THE GOVERNMENT
OF THE GRAND DUCHY OF LUXEMBOURG
Ministry of Justice

ML/TF VERTICAL RISK ASSESSMENT:

VIRTUAL ASSET SERVICE PROVIDERS

DECEMBER 2020

CONTENTS

1. EXECUTIVE SUMMARY

Over the past five years, virtual assets (VAs) have been increasingly adopted for various legitimate activities, including for investments or transactions. Notwithstanding, VAs have certain features that make them vulnerable to abuse by criminals for Money Laundering/Terrorist Financing (ML/TF) activities. The high adoption of VAs by criminals poses significant challenges to virtual asset service providers (VASPs), financial institutions, supervisors and law enforcement agencies.

Multiple factors have contributed to the need for a VASP vertical risk assessment. The 2018 and 2020 Luxembourg National Risk Assessment (NRA)s specifically mentioned VAs as an emerging and evolving risk. Furthermore, different international bodies have set standards for the mitigation of ML/TF risks stemming from VAs and VASPs. The Ministry of Justice has conducted the ML/TF vertical risk assessment on VASP in close collaboration with the relevant AML/CFT supervisory authority (CSSF), the Financial Intelligence Unit (CRF) and other private and public sector entities in Luxembourg.

The risk assessment develops a comprehensive taxonomy of different types of VAs and VASPs and describes the main ML/TF threats they pose. It describes the threats posed by VAs and VASPs in various stages of ML, and outlines the predicate offences that VAs can facilitate, including drug trafficking, fraud and forgery and theft.

The risk assessment identifies the inherent risk of eight VA types and sub-types. Pseudo-anonymous VAs, such as Bitcoin, and anonymous VAs, such as Monero, are deemed as having a very high inherent risk level due to their anonymity, usability and security features.

VA Type	Sub-type	Inherent risk
Exchange VAs	Pseudo-anonymous	**Very High**
	Anonymous	**Very High**
	Platform	**High**
	Stablecoins	**Medium**
Utility VAs		**Low**
Security VAs	Security VAs	**Low**
	Platform VAs with security features	**Medium**
Closed VAs		**Very Low**

The risk assessment also assesses the level of inherent risk of twelve VASP sub-types. The overall risk rating of VASPs is rated at “medium.” It should be noted that VASPs have been required to register with the CSSF since the adoption of Laws of 25 March 2020. Several VASPs are in the process of registration, however there have been no completed registrations at the time of the report which limits the overview of the VASP sector in Luxembourg. As such, this document constitutes a preliminary assessment of this sector to ML/TF risks.

VASP Type	Sub-type	Inherent risk
Issuance	ICO/IEO	**Medium**
Custody	Custodian wallet providers	**Medium**
	Dedicated custodians	**Medium**
Exchange	Centralised exchanges	**High**
	Peer-to-peer exchanges	**Medium**
	Brokers	**Medium**
	VA ATMs	**Low**

VASP Type	Sub-type	Inherent risk
Service and product exchange	Centralised applications	**Medium**
	Decentralised applications	**Medium**
Other	Anonymisation tools	**Medium**
	Fund managers	**Medium**
	Miners or validators	**Low**

The risk assessment also describes the mitigating factors that VASPs are obliged to implement to reduce ML/TF risk as per the 2004 AML/CFT Law, and the different measures implemented by the CSSF, the CRF and prosecution authorities. The CSSF has issued two general warnings on VAs and VASPs and eight warnings on entities, related to VAs, and has developed internal capabilities to deploy AML/CFT supervision of VASPs and is assessing the VASP registration files for several applicants as of mid-November 2020. The CRF has implemented multiple mitigating measures and built up relevant internal capabilities to conduct operational and strategic analyses on VASPs. In 2019, the CRF received 1 622 Suspicious Transaction Reports (STRs) linked to VAs or VASPs on voluntary basis from different entities. Luxembourg prosecution and law enforcement authorities have also implemented necessary internal capabilities to analyse VA-linked cases.

Finally, the risk assessment provides a list of legal obligations for the VASP private sector and presents a list of more than 40 red flag indicators developed jointly with the CRF that should specifically be considered in a VA context. Additionally, the FATF has published red flag indicators on 14 September 2020 which entities should take into account[1]. The list of red flag indicators should support private entities in setting up appropriate transaction-monitoring processes and improving their reporting to the financial intelligence unit. The risk assessment is intended to be updated in the near future when a more complete view of the market becomes attainable.

[1] FATF, *The FATF red flag indicators, September 2020*

2. INTRODUCTION

Over the past five years, VAs became increasingly adopted for various legitimate activities, for example, for investments or transactions. At the same time, VAs have certain features that make them vulnerable to abuse by criminals for ML/TF activities. In 2019 more than $10 billion worth of VAs were used for ML purposes[2]. The high adoption of VAs by criminals poses significant challenges for virtual asset service providers (VASPs), supervisors and law enforcement agencies.

Multiple factors drive the need for a VASP ML/TF vertical risk assessment. First, the 2018 Luxembourg NRA report mentioned VAs as an emerging risk. The 2020 Luxembourg NRA report also recognised the emerging threats of VAs and VASPs. Second, Luxembourg authorities recognised the rising threat of VAs early on and implemented several mitigating actions. Third, different international bodies have set standards for the mitigation of AML/CFT risks stemming from VAs and VASPs.

First, the 2018 NRA recognised VAs as an emerging and evolving ML/TF sectoral vulnerability and called for further risk and mitigation strategies development. In particular, the NRA stated that "the public and private sector would need to increase cooperation towards developing typologies to identify some of these risks and design mitigating measures." The risk assessment at hand aims to accomplish those specified goals. The 2020 NRA also considered the ML/TF risks posed by VAs and VASPs.

Second, in line with the risks identified in the NRA, the Luxembourg relevant authorities have set up mitigating actions to manage the risks of VASPs. Specifically, the Commission de Surveillance du Secteur Financier (CSSF) became the dedicated supervisory authority for VASPs for AML/CFT purposes by the Laws of 25 March 2020. Over the past years, the CSSF has also published several general and entity-specific warnings on VASPs and VAs. The Cellule de Renseignement Financier (CRF) receives information from entities functioning inside and outside Luxembourg, which are reporting suspicious transactions in relation to VAs and VASPs, and coordinates work with international financial intelligence units. To further assist the CRF, the CSSF and other relevant public and private sector entities to mitigate ML/TF risk originating from VAs, a more detailed and in-depth alignment of the landscape and the different risks involved is required.

Third, international authorities have also recognised the risk of VAs and VASPs. In 2018, the EU adopted the 5th AMLD, which subjected providers engaged in exchange services between virtual currencies, fiat currencies and custodian wallet providers to regulation for AML/CFT purposes. In 2019, the FATF published guidance[3] on the application of a risk-based approach to VAs and VASPs. It required countries to identify, understand and assess their ML/TF risks related to VAs and VASPs and to act in order to effectively mitigating those risks. In July 2020, the FATF published a review[4] of the implementation of its standards on VAs and VASPs. The FATF has previously published the "Guidance for a Risk-Based Approach to Virtual Currencies[5]" in 2015. The 2019 EU Supranational Risk Assessment (SNRA)[6] also highlighted the higher risk posed by VAs and VASPs. In addition, the European Banking Authority (EBA) conducted an assessment[7] of the applicability and suitability of EU law to cryptoassets in 2019.

The Ministry of Justice has conducted this assessment in close collaboration with the CSSF, the CRF and different Luxembourgish private sector entities.

---

[2] Ciphertrace, *Q3 2019 Cryptocurrency Anti-Money Laundering Report*, November 2019

[3] FATF, *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, 21 June 2019

[4] FATF, *12 Month Review of Revised FATF Standards - Virtual Assets and VASPs*, 2020

[5] FATF, *Guidance for a Risk-based Approach to Virtual Currencies*, 2015

[6] European Commission, *Supranational National Risk Assessment*, 2019

[7] European Banking Authority, *Report with advice for the European Commission on crypto-assets*, 2019

2.1. VA and VASP definition

2.1.1. VA definition

A definition of VAs and virtual currencies, which is consistent with the 5AMLD's definition of VAs and FATF guidance on VAs and VASPs[8], is included in article 1 (20a) and (20b) of the 2004 AML/CFT Law by the amendments of the Laws of 25 March 2020:

""Virtual currency" shall, in accordance with this law, mean a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by persons as a means of exchange and which can be transferred, stored and traded digitally."

""Virtual asset" shall, in accordance with this law, mean a digital representation of value, including a virtual currency, that can be digitally traded, or transferred, and can be used for payment or investment purposes, except for virtual assets that fulfil the conditions of electronic money within the meaning of point (29) of Article 1 of the Law of 10 November 2009 on payment services, as amended, and the virtual assets that fulfil the conditions of financial instruments within the meaning of point (19) of Article 1 of the Law of 5 April 1993 on the financial sector, as amended."

VAs have unique technological properties that enable pseudo-anonymous and anonymous transactions, fast cross-border value transfer and non-face-to-face business relationships. Those properties have the potential to improve multiple financial products and services such as trade financing, cross-border payments and financial instrument settlement. Traditional financial institutions have recognised those benefits. For example, a survey by the Bank for International Settlements of 63 central banks in 2018 showed that most of them were analysing the possibility to issue central bank-backed VAs[9].

VAs market adoption rate has been increasing globally. The number of VAs with at least $1 million market capitalisation has risen from 30 to approximately 1 000 between 2015 and 2020, with a combined capitalisation of all VAs approaching $300 billion[10].

VAs enable a diversified four-step value chain illustrated in Figure 1:

- **Issuance**: The creation of a VA and its subsequent distribution to investors and users
- **Custody[11]:** The process of storing a VA in a wallet or by a dedicated custodian
- **Exchange:** The process of exchanging a VA into another VA or fiat currency
- **Service and product exchange:** The process of using VAs as a medium of exchange enabling trade for services and products

Figure 1: VA value chain

[8] FATF, *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, 21 June 2019

[9] The Bank of International Settlement, *Proceeding with caution – a survey on central bank digital currency*, January 2019

[10] Coinmarketcap, *https://coinmarketcap.com/*, retrieved 14 February 2019

[11] Note that the terms custody and safekeeping are used interchangeably in this report

To conduct a granular risk assessment, it is necessary to describe the different types of VAs, as different types will have different risk profiles, depending on their properties. Table 1 provides an overview of the different VA types and sub-types world-wide, with description, examples and combined market value.

Table 1: Overview of VA types world-wide

VA Type	Sub-type	Description	Prominent examples	Total market value of all VAs within sub-type[12]
Exchange VAs	Pseudo-anonymous	• Used mostly as a means of exchange or store of value • Transactions can be linked to a specific sender	Bitcoin, Litecoin	~$180 billion
	Anonymous	• Similar to pseudo-anonymous VAs, but transactions cannot be linked to a specific sender	Monero, Dash	~$2.5 billion
	Platform	• Provide access to digital marketplaces and platforms • Primarily focused on use cases to the specific marketplace/platform, but are often used to exchange currency	Ethereum, ERC20 tokens	~$55 billion
	Stablecoins	• Attempt to offer price stability by being backed by a reserve asset (for example, a fiat currency)	Tether, USDC	~$5 billion
Utility VAs		• Assets that allow users to access a specific service of a planned or operational service or product (for example, exclusive benefits for users) and generally resemble vouchers	FC Barcelona Fan Tokens	Not applicable
Security VAs	Security VAs	• Are equivalent to traditional securities, that grant holders voting rights and provide dividend payments but that do not meet all the conditions of "financial instruments" as per MiFID II/MiFIR	Aspencoin	Not applicable
	Platform VAs with security features	• VAs that are presented by issuers as platform VAs, but have built-in functionality that resembles debt or equity (for example, VAs that provide revenue sharing to VA holders)	Binance, Huobi	~$5 billion
Closed virtual currencies		• Designed to be used as a medium of exchange inside closed ecosystems (for example, video games)	World of Warcraft gold	Not applicable

Based on the VAs described in the table above, traditional VA-linked financial instruments may be created. Those are traditional financial products (e.g. investment funds, derivatives) linked to VAs, and may include investment funds investing in VAs or futures based on the value of certain VAs.

[12] Coinmarketcap, *https://coinmarketcap.com/*, retrieved 14 February 2019

2.1.2. VASP definition

A definition of VASPs is included in article 1 (20c) of the 2004 AML/CFT Law, which is consistent with the definition outlined in the FATF international standards[13]:

"Virtual asset service provider" shall, in accordance with this law, mean one of the entities which provides, on behalf of or for its customer, one or more of the following services:

A. the exchange between virtual assets and fiat currencies, including the service of exchange between virtual currencies and fiat currencies;

B. the exchange between one or more forms of virtual assets;

C. the transfer of virtual assets;

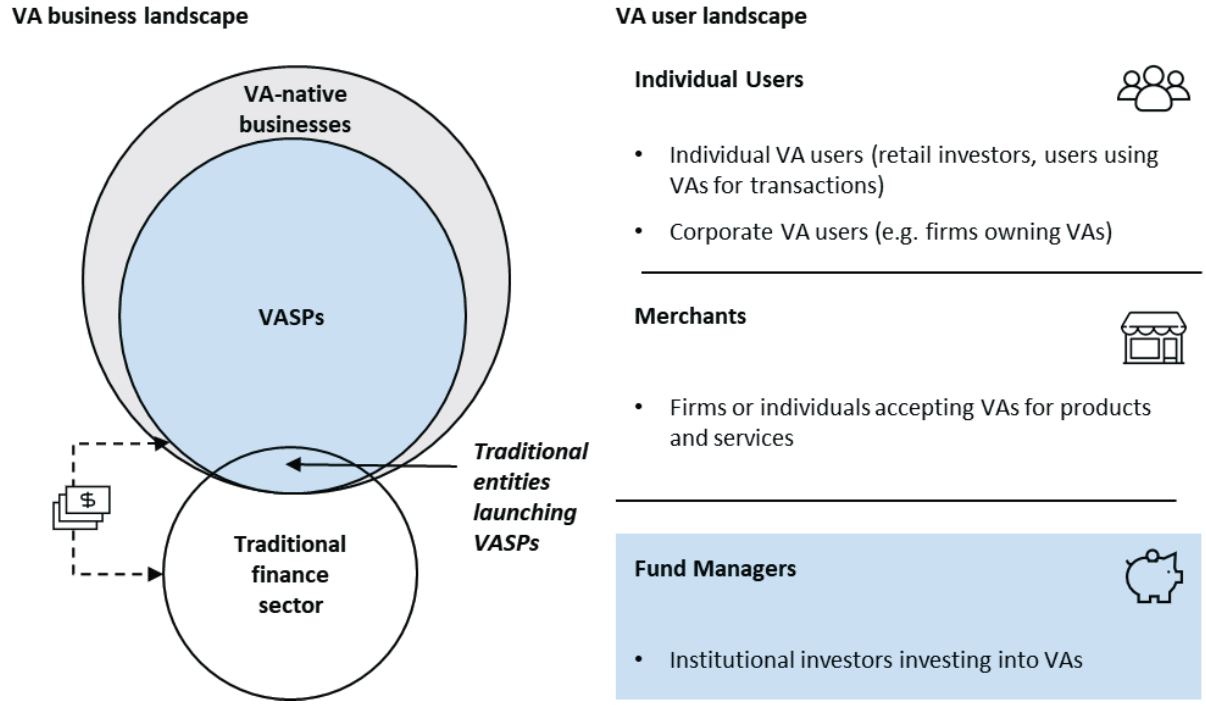
D. the safekeeping or administration of virtual assets or instruments enabling control over virtual assets, including the custodian wallet service;

E. the participation in and provision of financial services related to an issuer's offer or sale of a virtual asset."

Not all businesses that deal with VAs in some capacity fall under the definition of VASPs. Broadly, the VA business landscape consists of three types (see Figure 2, left-hand side):

- **VA-native businesses:** businesses that have direct exposure to VAs, for example through transactional activities
- **VASPs:** VA-native businesses that perform certain VA-based activities or operations in the name of or on behalf of the users. All VASPs fall under VA-native businesses, but not all VA-native businesses are necessarily VASPs
- **Traditional finance sector:** Traditional financial sector entities that launch separate VASPs, or entities that are exposed to VASPs by conducting business activities with them (for example a bank sending fiat currency transactions to an exchange for a user)

Figure 2: VA business and user landscape



[13] FATF, *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, June 2019

An example of a VA-native business that is not a VASP would be a non-custodial wallet. Such an entity offers users a software solution that allows them to self-manage VAs but does not perform transactions or activities in their name or on their behalf. A custodian wallet provider, however, holds private keys of VAs for its users and performs transactions on their behalf, thus classifying the wallet provider as a VASP.

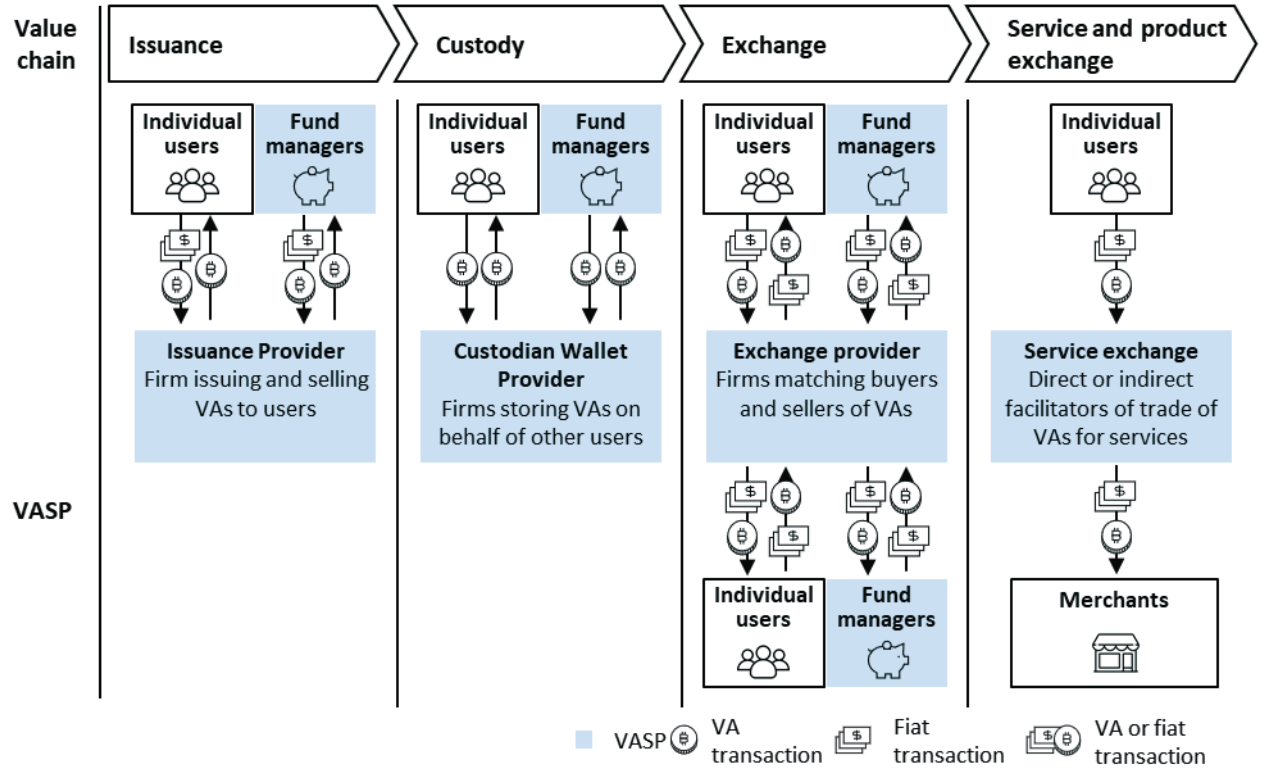
Figure 2 also outlines the three main types of VA users. These include individual users that invest or transact in VAs on their own behalf, such as retail investors and merchants. Investment companies that invest in VAs on behalf of their clients are described under a separate type "Fund managers" (which are any entities offering their clients to invest in VAs) and fall under the VASP classification.

This report will only consider the VASP business landscape, with a full taxonomy described in Section 3 of this report and will separately mention the traditional financial sector.

Most VASPs facilitate transactions between different users described in Figure 2. Figure 3 illustrates different VA or fiat transactions occurring between them:

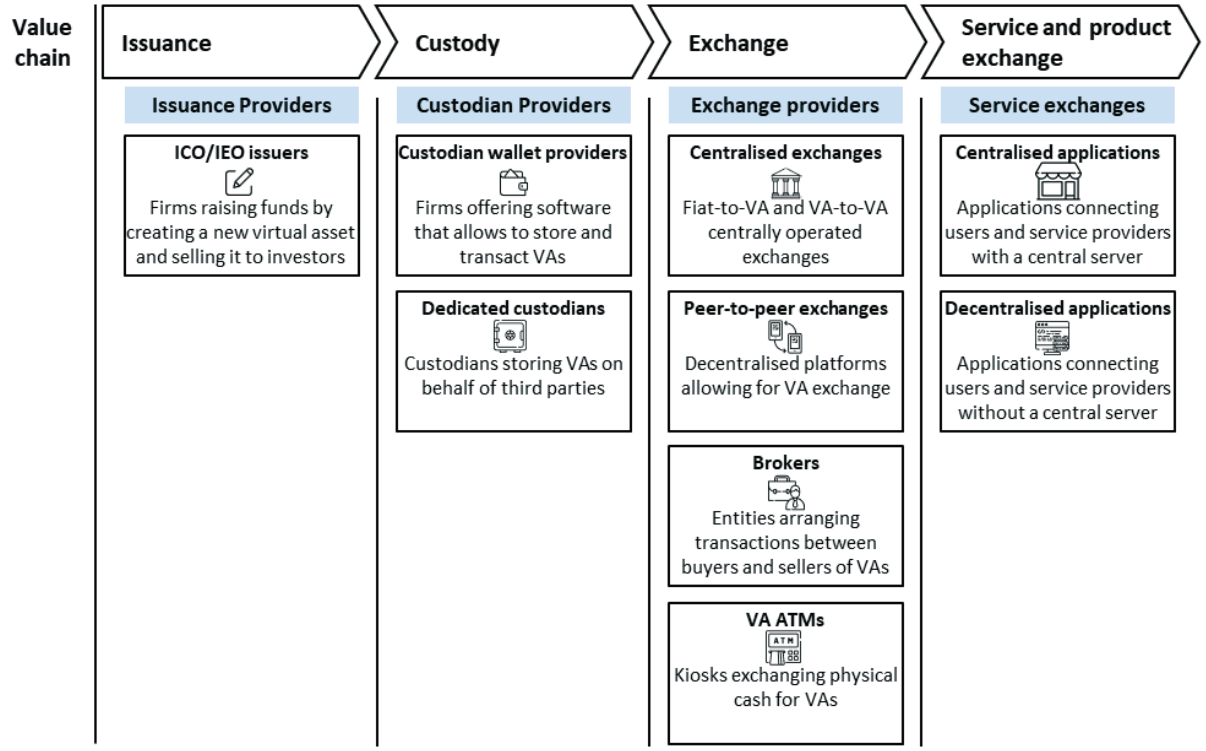
- In the **Issuance** step, individual users and fund managers purchase VAs from an "Issuance Provider". Typically, purchases are made in the form of VAs or fiat currency.
- In the **Custody** step, individual users and fund managers store their VAs using a dedicated "Custodian Wallet Provider" firm. Users can send VAs to the custodian and request subsequent VA withdrawal and transactions.
- In the **Exchange** step, individual users or fund managers send VAs or fiat currency to "Exchange Providers", which in turn match them with buyers and sellers for other VAs and fiat currencies. Most exchanges also serve the custody function, as they store VAs on behalf of their users before and after trade competition. In addition, in some cases, intermediaries may intervene between "exchange providers" and users.
- In the **Service and Product exchange** step, "Service Exchanges" facilitate transactions between merchants and individual users.

Figure 3: Interaction of VASPs and users operating across the value chain



For each of the VASPs operating in a specific value chain step, there may exist multiple sub-types. Altogether, nine main VASP types are operating along the value chain. They are classified and described in Figure 4 below:

Figure 4: Overview of main VASP types



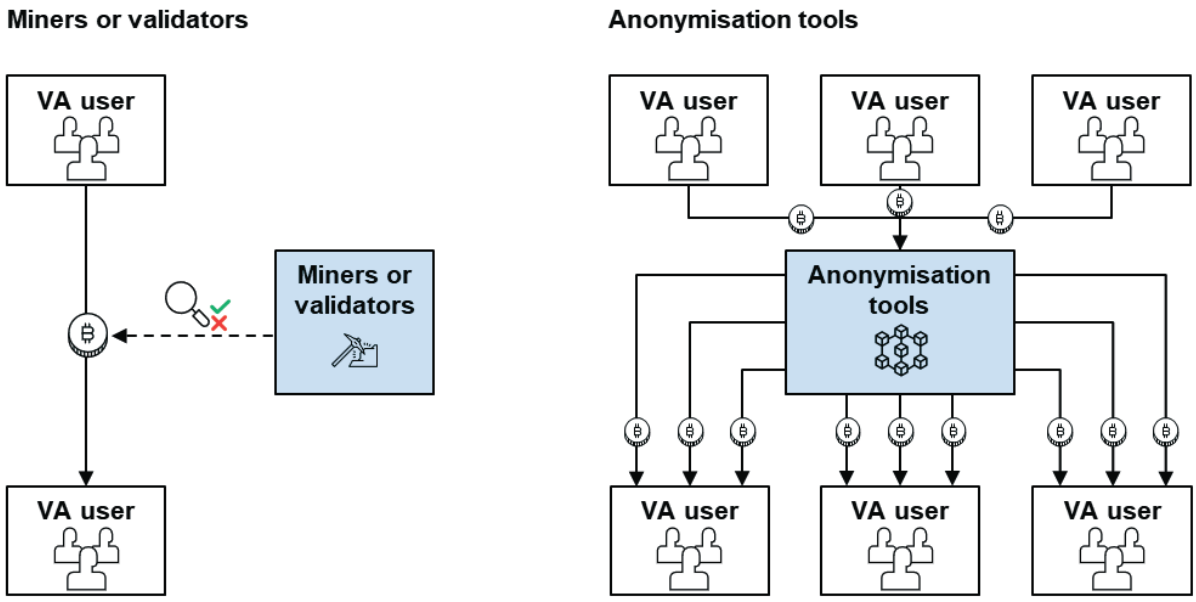
In addition to the nine defined VASP types in Figure 4 and the fund manager VASP in Figure 2, two further VASPs can be uniquely identified which lie outside of the four-step value chain. The two types are described in Figure 5 and include miners or validators and anonymisation tools.

Miners or validators perform cryptographic operations to validate VA transactions of decentralised VAs and receive VA rewards for successful validations. The majority of miners and validators do not conduct transactions on behalf of other users and thus would not be classified as VASPs. However, in some cases, miners or validators could have control over VA transactions (for example, through owning the majority of the "validation" power of the VA network by performing a 51% attack[14] or having specific network rights[15]). In those cases, miners or validators may fall under the definition of a VASP.

Anonymisation tools allow users to pool and mix their VAs to obfuscate transaction flows. They include both centralised solutions and decentralised solutions. In centralised solutions, an individual and/or an entity sends funds to a mixer, which then mixes them and sends funds back. Those mixers would fall under the definition of a VASP. Decentralised solutions refer to software instruments that allow users to mix coins between themselves without an intermediary (for example, through CoinJoin techniques[16]). Thus, such decentralised solutions may not necessarily fall under the definition of a VASP.

[14] More details on a 51% attack can be found here: Investopedia, *51% attack*, May 2019
[15] For example, some VAs have single miners or validators, that could theoretically reverse transactions
[16] More details on CoinJoin anonymisation techniques can be found here: Investopedia, *CoinJoin*, July 2018

Figure 5: Miners/validators and anonymisation tools overview



Description: firms or individuals that validate VA transactions of VA users, and receive VA rewards for successful validations

Description: application tools allowing users to obfuscate transaction information, making it harder for observers to link transactions to specific users

2.2. Overview of Luxembourg VASP landscape

Luxembourg's role as a global financial, investment and international payments centre, together with its stable regulatory framework, provides an attractive environment for new and established financial technology firms. Luxembourg has a track record of financial innovations and is committed to providing a productive and supportive environment for innovative finance businesses[17]. Luxembourg's domestic market offers an appetite for VA-related services, similar to other European countries. According to various surveys, 4 to 8% out of ~600k of Luxembourg residents own VAs[18] [19].

Those factors contributed to VA-related activity being present in Luxembourg. Since the adoption of the Laws of 25 March 2020, several entities have applied for a VASP registration for different types of VA activities (as defined in article 1 (20 c) of the 2004 AML/CFT Law), such as exchanges, custodian wallet services etc. As of mid November 2020, the applications are at different stages of the registration process and no registration is finalised yet.

bitFlyer Europe S.A. and Bitstamp Europe S.A., which are part of **bitFlyer Group** and **Bitstamp Group** respectively, have obtained a payment institution license in Luxembourg and are already supervised by the CSSF for the payment activities which are linked to VA activities (payment flows in fiat currencies). bitFlyer Europe S.A. operates a centralised VA exchange in Luxembourg and allows its clients Single Euro Payments Area (SEPA) transfer deposits and withdrawals (activity provided under the payment institution license). Bitstamp Europe S.A. does not operate a centralised VA exchange in Luxembourg – the exchange is provided by another Bitstamp Group company, Bitstamp Ltd., which is based in the UK.

bitFlyer Group is a Japanese headquartered group that operates three separate exchanges: in Japan (bitFlyer Inc.), in the EU (bitFlyer Europe S.A.) and in the USA (bitFlyer USA, Inc.). The EU exchange is headquartered and operated from Luxembourg. Users from the EU

[17] Luxembourg for Finance, *https://www.luxembourgforfinance.com/en/financial-centre/fin-tech/*, retrieved March 2020
[18] Statista, *How many customers own cryptocurrency?*, August 2018
[19] TNS Ilres, *Le concept des crypto-monnaies au Luxembourg*, February 2018

exchange trade with other users from the EU, but also have access to the Japanese exchange liquidity pool. bitFlyer Group's three exchanges have a combined 30-day trading volume that exceeds $1.5 billion[20]. More than 95% of the trading volume happens on the Japanese exchange, which makes bitFlyer the largest exchange in the Japanese market. They fall under the supervision of the Japanese Financial Services Agency with which CSSF is cooperating. Less than 2% of the volume occurs on bitFlyer's European exchange, with the 30-day trading volume being below $100 million. As of October 2020, bitFlyer Europe S.A. offers trading for four pseudo-anonymous exchange VAs (Bitcoin, Bitcoin Cash, Litecoin, Monacoin) and three platform exchange VAs (Ethereum, Ethereum Classic, Lisk), for a total of 7 VAs. Note that the Japanese exchange offers 4 more additional VAs: Ripple, Basic Attention Token, Stellar and NEM. bitFlyer Europe S.A. offers to trade VAs mostly to residents of the 27 EU member states, the UK and five other countries (e.g. Norway and Switzerland).

bitFlyer Europe S.A. offers two product types related to exchange. It offers "lightning" exchange, by which it facilitates VA trading and matches buyers and sellers on its trading platform. bitFlyer Europe S.A. also offers a "Simple Buy/Sell" feature, which is a more beginner-oriented product allowing customers to instantly purchase VAs from bitFlyer's own inventory. Users can buy VAs with credit cards, debit cards, Sofort, iDeal and GiroPay, and also SEPA transfers. Since September 2020, bitFlyer Europe S.A. also offers users to use PayPal to fund their accounts.

Bitstamp Group, one of Europe's first VA exchanges founded in 2011, has a subsidiary in Luxembourg, Bitstamp Europe S.A. Bitstamp Group's globally-focused business entity, Bitstamp Ltd., operates the Group Exchange and makes this available to Bitstamp Europe S.A. for it to enable its clients to trade ten exchange VAs: three digital currency VAs (Bitcoin, Bitcoin Cash, Litecoin), five platform VAs (Ethereum, XRP, Stellar, Chainlink, OMG Network) and two stablecoins (Paxos Standard, USDC). The actual exchange of VAs happens under the UK group entity Bitstamp Ltd. The combined 30-day trading volume of the exchange exceeds $3 billion[21]. Fiat deposits (through SEPA, international wire or credit card), and fiat withdrawals (through SEPA or international wire) can be linked to the Luxembourg payment institution, Bitstamp Europe S.A. Bitstamp Europe S.A. also allows its clients to make VA deposits and withdrawals, in order to enable them to trade on the exchange platform.

The VA industry in Luxembourg encompasses various software service providers that typically serve a global userbase. The sector includes VA securitisation providers, VASP service providers, other blockchain-related technology firms and other industry associations and groups. The description of their activities is provided below:

- **VA securitisation software providers:** firms that offer solutions to create security VAs from traditional assets
- **VA forensics analytics software:** VAs forensics firms that analyse public transactions of different VAs and develop transaction risk profiles for public authorities and VASPs
- **Blockchain technology firms:** Firms that provide technologies based on the blockchain. While not directly related to VAs, they use the underlying technology closely linked with VAs
- **Other (industry associations, research and education organisations):** Other organisations include industry groups and research institutions that promote the development of the VA industry (for example, LetzBlock)

[20] CoinGecko, *bitFlyer Statistics*, Retrieved 2 March 2020
[21] CoinGecko, *Bitstamp Statistics*, Retrieved 2 March 2020

2.3. ML/TF context of VAs and VASPs

At the international level, the global VAs and VASPs space has grown over the past five years. The various types of VAs and VASPs described in the previous sections highlight the overall development of the industry. The number of VA and VASP types has been accompanied by more VA users, transactions and revenues. The number of VAs users worldwide was 45 million in 2016 and around 139 million by 2019[22]. The VASP industry servicing VA users has also grown, with VA exchanges generating multi-billion revenues in 2019[23]. In Luxembourg, according to various surveys, 4 to 8% out of ~600k of Luxembourg residents own VAs[24] [25]. In 2019, the CRF received 1 622 STRs linked to VAs or VASPs on voluntary basis from different entities.

The increased user adoption of VAs and their inherent technological features led to a significant uptake of VAs for ML/TF activities. VAs power illegal products marketplaces and investment fraud schemes, the combined revenues of which exceeded $1 billion in the same year[26]. VAs are also increasingly used by terrorist financing groups, cybercriminals and sexual exploitation profiteers [27].

Globally, several jurisdictions and international bodies have recognised the rising ML/TF threat of VAs and VASPs. FATF highlighted virtual currencies as one of the key emerging risks to ML and TF, and in particular tax evasion and fraud offences[28]. The EU Supranational Risk Assessment recognised the rising risk of VAs and VASPs being misused for ML/TF purposes[29]. Further, some countries have explicitly analysed the vulnerability of VAs and VASPs and published correspondent risk assessments.

2.4. The regulatory status of VASPs in Luxembourg

The definitions for VAs and VASPs are included in the 2004 AML/CFT Law modified by the Laws of 25 March 2020. Since then, the CSSF is the competent authority in Luxembourg for the supervision of VASPs; however, the CSSF is only responsible for AML/CFT supervision. Any entity, including any entity already licensed or registered by a competent authority and in particular licensed financial institutions, which is established or offers or intends to offer in Luxembourg any of the virtual asset services as detailed in section 2.1.2 has to:

- Comply with the professional obligations and the conditions described in the 2004 AML/CFT Law, as amended by the Laws of 25 March 2020
- Register with the CSSF as a VASP

CSSF's role for the VASPs registered in Luxembourg is limited to registration, supervision and enforcement for AML/CFT purposes. The requirement of registration for applicants, who are established or provide services in Luxembourg, is without prejudice to any other license or registration or other status required either in Luxembourg or by other European or third countries for any other activities performed by the applicant.

[22] Cambridge Centre for Alternative Finance, *2nd Global Cryptoasset Benchmarking Study*, December 2018
[23] Messary Crypto, *Estimating "Real 10" Exchange Revenue*, 11 April 2019
[24] Statista, *How many customers own cryptocurrency?*, August 2018
[25] TNS Ilres, *Le concept des crypto-monnaies au Luxembourg*, February 2018
[26] Ciphertrace, *Q4 2019 Cryptocurrency Anti-Money Laundering Report*, February 2020
[27] Chainalysis, *2020 Crypto Crime Report*, January 2020
[28] FATF Report, *Virtual currencies – key definitions and potential AML/CFT risks*, June 2014
[29] European Commission, *Supranational Risk Assessment*, July 2019

3. STAKEHOLDERS, METHODOLOGY AND DATA

This section goes further into the methodology description of the VASP ML/TF vertical risk assessment. It describes the stakeholders that took part in producing this report, overviews taxonomy and methodology and describes the data used.

3.1. Stakeholders in this assessment

The **Ministry of Justice** has written this report. The following stakeholders have contributed to the report with analysis, feedback, case studies and data provision:

- **CSSF and CRF representatives**: both the CSSF and CRF experts have been key collaborators in producing this risk assessment by providing regular input and feedback in bilateral meetings, workshops and written correspondence
- **Public and private sector representatives**: Ministry of Justice has engaged with several public and private sector representatives to communicate views on VA/VASP ML/TF risks and mitigating factors. Information and opinions were exchanged in bilateral meetings with the following:
  - **Public sector experts:** *"Parquets d'Arrondissement,"* Judicial Police (SPJ), University of Luxembourg
  - **Private sector experts:** Chief Compliance Officers, Chief Executive Officers and other representatives from bitFlyer Europe S.A. and Bitstamp Europe S.A., Tokeny, LetzBlock (non-profit association created to promote the Luxembourg Blockchain ecosystem), ABBL (Luxembourg's Banking Association) and ALFI (Luxembourg's Investment Fund Association).

3.2. Methodology

The methodology in this report is closely aligned with the approach used in Luxembourg's NRA. It is based on an assessment of inherent risk from threats and vulnerabilities, illustrated in Figure 6, and an overview of mitigating measures.

Figure 6: Risk assessment methodology

The risk assessment thus identifies and evaluates ML/TF threats and vulnerabilities of VAs and VASPs (inherent risk), and then describes the mitigating measures integrated by the public and private sector participants (mitigating actions). As the last step, an action plan is formulated to identify additional potential mitigating measures. Each chapter of this report covers a specific risk assessment step.

Compared to the NRA, the risk assessment at hand does not assess the residual risk level of VASPs. The CSSF became the competent authority for the VASP registration process and the related AML/CFT supervision on 25 March 2020. As of mid November 2020, several entities are in the process of registration, and no entity has completed the full process. Therefore, a full view of the effectiveness of mitigating factors of the complete VASP sector, and a subsequent residual risk estimation, is premature and out of the scope of the report.

Sectoral vulnerabilities are assessed using a scorecard approach, described in detail further in this section. The scorecard approach consists of three steps: defining the risk criteria, collecting data and information for each criterion, and then scoring the risk. Note that the

scorecard approach is utilised for VAs and VASPs separately. The risk rating of VAs is used as an additional risk criterion for assessing VASPs risks.

3.2.1. Scope and taxonomy

The assessment considers the VASP taxonomy presented in Table 2, consisting of 12 elements. Note that in addition to the nine VASP types operating in the four-step VA value chain (described in Figure 4), the taxonomy includes three additional VASP types described in the Introduction section of this report: anonymisation tools, fund managers (any entity offering investments in VA to their clients) and miners or validators. Further, the assessment separately mentions VA-related ML/TF risks to the traditional financial sector of Luxembourg.

Table 2: VASP taxonomy

VA value chain step	VASP type
Issuance	ICO/IEO
Custody	Custodian wallet providers
	Dedicated custodians[30]
Exchange	Centralised exchanges
	Peer-to-peer (decentralised) exchanges
	Brokers
	VA ATMs
Service and product exchange	Centralised applications
	Decentralised applications
Other	Anonymisation tools
	Fund managers
	Miners or validators

The taxonomy for VAs vulnerability assessment consists of all types mentioned in Table 1, except VA-linked financial instruments, as they fall outside of the scope of the VASP sector.

3.2.2. Inherent risk: Threat Assessment

Threats are defined as different predicate offences that generate illicit proceeds that could lead to ML/TF activities. The goal of the threat assessment analysis is to identify the nature of the predicate offences and assess the exposure of VAs and VASPs to them.

The report examines the same threat taxonomy as defined in the 2020 Luxembourg NRA Table 3 overviews the threat taxonomy and describes total Luxembourg's ML/TF exposure to each threat, as assessed in 2020.

The report further describes in more detail the threats which are most relevant to Luxembourg's VASP industry. The selection of threats for analysis in this report was based on the overall threat level of predicate offences in the NRA, international volume, number of STRs in Luxembourg, Luxembourg VA features increasing risk and severity of non-monetary consequences. The detailed threat evaluations further in the report include overall VA

[30] Dedicated custodians are similar in their services to custodian wallet providers (safekeeping or administration of virtual assets or instruments enabling control over virtual assets, on behalf of or for their customer) with a difference that they offer their services to institutional investors

relevance to the threat, global and Luxembourg scale of offences, and case studies to illustrate their relevance to Luxembourg further.

Table 3: Threats taxonomy and total Luxembourg exposure as assessed in Luxembourg NRA 2020

Designated predicate offense	Exposure
Money laundering (average ML threat)	Very high
– Fraud and forgery	Very high
– Tax crimes	Very high
– Corruption and bribery	Very high
– Drug trafficking	High
– Participation in an organised criminal group & racketeering	High
– Sexual exploitation, including sexual exploitation of children	High
– Cybercrime	High
– Counterfeiting and piracy of products	High
– Smuggling	High
– Robbery or theft	Medium
– Trafficking in human beings and migrant smuggling	Medium
– Illicit arms trafficking	Medium
– Insider trading and market manipulation	Medium
– Illicit trafficking in stolen and other goods	Medium
– Extortion	Low
– Environmental crimes	Low
– Murder, grievous bodily injury	Low
– Kidnapping, illegal restraint, and hostage taking	Low
– Counterfeiting currency	Low
– Piracy	Low
Terrorism and terrorist financing	Medium

3.2.3. Inherent risk: Vulnerabilities Assessment

Vulnerability refers to the relative exposure of an industry sector or sub-sector for ML/TF purposes. The FATF uses the following definition for vulnerability: they are “things that may be exploited by the threat, or that may facilitate its activities”[31].

First, the report examines the vulnerability of each VA type described in Table 1. Each VA type risk is analysed along the same dimensions. The VA types vulnerabilities are assessed according to three broad dimensions presented in

[31] FATF, *FATF Guidance on National Money Laundering and Terrorist Financing Risk Assessment,* February 2013

Table 4: anonymity, usability and security. The dimensions reflect the factors driving a criminal to select one VA over another for ML/TF purposes.

Table 4: VA vulnerability assessment analysis dimensions

Dimension	Sub-dimension	Risk factor question	Data points (examples)
Anonymity	Inherent anonymity features	Can transactions and users be traced on the public blockchain?	• Public blockchain observer capabilities
	Second layer anonymity features	What software solutions exist that allow to further increase anonymity of VAs, and how effective are they?	• Number and type of available anonymity second layer features
Usability	Transaction liquidity	Is the virtual asset widely used and accepted?	• Transaction volume of asset • Number of users
	Exchange liquidity	Can the virtual asset be easily bought and sold?	• Market capitalization of virtual asset • Exchange volume
	Stability	Is the VA a good store of value?	• Volatility of exchange rate
	Ease of usage	Is it simple to store and send the VA to other users?	• Technical requirement for wallet creation and usage
Security	Governance and ownership	Can transactions and user be blocked or black-listed by virtual asset miners?	• Centralization/decentralization of virtual asset
	Technical security	Does the VA have vulnerabilities that might reduce its security (i.e. individual hacking risk/mining double-spend attacks)	• Hashrate and hashing algorithm

Second, the report examines the vulnerability of VASP types. The vulnerability assessment is conducted at the level of each element of the taxonomy specified in Table 2. The same evaluation criteria is used for each taxonomy element.

VASP vulnerabilities are driven by multiple factors that include market structure, ownership specifics, products and activities, geography, clients and transactions, and channels. Full dimensions for the vulnerability assessment are presented in Table 5 below.

Table 5: VASP vulnerability assessment analysis dimensions

Dimension	Sub-dimension	Data points (examples)
Structure	Size	• Assets • Revenue/turnover • Employees
	Fragmentation / complexity	• # of registered or licensed firms operating • Level of concentration (e.g. top 5 entity assets as a % of the market)
Ownership		• % ownership by foreign entities (of which from risky countries based on risk rating)
Products/ activities	VA type exposure	• Nature of VAs offered to clients (correlates with VA identified score)
	Product and activity specifics	• Underlying product and activity • Easy of usage for onboarding • Easy of usage for transactions

Dimension	Sub-dimension	Data points (examples)
Geography	International business	• % of international business (e.g. in clients' revenue, assets, transactions) • Branches and/or subsidiaries in high risk countries
	Flows with weak AML CFT measures geographies	• % of high-risk geographies based on FATF list of geographies with weak AML/CFT measures (e.g. in clients' revenue, assets, transactions)
Clients/ transactions	Volume	• Number and type of clients: Total number (stock) and new clients per year (flow) • Exchange volume (for exchanges)
	Risk	• % high risk clients (based on supervised entities internal models) • % PEPs (over time): domestic vs. foreign • Types of clients (e.g. natural vs legal persons)
Channels		• Type of interaction: % face-to-face, indirect (e.g. online), via intermediaries • Ability to know customer (e.g. decentralised applications would not know their users' identities)

Table 5 outlines the "VA type exposure" sub-dimension of a VASP. The sub-dimension reflects the relative ML/TF risk of VASP arising from interacting with different VA types. Thus, the VA risk assessment score is transposed into the overall VASP risk assessment.

3.3. Data

The risk assessment relies on both quantitative and qualitative information. The VA ML/TF risk assessment uses mostly publicly available data to identify products with the highest risk. The VASP ML/TF threat assessment utilises both publicly available information, information from the CRF and the CSSF and private information from entities operating in Luxembourg. Case studies provided by the CRF and private sector entities are used to further support the analysis.

For some threats and vulnerabilities assessments, only limited data were available. That limitation was driven by the inherently anonymous nature of some VAs and VASPs, as well as the general low maturity of the sector when compared to other financial industries. Thus, parts of the analysis for the risk assessment of threats and vulnerabilities relevant to Luxembourg were based on global benchmarks. Where information was missing, the assessed level of risk has been increased, in line with a conservative approach recommended by FATF.

4. INHERENT RISK – THREAT ASSESSMENT

The purpose of this section is to describe how VAs and VASPs can be abused for ML and TF purposes and describe the most significant threats to Luxembourg. The section consists of four sub-sections:

4.1 Exposure of VAs and VASPs to ML/TF threats: describes threats posed by VAs and VASPs in different stages of ML, from integration and layering to placement stage. It outlines mechanics of those threats and illustrates how VASPs across the VA value chain can be abused to commit predicate offences, and launder proceeds generated either in fiat currency or VAs.

4.2 Most significant VAs and VASPs ML threats to Luxembourg: identifies and evaluates most significant threats posed by VAs and VASPs to Luxembourg, which are drug trafficking, fraud and forgery, and theft. It further describes other emerging threats, which are smaller in scale but increasingly posing more risks, such as cybercrime, extortion and sexual exploitation.

4.3 VAs and VASPs TF threats to Luxembourg: describes how VAs can be used to finance terrorist activities and organisations. It further describes the development of VA TF-related threats globally and in Luxembourg.

4.4 Global threats of VAs and VASPs: describes the global nature of threats stemming from VAs, VASPs domiciled in Luxembourg and also VASPs not domiciled in Luxembourg but offering services in Luxembourg.

4.1. Exposure of VAs and VASPs to ML/TF threats

VASPs are exposed to ML at all stages of the ML process: placement, layering, and integration. Placement refers to the initial entry of illicit proceeds into the financial system. Layering refers to activities by which criminals distance the illicit money from its source. Integration refers to the process when criminals receive the illicit money, which appears to come from legitimate sources[32].

- During the **placement** step, the criminal places illicit proceeds into the VASP system. The illicit money can be already in the form of a VA (for example, due to selling illegal drugs on darknet markets), or in fiat. In the case of fiat placement, the criminal requires to first exchange fiat into VA and thus would send fiat money to a centralised VA exchange, OTC brokers, or VA ATMs. In the case of VA placement, the criminal may send VAs to a custodian wallet provider, a dedicated custodian or any other VASPs providing safekeeping services.
- The VASP exposure to the placement step scheme is complicated by the fact that criminals can use both VA and fiat in that step and could enter the VA industry across all value chain steps described in the Introduction chapter of this report.
- During the **layering** step, the criminal would obfuscate the transaction flow by sending illicit VAs to single or multiple VASPs. The criminal is constrained by the fact that most widely adopted and liquid VAs are pseudo-anonymous VAs, which increases the probability of their exposure by blockchain forensics software. However, modern VA-native tools such as anonymisation tools (i.e. mixers) and peer-to-peer exchanges have the potential to significantly reduce traceability of criminals' transactions.

[32] FATF, *Money Laundering Frequently Asked Questions,* retrieved 6 March 2020

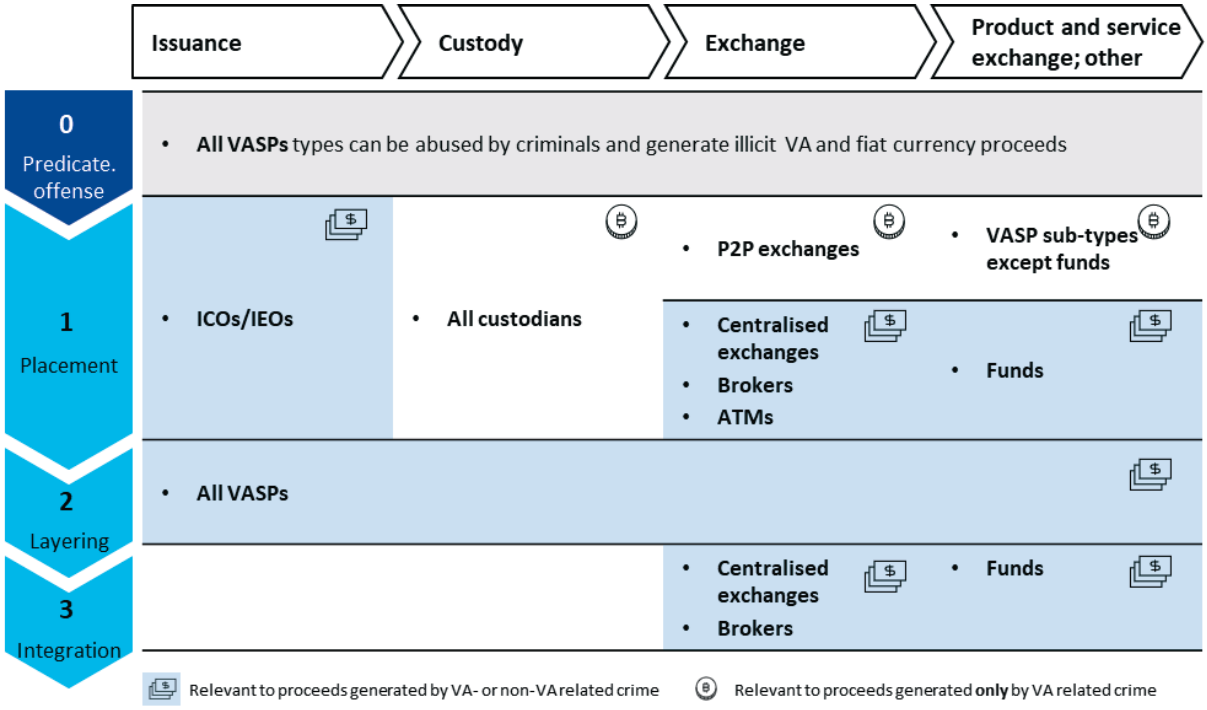
- The **integration** step involves the criminal withdrawing funds in fiat to a bank account or exchanging VAs into cash physically or using VA/laundered funds for buying goods and services. Thus, the last step almost always includes credit, e-money or payment institutions, which may operate accounts to which criminals receive money from exchanges.

Figure 7 below illustrates how VASPs operating across the different VA value chain steps can facilitate different ML steps. Further, the figure illustrates which type of proceeds can be laundered under each ML step: either just VA proceeds, or both VA and fiat proceeds.

The figure has three essential takeaways:

1. VASPs can be abused by criminals to commit the actual predicate offence.
2. All VASPs can be abused during the placement stage if the criminal generated crime proceeds in VAs, but only certain VASP types can be abused to place proceeds generated in fiat currency.
3. Only centralised exchanges, brokers and funds can be abused during the integration stage.

Figure 7: Potential exposure of VASPs to each ML step



The exposure of VASPs to ML-related threats is due to multiple factors, including the following:

- Anonymous properties of VAs
- Non-face-to-face business relationships
- International nature of business
- Limited censorship abilities of VAs
- Volume of transactions
- Technological complexity of VAs and VASPs

4.2. Most significant VAs and VASPs ML threats to Luxembourg

The technological and market factors of VAs and VASPs imply that proceeds from all predicate offences, identified in the NRA, can be laundered through them. This section aims to detail out some of the most significant threats to Luxembourg, selected based on multiple factors including most prevalent STRs observed globally, and has a sub-section for each one: **drug trafficking, fraud and forgery, theft and emerging** and **evolving threats.**

The sub-sections are structured similarly. First, they describe the VA's and VASP's relevance to the threat. Second, they describe the international volume of the threat and recent developments. Last, they evaluate Luxembourg's specific threat significance, with a case study to further support it.

4.2.1. Drug trafficking

Drug trafficking is a significant global threat and is estimated to generate ~30% of crime proceeds globally[33]. It has a high human and social cost, as it leads to drug addiction, health problems and death while also directly financing organised crime.

The VA space is relevant to drug trafficking in two significant ways. First, proceeds from drug trafficking can be laundered through VASPs. Criminals can generate drug trafficking revenue in fiat, convert that fiat into VAs, and then exchange VAs back into fiat currency. Second, VAs can be used as part of the criminal offence itself (step 0 in Figure 7) as a medium of exchange. Multiple online "darknet" markets exist that connect drug buyers and sellers, in which trade can be facilitated only with VAs.

Drug darknet markets offer certain advantages related to anonymity to criminals selling drugs. First, they allow obfuscating communication and transaction flows. Second, the process of drug transfer is also often anonymous. A frequent method to sell drugs via "darknet" marketplaces involves sellers hiding drugs in public areas and then providing locations to buyers. Thus, the buyer and the seller of the drug never actually physically meet.

Globally, drug "darknet" marketplaces have become a rising and resilient threat. The yearly sales approached $800 million in 2019[34], representing a 70% growth on 2018. The growth has been accompanied by an increasing transaction number from 9 million to 12 million. As of January 2019, more than 49 darknet markets operated, with the majority of them catering to a global userbase[35].

Important to note is the resilience of the drug markets to both exchange rate variability and closures. The "2020 State of Crypto Crime" report by Chainalysis stated that the "Darknet" transaction activity remains stable during volatile exchange rate periods, suggesting a weak link between speculation seasonality of VAs and drug sales[36]. Further, there is a steady demand driver for drug "darknet" marketplaces allowing for new marketplaces to emerge even as older ones are closed. For the eight darknet markets that have closed in 2019, eight new markets have launched[37].

[33] UNODC, *Report Estimating Illicit Flows Resulting from Drug Trafficking and Other Transnational Organised Crimes*, 2011

[34] Note that the figure includes non-drug "darknet" markets, for example specialised markets for stolen credit cards. However, the majority of volume happens on drug markets. (Source: Chainalysis, *2020 Crypto Crime Report*, January 2020)

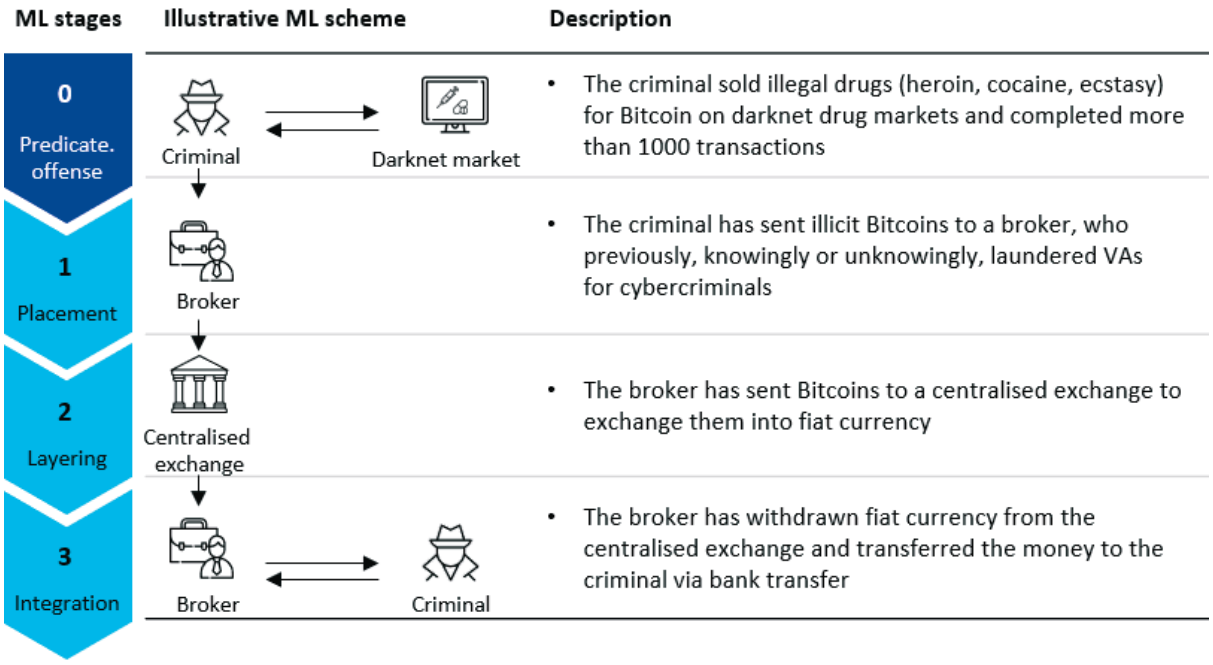
[35] Chainalysis, *2020 Crypto Crime Report*, January 2020

[36] Chainalysis, *2020 Crypto Crime Report*, January 2020

[37] Chainalysis, *2020 Crypto Crime Report*, January 2020

Both Luxembourg and VASPs are exposed to the drug trafficking VA-related threat. For Luxembourg, drug trafficking is one of the most significant domestic and external threats as identified in the NRA, and VAs offer new tools, thereby increasing the threat exposure. For Luxembourg operating VASPs, darknet markets expose a significant threat as the majority of world-wide outflows (43%) and inflows (32%) to and from darknet markets come from exchanges[38]. In 2019, the CRF recorded 25 STRs related to drug trafficking and VAs[39]. The CRF also received a significant number of reports that show exposure to darknet markets. Although it is not possible to prove what has been purchased, it is likely that a number of these reports could be linked to drug trafficking.

Figure 8: CRF Luxembourg VA Drug Trafficking Case Study



4.2.2. Fraud and forgery

This section analyses the relevance of VAs and VASPs to specific sub-categories of Fraud and Forgery, as categorised by the FATF National ML and TF Risk Assessment Guidance[40].

Fraud in this section generally refers to investment frauds, scams and phishing. VAs enable those threats as they allow criminals to remain pseudo-anonymous in their operations. Furthermore, historically specific VAs have offered substantial returns to investors within short periods (for example, the Bitcoin price increased from ~$1 000 to ~$14 000 between January 2017 and 2018)[41]. These returns enable criminals to promise potential victims substantial returns and increase the probability that victims will be deceived.

Forgery in this section refers to fake passports, identification and other documents. Criminals use forged documents to pass KYC/AML checks on VASPs and be able to use them.

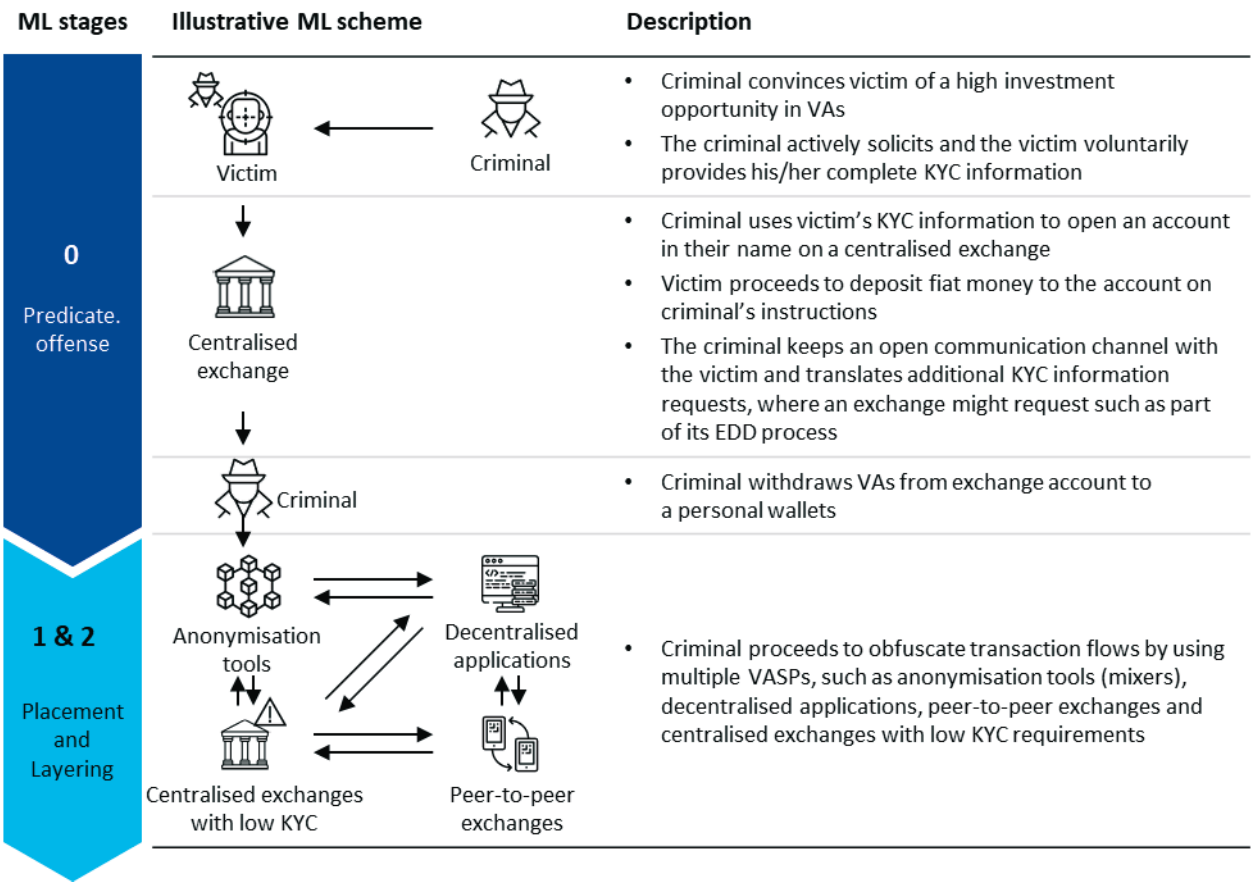
[38] Chainalysis, *2020 Crypto Crime Report*, January 2020
[39] CRF Data received on 2 March 2020
[40] FATF, *National money laundering and terrorist financing risk assessment*, February 2013
[41] Coinmarketcap, *Bitcoin 2017 price dynamics*, retrieved 15 February 2019

Globally, the total monetary amount of investment frauds, which use VAs in their operations, has reached $4 billion volume in 2019. The majority of those funds are linked to Ponzi schemes, which counted 2.4 million individual transactions. Significant amounts also can be linked to phishing, fake ICOs and other investment scams, the combined volume of which exceeded $100 million in 2019[42].

Luxembourg's position as an investment hub increases the probability that criminals can abuse or misuse the investment sector to conduct fraud. While no known large-scale Ponzi or investment schemes were operated from Luxembourg, several fraudulent VASPs falsely claimed they were regulated there. Criminals were abusing Luxembourg's reputation for having a stable investment and regulatory environment. The CSSF has been monitoring the global VASP space and has issued warnings on eight entities falsely claiming to have a license in Luxembourg in 2019, including an investment scam and a fake exchange. Altogether, the CRF has reported 600 VA fraud STRs, and 655 VA forgery STRs in 2019[43].

Luxembourg VASPs can be exposed to fraud as globally, many proceeds from fraud crimes are sent to exchanges (58% of all funds)[44]. VASPs are also exposed to forgery as criminals would try to pass KYC/AML checks with the use of fake IDs and documents.

Figure 9: Luxembourg VA Fraud Case Study



[42] Chainalysis, *2020 Crypto Crime Report*, January 2020
[43] CRF Data received on 2 March 2020
[44] Chainalysis, *2020 Crypto Crime Report,* January 2020

4.2.3. Theft

VAs have unique technological features that make them an attractive target to cybercriminals. First, most VAs have irreversible transactions, meaning that stolen funds are hard to retrieve. Second, VAs provide a certain level of anonymity, making it hard to trace criminals stealing funds. Third, VAs are based on new technologies, and users who are not adept at securing access to VAs are prone to being victims of organised cybercriminals.

VASPs, and in particular centralised exchanges with custody services, have been a target of cybercriminals thefts for many years. In 2019, 11 VA exchanges were hacked globally with stolen funds exceeding $282 million, while in 2018 $875 million was stolen from 6 exchanges[45]. More than 80% of all stolen funds from VA exchanges are transferred to other centralised exchanges[46].

Luxembourg VASPs can be exposed to theft through criminals laundering their proceeds through VASPs and by being a direct victim of a hack and subsequent theft. As exchanges operate in Luxembourg in some capacity, there exists a probability that they can be used for ML of theft proceeds. In addition, they may store VAs on behalf of their users and thus could be attractive targets to cybercriminals.

Figure 10: CRF VASP case study on theft

"The CRF received information that a foreign company computer system was infected by a malicious program which was used to take control of the victims' bank account and transfer money to a Luxembourgish entity. In total €293 616 were stolen, of which the CRF was able to freeze €124 776. The stolen assets were converted into approximately 22.2 Bitcoin and 220 Ethereum."

As of October 2020, the victim's national law enforcement agency was contacted, and the funds will be returned.

4.2.4. Emerging and evolving threats

All NRA threats can be linked with VAs and VASPs. The rapidly evolving landscape of VASPs implies that some threats will become more relevant in the future, which requires public authorities to analyse them in detail. This report will describe three of those evolving threats: cybercrime, extortion and sexual exploitation. Those threats have been rising globally and pose high social and human costs in addition to financial costs.

Cybercrime: Cybercrime threat in this report refers to proceeds generated from selling hacking services, such as ransomware. Ransomware enables criminals to hold computer systems hostage until the victims pay a ransom, which is often paid in VAs. Globally, more than $6.6 million was paid to ransomware wallets in 2019. The CRF reported 27 cybercrime VA-related STRs in 2019[47]. In one example, Belgium authorities reported to the CRF that an online platform selling access to hacked servers used a Luxembourg centralised exchange as the primary payments service. In response, the CRF has frozen all VAs of the suspect on the platform operator, and the Luxembourgish law enforcement seized €228 914.

Extortion: VA's have been increasingly used for various extortion schemes. They include ransomware attacks on companies and personal threats blackmailing individuals. Globally, the revenue coming from extortion reached $20 million in 2019[48].

[45] Chainalysis, *2020 Crypto Crime Report*, January 2020
[46] Chainalysis, *2020 Crypto Crime Report,* January 2020
[47] CRF Data received on 2 March 2020
[48] Chainalysis, *2020 Crypto Crime Report*, January 2020

The CRF has observed extortion reports in Luxembourg. In one case a Luxembourgish company got their files encrypted by a hacker group, who requested a ransom of €500 000 to be paid in Bitcoin. In another case, the CRF received a report that a non-Luxembourgish suspect, who used sexual photos and videos of his victims to blackmail them into paying a ransom with VAs, used a Luxembourg centralised exchange to launder proceeds. Altogether, the CRF received 15 VA-related extortion STRs in 2019[49].

Figure 11: CRF VASP case study on extortion

"The CRF was informed by a foreign law enforcement authority that a user at a Luxembourgish virtual assets exchanger was running a large-scale extortion scheme. The suspect used sexual photos and videos of his victims to blackmail them into paying a ransom with virtual assets. By analysing the transactions, the CRF found that the Luxembourgish virtual assets exchanger was only one of several exchangers that the suspect used in order to convert the proceedings of his ransom into fiat money. His intent was to transfer the fiat money to a foreign bank account and thus to launder the funds. Although the CRF was able to freeze the transaction, lack of conclusive evidence made it impossible to seize the funds."

Sexual exploitation, including sexual exploitation of children: VA's can be used to power darknet markets for illicit goods and services, including markets for child sexual abuse material (CSAM). While the volume of CSAM darknet markets is lower than for darknets for other illicit goods (with the most massive known CSAM VA marketplace having transacted less than $1 million in three years)[50], the human and social cost of those markets can be dramatically high. Note that as of November 2020, there have been no confirmation of this activity in Luxembourg

Figure 12: International VASP case study on sexual exploitation

An example of the scale CSAM darknet markets can reach is the South Korean "Welcome to Video" website, which was the most massive known CSAM market before it was down by US law enforcement agencies in 2018. Between 2015 and 2018, the site received nearly $353 000 worth of Bitcoin across thousands of transactions[51]. The subsequent investigation and international operation yielded in arrests of 337 subjects in 38 countries. Notably, the operation resulted in the rescue of at least 23 minor victims in the United States, Spain and the United Kingdom, who were being actively abused by the website's users[52]. The case further highlights the outsized human cost relative to the monetary value laundered of sexual exploitation darknet markets.

4.3. VAs and VASPs TF threats to Luxembourg

VAs represent a potential alternative to fiat currency for terrorism financing. VAs can be used by terrorist organisation donors to give donations pseudo-anonymously and avoid sanctions. According to a report published by The Middle East Media Research Institute, the list of terrorist organisations that have received donations in Bitcoin include ISIS, Al-Qaeda, Hamas and the Muslim Brotherhood[53].

The global scale of VA is challenging to quantify as most TF cases involve sensitive information and are classified for national security reasons. Current estimates of global VA TF

[49] CRF Data received on 2 March 2020
[50] Chainalysis, *2020 Crypto Crime Report*, January 2020
[51] United States Department of Treasury, *National strategy for combating terrorist and other illicit financing*, 2020
[52] The United States Department of Justice Office of Public Affairs, *Press Release Number: 19-1,104*, 16 October 2019
[53] Middle East Media Research Institute, *The Coming Storm – Terrorists Using Cryptocurrency*, August 2019

activity range from tens of thousands to millions of US dollars transferred annually for TF purposes[54] [55]. Similar to the sexual exploitation threat, TF threat coming from VAs has an outsized human and social cost relative to the monetary value of transactions, and thus should extensively be monitored by public authorities.

An alarming threat is the rising sophistication of terrorist organisations in relation to VAs. A report published by the New York Times in 2019 provided two examples of the technological progress made by TF criminals. In 2016 a designated terrorist organisation based in Gasa, Mujahedeen Shura Council in the Environs of Jerusalem, conducted a financing campaign and accepted donations in Bitcoin. The organisation provided a single Bitcoin address, which made it easier for law enforcement authorities to track funds. In 2019, a Hamas military wing also based in Gasa, ran a more advanced campaign and created a new Bitcoin address for each potential donor, which made tracking of illicit funds more challenging[56].

Luxembourg VASPs can be exposed to the threat due to them being potentially used as an interim step in terrorism financing. The CRF received five terrorism and terrorism financing STRs in 2019[57] related to VAs, with an example STR described in Figure 13. The majority of these reports were due to a Worldcheck or sanctions name match. Some of these were not linked to a person but to a blacklisted address for terrorism.

Figure 13: CRF VASP case study on terrorism financing based on a request from a foreign FIU

"A request from a foreign FIU was made upon suspicion of terrorism and financing of terrorism. CRF's foreign colleagues reported this individual due to known offences for drug trafficking and association to terrorist groups.

The suspect converted over €7 500 to BTC which were then sent to an address known to be part of a terrorist cluster. Multiple addresses had links to a Luxembourgish entity.

The CRF requested further information from the entity about the beneficiary of the transfers related to the terrorist cluster and was able to identify a previously unknown person to the foreign FIU. Furthermore, requests for information were sent to other reporting entities that were thought to hold further information about the suspects. The CRF found accounts related to the suspects at other Luxembourgish entities, but they were not used for any transaction.

Further analysis and feedback from a foreign FIU, helped to identify several others accounts with links to darknet markets and possibly related to drug trafficking."

4.4. Global threats of VAs and VASPs

It is important to highlight that Luxembourg can be exposed to ML/TF threats stemming from VASPs operating in other countries. Criminals based in Luxembourg could abuse international VASPs during each stage of ML/TF: placement, layering and integration.

The majority of VASPs serve a global user-base. VAs by design enable borderless electronic value transactions, and thus most VASPs by default are working with international clients. VASPs may provide their services in all countries they have targeted as being a potential market. Thus, the global activity of VASPs enables criminals to conduct ML/TF schemes without being tied to a specific geography. Binance, the world's largest centralised exchange

[54] Coindesk, *Palestinian Militant Group Has Received 3 370 Bitcoins in Donations Since 2015: Report*, 20 January 2020
[55] The New York Times, *Terrorists Turn to Bitcoin for Funding, and They're Learning Fast*, 18 August 2019
[56] The New York Times, *Terrorists Turn to Bitcoin for Funding, and They're Learning Fast*, 18 August 2019
[57] CRF Data received on 2 March 2020

by volume[58], illustrates the global reach of VASPs: it claims to have 15 million users from more than 180 countries and regions[59]. Further, the flows of VAs are highly international. For example, 66% of all payments sent by users of US exchanges are sent to VASPs operated in other countries[60].

While some types of VASPs can limit their exposure to users from geographies, other types of VASPs by design enable borderless activities. Decentralised applications and anonymisation, in most cases, would not prevent users from using their services based on location. For example, a criminal operating in Luxembourg and laundering money could use a mixer operated in another country to obfuscate transaction flows.

The global scale of VA adoption further highlights the rising international threats of VAs and VASPs. As of 2019, the total number of user accounts at VASPs exceeded 100 million, with 38% of them considered active[61]. VAs have achieved high levels of proliferation across geographies, with the share of residents reporting to own or have owned VAs exceeding 10% in Turkey, Brazil, Colombia, Mexico, Chile and Spain[62].

Operators of VASPs also tend to be based in multiple countries, making it easier for criminals to hide transactions by using different VASPs. For example, the Top-20 VA exchanges by volume are each headquartered in 13 different countries[63]. For some VASPs, owners are unknown altogether: as of February 2020, more than 3,000 decentralised applications were live globally, with a significant proportion of them not disclosing owners[64].

To conclude, the international scale of operations of VASPs poses ML/TF risks on all countries, independent of the presence of VASPs in them. For Luxembourg authorities, that means that criminals operating from Luxembourg are not limited to VASPs based in Luxembourg for ML/TF activities. Together, those factors require significant international cooperation on mitigating factors, which will be further described in the mitigating section of this report.

[58] Bitwise, *Bitcoin Trade Volume*, Retrieved 2 March 2020, https://www.coingecko.com/en/exchanges
[59] Binance, *Binance 2019 Year in Review*, 31 December 2019
[60] Ciphertrace, *Q4 2019 Cryptocurrency Anti-Money Laundering Report*, February 2020
[61] Cambridge Centre for Alternative Finance, *2nd Global Cryptoasset Benchmarking Study*, December 2018, global-cryptoasseamt-benchmarking.pdf
[62] Statista, *Statista Global Consumer Survey*, 2019
[63] CoinGec*ko, https://www.coingecko.com/en/exchanges*, retrieved 24 February 2020
[64] State of the DApps, *DApp Statistics*, retrieved 24 February 2020

5. INHERENT RISK – VULNERABILITIES ASSESSMENT

This section of the report consists of three main sub-sections. The first sub-section evaluates the ML/TF vulnerability of different VAs using the VA scorecard approach described in Table 4 of this report. It covers three main risk dimensions: anonymity, usability and security. The second sub-section covers the inherent risk of different VASP types. It consists of two analyses: a risk evaluation for VASP types that are already located in Luxembourg, and a risk evaluation of VASPs that could potentially emerge in Luxembourg in the future. The evaluation of VASPs is performed according to the scorecard methodology described in Table 5. The third sub-section provides an overview of how the traditional financial sector of Luxembourg may be exposed to VASP ML/TF related risks.

5.1. VA inherent risk assessment

The vulnerability assessment for VAs is summarised in Table 6, which presents the relative exposure of each VA type to ML/TF risk. The inherent risk ratings are used in the analysis of VASPs in the next sub-section, as a VASP dealing with riskier VAs would have a higher overall inherent risk rating.

Table 6: Inherent risk for VA types

VA Type	Sub-type	Inherent risk
Exchange VAs	Pseudo-anonymous	Very High
	Anonymous	Very High
	Platform	High
	Stablecoins	Medium
Utility VAs		Low
Security VAs	Security VAs	Low
	Platform VAs with security features	Medium
Closed virtual currencies		Very Low

The vulnerability assessment of VAs considers three risk categories, as per the scorecard outlined in section 3: anonymity, usability and security:

a. **Anonymity** refers to the ability of third-party persons or entities, which are not involved in a VA transaction, to link a sender's or receiver's VA address to a real-world identity. For example, in some VAs, all transaction history is publicly available, and once an identity was linked to an address, all future and past transactions can be monitored by 3rd parties, such as law enforcement agencies. An identity can be linked in cases when a user on a VASP has passed KYC procedure on it, and then sends or withdraws VA funds from the VASP. Different VAs have different levels of anonymity, and criminals would prefer VAs with more anonymity features, thus making more anonymous VAs more exposed to ML/TF risk.

b. **Usability** captures transactional or exchange liquidity of VA, its relative exchange rate stability and required technical knowledge for usage. Higher usability would increase a VA's susceptibility to ML/TF related crimes.

   The technological complexity of VAs has been considered a significant usability limitation of VAs, and thus prohibiting wider adoption of VAs by terrorist organisations[65]. However,

[65] Rand Corporation, *Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats*, 2019

the trend may be reversing. More terrorist organisations than before are using VAs such as Bitcoin for financing purposes[66]. Furthermore, some terrorist organisations start to show a deeper level of sophistication of VA technology. For example, in early 2019, a military wing of Hamas, the Izz ad-Din al-Qassam Brigades, ran a terrorism financing campaign and generated a new Bitcoin address for each donor[67].

c. **Security** refers to the probability that a user cannot have his or her transactions reversed, or balance forfeited. Those actions may occur if VAs do not have transaction irreversibility features or are prone to manipulation. More secure VAs would make it harder to reverse transactions for 3rd parties, making them more attractive for criminals for ML/TF purposes.

   Transaction irreversibility refers to the fact that some VA type transactions cannot be reversed. Transaction irreversibility provides significant advantages to criminals. In traditional financial instruments, such as credit cards, the merchant or a bank may reverse a transaction if it is fraudulent. In many VAs, transactions are irreversible, so even if fraud is identified early on, funds cannot be automatically returned.

   Transactions may generally be reversed in two ways. First, a VA may have transaction reversal capabilities enabled by default. For example, there exists a centralised administrator of a VA who may exercise censorship power on transactions. In decentralised VAs, there does not typically exist a single party that can reverse transactions. Second, even if a VA has transaction irreversibility enabled by default, it may be manipulated through a hack or a 51% attack[68]. VAs that have more miners securing their network and that rely on proven cryptographic protocols are less likely to be hacked or manipulated and are thus more secure.

This section will further describe the main specifics of each VA type across those three risk factors. The section is split into two sub-sections. The first sub-section evaluates Exchange VAs and covers pseudo-anonymous, anonymous, platform VAs and stablecoins. The second sub-section evaluates Utility VAs, security VAs and closed virtual currencies.

5.1.1. Exchange VAs

Exchange VAs include *anonymous*, *pseudo-anonymous*, *platform* and *stablecoin* VAs. *Exchange* VAs, except *stablecoin* VAs, are highly vulnerable to ML/TF risk. They offer significant anonymity properties to their users, have high user-bases and exchange liquidity and have high security levels. They typically do not have centralised administrators who may potentially reverse transactions and are generally prone to hacking through secure cryptographic protocols. This sub-section will further describe the risk factors of anonymity, usability and security factors for *exchange* VAs.

Anonymity: All *exchange* VAs offer significant anonymity features to their users, as compared to other types of VAs. The anonymity for *exchange* VAs can be caused either by default because of their inherent technological properties, or through second layer solutions, such as anonymisation tools.

By default, *anonymous* VAs provide the highest level of anonymisation to their users across all VA types. This means they make it impossible for outside observers to see the balances of addresses or transaction amounts. Examples of such VAs include Monero and ZCash[69].

[66] The New York Times, *Terrorists Turn to Bitcoin for Funding, and They're Learning Fast*, 18 August 2019
[67] Chainalysis, *2020 Crypto Crime Report*, January 2020
[68] A 51% attack is an attack on a VA by a group of miners or validators who control more than 50% of the network's power
[69] Note that for Zcash users can selectively enable transparency, thus making transactions traceable for observers

In contrast to *anonymous* VAs, *pseudo-anonymous*, *platform* and *stablecoin* VA types are transparent, meaning that transactions and balances are openly verifiable and traceable by any user. Thus, addresses that have sent or received VAs of those types may be potentially linked to a person's real-world identity. Further, online websites such as "blockchain.com" or "etherscan.io" allow public internet users to check the history of every address and transaction that ever occurred on the VA network. Figure 14 below provides a case study on how the CRF was able to trace back a suspect's transactions five years into the past and retrospectively identify the origin of funds.

Figure 14: Case study on bitcoin transaction tracing by CRF

In February 2018, the CRF received a report concerning a withdrawal of €115 000 from an entity to an account opened at a Luxembourg credit institution.

The CRF employed a transactional analysis of the reported user's wallet address. It identified that the user received between 26/07/2013 and 25/08/2015 121 transactions from a US exchange and 14 transactions from a mining pool. The CRF was able to identify that the origin of the funds could be traced back to mining activities, indicating that the suspect earned bitcoins through mining activities. The analysis has shown that only 0.19% of transactions were received from a mining pool that does not use KYC. As no suspicious links noticeable on the blockchain, no further action was taken by the CRF.

It is important to mention that in some cases, *pseudo-anonymous* and *platform* VAs can achieve similar anonymity level to *anonymous* VAs. Users can utilise anonymisation tools or intermediaries to obfuscate transaction flows and making it significantly harder to have a real-world identity linked to them. Such tools can include centralised mixers or special software solutions which allow users to mix funds between them without a coordinating entity[70]. Further, recent trends in Bitcoin protocol development suggest that anonymisation tools might become easier to implement in the future, making them more widely used[71].

Stablecoin VAs offer less anonymity to their users than *pseudo-anonymous*, *anonymous* and *platform* VAs. *Stablecoin* VAs are issued by a central governing entity and are typically not designed for maximising anonymous features.

Usability: Globally, *exchange* type VAs have high transactional and exchange liquidity, increasing their potential for ML/TF abuse. However, their adoption can be limited by exchange rate instability and technical requirements for usage.

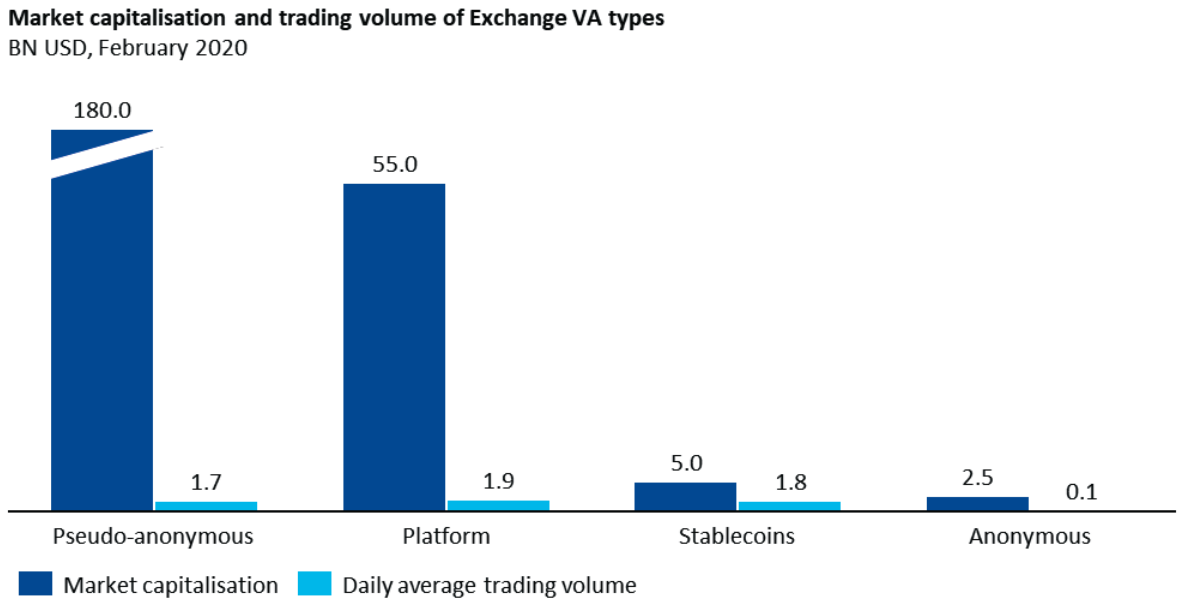
Exchange type VAs serve millions of users and power billions of transactions per year[72]. Combined, *pseudo-anonymous*, *platform* and *stablecoin* VAs have more than 500 thousand daily active addresses, with a total average daily total transaction amount exceeding $100 million for each type[73]. *Anonymous* VAs are not included in the figure as by default they are anonymous and do not allow for such statistic collection.

Adoption levels differ between different *exchange* VA types. This is reflected in their market capitalisation and exchange trading volume. Figure 15 presents the market statistics on all four *exchange* VA types, which shows the combined statistics on all VAs with a sub-type[74]. *Pseudo-anonymous* VAs have the highest combined market capitalisation with a value of $180 billion, driven mainly by Bitcoin, which is responsible for more than 90% of that value. *Pseudo-anonymous*, *platform* and *stablecoin* VAs have more than $1 billion of trading volume each. Anonymous VAs have less than $100 million daily trading volume on all global exchanges, caused by the fact that only a few major exchanges offer to trade for them. Thus, potentially more funds can be laundered through *pseudo-anonymous*, *platform* VAs and *stablecoin* VAs

[70] Coindesk, *Binance Blockade of Wasabi Wallet Could Point to a Crypto Crack-Up*, 26 Dec 2019
[71] Coindesk, *An Army of Bitcoin Devs Is Battle-Testing Upgrades to Privacy and Scaling*, 17 Nov 2019
[72] Cambridge Centre for Alternative Finance, 2nd Global Cryptoasset Benchmarking Study, December 2018
[73] Messari screener, *https://messari.io/screener*, retrieved 4 April 2020
[74] Messari screener, *https://messari.io/screener*, retrieved 4 April 2020

than through anonymous VAs. Note that in contrast to transaction liquidity, described in the previous paragraph, exchange liquidity for *anonymous* VAs can be collected from public sources, as centralised exchanges

Figure 15: Market statistics on Exchange VAs types



The high transaction and exchange liquidity lead to a higher number of VASPs available for criminals to launder their money.

A significant barrier for wider adoption of *pseudo-anonymous*, *anonymous* and *platform* VAs is their exchange rate instability. As the VAs value is not backed by any asset, their value tends to fluctuate highly. Further, VAs attract a significant number of speculative investors that may further increase the volatility. For example, the value of most *pseudo-anonymous*, *anonymous* and *platform* VAs dropped more than 50% between 15 February 2020 and 15 March 2020[75]. Only *stablecoin* VAs, the value of which is pegged to a central-bank issued currency, provide a high level of stability.

Another potential limitation for all *exchange* VAs' adoption is their technological requirements towards their users. First, to use VAs, users need to download and operate special purpose applications. Second, if users self-custody their VAs, they need to have an understanding of private key management as otherwise their funds may be irretrievably lost.

Security: *Exchange* VAs rely on strong cryptographic principles that make them difficult to hack. Further, the decentralised validating protocols powering *pseudo-anonymous, anonymous* and *platform* VAs make transactions irreversible and censorship-resistant. Those features increase security levels of VAs and thus increase their susceptibility to ML/TF abuse.

Inherently, a user's account of an *exchange* VA cannot be compromised if the user follows correct account management procedures. To be able to send transactions from an address, a user needs to know his or her private key, which is typically a random string of 64 or more characters. A hacker wishing to obtain control over an address and having no information on it except the address itself, will have no ability to access it. Researchers have estimated that it will take an attacker more than a billion years to try and "guess" the private key by iterating through every possible private key combination[76]. The security of an *exchange* VA lies in the hands of the user: should the user expose his or her private keys, an attacker will have immediate access to funds. However, if the user stores VAs using a third party (for example

[75] Coinmarketcap, https://coinmarketcap.com/, retrieved 14 February 2020
[76] Bitcoin.com, *How hard is to brute force a bitcoin private key*, October 2019

on a centralised exchange), the private key would not be known to the user. Thus, the user account can only be hacked either because of obtained passwords or due to other means such as hacking/malware.

Pseudo-anonymous, anonymous and *platform* VAs transactions are typically irreversible, making them more attractive for ML/TF abuse. Their transactions are typically validated by decentralised networks of many multiple difference or validators, spread globally. Reversing transactions would require miners or validators to coordinate their censorship activities, which in practice is very difficult.

In theory, a miner or validator can gain control over an *exchange* VA's transactions through a 51% attack. That would enable an attacker to reverse transactions, send transactions from other addresses or issue new VAs. In practice, however, such attacks are prohibitively expensive for major VAs, making them unlikely to occur.

Stablecoin VAs are different from *Pseudo-anonymous, anonymous* and *platform* VAs, as they do not offer the same level of transaction censorship resistance to their users. As stablecoins are issued and monitored by central governing entities, those entities may, in theory, block suspect transactions. This decreases their vulnerability to ML/TF. Note that there exist VAs that have a stable monetary value obtained through decentralised systems (for example, DAI). The risk levels of those VAs would be similar to *pseudo-anonymous* and *platform* VAs, as they share multiple technological features with them.

5.1.2. Other VA types

Utility VAs, *security* VAs and *closed virtual currencies* have lower vulnerability towards ML/TF activities than *exchange* VAs described in the previous sub-section due to multiple factors. First, their anonymity is limited, as many of them require users to disclose personal information to the VA issuers. Second, they lack significant transaction and exchange liquidity, which limit their usability. Third, their security is also confined: the transaction validation of those VA types is typically controlled by a central governing entity, that may impose specific restrictions.

Table 7: Inherent risk for utility VAs, security VAs and closed virtual currencies

VA Type	Sub-type	Inherent risk
Utility VAs		Low
Security VAs	Security VAs	Low
	Platform VAs with security features	Medium
Closed virtual currencies		Very Low

The factors causing other VA types to be less vulnerable to ML/TF abuse are shared between each sub-type. This sub-section further will thus highlight only the distinct specifics of each VA sub-type.

Utility VAs: *Utility* VAs transaction liquidity is usually limited to a single application. Further, *utility* VAs are not designed to be traded on exchanges, and exchange is typically done only between the user and the application owner. Figure 16 provides an example by describing those factors in a specific *utility* VA and contrasting those factors to an *exchange* VA. Together those factors make utility VAs largely unsuitable for ML/TF purposes.

Note that the FATF does not seek to capture the *utility* VAs ("*types of closed-loop items that are non-transferable, non-exchangeable, and non-fungible*"). Such items might include airline miles, credit card awards, or similar loyalty program rewards or points, which an individual cannot sell onward in a secondary market[77].

[77] FATF, *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, 21 June 2019

Figure 16: Case study on Socios (Utility VAs) and Bitcoin (Exchange VA) comparison

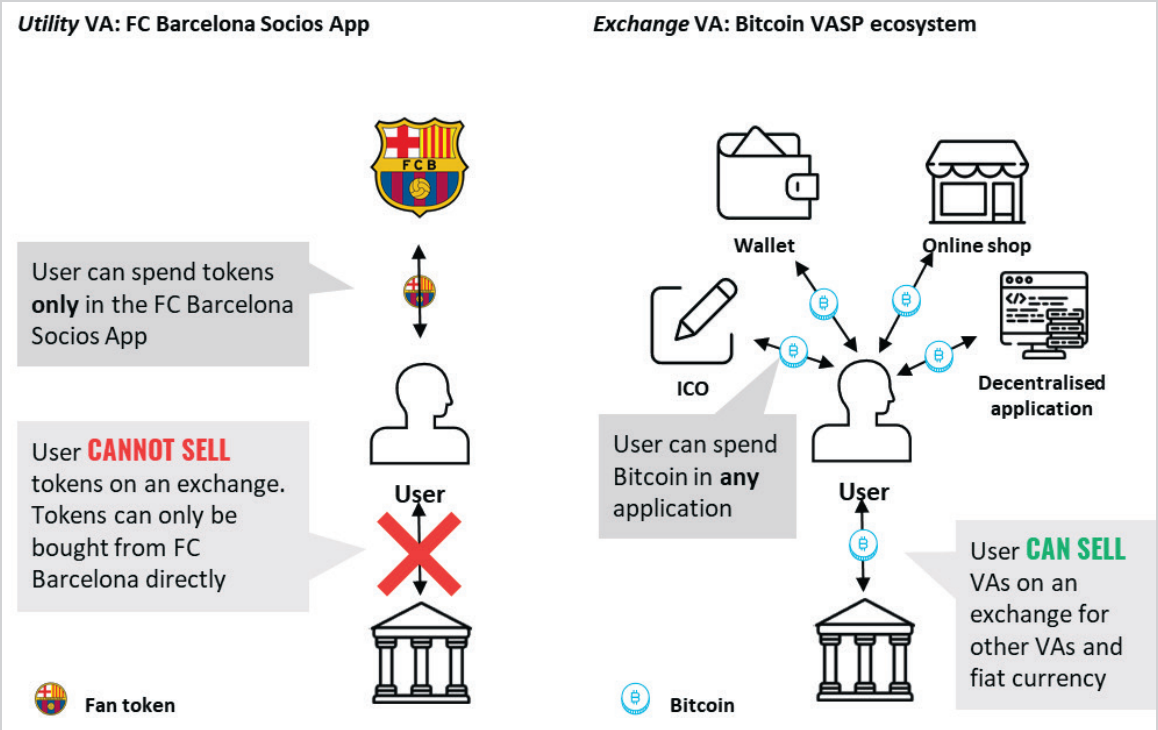
The figures below illustrate the difference between utility VAs and exchange VAs in terms of their usability.

The left figure describes the ecosystem of the utility VA "fan token" of FC Barcelona, a Spanish football club. FC Barcelona has issued the fan token through a special mobile app called Socios. A user can download and install the Socios app, and then get fan tokens. A user has only two ways to get fan tokens: by buying the fan tokens directly from FC Barcelona, or by earning them in special rewards campaigns, also run exclusively by FC Barcelona. Users can spend fan tokens only in the FC Barcelona Socios app, for example, to receive discounts on FC Barcelona's merchandise products or participate in special lotteries.

The right figure illustrates the ecosystem of the pseudo-anonymous exchange VA bitcoin. Users can buy bitcoins from a variety of exchanges and can spend bitcoins on a variety of services offered by different VASPs.

Comparing FC Barcelona fan tokens to bitcoins clearly illustrates how the latter is superior for money laundering purposes. If a criminal were to launder money through FC Barcelona tokens, he or she would not be able to exchange them for any other products other than FC Barcelona fan rewards. Even if fan tokens were available for exchange, their market capitalization and exchange liquidity would be limited because the demand for fan tokens comes only from FC Barcelona supporters. The low market capitalisation and low exchange liquidity would make it difficult for a criminal to launder significant sums of money. In contrast, bitcoins can be exchanged on hundreds of exchanges and can be spent on thousands of different VASPs. The significant flexibility in usage of bitcoins allows criminals to exercise different options of ML schemes and utilise various VASPs.

Note that the fan tokens in this case study are a utility VA, and thus fall outside of FATF scope.



Security VAs: *Security* VAs use similar technology to *exchange* VAs and could be considered as traditional securities, but which are not qualified as a financial instrument. Globally, the level of development of exchanges, custodians and investment firms offering *security* VAs remains nascent[78]. Overall, the low current adoption levels make *security* VAs less vulnerable to ML/TF risks. However, the sector of *security* VAs continues to develop globally. That may increase the adoption of the VA type and its subsequent ML/TF risk in the future.

Platform VAs with security features: *Platform VAs with security features* are *exchange platform* VAs described in the previous sub-section that have properties of a security, but which are not qualified as a financial instrument. Thus, they will have a similar risk profile to *exchange platform* VAs. The largest difference lies in their lower security levels.

Platform VAs with security features, in contrast to many *exchange platform* VAs, tend to be governed and controlled by centralised entities. Thus, in theory, the issuer of the VA may restrict transactions to specific users. Criminals laundering money through those VAs can have their ML/TF transactions reversed automatically, thus increasing the risk that their ML/TF activities will be unsuccessful. Thus, the ML/TF vulnerability of those VAs is reduced.

Closed virtual currencies: *Closed virtual currencies* are designed to be used only within a specific application, for example, an online computer game. In that respect, they are very similar to *utility* VAs. The case study in Figure 16 would be relevant to *closed virtual currencies*[79]*.* Similar to *utility* VAs, will have low ML/TF risk levels across nearly all risk dimensions identified in the scorecard approach.

One major difference between *closed virtual currencies* and *utility* VAs lies in the security levels. The security level of *closed virtual currencies* is significantly lower, as they do not rely on the same cryptographic principles. For example, a hacker trying to get access to a user's account would only need to guess the user's self-generated password.

Note that similar to the *utility VAs*, *closed virtual currencies* are closed-loop items that are non-transferable, non-exchangeable, and non-fungible, and thus fall outside of the FATF scope on VAs and VASPs.

5.2. VASP inherent risk assessment

Table 8 presents the overall conclusion of Luxembourg's current ML/TF vulnerability stemming from 12 different VASP types. Note that as VASPs can operate cross-border, VASPs of all types could potentially offer their services in Luxembourg. With the introduction of the Laws of 25 March 2020, VASPs which are established or provide services in Luxembourg must register with the CSSF. As of mid November 2020, several entities have applied for a VASP registration which are being reviewed by the CSSF. The analyses of other VASP types take into account the characteristics of entities of those types most often observed globally. This analyse constitutes a preliminary assessment as of today and may evolve over time once the first VASPs have been registered with CSSF.

Table 8: Inherent risk for VASP types

VASP Type	Sub-type	Inherent risk
Issuance	ICO/IEO	Medium
Custody	Custodian wallet providers	Medium
	Dedicated custodians	Medium
Exchange	Centralised exchanges	High

[78] Coindesk, *Security Token Offerings Are (Finally) Set for Takeoff in 2020*, 20 Dec 2019

[79] In the case study, FC Barcelona Socios App would be, for example, an online game, and the token could only be spent on items inside the game

VASP Type	Sub-type	Inherent risk
	Peer-to-peer exchanges	Medium
	Brokers	Medium
	VA ATMs	Low
Service and product exchange	Centralised applications	Medium
	Decentralised applications	Medium
Other	Anonymisation tools	Medium
	Fund managers	Medium
	Miners or validators	Low

5.2.1. Centralised exchanges

VA Type	Sub-type	Inherent risk
Exchange	Centralised exchanges	High

Globally, centralised exchanges are the most developed VASP sub-type by size and volume. The monthly trading volume on all centralised exchanges worldwide exceeds $50 billion[80]. At least 10 exchanges have a daily actual trading volume exceeding $1 million. Note that 150 exchanges reported daily actual volume to be above $1 million, however, due to lack of transparency a significant proportion of volume is likely to be non-economic in nature[81]. The market is relatively concentrated, with approximately 50% of trading volume happening on one exchange Binance.

Globally, there are ~1 000 000 daily users across top-4 exchanges[82]. Clients of centralised exchanges can be both retail clients and institutional clients. Some clients may be VASP themselves, for example brokers or entities involved in ICO that want to exchange raised VAs into fiat currency. The different types of client types increase ML/TF risks of centralised exchanges. The large volume and userbase of centralised exchange increase ML/TF risks both globally and locally in Luxembourg.

Centralised exchanges typically offer exchange of VAs. They may facilitate VA-to-VA and/or Fiat-to-VA trading between customers by matching prospective buyers and sellers. Centralised exchanges also typically offer custody of VAs and enable customers to deposit VAs and complete multiple trading transactions without the need to move VAs. Centralised exchanges typically offer activities with *pseudo-anonymous* or *platform* VAs, which are high and very-high risk VAs. Therefore, the aggregate sector's risk dimension level "activities and products" is assessed as very high.

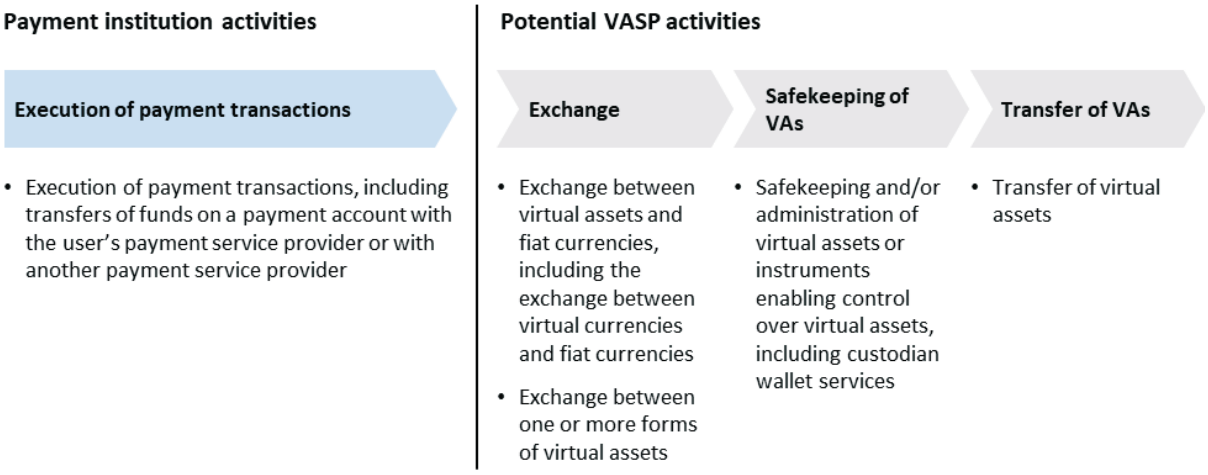
Various centralised exchanges are known to offer their services in Luxembourg. As described above, 4 to 8% out of ~600k of Luxembourg residents own VAs[83] [84]. Those residents who own VAs likely at some point have used a centralised exchange to purchase or sell VAs. As of November 2020, several exchanges (less than 20) have contacted the CSSF in view of

[80] BTC volume as reported by https://www.bitcointradevolume.com/ as of February 2020, and then adjusted for Bitcoin market cap vs other VAs market cap (assuming that market cap directly corresponds to trading volume), retrieved 12 March 2020
[81] https://www.sec.gov/comments/sr-nysearca-2019-01/srnysearca201901-5164833-183434.pdf, retrieved 12 March 2020
[82] https://www.newsbtc.com/2018/12/12/crypto-exchanges-active-users/, retrieved 10 March 2020
[83] Statista, *How many customers own cryptocurrency?*, August 2018
[84] TNS Ilres, *Le concept des crypto-monnaies au Luxembourg*, February 2018

possible VASP registration, with no registration fully complete, thus making it not possible to have a complete view of the scale of activities of centralised exchanges.

Figure 17 provides an overview of activities that a VASP may perform when facilitating VA purchases from fiat currency for their users. The figure splits those activities by payment institution (payment of fiat transactions), in case the VASP is also offering payment services under a payment institution licence, and VASP activities. Note that the figure only describes the process for a VA purchase, but the process for a VA selling is similar, albeit the steps are performed in the reverse direction. The payment institution activities are performed under a payment institution license, and VASP activities require a VASP registration. As a first step, the entity executes payment transactions i.e. allows a user to deposit fiat funds into payment account to facilitate the purchase of VAs. Those activities do not involve VAs and thus do not fall under the five activities of VASPs. Those activities also do not fall under the activities of a traditional exchange, as the role of a traditional exchange is limited to matching buyers and sellers. As the next steps, when a customer posts a market buy order for a VA on the exchange, the exchange finds orders posted by other users willing to sell VAs for fiat currency and facilitates subsequent trading. It credits the user's account with VA funds and safekeeps them for the customer. Note that safekeeping of funds is a characteristic of centralised exchanges: decentralised (peer-to-peer) exchanges, described further below, do not typically offer safekeeping of VAs. A user can then withdraw funds from the exchange to another address, and the exchange transfers VA funds from their wallets to the user's specified address.

Figure 17: Illustrative example of activities performed by an entity in order to facilitate a user's VA purchase from fiat currency



5.2.2. Other VASPs

While VASPs could potentially exist that are established or provide services in Luxembourg, there are no entities that have fully completed the VASP registration process as of mid November 2020. As VASPs of other types may successfully complete registration in the future in Luxembourg, it is important to assess their potential vulnerability with regards to their services offered and geographies served. A VASP established or providing services in Luxembourg would likely share similar characteristics to VASPs operated in other countries. It would offer similar products and services and would most likely cater users from similar geographies.

The "medium" risk score for 9 out of 11 other VASP types reflects the high-risk nature of products and potential users of them, with the combined inherent risk of VASPs being "medium". Most global examples of those types are exposed to high-risk of very-high risk VAs and are generally available to any internet user.

Before presenting individual vulnerability specifics, it is important to note that all VASPs are vulnerable to cybercrime threat. VA transactions are typically irreversible and are difficult to trace, making VASPs potential targets to cybercrime criminals. Criminals can exploit a VASPs technical vulnerability or conduct social engineering or other forms of deception to steal VAs.

The sub-section further summarises the ML/TF risk for each VASP type and outlines the main ML/TF relevant characteristics for each one.

5.2.2.1. Issuance: ICO/IEO

VA Type	Sub-type	Inherent risk
Issuance	ICO/IEO	Medium

An ICO and IEO issuer matches prospective buyers with a firm that issues a VA or issues a VA themselves. Thus, the issuer's core activity is inherently similar to the activity of a centralised exchange.

Compared to centralised exchanges, however, ICO and IEO issuers are less vulnerable to ML/TF abuse due to multiple factors. First, ICO and IEO issuers typically offer platform VAs, which have a lower risk rating than pseudo-anonymous or anonymous VAs. Second, they may offer less stability for ML/TF criminals. Typically, sometime needs to pass between an ICO/IEO issuance, and the date when the newly issued VA becomes available to trade. Thus, a criminal who would purchase VAs in an ICO or IEO would have to wait a certain amount of time before being able to transfer them. Once the VA becomes available on an exchange to trade, its price may significantly drop since the issuance. Thus, the criminal's proceeds may potentially be reduced, making an ICO or IEO less suitable for ML/TF purposes.

Globally, there has been a decline in ICO/IEO activity. We can therefore estimate that they are less likely to appear in Luxembourg. In 2018, 1253 ICO's have raised $7.8 billion in total. In 2019, 109 ICO's have raised $0.4 billion in total, representing a 95% year-on-year decline[85].

5.2.2.2. Custodian wallet providers

VA Type	Sub-type	Inherent risk
Custody	Custodian wallet providers	Medium

Custodian wallet providers are vulnerable to ML/TF abuse because criminals may use them to store illicit VAs and transfer them. Globally, there are multiple custodian wallet providers operational that may provide custody of very high-risk VAs, such as pseudo-anonymous or anonymous VAs.

The wider adoption of custodian wallet providers for ML/TF abuse is limited by their relative lack of security, which stems from the fact that their operators can freeze accounts and impose censorship on their users' transactions. Criminals could use alternative solutions, such as specialised software solutions, to self-custody their VAs, and minimise their exposure to third parties.

5.2.2.3. Custody: Dedicated custodians

VA Type	Sub-type	Inherent risk
Custody	Dedicated custodians	Medium

[85] ICO data, *https://www.icodata.io/stats/2019*, retrieved 6 April 2020

Dedicated custodians are similar in their services to custodian wallet providers, with a difference that they offer their services to institutional investors. Custodians tend to have high financial barriers to entry, thus potentially decreasing their ML/TF vulnerability. For example, Coinbase Custody, the largest custody provider in the world with $7 billion in assets under custody, accepts clients with a minimum balance of $1 million[86].

Further, similar to custodian wallet providers, custodians offer an anonymity disadvantage over self-custody solutions. Criminals planning to use custodians for money laundering would need to pass KYC checks. In contrast, self-custody solutions do not require users to disclose their real-world identity to third parties.

5.2.2.4. Exchange: Peer-to-peer exchanges

VA Type	Sub-type	Inherent risk
Exchange	Peer-to-peer exchanges	**Medium**

Peer-to-peer exchanges facilitate trade between two parties without a central matching entity. Matching of trades is done via computer algorithms, and trading parties do not typically need to disclose their real-world identity. Those factors enhance the anonymity of users, which may increase peer-to-peer exchanges' vulnerability to ML/TF abuse.

Peer-to-peer exchanges may also be used as a pure anonymisation tool. As peer-to-peer exchanges do not require KYC and do not have a central server, trades on them cannot be restricted. Chainalysis 2020 State of Crypto Crime report highlighted that those factors are increasing the adoption of peer-to-peer exchanges by criminals for ML/TF purposes[87].

In contrast to centralised exchanges, peer-to-peer transactions have high technological barriers to entry. Users already need to have specific platform VAs to use them. Peer-to-peer exchanges often can be accessed only through a special 3rd party software solution. For example, peer-to-peer exchanges on the Ethereum network cannot be accessed without a specific browser extension[88].

The technological complexity of peer-to-peer exchanges leads to an overall lack of liquidity on them. Peer-to-peer exchanges currently approximately handle $0.2 billion trading volume per month[89], which is less than 1% of all global VA trading volume. The low volume of exchanges makes it difficult for criminals to launder high sums of VAs through them, thus reducing their overall vulnerability to ML/TF risks.

5.2.2.5. Exchange: Brokers

VA Type	Sub-type	Inherent risk
Issuance	Brokers	Medium

Brokers make it possible for VA traders to exchange large volumes of VAs without losing to slippage, thus offering a potential advantage over centralised exchanges. Brokers typically cater to institutional clients and globally facilitate billions in $ worth of trades[90].

Globally, it has been observed that some VA brokers may knowingly provide services to criminals. They purposefully have low KYC requirements and trade their clients' VAs on

[86] Coinbase, *Coinbase Custody acquires Xapo's institutional business, becoming the world's largest crypto custodian*, retrieved 6 April 2020
[87] Chainalysis, *2020 Crypto Crime Report,* January 2020
[88] Ethereum applications can be accessed through a special browser (e.g. Mist) or a special browser extension (e.g. MetaMask)
[89] DApp Radar, *https://dappradar.com/rankings/category/exchanges*, retrieved 2 February 2020
[90] Finextra, *OTC crypto market at a glance*, retrieved 2 February 2020

centralised exchanges. For a centralised exchange, such a trade would look like it was made by a broker, who might have previously successfully passed CDD checks. Chainalysis, a VA forensics company, identified that the hundred most active brokers knowingly laundering funds for criminals received more than $3 billion in 2019[91]. Furthermore, PlusToken, the most massive pyramid scheme in 2019, laundered at least $185 million through 28 brokers[92].

5.2.2.6. Exchange: VA ATMs

VA Type	Sub-type	Inherent risk
Exchange	VA ATMs	Low

VA ATMs have a lower vulnerability to ML/TF risk that other VASP types. First, VA ATMs typically facilitate transactions in one way only and can convert fiat currency into a VA. Second, they do not allow for large volume purchases and typically have imposed daily transaction limits for a person, ranging from $1 000 to $20 000. Third, VA ATMs can be only used locally, and thus have limited exposure to users from other countries.

5.2.2.7. Service and product exchange: Centralised applications

VA Type	Sub-type	Inherent risk
Service and product exchange	Centralised applications	Medium

Centralised applications are applications that are run on a central server and facilitate internal transactions between their users in VAs.

Examples of centralised applications with VA transactions are online computer games which deal specifically with *closed virtual currencies*. In those online games, the game developer issues the VA and distributes it between players, who can then transact it between themselves or purchase in-game items. As described in the previous section, closed virtual currencies have a “very low” inherent risk, thus reducing the vulnerability of centralised applications. As described above, as *closed virtual currencies* fall outside of the FATF’s scope, the entities offering transactions of them would also fall outside the VASP definition.

There is a limited number of centralised applications that deal with VA-only transactions in VA types other than *closed virtual currencies*. One example of such applications is earn.com, a platform that rewards users in VAs for learning about the VA industry. Other applications may include online e-commerce stores that only accept VAs, which for the moment fall outside of the VASP definition.

Similar to custodian wallet providers, centralised applications considered as VASP offer limited security protection to criminals planning to abuse them. Centralised applications can enforce strict rules on a user’s’ transaction and block accounts.

5.2.2.8. Service and product exchange: Decentralised applications

VA Type	Sub-type	Inherent risk
Service and product exchange	Decentralised applications	Medium

[91] Chainalysis, *2020 Crypto Crime Report*, January 2020
[92] Chainalysis, *2020 Crypto Crime Report*, January 2020

Decentralised applications are like centralised applications, with the difference being that no central entity controls them. Users and merchants using them can directly interact with each other without a third party acting as a mediator.

Decentralised applications have high transaction volumes that may increase their vulnerability to ML activity. More than 2 000 operational decentralised applications transacted $8.4 billion in value in 2019[93]. They register on average 80 000 daily users.

It is important to note that not all decentralised applications have processes that can be abused for ML/TF activities. Decentralised applications have multiple sub-types that can include trading-card games or margin lending markets. Those applications have fragmented and low volumes and may require users to lock in their funds for a significant amount of time, making them unsuitable for large ML/TF activities. However, some decentralised applications, such as gambling platforms, can be abused by criminals, with their activity resembling anonymisation tools such as mixers described in the next paragraph.

5.2.2.9. Other: Anonymisation tools

VA Type	Sub-type	Inherent risk
Other	Anonymisation tools	Medium

Anonymisation tools, or “mixers” are operated specifically to obscure transaction flows and increase the anonymity of users. For custodial mixers, their operators collect VA funds from multiple addresses and then send them out to other addresses of the same users. While mixers can be used for privacy enhancement by legitimate users, they are often used by criminals to launder ML proceeds.

Custodial mixers may be used less widely in the future, with non-custodial mixers becoming more popular. Custodial mixers have a centralised server operator, which can be shut down by law enforcement. In those cases, criminals would lose their illicit proceeds and may reveal evidence about their illegal activities. In 2019, Dutch law enforcement authorities, together with Europol and Luxembourg authorities, clamped down one of the largest VA mixer operator “Bestmixer” which achieved a turnover of at least $200 million in one year[94]. In contrast, non-custodial mixers allow VA users to coordinate and mix VAs between themselves without a central coordinator. Chainalysis 2020 Crypto Crime report suggested that criminals wishing to mix their funds would increasingly go for non-custodial mixers in the future.

5.2.2.10. Other: Fund managers

VA Type	Sub-type	Inherent risk
Other	Fund managers	Medium

Fund managers offering their clients to invest in VAs are vulnerable to VA ML/TF risk as they provide investments into different VA types. They also facilitate custody, storing the funds of their users by using dedicated custodians, which creates an additional ML/TF abuse vector.

Fund managers are potentially unlikely to appear in Luxembourg in large capacity. Industry expert interviews that were performed during the preparation of this report suggested that the appearance of VA fund managers is constrained by both demand and supply. From the demand perspective, institutional investors currently have limited appetite towards VA investments. Note that, as an example, the global crypto hedge fund market is itself is

[93] Dapp.com, *Dapp.com 2019 Annual DApp Market Report*, December 2019 (excluding peer-to-peer exchange volume)
[94] Europol, *Multi million euro cryptocurrency laundering service bestmixer.io taken down*, May 2019

estimated to be relatively small, with 150 active funds having $1 billion in assets under management as of 2019[95].

5.2.2.11. Other: Miners or validators

VA Type	Sub-type	Inherent risk
Other	Miners or validators	Low

Miners or validators have two ways in how they can be abused for ML/TF purposes.

First, a criminal could use fiat currency to purchase mining equipment, which will then generate VAs for the criminal. Second, a criminal could obtain enough mining equipment or voting power on a VA network to conduct a 51% attack. In both cases, however, criminals would require sophisticated technical knowledge of setting up mining or validating processes. Further, a 51% attack requires significant capital and operational expenditure. Given this, the vulnerability to ML/TF risk is assessed to be low.

5.3. Traditional finance sector's exposure to VASP ML/TF risks

The traditional finance sector of Luxembourg may be potentially exposed to ML/TF risks related to VASPs. First, traditional finance entities may launch their own VASPs in the future or may consider offering VA related services. Second, some traditional finance entities can have fiat transactions with VASPs.

5.3.1. Traditional finance entities potentially launching VASPs

Luxembourg has a developed traditional finance industry, which continually drives innovation and growth. To serve their users' evolving needs, traditional finance entities may decide to offer VA-related services and thus would have to register as VASPs. Firms from the following industries have the highest potential probability of establishing a separate/additional VASP business:

- **Money and value transfer services:** E-money and payment institutions may enable their users fiat deposits and withdrawals to and from different VASPs, such as VA exchanges and may consider to start providing themselves VA related services and would in such case be exposed to VASPs-related ML/TF risk.
- **Custodians (banks)**: Luxembourg has a strong custodian industry, with 29 entities reporting a total income of €5.73 billion and assets of €179.4 billion and having a long experience in such services. An increased demand from the investment sector for VA investments could drive Luxembourg based custodial bank to consider launching VA custody services.
- **Investment sector (Brokers & broker-dealers):** Globally, there has been a demand for institutional level liquidity provision for VA trading. For example, a prominent US-based trading firm DRW launched a dedicated trading desk called Cumberland in 2014. In Luxembourg, brokerage is a large and fragmented industry[96]. As for other financial institutions, brokers established in Luxembourg could also consider offering VA related services.

[95] PwC & Elwood, *2019 Crypto Hedge Fund Report*, 2019
[96] Luxembourg NRA, 2020

5.3.2. Traditional finance entities directly or indirectly exposed to VASPs

Firms from the following industries have the highest likelihood of being directly or indirectly exposed to VAs:

- **Banks**: Banks are exposed to risk stemming from VAs as they are the point of contact of centralised exchange users with the traditional finance sector. Criminals using VAs for ML/TF activities need to convert VAs to fiat, or vice-versa. For these purposes, criminals use exchanges, the deposits and withdrawals from which are usually done to and from bank accounts. Luxembourg has a substantial retail & business bank sector, with large numbers of existing customers, including a high share of international users. As of 2019, no bank in Luxembourg itself had any activity in VAs, with a small minority of banks (less than a dozen) seeing a very limited number of customers involved or linked to VAs. As such, the VAs-related ML/TF risks to banks in Luxembourg are limited.
- **Money and value transfer services:** Payment and e-money institutions may offer payment services to VASP, allowing them to deposit or withdraw fiat funds to facilitate the purchase or sell of VAs. As for Banks, criminals using VAs for ML/TF activities need to convert them to fiat or vice-versa and may therefore open payment accounts with payment or e-money institutions. As of mid November 2020, only two payment institutions are offering such services. Thus, the VAs-related ML/TF risks to payment and e-money institutions in Luxembourg are limited.
- **Trust and companies service providers (TCSPs):** TCSPs aid their clients in the set-up, management, and administration of their affairs, and can offer those services to VASPs. As such, TCSPs may be potentially exposed to ML/TF risks stemming from VASPs. Lawyers, who can offer TCSP activities, may set up and operate legal arrangements for VASPs (including domiciliation), and thus be misused or abused for ML/TF activities.
- **Insurance:** VAs exchanges and custodians require insurance to secure their operations. Globally, there has been a rise of insurance providers to custodians. For example, in 2019, an international insurance broker launched a cold storage insurance program for loss of digital assets from internal and external theft, damage or destruction of private keys providing a limit of up to $150 million per insured through the Lloyd's market[97]. Insurers need to be able to analyse cybersecurity threats effectively, as VAs custodians can be a target of cybercriminals. Note that the insurance coverage of VAs is very limited globally[98], thereby further constraining the risk to the Luxembourg insurance sector. In the context of unit-linked life insurance policies, customers (High Net Worth Individuals) of life insurance undertakings may invest in assets that are linked to VAs (i.e. tracker funds). As of September 2020, only a small minority of life insurance undertakings reported limited investments in this type of financial product. As such, the VAs-related ML/TF risks to life insurance undertakings in Luxembourg are very limited.

[97] Insurance Business America, *HUB Security, Marsh partner to offer insured crypto storage solution,* 2020
[98] American Express, *Cryptocurrency Insurance Market Shows Promise Despite Cautious Approach by Major Insurers*, 2018

6. MITIGATING FACTORS

The purpose of this section is to identify and describe the mitigating measures in place to reduce ML/TF inherent risk of VASPs. The section is divided into four sub-sections:

1. **Prevention by VASPs**: describes the mitigating measures that VASPs are required to implement per the 2004 AML/CFT Law, as amended by the Laws of 25 March 2020. These can be categorised into four main areas, which follow professionals' AML/CFT obligations as described in the 2004 AML/CFT Law: ML/TF risk assessment; customer due diligence; cooperation with competent authorities; and internal organisation, governance and training.
2. **Supervision by the CSSF:** describes the mitigating measures put in place by the CSSF. These can be grouped into five areas: understanding of ML/TF risks; regulation and information (e.g. to promote of understanding of ML/TF risks by the private sector); market entry controls; oversight and supervision (e.g. on-site inspections); and rules enforcement with AML/CFT obligations (e.g. administrative fines).
3. **Detection by the CRF**: describes the mitigating measures established by the CRF, and covers the quality of STRs and SARs received by the CRF, the level of strategic analyses that the CRF is undertaking, international and national cooperation, and cooperation with the private sector.
4. **Prosecution and enforcement:** describes the mitigating measures established by the prosecution and enforcement authorities in Luxembourg in relation to VAs and VASPs.

6.1. Prevention by VASPs

With the adoption of the Laws of 25 March 2020 amending the 2004 AML/CFT Law, the CSSF became the AML/CFT supervisory authority for VASPs as defined in Article 1(20c) of the 2004 AML/CFT Law. In accordance with point (16) of Article 2(1) of the 2004 AML/CFT Law, VASPs fall under the scope of the 2004 AML/CFT Law and must comply with the related professional obligations as provided therein. In accordance with article 7-1 (2) d) of the 2004 AML/CFT Law, VASPs also have to comply with the professional obligations as provided for in Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfer of funds and repealing Regulation (EC) No 1781/2006.

Since the adoption of the Laws of 25 March 2020, several entities (less than twenty) have respectively been in contact with the CSSF or applied for a possible VASP registration. As of mid November 2020, the applications are at different stages of the registration process, and no registration has been finalised. This sub-section will thus describe the mitigating factors that VASPs are obliged to put in place.

VASPs are obliged to apply a range of measures to mitigate ML/TF inherent risks. Following professionals' AML/CFT obligations as described in the 2004 AML/CFT Law, these have been categorised in four main areas: (1) ML/TF risk assessment and understanding of ML/TF risks; (2) customer due diligence; (3) cooperation with competent authorities and (4) internal organisation, governance and training. The nature of these mitigating factors is outlined in the sub-sections below.

6.1.1. ML/TF risk assessment and understanding of ML/TF risks

In line with the 2004 AML/CFT Law, VASPs should take appropriate steps to **identify, assess and understand their ML/TF risks** (for customers, countries, VA types, products, services, transactions). VASPs should have a defined risk appetite, risk strategy and risk-based approach to client onboarding and transaction monitoring. The risk assessments should be documented, kept up to date through regular reviews and all relevant risk factors should be considered before determining the overall risk level and the level and type of appropriate measures to apply in order to manage and mitigate these risks. The risk assessment information should be provided to the CSSF and/or CRF upon request.

6.1.2. Customer due diligence

As per Article 3 of the 2004 AML/CFT Law and Article 1 (7) of the Grand-ducal Regulation 2010 as amended, VASPs should apply a number of customer due diligence (CDD) measures. These include amongst others the CDD process at onboarding, enhanced due diligence processes and ongoing due diligence throughout the business relationship.

When customers are onboarded, VASPs should assess the ML/TF risk and complete a **due diligence process (CDD)**, applying a risk-based approach. As per Article 3(2) of the 2004 AML/CFT Law, customer due diligence measures should comprise identifying the customer and verifying the customer's identity, identifying the beneficial owner and taking reasonable measures to verify his identity, assessing and understanding the purpose and intended nature of the business relationship, and conducting ongoing due diligence of the business relationship including scrutiny of transactions undertaken throughout the course of that relationship.

As per Article 3-2 of the 2004 AML/CFT Law, when VASPs identify customers with high ML/TF risks, they should perform **enhanced due diligence (EDD)**. An EDD may be triggered as a result of larger transactions, suspicious customer activity, when a customer's name fails a name check, for customers from higher-risk geographies, when a customer is a PEP or other risk factors. Article 3-2 of the 2004 AML/CFT Law provides an overview of cases for which an EDD is mandatory. In certain circumstances, senior management approval should be required before establishing business relationships with customers. Potential red flag indicators used by the CRF are provided in Appendix A of this report.

VASPs should also conduct **ongoing due diligence** on customers. They should ensure that documentation and data collected during CDD/EDD are kept up to date and do periodic due diligence on existing customers on a risk-basis. A VASP should put in place automatic re-screening of customer names, if a customer changes names, date of birth or provides new identification documents. VASPs should also use ongoing screening to ensure that a customer's name is not a PEP, from another high-risk group or figures on a sanction list. VASPs should keep all necessary records of fiat and VA transactions and documents obtained through CDD and EDD.

6.1.3. Cooperation with competent authorities

As per Article 5 of the 2004 AML/CFT Law, VASPs, their *"directors (dirigeants, members of the authorised management) and employees are obliged to cooperate fully with the Luxembourg authorities responsible for combating money laundering and terrorist financing"*, which for VASPs includes amongst others the CSSF and the CRF. VASPs are legally required to inform the CRF when they know, suspect or have reasonable grounds to suspect that money laundering, an associated predicate offence or terrorist financing is being committed or has been committed or attempted, in particular in consideration of the person concerned, its development, the origin of the funds, the purpose, nature and procedure of the operation.

This report must be accompanied by all supporting information and documents having prompted the report. VASPs should also provide without delay to the CRF, at its request, any information.

6.1.3.1. Transaction monitoring and suspicious activity reporting

VASPs should take appropriate steps to monitor transactions undertaken by customers to ensure that they correspond to the entities' knowledge of the customer and their risk profile. These activities include i.e. the screening of VA transactions against sanctions, PEPs and other high-risk lists. Activities also include monitoring transactions to identify suspicious activities and behaviours. An illustration of different "red flag" indicators published by the CRF which can be used by VASPs to assess the risk levels of transactions is provided in Appendix A.

Specialised third-party VA tracing analytics solutions to monitor incoming and outgoing VA transactions and identify those that are suspicious can be used by VASPs. The third-party VA tracing analytics solutions allow VASPs to identify if a customer transacted with high-risk VASPs (for example, if the customer used anonymisation tools or peer-to-peer exchanges) or potentially used VAs to purchase illicit goods or services. VASPs can use immediate and retrospective checks of VA transactions. Retrospective checks of transactions can provide particularly useful information, as they allow VASPs to analyse from where a customer has ultimately withdrawn VAs, even if the customer has done multiple interim transactions after the withdrawal. Institutions and authorities follow closely developments in the context of the implementation of the so-called « travel rule » (FATF R16). Since, no VASP has been registered yet, as of the date of the report, more detailed information is not available yet.

When a VASP has reasonable grounds to suspect or suspects that a transaction can be linked or related to ML/TF activities, it is obliged to report **suspicious activity (SARs)** and **suspicious transactions (STRs)** to the CRF, including for attempted transactions. The CRF and existing exchanges established in Luxembourg have developed special reporting templates that allow for effective data sharing of STRs and SARs: their cooperation is described in more detail in the "Detection by the CRF" section of this report.

6.1.3.2. Other forms of cooperation

VASPs might cooperate with competent authorities through various other channels. For example, they can communicate with the CSSF and CRF on a bilateral basis. They can have meetings with the CSSF, in which VA activities and developments are discussed. They also should provide additional information as appropriate, to the CRF and other relevant authorities (e.g. law enforcement) in relation to specific ML/TF investigations.

6.1.4. Internal organisation, governance and training

As per Article 4 of the 2004 AML/CFT Law, and implementing CSSF regulation, VASPs are required to put in place **policies, controls and procedures** to mitigate and manage the risks of ML and TF. These include defining their ML/TF risk appetite and ML/TF key risk indicators that are approved by the senior management, communicated to employees and regularly monitored. They also include documentation of key policies and procedures (e.g. transaction monitoring, CDD, EDD). VASPs should also include "participation of their employees in special ongoing training programmes to be informed of new developments, including information on techniques, methods and trends in money laundering and terrorist financing, and to help them recognise operations which may be related to money laundering or terrorist financing and to instruct them as to how to proceed in such cases".

6.2. Supervision by the CSSF

6.2.1. Understanding of ML/TF risk

The CSSF has taken steps to develop an understanding of the risks posed by VAs and VASPs. The CSSF identifies VA-related risks and publishes warnings as appropriate, cooperates with international organisations in further developing an understanding of the space and engages with private sector entities.

Table 9 below describes all VA-related warnings issued by the CSSF over the past years:

Table 9: Warnings issued by the CSSF concerning VAs and VASPs, 2017 - 2020 (as of October 2020)

Date	Warning description	URL
30 October 2020	Warning concerning the activities of an entity named Coinglobefx	https://www.cssf.lu/en/2020/10/warning-regarding-the-activities-of-an-entity-named-coinglobefx/
24 June 2020	Warning concerning the activities of an entity named Crypto Trade Center Ltd	https://www.cssf.lu/en/2020/06/warning-concerning-the-activities-of-an-entity-named-crypto-trade-center-ltd/
17 June 2020	Warning concerning the activities of an entity named Stock21options Ltd	https://www.cssf.lu/en/2020/06/warning-concerning-the-activities-of-an-entity-named-stock21stoptions-ltd/
31 January 2020	Warning concerning the website www.crypto-bull.io	https://www.cssf.lu/en/2020/01/warning-concerning-the-website-www-crypto-bull-io/
22 October 2019	Warning concerning the website http://fundrockcrypto.com	https://www.cssf.lu/en/2019/10/warning-concerning-the-website-http-fundrockcrypto-com/
13 August 2019	Warning regarding the activities of an entity named Cryptominingoptionsignal	https://www.cssf.lu/en/2019/08/warning-regarding-the-activities-of-an-entity-named-cryptominingoptionsignal/
1 August 2018	Warning regarding the activities of an entity named Cryptofinance	https://www.cssf.lu/en/2018/08/warning-regarding-the-activities-of-an-entity-named-cryptofinance/
14 March 2018	Warning regarding initial coin offerings (“ICOs”) and tokens	https://www.cssf.lu/en/2018/03/warning-regarding-initial-coin-offerings-icos-and-tokens/
14 March 2018	Warning regarding virtual currencies	https://www.cssf.lu/en/2018/03/warning-regarding-virtual-currencies/
23 August 2017	Warning regarding an entity named Onecoin Ltd.	https://www.cssf.lu/en/2017/08/warning-regarding-an-entity-named-onecoin-ltd/

6.2.2. Regulation and Information

The CSSF has established connections with VASPs entering the registration process via calls and written correspondence with key senior managers and compliance officers.

The CSSF has a dedicated web-page for VASPs[99] where it publishes relevant *communiqués* and guidance. On 15 January 2020, the CSSF has issued a *communiqué* on VAs and VASPs[100] in order to draw the attention of entities to the modified Interpretive Note to the FATF Recommendation 15 on New Technologies taking account of VASPs and the two draft bills of law amending the 2004 AML/CFT Law extending the scope of its application to include VASPs and introducing a new framework for AML/CFT supervision of VASPs that are active in Luxembourg. The CSSF also asked VASPs to start preparations for compliance with the new framework as soon as possible. The CSSF also published a *communiqué* providing entities with an overview of the VASP registration process and the CSSF published guidance on the VASP registration procedure[101]. The CSSF raises awareness to relevant documents, e.g. the FATF 12 months report or red flag indicators guidance, in its monthly Newsletter.

For all its supervised sectors (including VASPs), the CSSF provides guidance on AML/CFT obligations and ML/TF risks through circulars, public statements and monthly newsletters. The published circulars are typically relevant to multiple sectors and may also include information pertinent to individual sub-sectors. For example, the Circular 20/740 on the "*Financial crime and AML/CFT implications during the COVID-19 pandemic*" published on 10 April 2020, identified an emerging threat for VASPs rising from an increase in "online activity by those seeking child abuse material" due to COVID-19 isolation measures.

6.2.3. Market entry

According to Articles 1(20c) and 7-1(1) of the 2004 AML/CFT Law, VASPs which are established or provide services in Luxembourg, have to register with the CSSF in case they are providing one or more of the following services on behalf of or for their customers[102]:

- Exchange between virtual assets and fiat currencies, including the exchange between virtual currencies and fiat currencies;
- Exchange between one or more forms of virtual assets;
- Transfer of virtual assets;
- Safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets, including custodian wallet services;
- Participation in and provision of financial services related to an issuer's offer and/or sale of virtual assets

The CSSF then examines the registration file, and where appropriate, exchanges letters and/or organises calls/meetings with the relevant stakeholders. The CSSF reserves the right to ask for additional information and documents during the registration process. When the CSSF has finished its analysis, and a formal registration decision has been taken, the CSSF will complete the registration itself. After the registration has been completed, the registered entity is published in the national public register maintained by the CSSF.

The fact that a VASP is entered in the register of the CSSF cannot, under any circumstance, be described in any way whatsoever as a positive assessment made by the CSSF of the quality of the services provided by the VASP. The registration, the submission of a registration and/or the CSSF AML/CFT supervision may not be invoked or used for advertising or possible solicitations for business.

[99] https://www.cssf.lu/en/virtual-asset-service-provider-vasp/
[100] https://www.cssf.lu/en/2020/01/communique-on-virtual-assets-and-virtual-asset-service-providers/
[101] https://www.cssf.lu/wp-content/uploads/files/VASP_registration_procedure_eng.pdf
[102] Source: CSSF, *VASP Registration procedure*, 2020

If, after the registration, significant changes to the activities or to the key function holders notified upon registration occur, the registered entity must immediately inform the CSSF in writing. The CSSF has the right to withdraw the entity from the register in case of non-compliance with certain obligations as provided for in Article 7-1 (4) of the 2004 AML/CFT Law.

The requirement of registration for applicants, who are established or provide services in Luxembourg, is without prejudice to any other license/registration or other status required either in Luxembourg or by other European or third countries for any other activities performed by the applicant.

The VASP registration application form contains extensive information that allows the CSSF to assess ML/TF risks and mitigating factors implemented by an applicant. The form contains questions regarding identification details; program of operations and business plan; identification and suitability assessment of beneficial owners, directors and management team; and internal controls to comply with AML/CFT obligations.

For the CSSF to assess VASP-specific risks, the form requires an applicant to submit descriptions of different services offered, including:

- A step-by-step description of the type of virtual assets services to be provided,
- A detailed explanation of how the applicant determined that the activity fits into the definition of VASP as defined in Article 1 (20c) of the 2004 AML/CFT Law and in particular:
  - that it has assessed the ML/TF risks it is exposed to and is implementing a risk-based approach accordingly,
  - that it has procedures in place to identify and verify its clients at on-boarding and on an ongoing basis,
  - that it has implemented adequate mechanisms for monitoring transactions,
  - that it is reporting any suspicious transactions detected to the CRF,
  - that it has set an adequate internal organisation for managing ML/TF risks.
- A description of the provision of the VA services, detailing all the parties involved in the processes (if applicable), and including for the services provided:
  - list of the type of VAs already available and/or envisaged and the related qualification
  - whether the exchange platform is centralised or decentralised
  - a diagram of flow of funds/VAs
  - settlement arrangements
  - the strategy of the applicant and overview of its target markets: type of VA service users (natural and/or legal persons), countries where the VA services will be provided, use of third parties for distributing the products/services (by countries).

6.2.4. Oversight and supervision

CSSF's role regarding the VASPs registered in Luxembourg is limited to registration, supervision and enforcement for AML/CFT purposes only. In this respect, the CSSF is authorised to collect fees payable by the VASPs subject to registration and AML/CFT supervision. For the VASP supervision, the CSSF has all the AML/CFT supervisory powers foreseen in the 2004 AML/CFT Law, including the power to impose administrative sanctions and other administrative measures as provided for in chapter 3-1 of the 2004 AML/CFT Law. As of mid November 2020, CSSF has not formally registered any VASP yet.

6.2.5. Rules enforcement

The CSSF has the power to sanction VASPs for non-compliance with their AML/CFT obligations. If the CSSF has sufficient evidence on regulatory breaches, then it may directly trigger the remediation or enforcement process. The enforcement measures available to the CSSF for breaches of professional obligations on AML/CFT range from the lightest measure (warning) to the most severe measure (withdrawal or suspension of registration, and public statements). For VASPs, the maximum administrative fines imposed by CSSF can reach twice the amount of the benefit derived from the breach, where that benefit can be determined, or €5 million at most.

6.3. Detection by the CRF

6.3.1. STRs and SARs received by the CRF

When a VASP has reasonable grounds to suspect or suspects that a completed or an attempted transaction can be linked or related to ML/TF activities, it is obliged to report **SARs** and **STRs** to the CRF. The CRF also has the power pursuant to Article 5 (1) b) of the 2004 AML/CFT law to request information from reporting entities without any further delay.

6.3.2. Strategic analyses

The CRF has conducted multiple strategic analyses of VAs and VASPs. For example, In 2018, the CRF conducted an internal strategic analysis on VAs and their potential criminal exploitation for ML and TF purposes. The analysis included descriptions of risk indicators of suspicion and risk mitigation measures by the CRF, and it identified typologies and case studies related to VAs and VASPs. The analysis also identified emerging threats and vulnerabilities stemming from VAs, including VA conversion, gambling, extortion and terrorist financing.

6.3.3. National and international cooperation

In its role of supporting the work of regulatory, compliance, and supervision authorities, the CRF attended different international meetings in order to get the latest information on international regulatory initiatives. The CRF is part of the Luxembourg FATF delegation and participates at the different working groups related to VAs. On 5-6 September 2018, the CRF participated at the FATF Policy Development Group Intersessional Meeting in Hangzhou, China, where questions of regulation of VAs and update of FATF recommendations were discussed. The CRF also participated in the Europol Annual Virtual Asset Meeting in The Hague, Netherlands, and in the Interpol Darknet and Cryptocurrency Working Group in Nurnberg, Germany. The CRF participated in ongoing projects, namely the FATF Stablecoin and Travel Rule Expert Group, along with the CSSF in Paris from January 2020 onwards, and gave a presentation at the Blockchain Conference in January 2020 in Vienna.

6.3.4. Cooperation with the private sector

The CRF participated in conferences and events to get the best knowledge of the potential sector size in Luxembourg, including the “Virtual Assets: Legal Challenges” conference, “Electronic Money Association (EMA)” meetings, (part of the University of Luxembourg Cryptocrime Group) and informative events organised by the Luxembourg House of Financial Technology.

The CRF also provides feedback to entities that do not work in the VA field but are directly or indirectly affected by it. Persons who transfer money from an exchange to a Luxembourg bank account need to prove the economic origin of these funds and the CRF can give advice on the appropriate procedure.

6.4. Prosecution and enforcement

6.4.1. Service de Police Judiciaire

"Service de Police Judiciaire" (SPJ) is a national service within the Police Grand-Ducale which is in charge of the execution of investigations. The SPJ has executed investigations related to VAs and VASPs since 2016 and developed necessary internal capabilities and expertise that will allow it to effectively analyse any upcoming cases related to VASPs registered in Luxembourg.

6.4.2. Prosecution authorities

Prosecution authorities prosecute those who commit criminal offences, including ML/TF offences. The "Cybercrime" departments of the prosecution authorities, which sit under the respective "*Parquet d'Arrondissements"*, have experts knowledgeable in VAs and VASPs which execute VA- and VASP-related prosecutions, or support other departments in their prosecutions which involve VAs or VASPs.

7. AREAS FOR FURTHER ENHANCEMENT

Recommendations specifically targeted towards VASPs will contribute to increasing their understanding of ML/TF risks and AML/CFT obligations (Section 7.1).

7.1. Legal obligations for the private sector

All institutions conducting VASP activities should take a proactive approach to mitigate ML/TF risks. They should use this risk assessment to increase their understanding of ML/TF threats and vulnerabilities of VASPs in Luxembourg.

In line with the 2004 AML/CFT Law, regulations, this VASP ML/TF vertical risk assessment and the FATF Recommendations[103], the Ministry of Justice has identified several key obligations to entities seeking to obtain a VASP registration and conducting VASP activities.

The Ministry of Justice expects all obliged entities to fulfil their obligations as specified in the 2004 AML/CFT Law, with particular focus on the ones outlined in Table 11.

Table 10: Legal obligations for the private sector

	Legal obligations	How VASPs may show compliance (examples)
1	Develop internal risk assessments	Internal risk assessments should make a clear reference to this vertical risk assessment
2	Promote a strict compliance culture with a focus on AML/CFT throughout the whole organisation	Appropriate training programs in place including typologies relevant to the VASP industry
3	Ensure robust processes and tools are in place enabling VASPs to obtain, hold and exchange information about the originators and beneficiaries of virtual asset transfers (FATF VASP Recommendation 16 on “travel rule”) and in accordance with the obligations laid down in article 7-1 (2) d) of the 2004 AML/CFT Law.	Appropriate processes and tools used for identifying information of originators and beneficial ownership of VA transactions
4	Ensure internal control arrangements within the VASPs’ organisation, have resources proportionate to the risk of the activities and controls required	Level of FTE as well as technical resources & budgets allocated to AML/CFT activities justified based on level of risk/risk appetite
5	Collaborate closely with national authorities and contribute to the effectiveness of the national AML/CFT framework	Provide prompt and accurate responses to requests by CSSF, the CRF; share best practices or provide feedback on publications (e.g. publications by industry associations)
6	Report without delay suspicious activities and transactions to the CRF	STR/SAR/TFAR/TFTR reporting in line with risk exposure and CRF guidance
7	Implement effective technology solutions to strengthen the AML/CFT framework across key processes such as KYC, and transaction monitoring and reporting	Evidence of use of appropriate VA-related technology solutions as part of key AML/CFT processes

[103] FATF, *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, 21 June

APPENDIX A.RED FLAG INDICATORS

The table below details red flag indicators for identifying suspicious clients or transactions of VASPs, used by the CRF. The CRF has identified the red flag indicators through internal strategic analyses, operational cooperation with exchanges present in Luxembourg and cooperation with international authorities (e.g. Interpol). Note that the presence of an indicator does not in itself justify any conclusion that a predicate offence has been committed.

The FATF published further details on ML/TF red flag indicators on 14 September 2020[104], which the CRF plans to incorporate in its analyses.

The table below distinguishes VA addresses and accounts. VA addresses are controlled by a user and are not directly linked to a VASP. VA accounts are accounts that clients can open at VASPs and which enable them to use certain features of a VASP (e.g. withdraw or deposit VA or fiat currency, exchange different types of VAs). Clients may open accounts at VASPs and withdraw VAs to their addresses, or deposit VAs from their addresses to their VASP accounts.

[104] http://www.fatf-gafi.org/publications/methodsandtrends/documents/virtual-assets-red-flag-indicators.html

Table 11: Red flag indicators for suspicious activity of VASP clients (non-exhaustive list)

Categories	Risk flag indicators
Sanctions	• Client is included on a list of sanctions • Client transfers VAs to addresses at unregulated platforms linked to terrorist groups • Clients is linked to radical Islamism clusters
Use of front persons/companies	• Client uses money mules to deposit funds to a VASP, where the client purchases VAs and then sends them to a collector[105] address • Client receives VAs from other natural persons
Offshore based companies	• Client exchanges fiat currency to VAs while passing by advantageous tax jurisdictions, and then exchanges the traded VAs to another VA (e.g. from Bitcoin to Ethereum)
Cash transactions	• Client attempts to convert cash to VAs through unregulated exchanges or peer-to-peer networks
Use of forged documents	• Client provides forged passport or ID scans • Client provides forged notarised copies of identity documents • Client provides forged documents related to the source of funds (e.g. by forging a signature)
Fraudulent transactions	• Client has transactions linked to fraudulent ICOs • Client has transactions linked to investments in VAs proposed below market price • Client has transactions linked to hacker groups, which encrypt files of victims and request them to pay in VAs to retrieve the encrypted data • Client has transactions linked to extortion groups, which threaten individuals or companies with Distributed Denial-of-Service (DDoS)[106] attacks
Suspicious virtual assets (or cash) deposits and withdrawals to VASPs	• Clients' accounts are used as collector accounts • Client provides a bank statement showing multiple cash deposits and withdrawals as a proof of the source of funds • Clients' transactions are large in value, especially when linked to high-risk activities (e.g. fraudulent ICOs, potential inheritance frauds, unreported revenues from mining)
Smurfing	• Client withdraws VAs from a VASP to multiple different addresses or VASPs
Frequent transactions in small amounts	• Client exchanges VA to fiat currency without reporting it to the tax authorities • Clients' account or address receives multiple VA transactions from several individuals
Source of funds	• Client claims to receive gifts from family members or friends • Client claims the source of funds to be non-existent or defunct mining pool or exchange • Client claims the source of funds comes from an untraceable address (e.g. from an address linked to an anonymous VA)
Suspicious transaction pattern	• Client receives a VA transaction from an inheritance account before the court has made a decision on the inheritance

[105] Collector accounts or addresses are used to receive or withdraw VAs without any exchange

[106] Distributed Denial of Service (DDoS) is a cybercrime attack that attempts to make an online service unavailable by overwhelming it with traffic from multiple sources

Categories	Risk flag indicators
	• Client, who is a private individual, receives a VA transaction from an account belonging to a legal entity under the pretext of financial advisory (or vice versa)
Unusual behaviour of customers	• (Potential) client provides information to the VASP about a previously committed predicate offence, e.g. tax incompliance • Client uses several VASPs and VAs without a reasonable explanation • Clients' account opened only to deposit fiat currency, but VAs and transfer to third persons • Client registers an account on a VASP, deposits fiat currency, exchanges into VAs and withdraws VAs within a short period of time • Client accesses a VASP through a virtual private network (VPN)
Economic background of the account user	• Client transacted with addresses or accounts linked to high-risk activities, e.g. gambling, online casinos, night clubbing • Client has a previous criminal background
Open source indicators and information	• Client has a flawed background or reputation (e.g. subject to negative press articles) • Client's VA addresses published on public forums or social networks to advertise the sale of illegal goods or services (e.g. sale of drugs)
Reluctance of providing information	• Client provided inconsistent information, e.g.: – Client claims to be unemployed status but has a high annual income – Client sends invoices denominated in fiat currency but requests payments in VAs • Client provides inaccurate and complex source of funds documents • When confronted about inaccurate documents, client attributes it to discrepancies between the legal frameworks of different jurisdictions or cites language translation issues • Client refuses to provide required documentation or to deliver certain data regarding the source of funds or purpose of certain transactions • Client sends a large number of irrelevant documents to prove the source of funds
Other	• Client uses anonymous virtual assets • Client uses mixers • Client uses unregulated exchanges, particularly exchanges that enable trading of anonymous VAs • Client uses ATMs

APPENDIX B. ACRONYMS

Term	Definition
ABBL	Association des Banques et Banquiers, Luxembourg
AIF	Alternative Investment Fund
AIFM	Alternative Investment Fund Manager
ALFI	Association of the Luxembourg Fund Industry
AML	Anti-Money Laundering
ATM	Automated Teller Machine
BGRA	Bureau de Gestion et de Recouvrement des Avoirs
BTC	Bitcoin
CFT	Combatting the Financing of Terrorism
CRF	Cellule de Renseignement Financier
CSAM	Child sexual abuse material
CSSF	Commission de Surveillance du Secteur Financier
DDoS	Distributed Denial-of-Service
EBA	European Banking Authority
EEA	European Economic Area
EU	European Union
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
ICO	Initial Coin Offering
ID	Identity Document
IEO	Initial Exchange Offering
Inc.	Incorporated company
ISIS	Islamic State of Iraq and Syria
KYC	Know Your Customer
LHoFT	Luxembourg House of Financial Technology
Ltd.	Limited company
ML	Money Laundering
NRA	National Risk Assessment
OTC	Over-the-counter
S.A.	Société Anonyme
SEPA	Single Euro Payments Area
SPJ	Service de Police Judiciaire
STR	Suspicious Transaction Report
TF	Terrorist Financing
UCI	Undertakings for Collective Investment
UCITS	Undertakings for Collective Investment in Transferable Securities
USA	United States of America
VA	Virtual Asset
VASP	Virtual Asset Service Provider

APPENDIX C. LAWS

Term	Definition
2004 AML/CFT Law	Law of 12 November 2004 on the fight against money laundering and terrorist financing
5AMLD	Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU
Laws of 25 March 2020	Law of 25 March 2020 establishing a central electronic data retrieval system concerning payment accounts and bank accounts identified by IBAN and safe-deposit boxes held by credit institutions in Luxembourg and amending: 1° the Law of 12 November 2004 on the fight against money laundering and terrorist financing, as amended; 2° the Law of 5 July 2016 reorganising the State Intelligence Service, as amended; 3° the Law of 30 May 2018 on markets in financial instruments; 4° the Law of 13 January 2019 establishing a Register of beneficial owners; for the purpose of transposing: – 1° points (19) and (29) of Article 1 of Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering and terrorist financing risk, and amending Directives 2009/138/EC and 2013/36/EU; – 2° point (28)(d) of Article 1 of Directive (EU) 2019/878 of the European Parliament and of the Council of 20 May 2019 amending Directive 2013/36/EU as regards exempted entities, financial holding companies, mixed financial holding companies, remuneration, supervisory measures and powers and capital conservation measures; – 3° Article 64(5) of Directive (EU) 2019/2034 of the European Parliament and of the Council of 27 November 2019 on the prudential supervision of investment firms and amending Directives 2002/87/EC, 2009/65/EC, 2011/61/EU, 2013/36/EU, 2014/59/EU and 2014/65/EU Laws of 25 March 2020 amending: 1° the Law of 12 November 2004 on the fight against money laundering and terrorist financing, as amended; 2° the Law of 9 December 1976 on the organisation of the profession of notary, as amended; 3° the Law of 4 December 1990 on the organisation of bailiffs, as amended; 4° the Law of 10 August 1991 on the legal profession, as amended; 5° the Law of 10 June 1999 on the organisation of the accounting profession, as amended; 6° the Law of 23 July 2016 concerning the audit profession, as amended; with a view to transposing certain provisions of Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU