REPUBLIC OF SEYCHELLES

# ML/TF OVERALL NATIONAL RISK ASSESSMENT FOR VA & VASPS

Prepared by

BDS Forensics

July 2022

# Acknowledgements

*This report was written by Mr Danny Sanhye of BDS Forensics, UK, for the Seychelles Financial Services Agency to be used by the government to decide on policies regarding Virtual Assets and Virtual Assets Service Providers and comply with the FATF recommendations. The author would like to thank Mr Patrick Payet - Secretary of State, Mr Damien Thesee, Chief Executive Officer of FSA and Mr Randolf Samson – Director of AML/CFT Unit of FSA, for their support throughout this project. Special thanks also to the working group's participation for their valuable contributions to making this project possible.*

# Table of Contents


**ACRONYMS** ..... **4**

**LIST OF TABLES AND CHARTS** ..... **5**

**FOREWORD BY THE SECRETARY OF STATE** ..... **6**

**EXECUTIVE SUMMARY** ..... **7**

**PART 1 BACKGROUND** ..... **9**

*Introduction* ..... *9*
*The Current State* ..... *10*
*World Bank Methodology* ..... *13*
*The Scope* ..... *16*
*The Overall National Risk Assessment (ONRA) Process* ..... *18*

**PART 2 THE VA AND VASPS ECOSYSTEMS** ..... **20**

**A. THE VA LANDSCAPE IN SEYCHELLES** ..... 20
**B. ML/TF RISKS ASSOCIATED WITH THE VA AND PLATFORMS** ..... 22
**C. VASPS TRACED IN SEYCHELLES** ..... 24
**D. CONCERNS AGAINST THE ENTITIES** ..... 27
**E. OTHER PERCEIVED RISKS** ..... 28

**PART 3 VA AND VASP** ..... **30**

**THREATS AND VULNERABILITIES** ..... **30**

**A. THE OVERALL THREAT LEVEL** ..... 30
*Threats Analysis* ..... *32*
**B. THE OVERALL VULNERABILITY** ..... 41
*Assessing VASPs (Intermediate and Input Variables)* ..... *42*

**PART 4, THE ML/TF MITIGATION MEASURES FOR VA AND VASP** ..... **46**

*The Overall Mitigation Measures Level* ..... *46*

**PART 5 SECTORIAL ASSESSMENT** ..... **53**

**VA AND VASP INTERACTION** ..... **53**

*The Rationale* ..... *53*
*Banking Sector (High Risk)* ..... *53*
*Non-Banking FI Sector (High Risk)* ..... *54*
*Gambling & Gaming Sector (High Risk)* ..... *55*
*Designated Non-Financial Businesses & Professions (DNFBPs) – (Low Risk)* ..... *56*
*Lawyers and Notaries – (High Risk)* ..... *57*

**PART 6 MAIN FINDINGS** ..... **58**

*Strategic Findings* ..... *58*
*Analytical Findings* ..... *60*

**PART 7** ..... **62**

**APPENDIX 1 – GLOSSARY OF TERMS** ..... 62

# Acronyms

| | |
|---|---|
| AEV | Anonymity Enhanced Virtual Assets |
| AML | Anti-Money Laundering |
| CBS | Central Bank of Seychelles |
| CCC | Cooperation, Coordination and Collaboration |
| CFT | Counter Financing of Terrorism |
| CFTC | Commodity Futures Trading Commission |
| DeFi | Decentralised Finance |
| DOJ | Department of Justice |
| DNFBP | Designated non-financial business and profession |
| ESAAMLG | Eastern Southern Africa Anti-Money Laundering Group |
| FATF | Financial Action Task Force |
| FinCEN | Financial Crimes Enforcement Network |
| FSA | Financial Services Authority |
| FUR | Follow-Up Report |
| IBC | International Business Company |
| ICO | Initial Coins Offering |
| ICSP | International Company Service Providers |
| MER | Mutual Evaluation Report |
| ML | Money Laundering |
| NAC | National Anti-Money Laundering and Countering the Financing of Terrorism Committee |
| NFT | Non Fungible Token |
| NPO | Non-Profit Organisation |
| ONRA | VA and VASP Overall National Risk Assessment |
| PF | Proliferation Financing |
| R | FATF Recommendation |
| RBA | Risk-Based Approach |
| ROC | Registrar of Companies |
| STO | Security Token Offerings |
| TOE | Traditional Obliged Entities |
| TCSP | Trust and Company Service Providers |
| TF | Terrorists Financing |
| VA/VAs | Virtual Assets |
| VASP | Virtual Assets Service Providers |
| WG | Working Group |

# List of Tables and Charts

Figure 1: FATF Publications ..... 10
Figure 2: Components of the ONRA Model for VA and VASP ..... 13
Figure 3: Targeted institutions and sectors for the VA and VASP ONRA exercise ..... 14
Figure 4: Types of VASP ..... 18
Figure 5: VA Traced ..... 20
Figure 6: Categories of VA traced ..... 22
Figure 7: Types of VASP Traced ..... 25
Figure 8: Concerns against the Traced Entities operating as VASPs ..... 27
Figure 9: VA & VASP threat levels from the dimension of the product ..... 30
Figure 10: VA Nature & Profile – Summary of different risk elements ..... 32
Figure 11: Percentage of Total Concerns associated with VASP offering DeFi product ..... 33
Figure 12: Accessibility to Criminals – Summary of different risk elements ..... 34
Figure 13: Percentage of Total Concerns with VASP operating in mining activities ..... 35
Figure 14: Percentage of Total Concerns associated with VASP offering Stablecoins ..... 36
Figure 15: Source of Funding VA – Summary of different risk elements ..... 36
Figure 16: Operational features of VA – Summary of different risk elements ..... 38
Figure 17: Entities flagged by overseas regulators over various concerns ..... 38
Figure 18: Ease of Criminality – Summary of different risk elements ..... 39
Figure 19: Economic Impact – Summary of different risk elements ..... 40
Figure 20: Traced entities operating as VASP in Seychelles ..... 41
Figure 21: Overall VASP Vulnerabilities Exposure Summary ..... 42
Figure 22: Effectiveness of Mitigation - Government Measures ..... 47

# Foreword by the Secretary of State

The Republic of Seychelles continues to be committed to the fight against money laundering and terrorist financing (ML/TF), as well as the financing of proliferation and other related threats to the integrity of its financial system. In this regard, Seychelles has established its first overall Virtual Assets (VA) and Virtual Assets Service Providers (VASP) risk assessment consistent with FATF recommendations to protect its financial system from misuse.

In recent years, VAs have slowly gained legitimacy, and many institutional investors have begun to diversify in opportunities for VA-related investment. The popularity and public adoption of VAs in Seychelles and its ML/TF threats have also grown. Hence, Seychelles' obligation to conduct an overall national risk assessment of VA and VASP has increased in urgency to prevent abuse of its financial system and stay ahead of the curve.

This first VA and VASP ML/TF risk assessment are critical in developing the country's digital financial technology sector as it enters a period of renewed strategy to position Seychelles in this fast-developing area. It is critical to highlight the political commitment of the Seychelles government to uphold the AML/CFT international best practices that have led to the success of having the country removed from the European Union's Money Laundering Blacklist.

Seychelles commits to becoming a frontier of integrity, prudence, and fortitude in preserving its reputation with a fully compliant international financial sector and protecting its citizens.

It is intended that this first VA and VASP Overall National Risk Assessment (ONRA) will not only assess the country's exposures but set directions to have adequate mitigants in place to incite good legitimate VASP businesses to continue to flow in the country. The ONRA reinforces and introduces new areas of assessment, such as the emerging risks related to the rapid development in the use of VAs and the new players providing services connected with it.

The result of the ONRA will guide the country to adopt a cutting-edge framework to regulate activity and to help the financial services industry attract new clients and, in turn, contribute further to Government revenue while incentivising innovative entities to invest and operate from Seychelles at a time where investment is needed the most.

We graciously thank all the stakeholders involved in this assessment exercise and Mr Danny Sanhye from BDS Forensics, UK, for leading this exercise. The results of this ONRA will inevitably lead to pellucid targeted actions, which will build upon the assessed measures to continually improve the resilience of Seychelles' financial systems so that it remains well-guarded from the intent of criminals.

*Mr Patrick Payet*
*Secretary of State & Chairman of NAC*

# Executive Summary

This first Overall National Risk Assessment (ONRA) exercise of Money Laundering and Terrorists Financing (ML/TF) risks of Virtual Assets (VA) and Virtual Assets Service Providers (VASP) for Seychelles is built on a solid understanding of the threats and vulnerabilities of VA/VASP and its ML/TF impact. It provides the Seychelles authorities and private sector the foundation to meet the challenges identified in this study and take appropriate actions at the national and sector level to protect the country, individuals, businesses, and society to stay resilient against the unwanted risks associated with these ecosystems. This ONRA is vital to Seychelles' Government's commitment to meeting AML/CFT international standards and developing dedicated legislation for VA and VASP.

The ONRA assessed Seychelles' overall ML/TF risks of VA/VASP as '**Very High' (90%)**. This rating is explained largely by the unregulated activities happening in the Non-Banking Financial Institution (NBFI) sector, which is a vector of VA/VASP. The rating sets the alarm bells for policy reform in developing and adapting AML/CFT and financial products laws to meet the risks in VA/VASP unregulated sectors and prevent VA's illicit proceeds in the financial world. Many service providers traced to be domiciled or operating from Seychelles are using VA as vehicles for speculative investment, which may be skirting Seychelles' laws concerning AML/CFT, sanctions, and taxation. It also can enable cybersecurity threats and extortion via ransomware, as have been reported in many cases already in the public domain.

The ONRA found that banks' and DNFBPs' direct involvement with VAs has remained limited thus far. But the growing clients' interest and the indirect exposure to VA is '**Very High**' primarily due to weaknesses in existing AML/CFT prevention and detection measures related to traditional AML/CFT, and there is a lack of appreciation of indirect support being provided to peer-to-peer transactions and VASP's activities through fiat currency medium. This interconnectivity requires a proactive, cross-sectoral, and forward-looking approach to regulating and overseeing the emerging VA and VASP ML/TF risks. If left unaddressed, this evolving VA and VASP landscape would see traditional obliged entities relying on an unregulated activity which may trigger systemic ML/TF risks and adversely impact the economy.

Seychelles does not have a VASP licensing regime; the ONRA exercise has traced hundreds of entities operating as unlicensed VASPs in the NBFI sector, providing a mix of functional activities in different types of tokens from Seychelles. Many new VASPs have mushroomed in the country's offshore sector, driven by a lack of bespoke legislation, lack of disclosure and exploiting the infrastructure set for the non-VA ecosystem, which is creating a 'shadow VA financial system' that needs to be brought within the remit of regulations the soonest possible to prevent possible exploitation of customers and spoiling the reputation of Seychelles as a trustworthy financial centre.

The findings of the ONRA shed light on the different types of VASPs and concerns flagged against them by overseas regulators and Interpol. Many VASPs provide privacy coins, Ethereum, Bitcoin and stablecoins, to name a few. They also provide cloud mining services, DeFi exchange facilities and NFT. It also shows that a new set of market participants, consisting of VA exchanges, investment providers and other related activities, have arisen that deserves closer regulatory and supervisory scrutiny. These new intermediaries serve not only

retail clients but also other institutions, such as investment funds, and they should be subject to the same types of regulation and oversight as recommended by the FATF.

## Other Key Findings

1. Inherent cross-border risk – Many unlicensed VASPs operate in Seychelles with different varieties of VA and offer enhanced anonymity facilities. There is a risk that VASPs are being used to bypass sanctions against countries, nationals, and companies.

2. Entities operating as VASP with Concerns – The review of the nature of VASP entities traced in Seychelles with adverse media has unravelled that 38% are VA investment providers and 30% are Exchanges, with the highest risks exposure.

3. Regulatory Arbitrage – Patchy and scanty VA and VASP regulatory development globally is creating opportunities for regulatory arbitrage, and Seychelles may be exposed due to a lack of VA and VASP legal framework to regulate the activities of VASPs. Also, the absence of clarification of the taxation legislation on VA may allow tax dodgers to be domiciled in Seychelles.

4. Business Model – Several entities provide various VASP functional activities in several jurisdictions and offer their products and services globally.

5. Due Diligence – The fiduciary service and the capital and collective investment providers need to do more on KYC and KYCC information to identify IBCs operating as VASPs.

6. Exposure to unsafe VASPs – Although the FSA has issued cautionary notices advising on unrecognised VASPs, according to Cointobuy's analysis, Seychelles' VASPs have a safety ranking of 2.7/10.

7. VASP-related STRs - The number of STRs does not reflect the higher number of VASPs involved in the LEA enquiries, regulatory notices, and adverse media.

8. NFT and Stablecoins – A significant number of the VASPs are offering NFT, which may be for payment purposes, and stablecoins pegged with currency from unknown sources and consideration of financial risk is also unknown to the ONRA. As regulation and supervision of NFTs and stablecoins are nascent or non-existent in many jurisdictions, Seychelles could be emerging as a hub for these activities.

# PART 1
# BACKGROUND

## Introduction

1. This report sets forth the Republic of Seychelles' (Seychelles) risk assessment as recommended under Financial Action Task Force (FATF) recommendation 1 (R)[1] concerning the money laundering (ML), and terrorist financing (TF) risks associated with Virtual Assets[1] (VA) and Virtual Assets Service Providers (VASPs)[2]. The risk assessment was conducted as per the 'Guidance' and the 'Tool' designed by the World Bank.

2. In June 2019, R.15 was revised to include obligations related to VA and VASPs. Since then, the FATF has published various guidance to assist countries in interpreting the R15[3], which is intended to be read broadly and expansively. These new requirements include:

    a. Identifying, assessing, and understanding ML/TF risks associated with VA activities or operations of VASPs.
    b. Requirements for VASPs to be licensed or registered.
    c. Requirements for countries to apply adequate risk-based AML/CFT supervision (including sanctions) to VASPs and for such supervision to be conducted by a competent authority.
    d. As well as requirements to apply measures related to preventive measures and international cooperation to VASPs.

---

[1] 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.

[2] Virtual asset service provider means any natural or legal person who is not covered elsewhere under the 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:

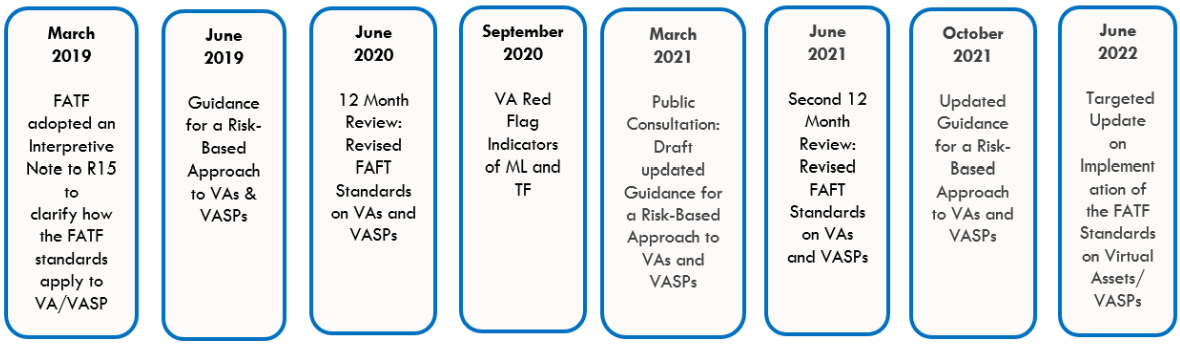
- exchange between virtual assets and fiat currencies;
- exchange between one or more forms of virtual assets;
- transfer1 of virtual assets;
- safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and
- participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.

[3] FATF's Recommendation 15 concerning New Technologies, clearly states that: "Countries and financial institutions should identify and assess the money laundering or terrorist financing risks that may arise in relation to:
(a) the development of new products and new business practices, including new delivery mechanisms, and
(b) the use of new or developing technologies for both new and pre-existing products.
In the case of financial institutions, such a risk assessment should take place prior to the launch of the new products, business practices or the use of new or developing technologies.
They should take appropriate measures to manage and mitigate those risks. To manage and mitigate the risks emerging from virtual assets, countries should ensure that virtual asset service providers are regulated for AML/CFT purposes, and licensed or registered and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations."

3. The FATF clarifies in its guidance[4] that 'the monitoring of new and emerging risks, including the risks relating to new technologies, should inform the risk assessment process of countries and obliged entities and, as per the risk-based approach, should guide the allocation of resources as appropriate to mitigate these risks. Therefore, countries must protect their economies by identifying and mitigating the inherent risks of VAs.

4. The following FATF guidance and the recommendations relating to VA and VASP were considered:

*Figure 1: FATF Publications*




5. As VASPs activities and VA transactions are not constrained by any geographical border and happen to be everywhere in the world and yet can be physically nowhere at all, they present enhanced ML/TF/PF risks. These risks represent a threat to Seychelles financial sector, and hence, this ONRA exercise is to inform policy decision-makers of the extent of the exposure and to put into place a comprehensive AML/CFT legislative and supervisory framework to mitigate the ML/TF risks that might be arising from such business activities. Also, to stay in compliance with FATF standards and ensure that Seychelles' financial centre remains competitive with best-in-class treaties, cooperation, and agreements with other jurisdictions.

## The Current State

6. **Legal Framework**: It is important to note that Seychelles does not have a VASP licensing law and there is no VASP supervision currently in place, and the existing AML/CFT and financial services legislative framework is out of step with the rapid transactional activities happening in the VAs space and digital financial transformation.
   **Note**: *All VASPs domicile or operating from Seychelles are unregistered, unlicensed, unregulated, and unsupervised for AML/CFT purposes*.

[4] https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf

7. In Seychelles, legal tender is considered as cash and non-cash payment methods. Under Part V[5] of the Central Bank of Seychelle (CBS) Act, 2004, notes and coins issued by the Central Bank shall be legal tender in Seychelles by which cheques, payment orders, collection orders, bank cards and other payment instruments as defined in part VII of the Act. Payment instruments outside of this scope are deemed to be illegal. VA falls outside the range of CBS's defined legal tender payment instruments and is not recognised as a means of payment in the country. Nor has the government of Seychelles or the CBS provided an avenue for using VA as legal tender. Internally, Seychelles has no lawful means for using VA as legal tender, and it is also not captured under Foreign Exchange Act 2009 as foreign currency.

8. The country's legal framework is not adapted to address the ML/TF risks and supervision of VA and VASP. Initial Coins Offering (ICO) is not defined as a 'security business' per the definition under the Securities Act, but if it is permitted to be traded online with a Seychelles resident, it may bring ICOs within the regulatory sphere of the Securities Act[6]. Seychelles authorities know that given its international business sector, the country may be vulnerable to VASPs (licensed and unlicensed) from overseas that may be domiciled for tax purposes or operate from Seychelles while doing business globally as VASPs.

9. On the other hand, if VA is qualified as a financial instrument within the current financial legislation, it is not robust enough to compel potential issuers to apply for a licence to conduct activities related to such type of VA. These regulatory gaps are due to legal, technological, and operational specificities associated with VA that may be qualified as a financial instrument.

10. **A considerable surge in VA and VASP activities in Seychelles**: There has been a global surge of interest in VA in the last few years. As a financial centre, Seychelles is exposed primarily to external or incoming ML threats, and VA activities may be happening through service providers that fall outside the scope of the current AML/CFT and tax legislation. Thus, the current situation creates challenges regarding, among other things, prevention, and detection of ML/FT activities, ensuring investor protection, market integrity, energy consumption and financial stability.

11. Amidst the constant price fluctuations in the VA market and its inherent volatile nature, its market size has been growing steadily globally in a new and unregulated environment. The

[5] Central Bank of Seychelle (CBS) Act, S 48. (1) Notes and coins issued by the Bank shall be legal tender in Seychelles by which, subject to the provisions of subsection (2), a debtor is legally entitled to discharge any monetary debt and a creditor is obliged to accept payment of any monetary claim unless a foreign currency is agreed to or contractually stipulated by the creditor and debtor. (2) Subject to the provisions of subsections (3) and (4), a tender of payment of money if made in notes and coins shall be legal tender – (i) in the case of notes, for the payment of any amount; (ii) in the case of coins, for each denomination of coins, for the payment of an amount not exceeding twenty times the face value of that denomination; and (iii) in the case of coins for the payment to and from the Bank of any amount.

[6] https://www.applebyglobal.com/wp-content/uploads/2019/05/Appleby-FinTech-Guide-Seychelles-Final.pdf

size of the global market peaked near $3T in November 2021, with a growth of 1,456 per cent since 2019[7]. Seychelles also witnessed a considerable surge in VA activities, principally in its international business company (IBC) financial services vehicles.

12. **Commissioning the ONRA for VA and VASP**: Seychelles took several measures and initiatives to strengthen its image as a sound and competitive financial centre in the African and Indian Ocean regions. The authorities are also aware of the growing number of VASPs' interest in Seychelles and want to offer a regulated environment for them to operate within its jurisdiction while complying fully with all the AML/CFT obligations.

13. The authorities also want to understand the VA actors operating in Seychelles and the threats and vulnerabilities of their activities. Also, given that many VA actors are new on the market, may not be applying AML/CFT controls and are relatively new to the AML/CFT world globally. The country may be exposed to the service providers operating in Seychelles' jurisdiction due to issues such as poor systems and controls, low price transparency and conflicts of interest and lack of KYC process, with potentially adverse implications for the financial stability of Seychelles' economy as the market grows and VA becomes more widely used.

14. Witnessing the increasing popularity of the use of VA within a short period and the potential of abuse due to the absence of a dedicated regulatory and legislative framework; the Financial Services Authority (FSA) commissioned this ML/TF risk assessment exercise for the Government of Seychelles, to cover all the sectors that may be affected with VA and VASP activities in the country.

15. The ONRA looks at risks of ML/TF, including mitigating the risks to consumers, which may stem from consumers purchasing unsuitable VAs without having access to adequate information, fraudulent activity, and the immaturity or failings of market infrastructures and services. The authority is fully aware of the adverse reputational risks that may impact the jurisdiction due to fraudulent and operational risks arising from unlicensed operators and customers' access to their invested funds.

16. **The objective of the ONRA**: This exercise is expected to contribute to a future-proof economy that works for the country while cashing in on the legitimate benefits of VA activities and its infrastructure.

    a. To enable Seychelles to identify, assess, and understand its ML/TF risks associated with VAs and VASPs.
    b. To pass and implement relevant legislation and use a risk-based approach to combat its ML/TF risks.

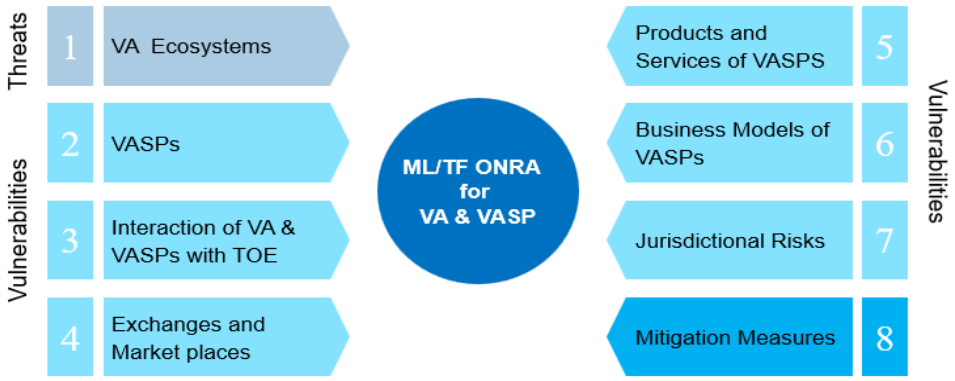
[7] https://ciphertrace.com/crypto-crime-combatting-hacks-thefts-and-fraud-in-the-decentralized-finance-ecosystem/

c. To ensure that the risks are mitigated effectively or contained within an acceptable tolerance threshold, thereby strengthening and improving Seychelles' AML/CTF regulatory framework.
d. To promote Seychelles as a place for good business and attract legitimate actors to invest and operate within a defined legal framework.
e. In the current tax regime in Seychelles, there is limited understanding of whether income derived from VA-related transactions is subject to tax. This first ONRA exercise will help Seychelles better understand the intricacies underlying the operating structures and vehicles through which VA-related activities can be conducted and ultimately provide insights into how to regulate VAs, including the Tax aspects to prevent tax evasion.

## World Bank Methodology

17. The ONRA exercise was led by an international consultant of BDS Forensics from the UK, who designed the World Bank's Risk Assessment tool. The whole exercise followed the World Bank guidance, methodology and model to assess the ML and TF risks for VAs and VASPs in Seychelles. The methodology followed eight components for which specific "input and intermediate variables" are used to understand the ML/TF threats and vulnerabilities of VA and VASP and the existing mitigation measures available at the government, traditional obliged entities and VASP level.

*Figure 2: Components of the ONRA Model for VA and VASP*




18. The risk assessment also considered the 2018 FATF Recommendations, the 2019 revised FATF R15 and the FATF's guidance up to June 2022 for this exercise.

19. The analysis is based on a five-pronged approach which captures the following steps:

a. Carrying out thorough open-source research to trace service providers and VAs that might be in circulation in the country
b. Collecting and analysing suspicious transaction reports related to VA and VASP activities.
c. Official and informal requests to and from a law-enforcement body made to or from foreign jurisdictions and exchanges of information carried out by the FIU to and from overseas FIUs.
d. A process of collecting targeted information from various sectors in Seychelles through bespoke questionnaires to public and private sectors (reporting and not reporting institutions for AML/CFT purposes).
e. Carrying out a thorough review of existing legislation, latest MER and FUR, STR analysis related to VA and VASPs and cases investigated by the Police.

20. A sectoral approach was adopted per the World Bank tool for the risk assessment. The aim was to establish the direct and indirect exposures of the identified sectors to ML/FT risks of VA and VASP. And to identify areas of current need and a roadmap for each authority and sector to establish a solid and effective supervisory, intelligence and investigation framework. As the model looks at the VA and VASPs ML/TF risks from both a horizontal and a vertical approach, various public and private sectors and subsectors were brought into the equation. The sectors and institutions targeted are shown below:

*Figure 3: Targeted institutions and sectors for the VA and VASP ONRA exercise*

f. **Banking sector** – Although VA activities offer an alternative to traditional banking activities, banks can be involved in VA activities directly as investors or indirectly through their products, services, or customers. Because of these exposures and the possibility of providing custody services for customers, including holding unique cryptographic keys associated with accessing private wallets, the banking sector is brought into the exercise. The MER report portrayed this sector as dominant in the Seychelles financial sector, where commercial banks process most financial transactions. The banking sector may be interacting with VA activities as it provides a non-resident business banking platform for the IBCs or through omnibus accounts through the Trust and Companies Service Providers (TCSP), which often provides complex corporate structures that may be involved as a VA service provider overseas.

g. **The non-banking financial sector** – The nature of services and products in the sector makes it attractive to VASPs that could be set up as IBC and take advantage of the absence of a VASP licensing process in the country. Their trading activities in VA may take place on platforms operating outside Seychelles' regulatory perimeter (or, in some cases, failing to comply with applicable laws and regulations) and see the opportunity to harness the unregulated market in Seychelles. Many offshore jurisdictions are trying to reinvent themselves to adapt to new VA economic realities, but although there is caution from the regulator, many types of VA services are already being provided by IBCs and other offshore vehicles domiciled in Seychelles for overseas markets. The ONRA exercise carefully examined the various exposures from different players and considered the attraction of big VASPs operators in Seychelles and the risks they cast on Seychelles' reputation.

h. **Gaming Sector** - The development of VA has spread into the online gambling industry, and AML/CFT supervisors worldwide are not sufficiently equipped to conduct inspections of the online platform. The anonymity and decentralisation of such playing platforms are on the rise. There is also a surge in the popularity of VA games through decentralised apps (Dapps) built on the overburdened and unscalable Ethereum network allowing users to purchase in-game items with Bitcoin, Ether or other VAs and to earn a game-specific VA through gameplay and to withdraw the VA they earned in-game for use elsewhere. Many online gambling services do not require KYC and CDD information; hence, the sector is considered by this ONRA.

i. **DNFBP** - Under the RBA, countries could also consider regulating DNFBPs that send, receive, and store VA but do not provide an exchange or cash-in/cash-out services between virtual and fiat currency. The ONRA exercise looks into this group's awareness level and any possible interaction with VA and VASPs.

j. **Companies and non-profit making organisations** – The ONRA exercise considered if there has been an increase in IT-related companies and the nature of their activities, which could be related to mining, validation, mixing or other nexus VA-oriented support services. The NPO is also considered to see if donations in the form of decentralised and convertible VA such as Bitcoin or centralised convertible form currency are given as donations.

k. **Government Institutions** – Although no VA and VASPs regulatory framework is not in place, Seychelles is already witnessing cases of fraud, ML and other inappropriate activities involving Seychelles-based VASPs. The enforcement action against BitMEX saw Seychelles bore the brunt of some headline-grabbing. The inclusion of critical strategic government agencies and ministries in the ONRA was to look at the coordination or lack of it in the strategy to monitor, control and plan the development of VA and VASPs activities in the country.

## The Scope

21. VA-related activities represent a growing ML/TF threat. FIUs across the FATF global network have seen a rise in the number of suspicious transaction reports and suspicious activity reports related to VAs[8]; this is likely to accelerate once every country starts legislating and enforcing VA and VASP regulations to counter ML/TF. The ONRA considers VAs of decentralised and convertible nature; and centralised and convertible VA, such as WebMoney[9], when no decentralised convertible token is involved. It also considers Stablecoins, which could be backed by fiat currencies, financial instruments, commodities, and other VAs.

22. The VA landscape is evolving rapidly (both centralised and decentralised assets that are convertible to money or another type of VA); hence, VAs outside the FATF definition are not considered for this ONRA exercise. Some VA types excluded from the FATF definition may eventually be revealed to possess attributes of VAs or have financial integrity implications. Hence, ongoing monitoring of the developments in the VA ecosystem will therefore be required by the Seychelles authorities to ensure that all relevant VAs is captured within the AML/CFT framework.

[8] 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

[9] WebMoney is an online payment settlement system established in Russia in 1998. It is one of the largest electronic payments processors in Russia by a number of users, with the company reporting 45 million registered accounts and 300,000 active weekly users in early 2020, and 100,000 stores accepting payments via the system. WebMoney is owned and operated by WM Transfer Ltd.

23. Non-fungible token (NFT),[10] which gained popularity in 2021 and 2022, is a unit of data on a blockchain that is not interchangeable. NFTs[11] provided through an intermediary and used as a means of payment are considered in this exercise.

24. The following critical categories of coins or tokens are considered:
    a. VAs (coins and payment or exchange tokens) as means of exchange but do not meet the definition of e-money as they are not backed by any central authority and have no claim on any counterparty.
    b. E-money tokens or electronic fiat money provided in a stablecoin arrangement
    c. Utility tokens (ICO) that confer various network-associated rights, including granting the holders access to a current or prospective product or service.
    d. Security or asset tokens (STO) that provide specific rights and obligations like specified investments (equity, debt, unit investment).
    e. Hybrid tokens that have multiple characteristics during their holding lifecycle (e.g., having utility token and security token features simultaneously).

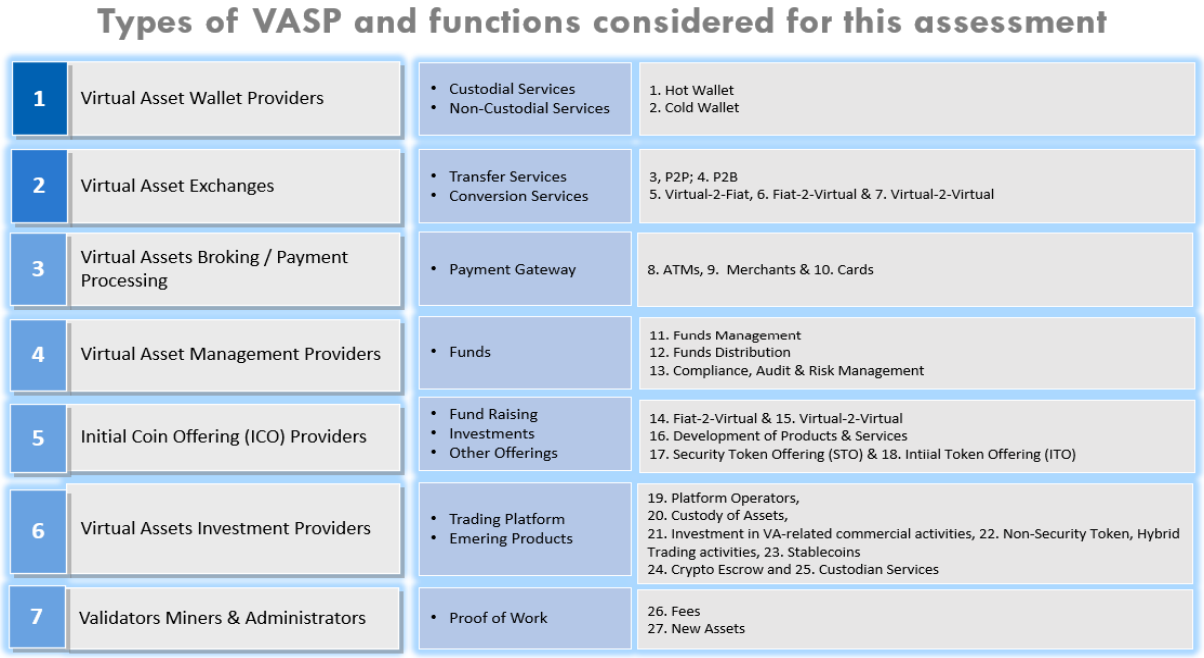
25. The use of VAs by specific providers gave rise to a new class of professionals which the FATF termed as VASPs. The exercise considers all the different types of VASP and any new or existing AML/CFT reporting institutions that could be offering the function of a VASP.

26. Although peer-to-peer transactions are outside the scope of FAFT R15, this exercise considers the threats posed by the types of VA in the peer-to-peer activity as some VA users prefer to handle their VAs without having recourse to a financial intermediary. These sorts of transactions may be attractive to illicit actors. It is worth continuing to monitor these new activities to understand if their actions or business models evolve to that of a VASP and be subject to AML/CFT regulation[12].

27. The World Bank Risk Assessment tool considers seven types of VASPs, offering 12 VASP functions and 27 activities through which there could be potential interaction with different sectors in or outside Seychelles. The questionnaires developed for this assessment cover any area where these 27 activities could interact with the traditional obliged entities[13]. The types, functions and activities considered are:

[10] NFT could be resold amongst related parties or even the same underlying party, which can artificially inflate the value of the asset. Much like tangible physical assets (i.e., artwork and luxury goods), NFTs also have an aura of legitimacy, and there is typically much less application of AML controls on NFTs as compared with cryptocurrencies.
[11] Non-fungible means that it is unique. NFT's exist on the blockchain and hold a unique digital signature, like a certificate of authenticity, that cannot be duplicated. They are 'tokenised'. An example of an NFT would be digital artwork or music.
[12] FATF suggests that fitting into VA/VASP categories is less about the terminology and technology and more about the specific use case.
[13] AMLD4 introduced the term "obliged entity", modifying it from 3AMLD's "designated entity" definition to bring certain financial institutions slipping through the cracks under its regulatory AML/CFT scope. The 5AMLD took it a step further and now also considers certain cryptocurrency-dealing companies and a few other enterprises to be in its scope.

*Figure 4: Types of VASP*




## The Overall National Risk Assessment (ONRA) Process

28. The assessment team consisted of the expert consultant from BDS Forensics and a dedicated working group (WG) comprised of most of the institutions which are part of the National Anti-Money Laundering and Countering the Financing of Terrorism Committee (NAC). The WG was set up where all the sectors and institutions identified relevant for this exercise were bundled into eight sub-working groups.

    a. The representatives of the institutions that were part of the WG were:
        i. Financial Services Authority (Representatives for Capital Market, Trust and Company Service Providers, Casino)
        ii. Central Bank of Seychelles (Representatives covering banks, Bureaux De Change, Development Bank, Payment Service Providers, Credit Union)
        iii. Ministry of Finance; Registrar General and Seychelles Revenue Commission
        iv. Police – Financial Crime Investigation Unit
        v. Financial Intelligence Unit

    b. While the focus of the WG was to ensure a comprehensive representation of various stakeholders in the ONRA, it was also driven by the emphasis on collecting quantitative data from multiple government sources to arrive at a qualitative expert judgement of the

threats and vulnerabilities. This is an essential aspect of the stakeholders and the data collection process.

c. In addition to relying on a combination of quantitative and qualitative data in the analysis stage of this ONRA, several WG discussions were held to analyse and interpret the findings from the data to validate its accuracy before using the same for discussion in filling the World Bank model.

d. The questionnaires covered 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 and DNFBPs, and government ministries to understand to explain the ONRA process and gather feedback on VAs and VASPs activities, where applicable.

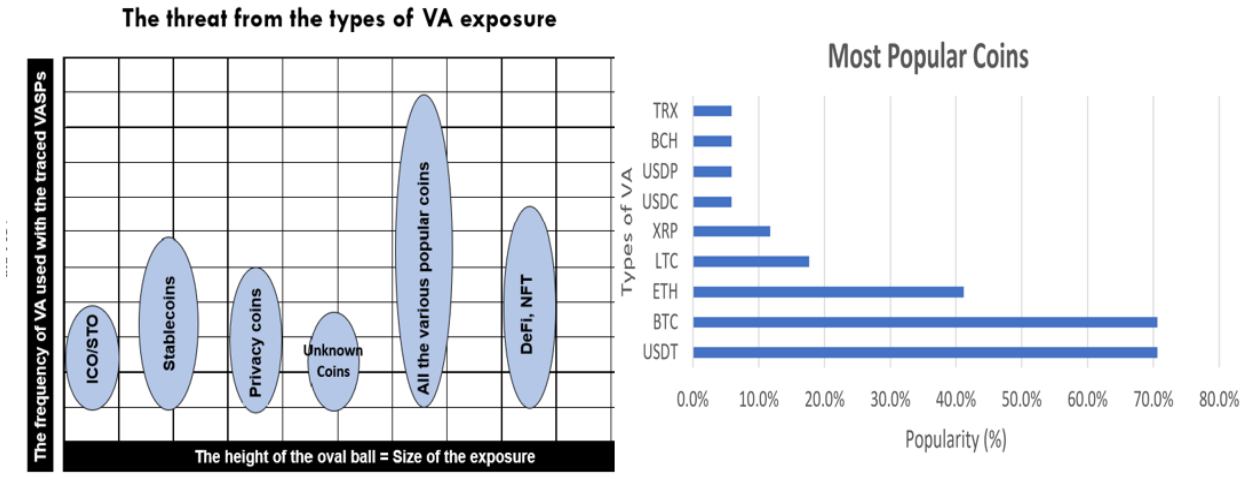
29. The process also follows the three stages defined by FATF as part of the risk assessment process (FATF, 2013, p. 21):
    - Identification – identifying threats, vulnerabilities, and other risk factors
    - Analysis – related to the assessment of these factors
    - Evaluation – considering the assessed risks and determining intervention priorities

# PART 2
# THE VA AND VASPS ECOSYSTEMS

## A. The VA Landscape in Seychelles

30. As VAs are not issued, regulated, or backed by a central authority and VASPs are not licensed in Seychelles, many types of operators could exist on the market. Several types of VA have been traced to VASPs domiciled for tax purposes in Seychelles or using the address of Seychelles. Some are popular household names like Bitcoins 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. It is not a secret that VA-related activity represents a growing ML/TF threat. Financial Intelligence Units (FIUs) across the FATF global network have seen a rise in the number of suspicious transaction reports (STR) related to VAs, and Seychelles' FIU has been very active in dealing with STRs and requests for information from overseas counterparts. This will likely accelerate as more countries start legislating and enforcing AML/CFT compliance on VA activities.

*Figure 5: VA Traced*




31. The VAs are being used as part of ML/TF schemes and are particularly associated with several predicate offences, including fraud and drug trafficking. They are also widely used as a means of payment for illegal goods and services offered online and offline as there is no requirement

to go through an intermediary. Transactions involving VAs have no restriction on the geographic location; hence, a transfer of VA can occur regardless of the country of those seeking to initiate the transaction. Such freedom has triggered widespread recourse to VA. The absence of dedicated VA and VASP law in Seychelles saw numerous VA activities being offered from its location through numerous VASPS. The VA traced contain features of:

32. **Enhanced Anonymity:** Many of the Traced VASPs entities offered enhanced anonymity VAs (AEVs), such as Monero, Dash, and ZCash, which are designed to obscure the links between wallet addresses which could be traced through blockchain analytics. AEVs use obscured blockchains that limit or eliminate the traceability of those assets. The use of AEVs, combined with weaknesses in the AML/ CFT regime by the VASPs operating in Seychelles, may become attractive to criminals to hide their source or movements of funds. AEVs are often exchanged for other virtual assets like bitcoin, which may indicate a cross-virtual-asset layering technique for users attempting to conceal criminal behaviour.

33. **Pseudonymity**: They are pseudonymous as most VASPs associated with VA traced from Seychelles have not yet implemented the 'Travel Rule'. Given the porous KYC attributed to Seychelles-based-VASPs in the Ciphertrace report[14], there is an exacerbation of activities from Seychelles domiciled providers as, for the time being, they do not feel the pressure of establishing the source of funding for the VAs and the identity of the transferer or beneficiary. The lack of KYC may also motivate illicit actors to transfer VAs to exchange companies that offer to exchange VAs for fiat currency or other types of VAs.

> *On February 13, 2020, the Department of Justice announced the indictment and arrest of the alleged administrator of Helix, a darknet cryptocurrency laundering service. According to the indictment, Helix functioned as a bitcoin "mixer" or "tumbler," allowing customers to send bitcoin to designated recipients in a manner that was designed to conceal their source or owner.*
>
> *Source : https://www.justice.gov/cryptoreport - October 2020*

[14] https://ciphertrace.com/2020-geo-risk-report-on-vasp-kyc/ - Seychelles a Potential Money Laundering Heaven 72% of African-Domiciled VASPs are registered in the Seychelles. 70% of Seychelles-domiciled VASPs have bad or porous KYC, totalling 75% of all of Africa's KYC-deficient VASPs, and thereby making the small island country a boon for potential money launderers. Further analysis shows that a majority of the customer base for Seychelles-domiciled VASPs are foreign users, highlighting the nation's money laundering potential. While the Seychelles' Anti-Money Laundering Act 2017 sought to bring more regulation into the country, most VASPs simply "maintain the right" to verify a user's identity for the purposes of complying, without ever actualizing that right. The new AML/CFT Act 2020 and Beneficial Ownership (BO) Act 2020 seek to rectify these deficiencies.

34. **Obfuscation Services**: Several mixing and tumbling[15] services were traced from entities. Criminal actors may take additional steps designed to anonymise VA transactions on several blockchains by using a series of obfuscation services offered by the entities.

## B. ML/TF Risks associated with the VA and Platforms

35. **Myriad of VA**: Various types of VAs have been observed from the Traced VASP entities. Most of them provide the whole gamut of VAs through centralised exchanges or decentralised DeFi involving well-known coins such as Bitcoins to unknown ones or privacy coins. Fiat currency and vice versa are facilitated by using Bitcoin ATMs (ATMs). Decentralised Finance ("DeFi") is another crucial element observed among the threats to Seychelles. While traditional exchanges are focussed on turning fiat currencies into VAs, decentralised exchanges are focussed on turning VAs into other coins and tokens.

*Figure 6: Categories of VA traced*

| *VA Type* | Inherent Risk |
|---|---|
| *Anonymous/Privacy VA* | Very High |
| *Pseudonymous Payment VA* | High |
| *Platform Tokens* | High |
| *Utility Tokens* | Medium-High |
| *Stablecoins* | Medium-High |
| *Metaverse* | Medium-High |
| *DeFi* | Very High |
| *NFT* | High |
| *Security Token* | Medium |
| *Centralised Convertible* | Very High |
| *Hybrid Trading Platform Token*[16] | Medium-Low |

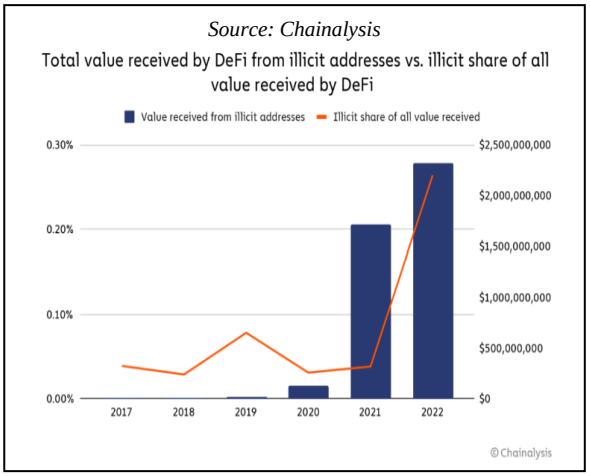
36. **Stablecoins**: Several VASPs were traced offering stablecoins. It is not known if the Stablecoins arrangements have gone through regulatory scrutiny elsewhere on its design of the transfer of value system and the governance around the counterparties, cyber, and reputational risks. The Stablecoin arrangements operating in a cross-jurisdictional context

[15] A "mixer" or "tumbler"—i.e., software services that mix otherwise traceable virtual assets with other funds, frequently including funds received from other customers, before sending it to the requested recipient address; (2) engage in "chain hopping," which involves the rapid swapping of one virtual assets for another; and (3) engage in "off-chain transactions," which involves the transfer of private keys from one person to another without recording the transaction on the blockchain.

[16] Their function has attributes of stablecoins, and they also confer discounts or other benefits for users on their respective platforms. As there is a tendency for them to remain within the ecosystem of their platform, and not move across platforms, the relevant platform has high potential visibility into the users and transaction behaviours, including ability to detect suspicious activity on a disclosed basis. A user could convert from one VA to a Trading Platform Token to another VA within the same exchange.

may have heightened legal risk[17] regarding the legal underpinning of the ownership or transfer of assets and its settlement. There is also a perceived risk concerning compliance with sanctions, given the capability of operating as cross-border payments. Since more complexities are involved, ML/TF risks are typically higher in the cross-border context. The ML/TF risks are higher when peer-to-peer transactions can be performed in some stablecoin arrangements.

37. **DeFi**: According to Chainalysis[18], '*DeFi protocols are the go-to hacking target'.* The value stolen from DeFi protocols has been trending since the beginning of 2021, reaching its highest levels in Q1 2022. Many Seychelles domiciled VASPs are offering DeFi services. These financial instruments and other products allow participants to lend or borrow funds from others, speculate on price movements on assets using derivatives, trade VAs, insure against risks, and earn interest in savings-like accounts. DeFi presents opportunities for criminal exploitation and offers a mechanism for laundering money without applying KYC provisions.




38. According to FATF 2022 12-month review[19], it is reported that DeFi is increasingly used for money laundering, and the percentage of funds sent from illicit wallets to DeFi protocols compared to centralised exchanges is increasing; DeFi received 17% of all funds sent from illicit wallets in 2021 (15% in 2020) Crypto Crime Report 2022. Seychelles is exposed to ML risks, as there has been a rise in DeFi protocols for funds sent from illicit addresses over the last two years.

39. **Non-fungible tokens (NFTs):** The NFT traced allows specific individual items to be sold and traded on the blockchain[20]. NFTs are digital high-value goods that use blockchain to record their ownership. The tokenisation of these assets makes buying, selling, and trading them more efficient. NFT markets may be vulnerable to money laundering schemes reflective of trade-based money laundering (TBML), which involves using the purchase of goods and services of large volume to layered illicit proceeds. TBML schemes have been rife in the

[17] https://www.bis.org/cpmi/publ/d187.pdf
[18] https://blog.chainalysis.com/reports/chainalysis-web3-report-preview-safety-compliance-defi/
[19] https://www.fatf-gafi.org/media/fatf/documents/recommendations/Targeted-Update-Implementation-FATF%20Standards-Virtual%20Assets-VASPs.pdf
[20]Like Ethereum or Bitcoin, NFTs are a store of value, but unlike these coins, these digital goods can have a high value. NFT offered the opportunity to criminals to stack a large amount of value in a unique item.

physical art and antique world, and the NFT space is also vulnerable to similar risks. NFTs offer a new potential method of money laundering using VAs and presenting opportunities for fraud and manipulation.

40. **NFT Platforms**: These providers act as intermediaries for importing, minting or trading the assets representing proof of ownership of artworks or collectables. The risk associated with unregulated NFT platforms is that criminal actors can hack into user accounts on NFT marketplaces and transfer NFTs to their own accounts. After transferring the NFTs, the hacker can quickly sell the stolen token(s) and attempt to launder the proceeds

41. **Privacy Coins:** Other types of coins traced are Privacy Coins (Monero) which are privacy-focused that encrypt their transactions using zero-knowledge proofs or similar private technology. The FATF's report[21] on virtual assets red flags draws special attention to unlicensed and non-compliant exchanges that offer privacy coins as an area of specific and significant risk

42. **Metaverse Tokens**: This type of VA has also been traced. It is a unit of currency used to make transactions within the metaverse ecosystem, and while some metaverse tokens can solely be spent within the metaverse world, some are also available on well-known exchanges. It is a self-contained virtual ecosystem where the sale and purchase of goods, services and other complex social interactions can be facilitated by VAs. These innovations have attracted the likes of big banks and other institutional firms engaging in the VA space.

43. **Mining Pool**: Mining is the process of validating and adding transactions to the blockchain in exchange for newly generated VA. There is a reliance on several individual miners of unknown locations providing their own computing power resources. Although blockchain analysis could be used to trace the path of any given coin and ensure that it came from an ethical miner, VAs passing through exchanges that offer the services like 'chain hopping' and other commingle activities to obfuscate the original source would be challenging to trace.

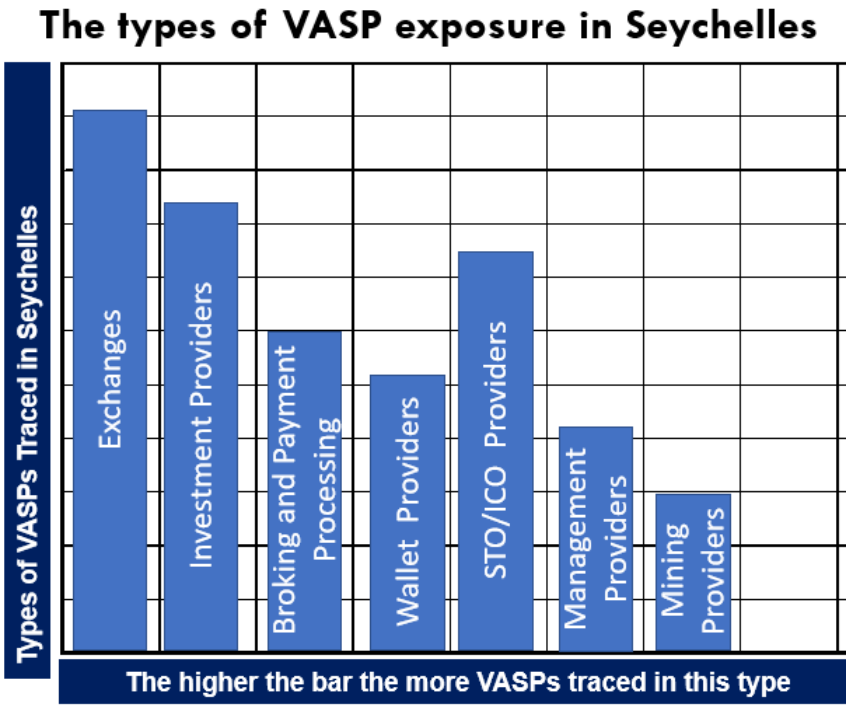
## C. VASPS Traced in Seychelles

44. To understand the VA landscape, the ONRA looks at the VASPs operating in Seychelles and the types of VA they are dealing in. According to FSA's[22] 2020 annual report, the cumulative number of international business companies (IBCs) is 224,525, but the number of active IBCs to date is around 50,000. The FSA faces challenges in supervising these many IBCs and assessing AML/CFT requirements to comply with data protection and privacy rules. Therefore, much emphasis was placed on this sector to trace players operating as VASPs.

[21] https://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-Red-Flag-Indicators.pdf
[22] https://fsaseychelles.sc/media-corner/annual-report

45. More than 500 VASPs have been traced to be operating in the offshore sector (Fiduciary, Capital Market and Collective Investment and Insurance) were traced through Web-scraping, open-source research, STRs, overseas requests made to the Police, and disclosure through the ONRA questionnaires. These companies are either domiciled in Seychelles or using a Seychelles address and linked to virtual assets activities and ancillary services, and more than a third of them were found to have been flagged over regulatory warnings or under overseas Law Enforcement Agencies (LEA) enquiries and other adverse concerns linked to scams or poor controls to identify their customers (KYC) or diligently follow AML/CFT related processes. Appendix 2 describes the activities of each type of VASP.

*Figure 7: Types of VASP Traced*




a. **VA Exchanges** – Exchanges may occur between one or more forms of virtual assets or between virtual assets and fiat currency. The VA exchanges provide a digital online platform to facilitate virtual asset transfers and exchanges. Exchanges can be, for example, online, platform-based or in-person, such as trading platforms that enable peer-to-peer or kiosk-based exchanges. However, many Traced entities are not dedicated VA exchanges as many of them also provide many other types of functions.

b. **VA Investment Providers** - Providing an investment vehicle to enable investment in or purchase of virtual assets (that is, via a managed investment scheme or a derivatives issuer providing virtual asset options, or via a private equity vehicle that invests in virtual assets).

Typical services include platform operators, custody of assets; investment into VA-related commercial activities; non-security tokens (which are not protected by securities laws), and hybrid trading activities (which display hybrid features). They also provide Stablecoins, VA escrow services and VA custodial services.

c. **ICO Providers** - Typically involve issuing and selling virtual assets to the public, and they might involve participating in and providing financial services relating to the ICO. They also perform fundraising for ICOs through investments through fiat converted to new virtual assets or other virtual currencies. The investments could also be used for developing products and services or as Initial exchange offerings (IEOs) or STO could also be offered.

d. **VA Broking/Payment Processing** - VA brokerage services facilitate the issuance and trading of VAs on behalf of a natural or legal person's customers. They also provide order-book exchange services, which bring together orders for buyers and sellers, typically by enabling users to find counterparties, discover prices, and trade, potentially using a matching engine that matches the buys and sells orders from users. Brokerage companies are not as safe and legit, often involved in scams through investment services for people seeking to trade stocks, options, and other forms of securities.

   Some advanced trading services allow users to buy portfolios of VAs and access more sophisticated trading techniques, such as trading on margin or algorithm-based trading.

e. **VA Wallet Providers** -Virtual Asset Wallet Providers, provide storage for virtual assets or fiat currency on behalf of others. It then facilitates exchanges or transfers between virtual assets and fiat currency. They include Custodian Wallet and the Non-Custodian Wallet.

f. **VA Assets Management Providers** – They focus on VAs as the underlying assets, typically involving fund management, fund distribution, audit, and risk management.

g. **Validators/Miners/Administrators** - Some jurisdictions would classify validators/miners as VASPs when the user engages as a business in issuing (putting into circulation) a VA and redeeming (withdrawing from circulation) such VA. Institutional units that validate and confirm the transactions are called "miners." Miners are considered bookkeepers or distributed ledger updaters in a virtual asset transaction. A transaction can only be regarded as 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). Remote hosting or cloud mining services for mining services were traced among the IBCs in Seychelles.

# D. Concerns against the entities

46. Several international investigations into VAs trading platform scams have been traced back to Seychelles. A VA intelligence company conducted a review of VASPs in 80+ countries and suggested in their report[23] that 72% of African-Domiciled VASPs are registered in Seychelles, 70% of Seychelles domiciled VASPs have bad or porous KYC, totalling 75% of all of Africa's KYC-deficient VASPs, and **thereby making Seychelles a preferred destination for potential money launderers**. The same report also assessed the outflows of Seychelles-domiciled VASPs and found that 96% of the exchange-to-exchange BTC volume was cross-border, with 51% of the total cross-border volume being sent to VASPs with demonstrably weak KYC.

*Figure 8: Concerns against the Traced Entities operating as VASPs*

**Domiciled in Seychelles or using Seychelles address**

| TYPES OF VASPS TRACED | % With concerns |
|---|---|
| VA EXCHANGES | 30% |
| VA INVESTMENT PROVIDERS | 38% |
| INITIAL COIN OFFERING (ICO) PROVIDERS | 24% |
| VA BROKING / PAYMENT PROCESSING | 20% |
| VA WALLET PROVIDER | 26% |
| VA MANAGEMENT PROVIDERS | 13% |
| VALIDATORS / MINERS / ADMINISTRATORS | 21% |

**Sources**

- ✓ Web-scraping and open-source research
- ✓ ONRA Questionnaires
- ✓ Searching for online advertising and solicitation for business;
- ✓ Information from industry circles (channels for receiving public feedback)
- ✓ FIU, LEA, Regulators
- ✓ Non-publicly available information,
- ✓ Law enforcement and intelligence reports; as well as other investigative tools or capabilities.

[23] CipherTrace, Cryptocurrency Crime and Anti-Money Laundering Report – February 2021. https://ciphertrace.com/wp-content/uploads/2021/01/CipherTrace-Cryptocurrency-Crime-and-Anti-Money-Laundering-Report-012821.pdf

## E. Other Perceived Risks

47. **Darknet Market**: The VASPs in Seychelles could be operating on the darknet market. These commercial websites accept VAs for sale and acquire illicit and illegal material using anonymised browsers like Tor and I2P.

> *In October 2019, the U.S. Department of Justice indicted 23-year-old South Korean national. Jong Woo Son, who operated a dark website exclusively devoted to CSEM. Welcome to Video, commonly referred to as "WTV," began operating in the summer of 2015 and as of around March 2018 had over 200,000 unique video files on its server.7 WTV customers created free accounts on the site and downloaded videos by redeeming points. Customers could purchase points with Bitcoin or earn them through new customer referrals or by uploading their own videos depicting CSEM. Users that created an account with the website received a unique Bitcoin address. From the site's inception in mid-2015 through around March 2018, WTV received at least 420 BTC through at least 7,300 transactions, worth over $370,000 at the time of the respective transactions.*
>
> Source: Cryptocurrency and the Trade of Online Child Sexual Abuse Material
> https://cdn.icmec.org/wp-content/uploads/2021/03/Cryptocurrency-and-the-Trade-of-Online-Child-Sexual-Abuse-Material_03.17.21-publish-1.pdf

Many VA-related crimes investigated by LEA worldwide relate to the Darknet market. The marketplaces on the darknet allow criminals worldwide to connect in an unregulated and unmonitored environment with greater anonymity. Examples are Empire, Point, and Silk Road 3.1.

48. **Unregulated ICO/STO Market**: Buying and selling VAs are outside the remit of the Seychelles regulator and present opportunities for fraudsters to take advantage of this market by offering investments in VAs. Unregulated VA providers may manipulate software to distort prices and investment returns to incentivise buying non-existent VAs. The ICOs can take different forms, such as a share in a firm, a prepayment voucher for future services or, in some cases, may be fictitious.

49. **DeFi Platform**: DeFi platforms[24] were uniquely vulnerable to attack and lost roughly 33% of all VAs stolen in 2020 and were victims in nearly half of all individual attacks. Cybercriminals stole over $170 million worth of VA from DeFi platforms.

> *In May 2021, one or more hackers exploited a code vulnerability to steal over $30 million worth of cryptocurrency from the protocol — mostly its native SPARTA token. The hacker then converted much of those funds into any ETH and any BTC.*
>
> *Source : https://blog.chainalysis.com/reports/2022-crypto-crime-report-preview-cryptocurrency-money-laundering/*

50. **Business Model:** Most of the entities traced as operated from Seychelles are IBC, offering many functional services globally through the internet, and have a complex set-up, where they have either physical or virtual presence in multiple jurisdictions. Many VASPs traced lack regulatory oversight on their exchange activities, ICO offerings and payments services and are operating without significant regulatory scrutiny on their products and services. The providers have

[24] Who's Who on the Blockchain? Mapping the Key Players in the Cryptocurrency Ecosystem - Chainalysis

numerous VA spanning from stablecoins to DeFi, different ICOs and non-fungible tokens (NFTs). There is a risk of their continuous growth as an unregulated sector in Seychelles and their likely interlinkages with other parts of the financial system in the country. The business model is challenging when one entity involves in various VA operations through joint ventures or other non-incorporated entities, such as Trust structures and even individuals as owners of key portions or assets of the business.

51. **Jurisdictional Concerns**: Many of the entities traced are within the offshore sector, registered as IBCs and the capital market, and not licensed in Seychelles or overseas as VASP. Their domiciliation in Seychelles is for tax purposes: they have no physical presence in the country and may not meet the "meaningful mind and management" test, given the nature of IBC's registration. The FATF's first 12-month Review Report of June 2020 reported that many entities seem to have adopted a decentralised structure with no obvious home jurisdiction. Seychelles Fiduciary Providers' addresses seem to be used for that purpose.

# PART 3
# VA AND VASP
# THREATS AND VULNERABILITIES

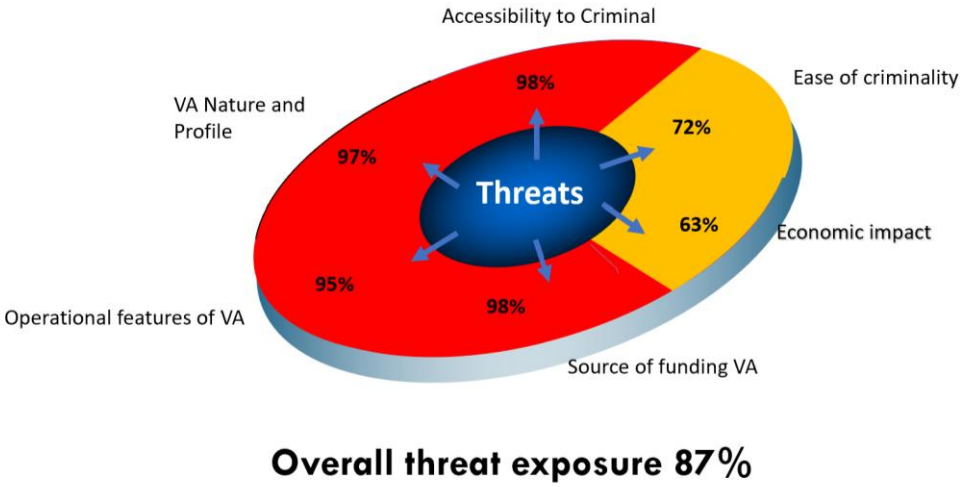
*This part looks at the Threat and Vulnerability of both VAs and VASPs. The approach uses a unique and relatively complex logic based on information gathered, weighted averages, and built-in formulas in the assessment model. The assessment considers intermediate and input variables of threats and vulnerabilities from a domestic and international perspective ranging from large multinational VA providers with extensive customer bases to small VA businesses and a host of different types of VAs.*

## A. The Overall Threat Level

52. The overall ML/TF threat of VA and VASP in Seychelles is **Very High (87%)** due to the significant number of VASPs traced and the large varieties of VA within their operations. Most operators are established as offshore entities in the NBFI sector, mainly through the capital, securities, and IBC market. The number of VASPs domiciled in Seychelles in the global business is unknown due to the poor KYC of the fiduciary service providers. All the so-called domiciled VASPs are incorporated as IBCs or are existing firms in the capital market with complex structures.

53. The figure below shows six intermediate variables for threats of VAs and VASPs. These inherent ML/TF risks are assessed before implementing any controls or mitigation measures.

*Figure 9: VA & VASP threat levels from the dimension of the product*



54. The threat level is exacerbated by the lack of dedicated legislation to regulate and supervise the VA activities of these providers. Also, the opacity that lies in the UBOs of the VASP entities as they are incorporated through nominee shareholders and corporate directors. Seychelles does not have a fully up-and-running UBO register to verify the true identity of all relationships and operations related to VA and VASP. Currently, the law does not require that sufficient information be provided on the nominators, but this is somewhat mitigated by the fact that TCSPs are reporting entities for AML/CFT purposes and have an obligation to report STRs to the FIU and are obligated to collect the full beneficial ownership information from their clients.

55. As per the Ciphertrace[25] report, Seychelles is at the centre of the whole of Africa, with the most VA activities and with the poorest KYC VASPs entities. The report advocated that 96%of global exchange-to-exchange BTC volume was cross-border, with 42% of BTC from Seychelles' VASPs with weak KYC. The gravitation toward Seychelles may be due to the lack of capacity among supervisors, investigators and intelligence bodies to adequately deal with ML/TF cases and its offshore services.

56. Seychelles' Very High level of ML/TF threats to VA and VASP is also due to the nature of the products and the financial secrecy that prevails in the international businesses. Although Seychelles was removed from the European Union's official blacklist of tax havens, its inherent threat still persists since there is still a lack of robust financial and human resources, adequate training and sophisticated technology-based systems for combating ML/TF risks associated with VA and VASP. The lack of capacity of prosecutors and investigators for VA ML/TF matters and the absence of a national strategy to combat VA ML/TF also contribute to Seychelles' very high threat level.

57. Despite these high numbers of VASPs, the investigations and prosecutions successfully tried two cases connected with VA[26]. The FIU, on the other hand, received an increased number of VA-related defensive STRs, as the reports were related to mainly three or four significant VASPs exchange for which adverse information on them was already in the open source.

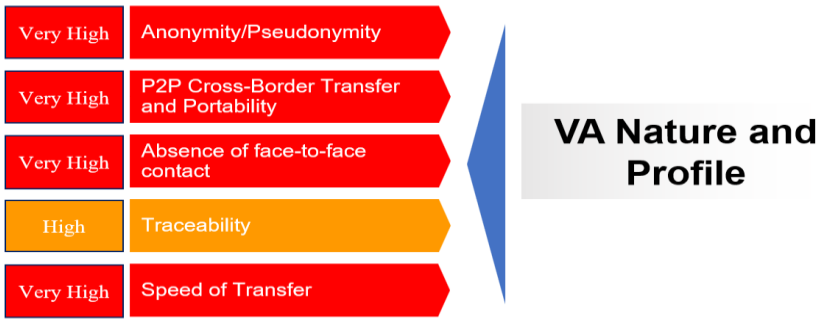
[25] https://ciphertrace.com/wp-content/uploads/2021/01/CipherTrace-Cryptocurrency-Crime-and-Anti-Money-Laundering-Report-012821.pdf- page 23

[26] Stolen VAs were identified in wallets in possession or under control of four VA exchanges registered in Seychelles. In the other case, 18,943,721.94 counterfeit tokens (with an approximate FIAT currency value of USD $ 11.36 million) were deposited onto the KuCoin virtual currency exchange which is registered as an IBC in Seychelles.

## Threats Analysis

### a. VA Nature and Profile

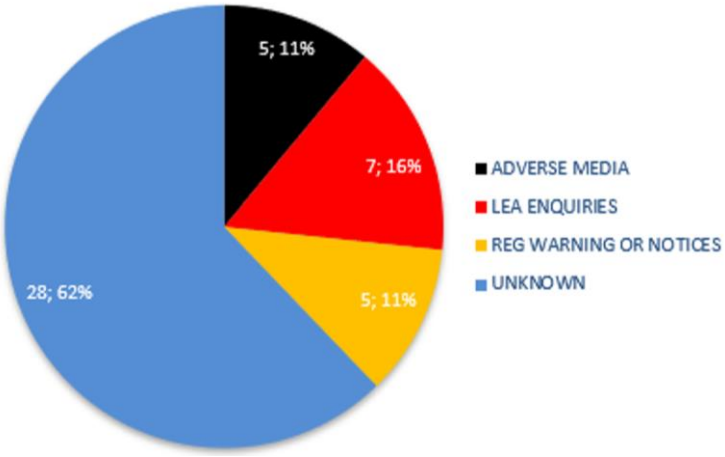
*Figure 10: VA Nature & Profile – Summary of different risk elements*




58. **Anonymity and pseudonymity (Very High)** – Because of significant variability in the definition of the regulatory perimeter across jurisdictions and no common understanding of the entities and activities, many countries are at different stages of legislating and enforcing VA regulations. The absence of legislative directions from Seychelles saw several providers using IBCs to provide a whole host of VA products and services. These gaps and loopholes in Seychelles and the global regulatory framework also provide a platform for criminals to take advantage of VA's anonymity and pseudonymity. This ONRA has unravelled NFT, privacy coins, different decentralised convertible tokens and the use of mixing services offered by Seychelles.

59. **Peer-to-Peer cross-border transfer and portability (Very-High**) – The unique characteristics of VA observed, coupled with the international financial activities in Seychelles, may offer a conduit of cross-border transfer to high-risk jurisdictions as an input asset or output asset, or in the form of payment to individuals and entities who would not use the traditional system to conduct such transfer. The ONRA has not uncovered activities at the peer-to-peer, but there is a threat that VA transfers could be happening on the internet outside the scrutiny of Seychelles authorities in payment forms across frontiers by the high-profile foreign individuals or nationals from high-risk countries living and operating businesses in Seychelles. More extensive assessment needs to be carried out by Seychelles authorities on the mechanism to transfer the VA's ownership (for example, centralised, peer-to-peer, decentralised, DeFi) and control over the ledger (for example, open to the public, open to specific parties, close to a limited number of authorised parties). These would assist in managing these threats and prevent the country from harbouring sanction circumvention.

*Figure 11: Percentage of Total Concerns associated with VASP offering DeFi product*




60. **Absence of face-to-face control (Very-High)** – The absence of face-to-face is inherent in Seychelles' international financial activities, and taking into account the volume of transactions highlighted in the Ciphertrace report, the degree of anonymity/pseudonymity and the peer-to-peer transferability without bespoke control, this input variable is by default rated as very high. There is a very high threat that non-face-to-face activities could lead to transactions with high-risk individuals or entities, transfer of value, or undertaking third-party funding through virtual exchanges. Hence, VA-related activities represent a growing ML/TF threat.

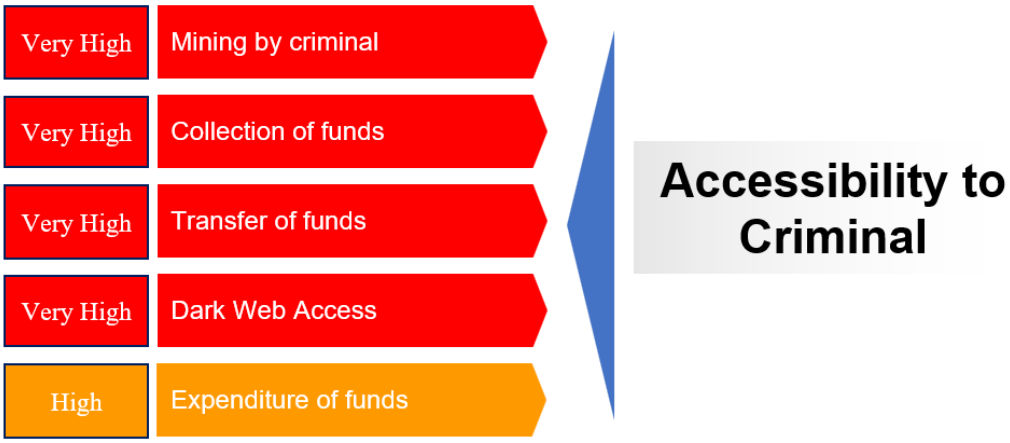
61. **Traceability (High)** - Blockchain technology provides transparency and traceability for all transactions; nevertheless, an actor's true identity may never be known if the travel rule is not implemented. Although there are no obligations from Seychelles authorities on the unlicensed VASPs to implement the 'travel rule', there are several attributes that law-enforcement agencies may use to trace users and uncover anonymity. These could be through unique Internal Protocol (IP) addresses and transaction history through blockchain forensics. VAs can be analysed through different criteria to understand their ML/TF risks. Nevertheless, VAs carry significant ML/TF threats due to the unavailability of dedicated tools at Seychelles' disposal to effectively and efficiently traced VAs on the blockchain.

62. **Speed of transfer (High)** – Although transactions involving VAs are, in most cases, quickly verified and permanently recorded on distributed ledgers publicly, the ability to send large volumes of value across borders is very much easier than through traditional financial institutions. With no control over the size and value than can be transferred, the system is vulnerable to abuse by criminals or unscrupulous actors. Also, the vulnerability is enhanced due to the lack of tools and training for law enforcement in Seychelles to trace a financial

transaction through a public ledger. The lack of potential to trace, monitor, and detect suspicious criminal activity encourages 'speed transfer' by service operators. The threat of evading investigations and probing from competent authorities is high.

## b. Accessibility to Criminal

*Figure 12: Accessibility to Criminals – Summary of different risk elements*




63. **Mining by Criminal (Very-High)** – VA markets is underpinned by various forms of intermediation without any KYC obligations that are outside the radar of regulators and law-enforcement agencies and offer an attractive environment to criminals to exploit vulnerabilities in the ecosystems. The rise of centralised mining pools of VA permissionless blockchains gave rise to cryptojacking[27]. The ONRA shows that unlicensed VASPs offering applications for mining globally and in Seychelles are a growing threat, especially with the lack of computer security awareness and the lack of dedicated internet security policing by competent authorities. For example, the ONRA found little awareness of the synergy between computer security and VA activities in many public and private institutions in Seychelles.

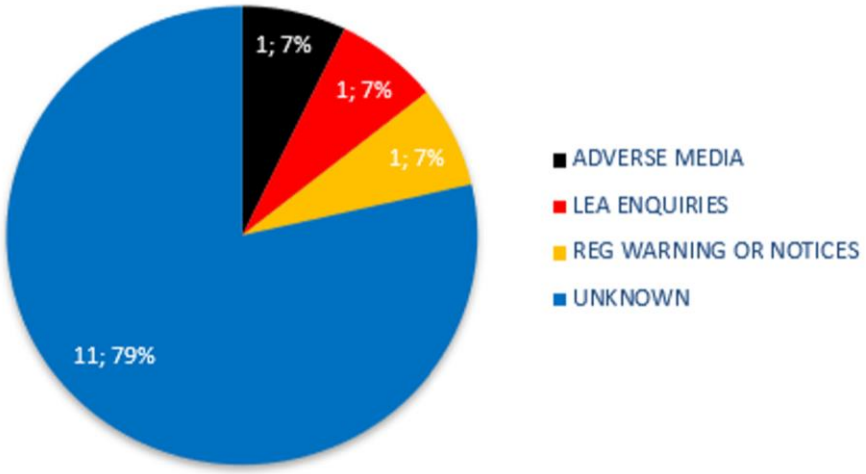
    It should be noted that many cryptojacking enterprises are taking advantage of the scalability of cloud resources by breaking into cloud infrastructure and tapping into an even broader collection of computing pools to power their mining activity[28]. "Today, attackers are targeting

[27] Cryptojacking is a type of cybercrime where a criminal secretly uses a victim's computing power to generate cryptocurrency. This usually occurs when the victim unwittingly installs a programme with malicious scripts which allow the cybercriminal to access their computer or other Internet-connected devices, for example by clicking on an unknown link in an e-mail or visiting an infected website. Programmes called 'coin miners' are then used by the criminal to create, or 'mine', cryptocurrencies. https://www.interpol.int/en/Crimes/Cybercrime/Cryptojacking#:~:text=Cryptojacking%20is%20a%20type%20of,computing%20power%20to%20generate%20cryptocurrency.

[28] A study last fall by Google's Cybersecurity Action Team reported that 86% of compromised cloud instances are used for cryptomining.

cloud services by any means to mine more and more VAs, as cloud services can allow them to run their calculations on a larger scale than just a single local machine.

*Figure 13:Percentage of Total Concerns with VASP operating in mining activities*

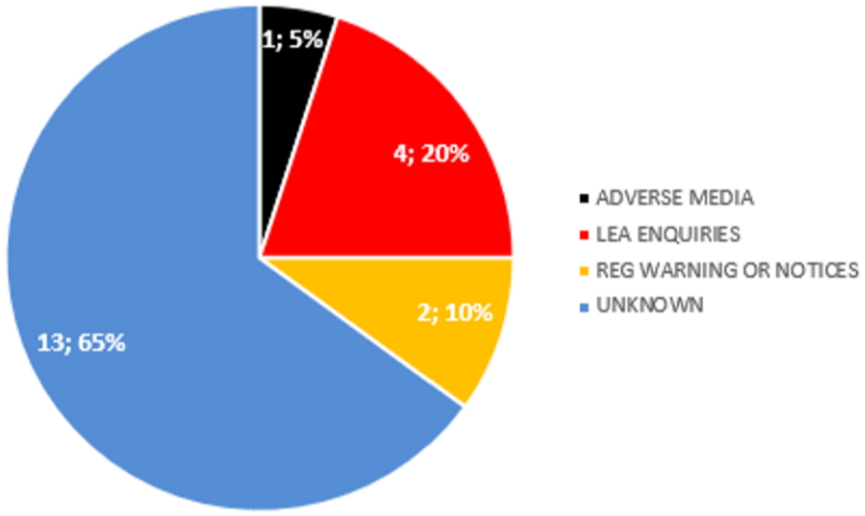



64. **Collection of funds (Very-High)** - VAs have become magnets for illicit activities such as theft and fraud, and given the nature of VAs, there is a possibility that VAs might be used to fund terrorism or terrorist attacks more efficiently than is done today with fiat currencies. VAs might aid terrorists in the receipt of funding through various means. Supporters of extremist groups might donate their own VAs or use VAs to transfer funds through broker intermediaries. Funds could be collected through crowdfunding, a convenient way for the terrorist organisation to supply funding to the attacker.

65. **Transfer of funds (Very-High)** – As per the assessment of the nature and profile of VA, the transfer of money to the less developed regions where terrorist groups may operate could be an attractive medium as it is the same for individuals and entities under sanctions. These threats are consistent with the input variable, such as the 'Absence of face-to-face control' and 'Speed of transfer' indicated above. This input variable is perceived as very high.

    Also, the ONRA noted the presence of various unlicensed Stablecoins operators domiciled in Seychelles that may be facilitating or issuing VAs on a 1-to-1 basis with fiat reserves where dirty money could be used to underpin the stablecoins activities.

*Figure 14: Percentage of Total Concerns associated with VASP offering Stablecoins*

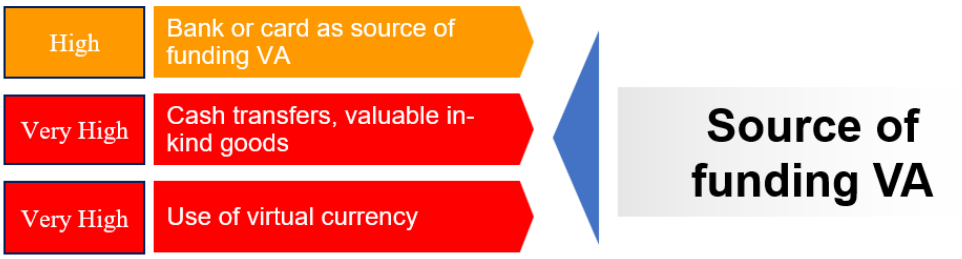



66. **Dark Web and Darknet Access (Very High)** – The ONRA has taken cognisance of some VASPs indicative of darknet market operations in the Ciphertrace report. These markets, which operate on platforms with greater anonymity, offered VAs as the preferred form of payment for illicit items or procurement of restricted or sanctioned items usually acquired for criminal activities or nefarious transactions. The service providers offer Web that relies on encrypted services to shield users' identifying information and communications.

67. **Expenditure of funds (High)** – The threat that criminals may integrate dirty money into new technologies that support the VA ecosystems. Given that many actors are exploring opportunities in the VA market for radical innovation and entrepreneurship in financial solutions without relying on government and central authorities, these mediums may encourage criminals to come on board to integrate dirty money with the least worry of being tracked by legal authorities.

## c. Source of funding VA

*Figure 15: Source of Funding VA – Summary of different risk elements*




68. **Bank or card as the source of funding VA (High)** – VASP platforms with insufficient AML/CFT controls may be more attractive to criminal proceeds where the source of VA funding could be tied to illegal activities. For example, the stolen Bitcoin[29] of 1.8087 BTC (21,000.00 USD)[30] from a well-known VASP was layered into another VA. The hackers used various other exchanges to liquidate the stolen VAs. Most of the exchanges used had negative news against them, particularly about their funding source, and they have a presence in Seychelles.

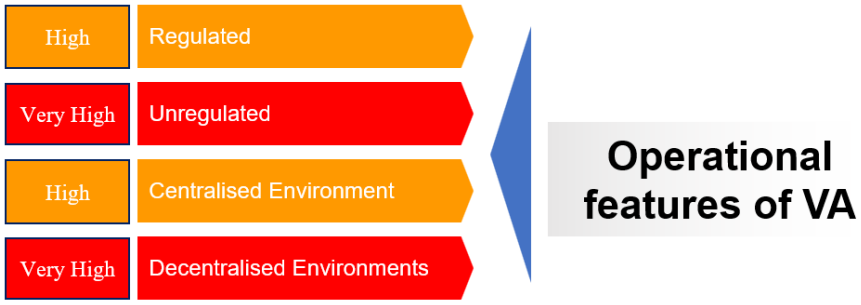
69. **Cash transfers, valuable in-kind goods (High)** - The absence of Travel Rules enforcement and technological solutions for tracing transfers, especially for VAs that could be financed through proceeds of crime and those with unhosted wallets, could expose Seychelles to high-risk VA activities. The country could also be exposed to a rise in thefts of valuable goods as the market for non-fungible tokens (NFTs) grows. The problem is that anyone can "mint" a digital file as an NFT, whether they have rights to it in the first place, as the process is anonymous.

70. **Use of Virtual Currency (High)** – FCIU of Seychelles Police had requests[31] for investigations relating to multiple transactions involving the transfer of 230,000 Bitcoins worth over $10 billion[32] in what's become known as the OneCoin pyramid scheme. Seychelles is currently offering a safe haven to many unlicensed VASPs, and as of November 2021, Seychelles was among the countries with the largest number of exchanges[33]. Thirty-five exchanges were reported to be domiciled in Seychelles, and Crystal Blockchain reported that 31 per cent[34] of the global transfer volumes of Bitcoins in the first half of 2020 were covered by Seychelles exchanges**.**

[29] https://www.coindesk.com/markets/2019/07/16/hackers-are-turning-binances-stolen-bitcoin-into-other-cryptocurrencies/
[30] https://www.blockchain.com/btc/tx/e8b406091959700dbffcff30a60b190133721e5c39e89bb5fe23c5a554ab05ea
[31] http://www.jlevy.co/wp-content/uploads/2021/08/Seychelles-FCU.pdf
[32] http://www.jlevy.co/2021/08/19/over-10-billion-in-one-coin-loot-linked-to-seychelles/
[33] https://crystalblockchain.com/geography-of-international-blockchain-transactions/
[34] https://insidebitcoins.com/news/new-report-shows-seychelles-dominance-in-crypto-transaction-outflows

## d. Operational features of VA

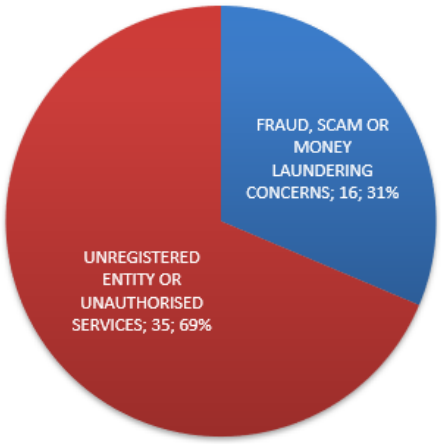
*Figure 16: Operational features of VA – Summary of different risk elements*




71. **Regulated (High)** – The IBCs are regulated entities in Seychelles that fall within the ambit of AML/CFT under the fiduciary service providers, but the threat for the country is that these entities provide services outside the reach of existing domestic legislation. The FSA's financial service regulatory powers are not far-reaching, and there is no defined regulatory perimeter for such activities. The ONRA also assessed that most of the VASPs provide services globally and to a handful of countries where VA is a regulated activity, but many of them have also been denied services in highly regulated countries like the UK and the US.

72. **Unregulated (Very High)** – Many Seychelles domiciled entities have been traced as unregulated entities by overseas regulators providing unauthorised services such as forex, investment and exchanges of VAs[35].

*Figure 17: Entities flagged by overseas regulators over various concerns*




73. **Centralised environment (High)** – Most VASPs operate through a centralised environment and tend to be very exposed to cybercriminal threats. According to Cointobuy's analysis,[36]

[35] Website: iqmining.com (reported by RUCBR-IFMP, Oct 2021).
[36] https://cointobuy.io/countries/seychelles

the VASPs in Seychelles have a safety ranking of 2.7/10. Also, only 6 VASPs[37] were found to be trusted by 'bitrawr' (a company providing advice on bitcoin and recommends activities on trusted exchanges).

74. **Decentralised environments (Very High)** – Unhosted wallets and Decentralised Finance (DeFi) are the medium of the VA ecosystem aiming to reduce or eliminate transaction intermediaries through decentralised computer networks. The system works without intermediaries like VASPs, and banks. There is also NFT which operates through smart contracts.

## e. Ease of Criminality

*Figure 18: Ease of Criminality – Summary of different risk elements*


75. **Tax evasion (Very High**) – Seychelles is listed among the top 15 'Crypto-Friendly Tax Havens',[38] where VA income is generated by the VASPs through VA trading or exchange operations in Seychelles and is entirely free of tax. This is a very high threat for Seychelles, where existing license conditions are being abused for activities that may occasion illicit financial flow.

76. **Terrorist financing (High)** – Although cases of terrorist financing through VA are not much seen, the threat of this method of financing is very present and especially when considering the 'absence of face-to-face control (Very-High)', 'speed of transfer (High)' and unregulated sector (Very High) exposure to other input variables.

77. **Disguising criminal proceeds to unregulated VA** (**Very High**) – VA is being used as a means to facilitate cybercrime, ransomware[39], and other digital extortion activities.

[37] https://www.bitrawr.com/seychelles
[38] https://cryptobriefing.com/the-top-15-crypto-friendly-tax-havens/
[39] Ransomware is a form of malicious code that blocks access to a victim's computer system or data, often by encrypting data or files on computer networks to extort ransom payments from victims in exchange for a decryption key to restore a victim's access to their systems or data

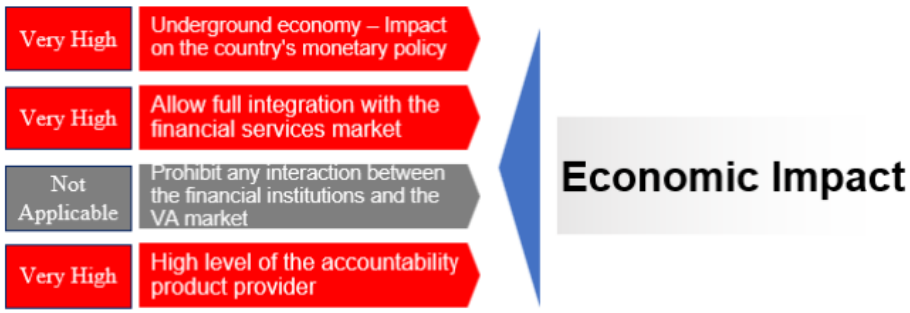
Ransomware perpetrators use VA as a preferred means of ransom payment, and they would use unrelated VASPs to assist them in converting to other forms of VA or fiat money.

78. **Trace and Seize difficulty** (**High**) – This is consistent with the input variable of 'Traceability' noted above, where blockchain inherent features provide the opportunity for law-enforcement agencies to trace and seize. However, the task is complicated as special blockchain forensics tools are required, and Seychelles also lacks dedicated Blockchain specialists within law enforcement to successfully carry out this function.

79. **Circumvention of Exchange Control – (Medium)** – The threat of existing or unknown VASPs in Seychelles could or may be involved in facilitating circumvention of exchange control overseas where this restriction exists and hence undermine government authority by circumventing capital controls[40] imposed by it.

## f. Economic Impact

*Figure 19: Economic Impact – Summary of different risk elements*




80. **Underground Economy – Impact on the country's monetary policy (Very High)** – Most VAs are within the control of private entities who may influence the money supply through market capitalisation and disturb a country's monetary policy. The threat is also very high as an absence of regulatory measures and other interventions could make VAs more likely to be adopted on a Peer-to-Peer basis and encourage tax evasion domestically. As far as VASPs are concerned, their VA services may become attractive to countries where the size of the underground economy is huge or where confidence in monetary policy is low. Seychelles may unwittingly offer a prospective appeal to criminals through unlicensed VASPs without passing a fit and proper test.

[40] IMF- Crypto, Corruption, and Capital Controls: Cross-Country Correlations, WP/22/60, March 2022

81. **Allow full integration with the financial services market (Very High)** – As seen from the input variable above, the anonymity and cross-border reach of VAs raise genuine concerns from a financial integrity standpoint. As VAs can be used to conceal or disguise the illicit origin or sanctioned destination of funds, thus facilitating ML/TF and the evasion of sanctions, the threat is that VA may offer the layering and integration stages of ML in cyber-related criminal activity.

82. **Absence of a high level of accountability of product providers (Very High)** – The threat is very high as the level of the inherent ML/TF risks of Seychelles is also very high because of the absence of legislation. Also, the jurisdictions where the unlicensed VASPs operate may not have well-developed AML/CFT frameworks. The level of accountability also diminishes with the rise of DeFi platforms where intermediaries are called to play a lesser role and hence the challenge for law-enforcement agencies to freeze, seize and confiscate illicit VAs

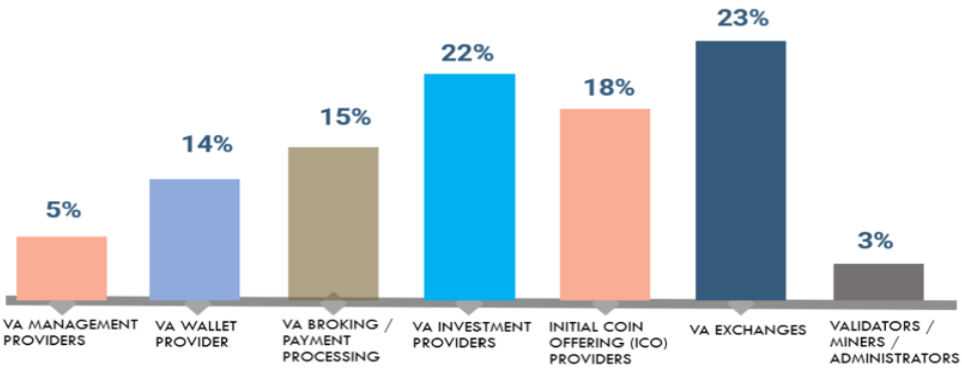
# B. The Overall Vulnerability

83. In assessing the overall national vulnerability of the VASP, the features of Seychelles' economic, legal, and geographic environment were reviewed to identify elements that make the country attractive to VA and VASP ML/TF activities. Accordingly, two factors impacted the overall national vulnerability outcome, namely, the nature of VA services offered by service providers as part of the international financial sector and the VA and VASP's interaction with the overall AML/CFT traditional obliged entities in Seychelles and other countries, especially those with weak AML/CFT framework on VA and VASP. The former identifies vulnerabilities specific to VA service providers, their financial products and services that made it possible for the proceeds of predicate crimes to enter the formal financial system without being detected and later about gaps in the traditional regulations, domestically and abroad, to prevent and respond to ML/TF vulnerabilities because of the interaction with unlicensed VASPs.

84. The overall national vulnerability for Seychelles is rated "**Very High**" at **94%**. This is because the sector, one of the key pillars of its economy and integrated with many countries' financial markets worldwide, offers VA services outside the FSA's purview. Although the traced service providers are operated as subterfuge through licensed reporting entities in Seychelles and are subject to AML/CFT requirements under the AMLA, their VA activities are outside the scope of what FSA is mandated to supervise and regulate.

85. The chart below shows the percentage of categories of VASP traced as domiciled in Seychelles

*Figure 20: Traced entities operating as VASP in Seychelles*




86. The chart above shows a representation of VASPs (over 500) identified to operate in Seychelles. They are currently not subject to AML/CFT regime as they are not licensed. What has been identified in this ONRA might change due to the rapidly evolving landscape of VASPs and as VAs products and services enter and leave the market and the sector. But, whatever the products and services mix offered by these VASPs, it may still be captured within the far-reaching FATF functional definition of VASPs. So, Seychelles authorities need to consider a licensing process for allowable functions through dedicated legislation.

## Assessing VASPs (Intermediate and Input Variables)

87. The measures considered in this assessment are strictly restricted to transactions facilitated by VASPs. Non-VASP transactions, such as person-to-person transfers, are not directly covered. The peer-to-peer transfers of VAs, without the use or involvement of a VASP or financial institution, are not explicitly subject to AML/CFT obligations under the revised FATF Standards. Indirectly, however, the measures may have some impact on transfer activity. The ML/TF risks of these unregulated transactions will be high.

*Figure 21: Overall VASP Vulnerabilities Exposure Summary*

| 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 | Very High Risk |
| | Products/services | Very High Risk |
| | Methods of delivery of products/services | Very High Risk |
| | Customer types | Very High Risk |
| | Country risk | Very High Risk |
| | Institutions dealing with VASP | Very High Risk |
| | VA (Anonymity/pseudonymity) | Very High Risk |
| | Rapid transaction settlement | Very High Risk |
| | Dealing with unregistered VASPs from overseas | Very High Risk |

***OVERALL VULNERABILITY EXPOSURE IS 94%***

88. **Licensed in the country or abroad (High Risk)**

It is unknown how many of the traced VASPs are licensed abroad, but the ONRA has established that many of them are banned in some jurisdictions. The existing AML/CFT legislative framework does not restrict any licensed or unlicensed VASP overseas from transacting, domiciling or operating from Seychelles. Also, the existing law does not prevent players providing fiduciary services or other securities and investment products and services from operating as VASPs. In this context, it is practically impossible for the FSA to assess the fitness and propriety of the unlicensed VASPs and assess their knowledge and measures concerning ML/TF risk. Criminals from overseas may resort to unregulated VASPs in jurisdictions with weak AML/CFT controls through any of the activities indicated above to hide their illicit proceeds.

89. Based on the above, the input variable - Licensed in the country or abroad, indicates a high level of vulnerability concerning the VA/VASP ecosystem and thus has been rated as 'High risk'.

90. **Nature, size, and complexity of business (Very High Risk)**

Some very large VASPs are domiciled in Seychelles, attracting numerous risks to the offshore sector with complex business structures and offering most, if not all, the products and services of VA. The ONRA results show that many VASPs have had a rapid transformation in terms of change of name, shareholders, jurisdictional boundaries for their operations and decommissioning or introduction of new VA products and services, often with minimal regulatory oversight or controls. The ONRA has also traced many small players who could have a very short business existence.

91. Given the above complexities and the borderless nature of VAs, it is very improbable that all the unlicensed VASPs are currently operating the Travel Rule requirements to identify customers that can be associated with ML/FT, and whether the size and nature of business do allow for ML/TF risks being adequately identified and managed on a risk-based approach. Many traced VASPs have adverse media, which would be deemed a high-risk profile when considering the cross-border, internet-based nature and global reach of most VA activities they provide.

92. Based on the above, this input variable was assessed as having a very high level of vulnerability.

93. **Products/services (Very High Risk)**

The vulnerability of the traced VASPs depends on their services with varying high-risk characteristics. The ONRA results show Anonymity-Enhanced VAs, mixers, tumblers, DeFi platforms, privacy coins and Stablecoins being offered by the service providers. Other products or services that enable or allow for reduced transparency and increased obfuscation of financial flows could also be provided by some through the Darknet market.

94. Considering their business activities, business model, delivery channels, customer profiles, the level of governance and the assessment of ML/TF risks, the input variable is assessed as very high vulnerability.

95. **Methods of delivery of products/services (Very High Risk)**

The internet-based nature of VA activities, the non-face-to-face method and the offering of DeFi exchanges as a delivery method may be attractive to criminals, PEPs and high-net-worth individuals. These could offer a conduit to allow payments to be received from unknown or unassociated third parties. Also, exposure to Internet Protocol (IP) anonymisers may further obfuscate transactions or activities and inhibit a VASP's ability to know their customers and implement effective AML/CFT measures.

96. There is no assurance that enhanced due diligence measures and Recommendation 16 are in place to mitigate the potentially higher risks associated with the factors mentioned above. Based on these factors, this input variable is assessed as a very high vulnerability.

97. **Customer types (Very High Risk)**

The VASP sector tends to be at a very high risk of exposure to criminals and organised crime, and the sector is considered attractive to this type of customer due to its reduced transparency. Terrorist financing risk is also significant - terrorist organisations, their supporters, and sympathisers are also continually looking for ways to raise and transfer funds without detection or tracking by law enforcement.

98. As the service providers traced mostly operate in the offshore sector, it is very unlikely that Recommendation 12 is being applied as part of risk management systems to determine whether customers or beneficial owners are foreign politically exposed persons or related or connected to a foreign politically exposed person. And whether measures to establish the source of funds and wealth are carried out wherever relevant. On that basis, this input variable is assessed as very high vulnerability.

99. **Country risk (Very High Risk)**

The VASP sector has significant exposure to higher-risk jurisdictions through internet channels as it is borderless. Most traced VASPs offer their services globally, and those domiciled in Seychelles are unsupervised and may have limited or no AML/CFT obligations. Also, the VA sector is very new, and many of the operators are not familiar with the AML/CFT compliance measures and may be offering their products and services in jurisdictions deemed as high risks or listed on the international sanctions and embargo list. It is also much easier for the unlicensed VASPs to conduct transactions with countries having significant levels of organised crime, corruption, or other criminal activity or countries where illegal drugs, human trafficking, smuggling, and illegal gambling are rife.

100. The VASP vulnerability is assessed in the contextual factors to be very high, especially when considering the type of VA offered by the traced VASPs.

101. **Institutions dealing with VASP (Very High Risk)**
According to the Crystal report[41], 33% of the volume transferred between exchanges in 2021 (w/o Dec) was transferred by G20 countries, while Seychelles transferred about 19% of this volume. This 19% volume primarily consists of transactions sent to and from major exchanges. Given the size of the transfer from Seychelles domiciled VASPs, the number of non-VASPs actors could be massive. It is noted that billions of transfers were made to European countries, the US, and the sanctioned countries. With the above observations, this input variable is rated as very highly vulnerable.

102. **VA (Anonymity/pseudonymity) – (Very High Risk)**
The ONRA traced that many of the unlicensed VASPs are offering VA with enhanced anonymity and also offering privacy coins. As already established with the threat variables above, these VAs are attractive to criminals and make it harder for law-enforcement agencies to successfully trace the private key and the holder. Consistent with the rating of the threat of VA, this input variable is also assessed as very high vulnerability.

103. **Rapid transaction settlement (Very High Risk)**
The transactions in VAs are executed rapidly due to the elimination of interbank payments and settlements. With the rise of stablecoins like Tether, Multicollateral DAI (DAI) and Gemini Dollar (GUSD), among several others, the vulnerability of this input variable is considered very high and is consistent with the speed of transactions threat identified for VA above.

104. **Dealing with unregistered VASPs from overseas (Very High Risk)**
Many of the traced VASPs in Seychelles sits at the intersection between the anonymity of VA transactions and operating without overseas regulatory scrutiny and authorisation. Many regulators in advanced economies are investigating unauthorised[42]. VA firms[43].

105. This input variable is assessed as very high.

[41] ibid
[42] https://www.newsbtc.com/tech/long-time-critic-explains-why-bitfinex-is-unable-to-work-with-banks/#:~:text=However%20if%20weak%20or%20non-existing%20KYC%2FAML%20is%20the,partner%20in%20the%20months%20and%20years%20to%20come.
[43] https://www.protocol.com/fintech/global-crypto-regulation

# PART 4
# THE ML/TF MITIGATION MEASURES FOR VA AND VASP

*This part considers the adequacy and effectiveness of the existing AML/CFT framework of the government, the reporting institutions and the VASP to mitigate the threats and vulnerabilities identified above.*

## The Overall Mitigation Measures Level

106. In assessing Seychelles' overall effectiveness of mitigation measures against the threats and vulnerabilities, the features of Seychelles' legal, financial and human resource capabilities were reviewed to identify elements that make the country attractive to ML/TF activities.

Accordingly, two factors impacted the overall national effectiveness outcome: its national combating ability in the legislative framework and its application to contain the overall sectoral vulnerability. The former identifies weaknesses and gaps in the country's legal framework and the ability to prevent and respond to ML/TF VA and VASP threats and vulnerabilities, and the latter identifies features of specific sectors, financial products and services that made it possible for VASPs to infiltrate and launder proceeds of predicate crimes in the regulated sector without any knowledge from regulators of their operations.

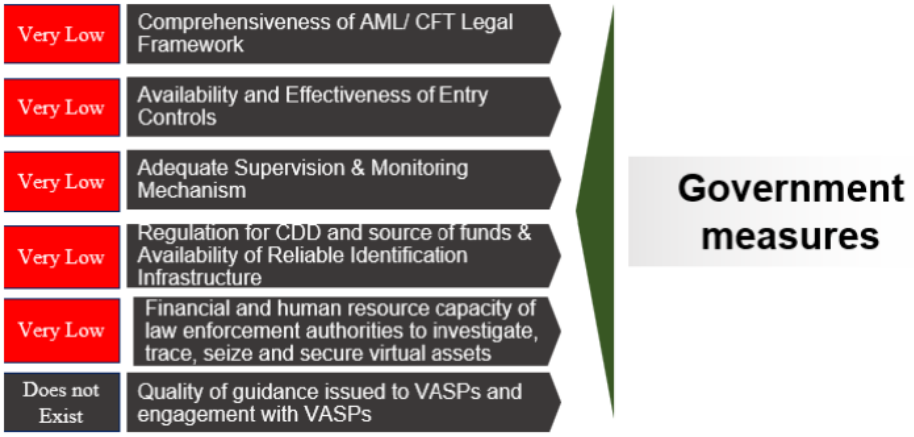
107. The overall national effectiveness of mitigation measures of Seychelles is rated as "**Very Low**", **at 17%** effective in mitigating the ML/TF threats and vulnerabilities exposure. This stemmed from a lack of dedicated legislation, capacity to investigate and prosecute financial crimes related to VA and VASP, and the dedicated regulatory framework for licensing, monitoring, and supervision.

## a. Government Mitigation Measures – 17% (Very Low)

108. The mitigating factors from the government and supervisory perspective for VA and VASP ML/TF risks as per FATF guidance of 2019-2021 are assessed to be **very low**. The message that comes out from this rating is to take steps to develop and pass legislation to register, license, and monitor VASPs; cooperate with other authorities domestically and internationally; implement measures to control market entry by VASPs and restrict market entry by owners or managers who are unfit; proving oversight and supervision of VASPs; reporting of STRs; and effective prosecution and enforcement.

109. Supervisors, particularly FSA, will require sufficient human and technical resources, including information technology tools such as commercially available VA forensic and database and transaction monitoring tools. The complexity of the underlying technology of VA and VASPs and its rapid ongoing evolution will require such tools and skills for the staff monitoring VA and VASPs.

*Figure 23: Effectiveness of Mitigation - Government Measures*




## The Comprehensiveness of AML/CFT Legal Framework

110. **Legislative framework**: VAs have many potential benefits, but it remains outside the legal framework of many countries, and hence they are susceptible to a wide range of criminal activities and financial crimes. The ML/TF risks manifest through the whole lifecycle of any VA, from the minting and issuing process, the intermediaries that enable consumers to access the system on DLT, the technology providers and the types of customers. Also, the nature of VAs has created different delivery systems and business models for VA entrepreneurs with different regulatory risk appetites compared to the traditional financial services providers. The existing legal framework of Seychelles needs to be revised and fine-tuned to adequately address the challenges associated with those types of products and services.

111. **ML Scope:** Although Seychelles' ML crime in the AML/CFT legislation is very comprehensive, with a wide range of predicate offences, which are proportionate and dissuasive, the definition needs to be broadened to capture new behaviours and mechanisms that are strictly VA-related. Seychelles' domiciled VASPs may be heavily exposed and unwittingly facilitate potential sanction circumvention or proliferation financing through the medium of VA as payment. FATF Recommendation 7 is adequately captured in the AML/CFT legislation; however, dedicated specific regulations and guidance need to be issued by

regulators to dissuade and disrupt the use of VA financial products and services directly related to trade in proliferation-sensitive goods, sanction circumvention or illicit revenue-raising activities through VASP.

112. **Tax legislation:** Tax evasion through VA is a very high threat and vulnerability for Seychelles. Given the perception of offshore financial centres and the country's ranking in the financial transparency index, the existing tax legal framework should be revisited to bring VA activities within its scope. The tax implications can arise from transactions involving VAs to assist Peer-to-peer mining activities, professional advisers and VASP activities in the country. The tax legislation review will allow SRC to adapt the law for VA purposes.

## Availability and Effectiveness of Entry Control

113. **Regulatory Requirements**: Seychelles has no legal or regulatory requirement to prevent unlicensed or non-registered VASPs from seeking a license such as IBC or other offshore licenses to engage in VASP activities.

114. **Open to worldwide and unknown jurisdictions:** Seychelles is unwittingly engaging with VA globally. Many VASPs in the IBC sector are established global entities with lots of adverse media coverage and claim to be Seychelles registered license owners. The country is moving faster than policy can catch up, making it a tax and money laundering haven for VA[44]. Some of these companies have attracted attention from various regulators in the country of operations, which led to the release of regulatory warnings and advisory on the funds.

115. **Unregulated activity**: Currently, the VA falls outside the scope of a currency to be regulated by the central bank and the licensing conditions of the FSA. Although stablecoin could be backed by fiat money, it is not e-money, but there are no directives from competent authorities to situate the regulatory status of stablecoins. The legislative vacuum has provided a revolving door for existing and new actors in the international business to domicile as VASP from Seychelles without any regulatory oversight.

116. **Sanctions jurisdictions**: Seychelles has no mitigation mechanism to prevent exploitation of its international business regime by VASP domicile in its jurisdiction but operates globally. There is a serious risk of the potential of sanctions circumvention and related violations. Many platforms, stablecoins and other VA products are delivered through complex operations and obfuscation methods, and these may easily be used as a payment method to evade financial sanctions.

[44] https://decrypt.co/19204/top-7-crypto-companies-based-in-tax-havens

The absence of fit and proper tests and continued supervision of VASP entities may lead to a sanctioned country colluding with unlicensed VASPs to move VAs from one jurisdiction to another.

### Adequate Supervision & Monitoring Mechanism

117. **Guidance on the direction of travel**: When AML/CFT international standards were being discussed at the international level, which led to the amendment of the FATF R 15 in 2019, many countries put in place some jurisdictional directions and boundaries to prevent their system from being abused for unlicensed activities. While the range of legal development varies in many countries, some do not do anything and adopt a 'Wait and See' position. This slow reaction has created continuing difficulty for supervisors and the private sector in defining which regulation covers the gamut of VAs and what level of AML/CFT requirements to enforce in a sector which mimics traditional financial services but offers services outside the supervisor's jurisdiction. In Seychelles, the 'Wait and See' approach has resulted in a lack of effective compliance by the Traced VASPs. To date, no supervisory authority has been identified to supervise VAs and VASPs for AML/CFT.

118. **Anonymised Payment and Transfer Services**: Many Traced VASPs have been set up for payments and transfers of VAs, which may heighten ML/TF risks. The existing legislation does not give the supervisor the necessary power to monitor technology that prevents transparency, such as tumbling or mixing services or anonymity-enhanced coins (AECs) supplied by certain providers under the IBC business license. The speed of transactions, the VA's global reach, and the potential for increased anonymity and obfuscation of transaction flow to high-risk counterparties cannot be monitored by the FSA under the existing regulatory setup. New supervisory methods need to be developed by the FSA and other AML/CFT supervisors to cope with the increased complexity in financial technology businesses and VA services. That should allow them to make more intensive use of data and technological tools like blockchain analytics to improve the effectiveness of their supervisory frameworks.

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

119. **CDD and source of fund:** VASPs must undertake customer due diligence measures per FATF R15 and apply the Travel Rule per R16. There is no evidence that CDD measures are being applied by the unlicensed VASPs and verifying the customer's identity using reliable, independent source documents, data, or information. Also, while FATF R10 requires scrutinising the source of funds where necessary as an effective means of mitigating ML/TF risks, again, there is no evidence to suggest that the unlicensed VASPs apply the requirements of R10.

120. **Availability of Reliable Identification Infrastructure:** Seychelles is currently implementing its Beneficial Owner Register to fully comply with the FATF requirements. Understanding and obtaining information on the purpose and intended nature of the business relationship is an important element of the mitigating measures, and such information should be made available to competent authorities and, to some extent, to the public when appropriate. The country needs to have an adequate legal or regulatory requirement system to ensure that VASPs undertake customer due diligence and counterparty VASP due diligence once licensed.

### Financial and human resource capacity of law enforcement authorities to investigate, trace, seize and secure virtual assets

121. The skills and expertise necessary to conduct thorough and complex investigations involving VAs remain highly specialised. VA technology is still in its infancy in Seychelles, and a national strategy paper needs to address VA's challenges and upskilling law enforcement and regulatory staff. Bespoke training to supervisors and law enforcement agencies on the use of the technology and how to investigate and prosecute related crimes must be planned and implemented accordingly. The survey conducted for this ONRA exercise shows that government agencies, investigators and supervisors have had limited or no exposure to VAs in their investigations and face a steep learning curve due to the perceived technical complexity of VAs.

### Effectiveness of international cooperation

122. Both Seychelles' FIU and FCIU actively engage with their overseas counterparts to exchange information. While the requests are mostly from overseas, these are putting extra pressure on these agencies' already existing stretched resource capacity. The effectiveness depends on the swiftness of providing the required information, the quality, and the procedure of obtaining it. As Seychelles had exposure to many VASPs that are the target of overseas regulators or law-enforcement bodies, the international cooperation could have been improved by playing a more active role in the overseas investigation to build up technical capability and positioning the country as a positive partner willing to assist in fighting such criminality.

Also, effectiveness is two-way street traffic; given the lack of legislation in Seychelles to enforce compliance of AML/CFT in the VASP sector, not many VA-related requests from LEA went out for full investigation, supervisory sanction, or intelligence purposes.

### Quality of Guidance Issued to VASPs and Engagement with VASPs

123. Seychelles has not issued guidance on VA and VASP to enable prospective VASPs to understand the regulatory expectation and ML/TF risks associated with VAs and related activities and compliance requirements and undertake appropriate measures. Due to the absence of legislation, there is no active engagement with the sector for this purpose.

## b. Traditional Obliged Entities (20%) And VASPs (15%)

124. **VASP Preventive measures:** All the VASPs domiciled in Seychelles are subject to AML/CFT requirements for unrelated VA services. The entities are serviced through fiduciary license owners or capital markets and investment providers under the relevant legislation regulated by the FSA, and these licensees have the same obligations as a bank or other Traditional Obliged Entities (TOEs) would have. Therefore, on that premise, the assessment noted that the existing obligations of these licensees mitigate to some extent (15%) the ML/TF threats and vulnerabilities even though the VA-related transactions fall under the ambit of the current AML Act.

125. Also, the survey revealed a lack of awareness of these licensees about the business activities of their customers and a lack of knowledge of VA activities synergy with the payment, investment, insurance, and capital businesses. Supervisors are likewise critical in ensuring that these licensees apply the controls and measures within their capabilities in proportion to the risks of their licensed services.

126. **TOE Preventive Measures**: Given the issues discussed above, TOEs have a very sceptical approach to services and customers connected to VA due to a lack of full understanding of their respective roles with VAs and any potentially elevated risks. However, as with any new line of business, the TOEs need to factor in these services, products, and customers in their AML/CFT compliance question and risk assessment and tailor policies and procedures to support or not support VA.

127. The ONRA survey noted that more work needs to be done in TOEs sectors in terms of products and services of VASP and how these could directly or indirectly interact with their sector. As a matter of good practice, TOEs need to assume that their exposure to VA is dramatically higher than they think and understand how the ‘unknown’ and ‘unseen’ interacts with their sector. For example, Investment and security dealers and advisers, assets under investment providers may have direct exposure to VA where prospective customers looking at short investment gain. Accountants and lawyers may also be affected through advice or preparation of financial statements with tokenised assets of the entity.

128. **Control of VASP entities**: Most STO and ICOs are outside the scope of the current regulation of the FSA. In the absence of such power, FSA needs to place some conditions on an issuer of an ICO or an STO through the powers conferred on it by the existing statutory instrument governing registration or approval from the FSA to establish a Seychelles company where the FSA may choose to impose certain conditions on the company to which the registration is granted. As a general policy, the VASPs' ICO and STO issuers must be incorporated as a Seychelles company and administered through a TCSP licensed by the FSA. Through this process, the FSA could seize the opportunity to mitigate ML/TF risks by ensuring that STO and ICO issuers do not use the registration process as a green light for VA activities.

129. These controls could be supplemented with guidance notes to clarify the registration process that the FSA expects to adopt for future ICO/STO issuers when a licensing process is in place.

# PART 5
# SECTORIAL ASSESSMENT
# VA AND VASP INTERACTION

*The part provides a snapshot of the observations of the impact of VA and VASPs activities on the Traditional Obliged Entities sectors*

## The Rationale

130. The existing Traditional Obliged Entities (TOEs) sectors were assessed to achieve an overall risk assessment of VA and VASP. The sectoral risk assessment shows the exposure of VA and VASP ML/TF risks from a transversal risk perspective for these sectors. Irrespective of the types of VA, it is a transversal risk factor that affects the TOEs through its distribution channel via VASPs or decentralised exchanges or peer-to-peer transactions. TOEs could also engage as VA intermediaries or partner with VASPs in providing a particular VA function. The transversal risk of VA will continue to evolve as new products and services come on the market and the necessity of support from TOEs players for its design and delivery.

131. Due to problems accessing precise aggregate data for this assessment, bespoke questionnaires were designed for each sector to collect pertinent information on VA and VASP interaction. As it has not been possible to collect more related information from these service providers, the assessment relied on information gathered from supervisory and law enforcement authorities and the open-source to draw documented conclusions on the exposure of risks in these sectors.

## Banking Sector (High Risk)

132. **Banks (***High Risks***)**: The ONRA survey revealed that banks in Seychelles are not onboarding customers dealing in VA activities and are not themselves engaging in VA either as an investment medium or assisting in financing the development of specific technology for use in the VA ecosystem.

133. Certain entities licensed as fiduciary service providers or security and investment providers are involved in NFT. Under the FATF framework, an NFT could be a VA or an investment if it is not for payment purposes. Therefore, when banking such players, banks had to perform a test to determine if clients dealing in NFT are VASPs or investment providers. The ONRA did not see any indication that such tests were being performed.

134. According to responses received from the sector, banks tend to have a lack of appetite for VA due to a lack of understanding and a lack of legal framework in Seychelles. The survey results indicated that no bank has VASP as a client. However, despite the cautious approach, the ONRA exercise has revealed that from the list of the Traced VASP entities, a random check shows that 13 entities set up to provide services under the Securities Act 2007 have bank accounts in Seychelles. As security dealers' entities must have client accounts and operational accounts, four entities have client accounts. The ONRA also observes that these accounts are from long-established clients and predate VA.

135. The above finding indicates that banks may not have a proper risk assessment to detect VASP clients and may not have tailored monitoring activities for VA transactions. It was also observed that banking customers are already using banking products and services such as debit and credit cards to acquire VA online. Customers also undertake wire transfer transactions to VASP exchanges for investment in VAs, principally Bitcoins.

136. **Bureaux de Change (BDC**) – *High Risk*: despite no appetite for VA in the sector, the ONRA assess that because VA is here to stay, BDC may face direct competition from VA exchanges which provides an easy and cost-effective way of transfer of value. There is an indication that BDC is partnering with stakeholders in the VA ecosystem or banks to explore using a dedicated network to effect transfer to a country with heavy reliance on money service business. BCD could also be positioned to convert fiat to VA or vice versa.

137. **Seychelles Credit Union (SCU**) - *Low Risk*: As per responses from the questionnaire, information review, and open-source research, no exposure is noted with the SCU.

138. **Development Bank of Seychelles (DBS**) - *Low Risk*: No exposure is noted from the questionnaire and information review.

139. More information on the banking sector can be accessed from the sector report.

## Non-Banking FI Sector (High Risk)

140. **Fiduciary Services *(High Risk)***: There are no legal barriers to entry in Seychelles for foreign companies to set up as IBCs and use the entity as a subterfuge to operate as VASPs.

A foreign company looking to conduct business in Seychelles would be required to set up an IBC and receive necessary approvals and licenses from the Seychelles authorities.[45]

[45] It would also be required to obtain the approval from the Seychelles Investment Board (SIB) for licensing purposes. The licence would depend on the business that the foreign company seeks to do in Seychelles. Further, a foreign company shall also require government sanction in order to rent or lease any immovable property in Seychelles for the purpose of conducting business in Seychelles.

Seychelles manages one of the fastest-growing IBC registers in the world, and it also hosts the largest share of the unregulated virtual asset industry – with the largest unregulated exchanges and brokerage firms operating via Seychelles IBCs.

141. In a survey conducted with 64 TCSPs for this ONRA, many licensees indicated that they do not verify whether their IBCs engage in VA activities or not and do not verify if they are licensed in the country where they conduct this activity. The response demonstrates a serious flaw in the TCSP KYC system and risk management programme.

142. **CM&CISSS *(High Risk)***: The Capital Markets & Collective Investment Schemes Supervision Section ("the CM&CISSS") has licensed over 130 entities, of which all fall under the purview of the FSA under the Securities Act. The ONRA exercise identified that at least 27 entities are operating as VASPs, although their license was granted to perform activities solely in Schedule 1 of the Security Act.

143. Unlike the TCSPs, 36 respondents self-declared to be operating as VASPs, but further work needs to be carried out outside the ONRA exercise to establish if all the self-declared entities are providing any function that falls within the VASP functional definition of the FATF.

144. **Insurance** – ***(Low Risk)*:** The ONRA covered insurance companies and brokers offering digital assets insurance, cyber liability and cyber insurance, and commercial crime. Thirty-eight (38) companies in this sector were targeted for the ONRA survey 37 responses were received. Based on responses received and information reviewed, there is currently no exposure to VA and VASP AML/CFT risks in this sector. However, more work would need to be carried out post the ONRA exercise to establish the correlation between claims for digital assets and cyber insurance and the claimants, their location, the nature of their business and the amount insured.

145. More information could be accessed in the sector report.

## Gambling & Gaming Sector (High Risk)

146. Currently, there are five slot machine operators and four casinos which offer a wide range of gambling activities to their clients. To date, interactive gambling is not permissible within the market, and there are no entities licensed by the FSA providing interactive gambling in Seychelles. However, the ONRA identified that two online casinos misleadingly claim to be licensed in Seychelles and offer gaming platforms through VA. Also, other research has unravelled five entities in the IBC sector operating in the gaming sector and offering metaverse products, a convertible VA token, on gaming platforms. The research also shows that one of the entities has adverse media for the allegation of fraud.

## Designated Non-Financial Businesses & Professions (DNFBPs) – (Low Risk)

147. **Dealers in precious stones and metals, Real Estate, Motor Vehicle Dealers – (***low risk):* These players in the DNFBP sector in Seychelles are quite small and comprise ten real estate agents and 24 motor vehicle dealers 11 dealers in precious stones and metals. These businesses are licensed by the Seychelles Licensing Authority (SLA) under the Licences Act and are defined as reporting entities under the AML/CFT Act, 2020 and are therefore required to comply with KYC/CDD requirements, recordkeeping, suspicious transaction reporting, etc.

148. The VA and VASP interaction in these sectors is quite remote, and the level of awareness of VA is quite mixed. Although more than 50% of the respondents affirm to have heard of VAs, most do not understand VA's technicalities.

149. The ML/TF risk exposure associated with VA is very low, but this is expected to change as the peer-to-peer activities are picking up in Seychelles and abroad, and the level of awareness of the operators in the precious stones and metals dealers grows.

150. **Accountants, Auditors & Tax Agents – (***High risk):* These sectors are also quite small and comprise 46 accountants, 43 auditors and 26 tax agents. Accountants and auditors are licensed by the Seychelles Licensing Authority (SLA) under the Licences Act, 2010. However, tax agents are licensed by the Tax and Customs Agent Board under the Seychelles Revenue Administration Act, 2009. While the legislations grant power to the authorities to vet licence applicants, request information from the applicants and licensees, and take enforcement action against licensees, it is to be noted that these powers do not extend to VA/VASP activities. However, it is also to be noted that these businesses are defined as reporting entities under the AML/CFT Act and are therefore required to comply with the AML/CFT obligations under the AML/CFT Act.

151. The ONRA survey revealed a high level of awareness of VA, and most respondents believed that VA could be used for money laundering, terrorism, and proliferation financing.

152. These professionals could interact with VASP in many ways and may wittingly or unwittingly advise or prepare a financial statement in such a way to mask VA activities as there is no VA and VASP legislation in place, as Seychelles has not yet endorsed the international accounting standards on accounting for VA in financial statements. Given the large number of VASPs uncovered and the interaction of these professionals with the offshore sector as nominee shareholders and directors or as accountants, it is assessed that they may be turning a blind eye to the VA activities to preserve their business relationship with the Fiduciary service providers and other VASP entities.

## Lawyers and Notaries – (High Risk)

153. The Legal Professionals sector in Seychelles comprises 60 lawyers and notaries. Lawyers are licensed under the Legal Practitioners Act, 1994, by the Chief Justice of the Supreme Court of Seychelles. However, notaries are appointed by the President of the Republic under the Notaries Act, 1991.

154. The ONRA survey revealed that many Legal Professionals have heard about VA and are aware of the term Virtual/Digital/Crypto Currency. However, most respondents have not heard of the term centralised or decentralised VA.

155. In the absence of a regulatory direction of travel, just like the accountants, lawyers too may wittingly or unwitting partner with digital currency entities to provide legal support on VA issuance, developing VA focus fund development and management, and hopefully benefit as they achieve traction in the market.

156. It is expected that the threats and vulnerabilities from the DNFBP sector will be heavily mitigated once dedicated VA legislation is in place.

157. For more information, please see the sectoral report.

# PART 6
# MAIN FINDINGS

## Strategic Findings

158. **The country's exposure** - The overall exposure of Seychelles to ML/TF risks arising from VA and VASPs is at 90% (Very High)

| Threats | Vulnerabilities | Mitigation Measure | Overall Risk |
|---|---|---|---|
| Very High (87%) | Very High (94%) | Low (17%) | Very High (90%) |

As Seychelles has not clarified its position on FATF R15 and R16 (Travel Rule), there is a significant deficiency in the existing AML/CFT legislation, which needs to be addressed in dedicated VA and VASP legislation. This is a vulnerability to Seychelles' status as an IFC and its position in the tax transparency and financial secrecy index. These contributing factors heighten its overall exposure to ML/TF risks associated with VA and VASPs. The weaknesses in the existing AML/CFT framework are conduits for the meteoric rise in VA and VASPs in the country.

159. **Inherent cross-border risk** – The nature of VA services from the traced unlicensed VASPs are legally domiciled in Seychelles but offer services globally. These providers are seizing the absence of legislation to offer, DeFi, NFTs, stablecoins, metaverse, privacy coins, WebMoney and other new facets of the ecosystem, providing alternative mechanisms for consumers to engage with virtual assets. Many of the Traced VASPSs are offering their services worldwide where their website can be accessed globally except in a few countries where they are experiencing regulatory investigations, like the US, UK and Europe or have been banned accordingly, for example, in Japan, the US, UK or Hong Kong.

160. **Unlicensed VASP with Concerns** – The review across different VASP types operated from Seychelles with adverse media are: VA investment at 38% and Exchanges at 30%, with the highest risks exposure. Except for Management Providers with medium-low risks, the other types of VASPs are all of the medium risks.

161. **Regulatory Arbitrage** - Because of growing regulatory scrutiny by international institutions like the FATF, more and more countries worldwide started passing legislation to comply with international best practices on AML/CFT and to control the nature and scale of VAs in their jurisdictions. There is a shift towards countries like Seychelles, which may be facilitating

regulatory arbitrage due to its insufficient disclosure mechanisms to regulate activities of VASPs, which may have serious repercussions on the reputation of Seychelles.

162. **High Risks VA** - Many unlicensed VASPs operate in Seychelles with different varieties of VA and offer enhanced anonymity facilities. An ever-growing obfuscation mechanism is being provided by the VASPs, making the entities perceived as high risk for ML/TF as the transparency of wallet addresses is hidden. This rise could be due to the banning of 'privacy-centric dark coins' in many jurisdictions because of its attraction to cybercrime syndicates and money launderers.

163. **The legality of VA**[46] – VA is currently outside the scope of Seychelles' taxation law but falls under the property definition for criminal investigation purposes. Hence, VA is not legally recognised as a medium of payment and store of value, but the country does not prohibit the purchase and sale of VAs and their use. The CBS has not issued guidelines, and neither are the SRC and FSA to clarify the legality of VA, which implicitly or explicitly recognise the use of VAs as legal: Guidance acknowledging the legality of VAs include dedicated laws or regulation defining them and the regulatory requirements they are subject to,

164. The absence of taxation legislation to clarify the impact of income tax, value-added tax, corporation tax, capital gains tax and property tax may provide an opportunity for tax dodgers to be domiciled in Seychelles.

165. **Business Model** - The country is currently domiciling many Decentralised and DeFi exchanges where no entities are responsible for collecting KYC data on customers or monitoring transactions for suspicious transactions, heightening the risks of ML/TF. These exchanges enable peer-to-peer exchanges of VAs, whereby users keep their private keys and trade directly with one another. The VASPs intervene as a broker in matching buyers and sellers. The absence of legislation has made it difficult for supervisors to have full visibility and assess the relative merits, risks, and value of the increasing myriad of VAs offered by the unlicensed VASPs from Seychelles.

166. **Lack of Due Diligence** – The fiduciary service and the capital and investment providers lack KYC and KYCC information. Proper collection and maintenance of customer and transactional information to identify illicit activities seem to be not happening.

167. **Lack of experience in the private sector –** There is a lack of general AML/CFT experience of VA and VASPs in the private sector. In other countries, supervisory and regulatory bodies have partnered with specialist firms to organise various awareness sessions, and such initiative

[46] https://www.oecd.org/tax/tax-policy/taxing-virtual-currencies-an-overview-of-tax-treatments-and-emerging-tax-policy-issues.pdf

would have benefitted the private sector. A possible mechanism to deepen this process could lie in encouraging the formation of industry associations and trade groups to facilitate this engagement. This is particularly helpful given the diversity of the businesses making up the sector.

168. **Exposure to unsafe VASPs –** Although the FSA has issued cautionary notices advising on unrecognised VASPs, according to Cointobuy's analysis, Seychelles' VASPs have a safety ranking of 2.7/10. Also, only 6 VASPs were found to be trusted by 'bitrawr' (a company providing advice on bitcoin and recommends activities on trusted exchanges). The rating indicates the level of toxicity of the VASPs exchanges in the country.

169. **Not restricting VA activities**: Although most STO and ICOs are outside the scope of the current regulation of the FSA, these could have been restricted by placing some conditions on licenses issued under the powers conferred on FSA by the existing statutory instrument governing registration or approval of an application to establish a Seychelles company. Imposing specific license conditions to prevent VA activities could have been a first step in preventing or restricting the exploitation of existing licenses.

## Analytical Findings

170. **A significant gap in the detection of STR** - The open-source research has flagged many VASPs over criminal and money laundering schemes, including Drug Trafficking, Fraud, Tax Evasion, Sexual Exploitation, Cyber Crime, and Dark-net Market Activities, Extortion, Kidnapping, Terrorism Financing, and Investment Scams. The higher number of VASPs involved in the LEA enquiries and regulatory notices and warnings against the low number of VASP STRs highlights a significant gap in the STR detection capabilities of criminal schemes.

171. **Facilitating unlicensed money services businesses** - A majority of the VASPs, which are flagged over the regulatory notices and warnings in other countries, were identified to be facilitating unlicensed money services businesses (MSBs) through their digital wallet and/or exchange services, unauthorised investment, or financial services, or providing fraudulent investment schemes. Many VASPs are also flagged as having porous KYC or allegedly involved in fraudulent schemes.

172. **Cyber Attacks** - Many large Seychelles-based VASPs have also been victims of cyber-attacks or used as a platform to launder criminal ill-gotten proceeds.

173. **DeFi Products** - The assessment of the VAPSs flagged many companies which are decentralised VA platforms extending Decentralised finance (DeFi) products, and a

considerable proportion of them were previously identified against the LEA enquiries or negative media reviews, including concerns over fraud, drug trafficking and other serious criminal offences. Some of these companies have started offering NFT and metaverse-related products, which will likely grow in market size and utilities in the coming years.

174. **NFT and Stablecoins** – A significant number of unlicensed VASPs are offering NFT, which may be for payment purposes, and stablecoins pegged with currency from unknown sources and consideration of financial risk is also unknown to the ONRA. As regulation and supervision of NFTs and stablecoins are nascent or non-existent in many jurisdictions, Seychelles could be emerging as a hub for these activities.

# PART 7

## APPENDIX 1 – Glossary of Terms

| *TERM* | DESCRIPTION |
|---|---|
| *Algorithm* | A process or set of rules to be followed in problem-solving or calculation operations, usually by a computer. |
| *Bitcoin (BTC)* | The largest and best-known cryptocurrency. |
| *Blockchain* | Nearly all cryptocurrencies use the underlying technology. A blockchain is a complete ledger of transactions held simultaneously by multiple nodes on a network. |
| *Centralised Exchange* | Centralised exchanges are a type of cryptocurrency exchange operated by a company that owns it in a centralised manner. |
| *Cloud Mining* | Cryptocurrency mining with remote processing power rented from companies. |
| *Coin Mixer* | Coin mixers allow users to mix up transactions between different cryptocurrency addresses, so they become untraceable and cannot be followed back to the initial sender or receiver of the assets. |
| *Contract* | In traditional finance, a contract is a binding agreement between two parties. In cryptocurrencies, smart contracts execute functions on the blockchain. |
| *Crowdfunding* | Crowdfunding enables fundraisers to collect money from a large number of people through a variety of different platforms. |
| *Cryptocurrency* | A digital asset can be used as a store of value or a medium of exchange for goods and services. Transactions are verified and recorded using cryptography by a distributed network of participants rather than a centralised authority such as a bank or government agency. |
| *Cryptography* | A method of keeping information secret and secure by scrambling it into indecipherable codes. The information can only be decrypted and read with the necessary key. |
| *Cryptojacking* | The use of another party's computer to mine cryptocurrency without their consent. |
| *Custodial* | Custodial cryptocurrency businesses are the ones that have their customers' funds for the duration of the use of their services. |
| *DAO* | An acronym that stands for a decentralised autonomous organisation. A DAO is a group of people who work together toward a shared goal and abide by rules written into the project's self-executing computer code. Bitcoin (the project, not the currency) is the earliest example of a DAO. |
| *Data Privacy* | Data privacy refers to the area of data protection and security responsible for handling sensitive data. |
| *Decentralised API (dAPI)* | API services intrinsically interoperable with blockchain technology are known as decentralised application programming interfaces (dAPIs). This is an invention of the API3 protocol. |
| *Deep Web* | The "deep web" is the part of the internet that is hidden from regular search engines. |
| *DeFi* | Short for decentralised finance. Finance is traditionally centralised because it relies on trusted intermediaries. For example, if you want to send money to a |

| | |
|---|---|
| | friend or relative, you rely on your bank to send it to the recipient's bank. DeFi requires no intermediaries, and participants can send and receive assets directly. In theory, this makes transactions faster and cheaper. |
| *Derivative* | A financial instrument derives its value from the value of an underlying asset. |
| *Digital Asset* | A digital asset refers to the digital representation of something of value. |
| *Distributed ledger* | Distributed ledges use nodes, or independent computers, to record, share, and synchronise transactions on the electronic ledger. A blockchain is a type of distributed ledger. |
| *Encryption* | The process of making digital information into a form that prevents unauthorised access. If you use a password to access a website, the site should encrypt it so that it is of no use to hackers if stolen. |
| *Escrow* | A financial instrument where a third party holds assets or cash while a buyer and a seller complete a deal. |
| *Ether* | The form of payment used in the operation of the distributed application platform, Ethereum. |
| *Ethereum* | The second-biggest cryptocurrency by market capitalisation after Bitcoin. |
| *Exchange* | A website or app that allows users to buy and sell crypto assets. |
| *Fiat currency* | Currencies with legal tender, for example, the U.S. dollar, the euro or the British pound, are major fiat currencies. |
| *Fungible* | In cryptocurrency, fungibility is when any other identical coin or token can replace a coin or token. |
| *ICO* | An acronym stands for initial coin offering. An ICO is the cryptocurrency equivalent of an initial public offering (IPO), and it offers investors the opportunity to back a new crypto project. |
| *Know Your Customer (KYC)* | Although not required, many crypto exchanges carry out certain identity checks on their customers under KYC rules. |
| *Metaverse* | A metaverse is a digital universe containing all the real world's aspects, such as real-time interactions and economies. It offers a unique experience to end-users. |
| *Miners* | Contributors to a blockchain taking part in the process of mining. They can be professional miners, organisations with large-scale operations, or hobbyists who set up mining rigs at home or in the office. |
| *Mining* | Crypto mining is verifying transactions via a proof of work consensus mechanism. Mining involves using computer hardware to solve a hash with trillions of possible combinations. The more computing power you have, the more guesses you can make within each given window of time, and the greater your chances of earning newly minted crypto. |
| *NFT* | An acronym is a non-fungible token, a digital collectable that uses the same underlying technology as cryptocurrencies. |
| *Non-Custodial* | Usually referring to the storage of keys concerning wallets or exchanges, a non-custodial setup is one in which private keys are held by the user directly. |
| *P2P* | Short for peer-to-peer. Refers to a transaction between two people without an intermediary or central authority. |
| *Private key* | Also known as a secret key, this is essentially the encrypted password to someone's crypto holdings. It's an impossibly long number that's practically impossible to guess. You authorise a transaction by signing it with your private key, and private keys can be used to access and manage your crypto assets. |
| *Proof of work* | Commonly written as PoW, many blockchains employ this consensus mechanism to prove that miners have done the computational work to guess |

| | |
|---|---|
| | the 64-character hash necessary to add a block to the blockchain. Broadcasting the solution allows other nodes to quickly verify that your hash is correct and that you have completed the work required. |
| *Public key* | The public-facing address of your crypto wallet. You must share your public key to receive funds into your account. Each public key pairs with a private key, and the private key is only known, in theory, to that user. |
| *Ransomware* | Ransomware is a type of malware used by hackers to steal or encrypt their victims' files to extort them for a ransom in exchange for file decryption or restoration. |
| *Regulated* | A market in which players must follow certain rules of risk fines and/or the loss of their operating licenses. |
| *Spot* | A contract or transaction buying or selling a cryptocurrency for immediate settlement or payment and delivery of the cryptocurrency on the market. |
| *Token* | An individual cryptocurrency. Specifically, it's a way to refer to crypto that runs on a particular blockchain. For example, XRP is a token on the Ripple blockchain. |
| *Tumbler* | A mixing service that helps make cryptocurrency funds and transactions more anonymous. |
| *Wallet* | A digital storage device or location for keeping crypto assets secure. Wallets can be online (also known as a hot wallet) or offline (also known cold wallet). |