25 July 2023. Angola drafted a legal framework for VAs and VASPs known as the **Virtual Assets Delimitation Law**, which is currently awaiting Parliament's approval. Eswatini, Ethiopia, Kenya, Lesotho, Malawi, Rwanda, Uganda, and Zimbabwe, have not yet adopted a legal framework governing VAs and VASPs in their respective jurisdictions.

[10] VASPs are regulated under existing FAIS and FIC Acts. There is no bespoke legal framework.



2. Guidelines:

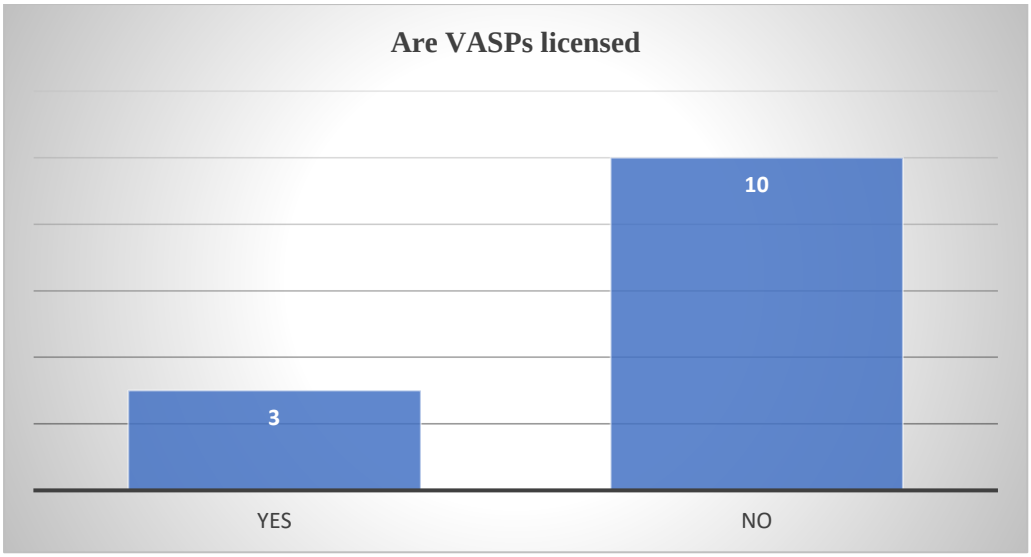
With the exception of Namibia, none of the countries have issued any new guidelines in 2023. Angola, Botswana, Mauritius, and South Africa had issued AML/CFT/PF guidelines for VAs or VASPs prior to 2023.

3. VA activity:

Eleven (11) countries, namely Angola, Botswana, Kenya, Lesotho, Malawi, Mauritius, Namibia, Rwanda, South Africa, Uganda, and Zimbabwe have confirmed VA activities and VASP operations in their respective territories. Eswatini and Ethiopia have not reported any VA activities or VASP operations.

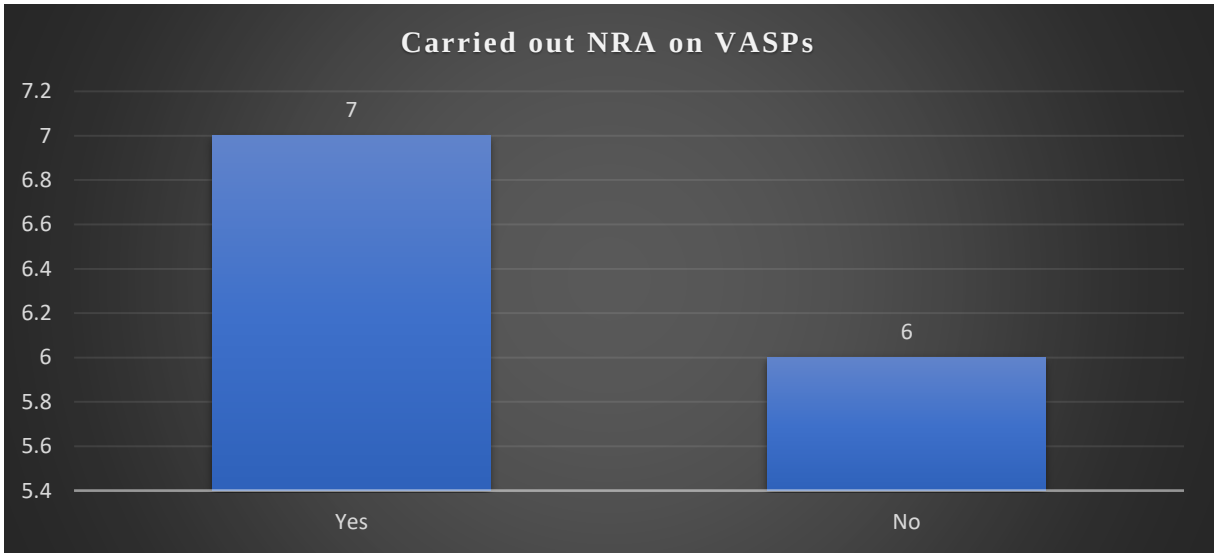
4. VASP Licensing:

In addition to the two licensed VASPs, Botswana licensed a third one in 2023. Mauritius granted eight (8) VASP licenses and South Africa granted through the FIC registered 87 crypto asset service providers and it's still yet to license them under the FSCA.



5. VA and VASPs Risk Assessments:

Seven (7) countries, namely Botswana, Eswatini, Ethiopia, Kenya, Mauritius, Namibia, and South Africa have completed their National Risk Assessments (NRAs) for VAs and VASPs. Two (2) countries; Angola and Zimbabwe launched their NRAs in 2023 and are still in progress while four (4); Lesotho, Malawi, Rwanda and Uganda are yet to complete the NRA on VAs and VASPs.



6. VAs and VASPs cases:

Mauritius, Namibia, Rwanda, and South Africa have reported cases of VAs and VASPs. Mauritius recorded 12 cases; Namibia recorded 488 STRs; Rwanda recorded one case and South Africa recorded 27 cases. in 2023.

Namibia reported STR-related illicit use of VAs for money laundering, which has been investigated but not yet resolved.

None of the member countries that responded have frozen, seized, or confiscated proceeds of crime related to VA activities, and none of the member countries have imposed any sanctions related to VAs and VASPs.

7. VAs and VASPs trainings:

Ten (10) countries; Botswana, Eswatini, Ethiopia, Kenya, Malawi, Mauritius, Namibia, Rwanda, South Africa, and Zimbabwe have conducted or received training on VAs and VASPs. However, three (3); Angola, Lesotho, and Uganda are yet to receive training on VAs and VASPs.