Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Justice and Police DFJP
Federal Office of Police fedpol

January 2024

National Risk Assessment (NRA)

Risk of money laundering and the financing of terrorism through crypto assets

Table of contents

1. Glossary

AML/CFT	Anti-money laundering/Countering the Financing of Terrorism
Blockchain technology	One of several possible variants of distributed ledger technology
CeFi	Centralised finance
CEX	Centralised exchange
CGMF	Interdepartmental coordinating group on combating money laundering and the financing of terrorism
CTM	Crypto automated teller machine (crypto ATM)
DAO	Decentralised autonomous organisation
DeFi	Decentralised finance
DEX	Decentralised exchange
DLT	Distributed ledger technology, allows data to be stored and managed decentrally on multiple computers, making transactions transparent, secure and tamper-proof.
FATF/GAFI	Financial Action Task Force/Groupe d'action financière
FI	Financial intermediary
Fiat money	Central bank-issued legal tender that, unlike commodity money, is not backed by physical goods or natural resources.
FIU	Financial intelligence unit
Hosted / Custodial wallet	Client wallet where the financial intermediary with VASP activities has access to the client's VAs.
KYC	'Know your customer' is a procedure implemented by FIs to verify the identity of clients, assess and monitor client risk and prevent illegal activities such as money laundering.
LEAs	Law enforcement agencies

Metaverse	Virtual world bringing physical and digital elements together, enabling users to interact in an immersive environment.
ML/TF	Money laundering/terrorist financing
Multisig wallet	Multisig wallets (multi-signature wallets) are cryptocurrency wallets that offer greater security by requiring multiple private keys (i.e. usually requiring several people to give their consent) in order to validate transactions.
NFT	Non-fungible token
Off-chain transaction	VA transaction not registered on a blockchain
On-chain transaction	VA transaction registered on a blockchain
Peer-to-peer (P2P)	Network model in which participating devices are directly connected without relying on a centralised server. This ensures decentralised interaction between devices on a level playing field.
PEP	Politically exposed person
Privacy coin	Cryptocurrency designed to enhance the privacy and anonymity of users by obscuring the flow of transactions across their networks (e.g. Monero or Zcash).
Rug pull	When a development team (e.g. a decentralised finance platform) suddenly abandons a project and sells or removes all its liquidity.
Smart contract	A program stored on the blockchain that automatically executes a transaction as soon as the conditions agreed by the contracting parties have been met. Smart contracts remove the need for intermediaries and manual intervention.
Smurfing	Breaking down a large sum of money into smaller transactions that fall below the reporting thresholds in order to conceal the true value of the transaction and avoid detection by ML/TF regulatory authorities.
Stablecoins	VAs that are designed to maintain a stable market price by pegging their value to the price of a commodity (e.g. 1 g of gold = 1 stablecoin unit) or currency (e.g. 1 CHF = 1 stablecoin unit).

TBML	Trade-based money laundering
Travel Rule	Based on FATF Recommendation No 16, this rule requires financial institutions with or without VASP activities to share client data with each other when carrying out cross-border transactions.
Unhosted / Non-custodial wallet	Wallet in which virtual assets are held directly by an individual without any form of third-party access.
VA	Virtual asset
VASP	Virtual asset service provider
Web3	A new iteration of the Internet where decentralised applications and systems are built using blockchain technologies.

2. Executive Summary

Over the past ten years, cryptocurrencies (virtual assets, VAs) have evolved from a niche activity to a mass phenomenon that is having an impact on the traditional financial system. The use of VAs has become more common for both private individuals and companies. In Switzerland, an increasing number of FIs are offering VA services, leading to the emergence of virtual asset service providers (VASPs). At the same time, however, criminals have also recognised the potential of this payment system. VAs are now being misused for a wide range of illegal purposes, from 'simple' theft and fraud offences to the most serious forms of transnational crime, including money laundering and terrorist financing (ML/TF). These developments pose considerable challenges for all stakeholders involved in anti-money laundering efforts.

In 2018, the interdepartmental coordinating group on combating money laundering and the financing of terrorism (CGMF) published its first risk analysis on the misuse of cryptocurrencies for ML/TF and categorised the risks and vulnerabilities for Switzerland as 'considerable'. At that time, however, the Money Laundering Reporting Office Switzerland (MROS) had only received a few suspicious activity reports (SARs) in connection with VAs.

The impact and importance of VAs has fundamentally changed since 2018. The level of awareness and knowledge in the market is now much greater. MROS currently receives VA-related SARs on a daily basis – for law enforcement agencies, VAs have become part and parcel of their everyday work. MROS has identified four key developments:

1. In Switzerland, the number of FIs with VASP activities has risen significantly from less than ten in 2018 to over 204 at the end of 2022. Despite this, at least 180 of these FIs have not submitted a single suspicious activity report to MROS.

2. Between 2018 and 2023, VA use in Switzerland intensified; a growing number of private individuals and companies are using and accepting VAs for payments in commerce, for services and for investments. The boundaries between the traditional financial sector and the VA sector are becoming increasingly blurred; VAs are being integrated into traditional payment platforms to a greater extent and the 'two worlds' are converging.

3. The criminal use of VAs has risen both in Switzerland and globally. It has also become much more diverse. Law enforcement agencies are increasingly confronted with VA-related cases involving different economic sectors. For example, more and more criminal charges are being filed in connection with theft or other forms of misappropriation (e.g. fraud, embezzlement) of VAs. The amount of damage caused by VAs has soared and is expected to be at least in the double-digit millions in Switzerland in 2022 (compared to just under CHF 7 million in 2007). The use of VAs has become routine in certain criminal offences (e.g. investment fraud, ransomware). VAs have become a common tool of financial crime.

4. In recent years, FIs in Switzerland have increasingly identified suspected cases of ML/TF involving VA-related transactions on client accounts. This has led to a sharp increase in the submission of VA-related SARs to MROS: in 2022, nearly 14% of all suspicious activity reports were linked to VAs. These included links to politically exposed persons (PEPs), international corruption scandals, transnational organised crime groups or state actors.

This risk analysis concludes that ML/TF risks in the VA sector have grown compared to 2018. Threats and vulnerabilities that were already identified in 2018 have largely become more acute and broader. Due to their heightened importance and the risks associated with them, VAs require the necessary attention from all stakeholders.

Despite the identified threats and vulnerabilities for Switzerland in relation to ML/TF in the VA sector, various factors help to mitigate these risks:

- International cooperation in VA-related investigations shows that increased tracing, freezing and confiscation of VAs are effective in combating money laundering and terrorist financing.
- Many small VASPs have now disappeared or merged. This has also prompted large crypto exchanges to strengthen their compliance measures, which reinforces anti-money laundering and counter-terrorist financing (AML/CFT) efforts worldwide.
- Blockchains are inherently more transparent than traditional payment systems. This leads to better traceability of VAs; blockchain analytics tools can identify and track suspicious activity more easily.
- Finally, in Switzerland, the expansion of the definition of financial intermediation in the VA sector has helped to bring a broader range of actors under the scope of the Anti-Money Laundering Act. This closes gaps within the AML/CFT system.

The CGMF proposes four measures to strengthen the current AML/CFT arsenal in the VA sector:

1. **Improve the level of data and knowledge about the VA sector in Switzerland**
   Information on the VA sector and the criminal use of VAs in Switzerland is essential to adequately identify, understand and assess ML/TF risks.

2. **Encourage FIs with VASP activities to become more proactive in their reporting practices**
   In the future, VASP FIs should step up their ML/TF monitoring activities in order to be in a better position to detect suspicious transactions and report them to MROS.

3. **Provide sufficient capacity and resources for AML/CFT efforts in the VA sector**
   Cooperation between all relevant stakeholders must be strengthened in order to address ML/TF challenges in the VA sector.

4. **Intensify international cooperation**
   Switzerland should continue to work at international level to effectively tackle criminal risks in the financial sector and expedite implementation of the Recommendation made by the Financial Action Task Force (FATF).

To conclude, it is important for Switzerland to take VA-related risks seriously and adopt appropriate measures to effectively counter money laundering and terrorist financing. VAs are becoming an increasingly important part of the financial sector; Switzerland must rise to the challenges in order to keep pace with rapid developments.

3. Introduction

The use of virtual currencies (also referred to as virtual assets – or VAs, see Section 4.1) has risen sharply in the last five years. Their legitimate uses have become commonplace, e.g. for investment, payment of goods and services or for money transfers worldwide. However, VAs also have certain characteristics that can be exploited for money laundering and terrorist financing purposes (ML/TF). The increased use of VAs for criminal purposes in general and for ML/TF purposes in particular creates significant challenges for financial intermediaries, supervisory authorities and law enforcement agencies.

The first general ML/TF risk assessment of VAs that specifically focused on Switzerland was published back in 2014.[1] At the time, it was reported that there were no major cases of money laundering or terrorist financing involving VAs in Europe and the Money Laundering Reporting Office Switzerland (MROS) stated that it had received only a small number of suspicious activity reports (SARs) in relation to Bitcoin. In 2018 the Interdepartmental coordinating group on combating money laundering and the financing of terrorism (CGMF) published its first sector risk analysis on the subject.[2] On that occasion, the CGMF closely examined ML/TF risks posed by these technologies and concluded the Swiss financial market was exposed to 'considerable' risks, threats and vulnerabilities. In 2021 the CGMF drafted a second sectorial report on the risks of money laundering and terrorist financing in Switzerland[3] after 2016. The 2021 report recommended close monitoring of the situation, given Switzerland's growing vulnerability to VAs, the rapid development of this sector, and the difficulties involved in measuring the related risks. Moreover, it was pointed out that the information in the 2018 sector report may need to be updated. The present report is a follow-up on that recommendation.

MROS took over this mandate from the CGMF. The latter is a standing interdepartmental coordinating group established by the Federal Council at the end of 2013. It is responsible for coordinating AML/CFT polices and assessing corresponding risks in these areas.[4] This report is the result of their work, which was carried out in close cooperation with supervisory bodies, law enforcement and other federal agencies and offices.

Fulfilling the mandate proved to be difficult, as much of the information required for an accurate assessment of ML/TF risks for Switzerland in relation to VAs was not available. On the one hand, this includes information regarding the size of the legal entities and natural persons operating in the VA sector[5] as well as information on the criminal use of VAs in Switzerland, such as consolidated figures on the number of cases in Switzerland, the offences being investigated, the amounts involved, as well as the outcomes reached. Despite these knowledge gaps, certain statements on the significance and growth of the VA sector and the associated money laundering and terrorist financing risks can be made. Several surveys were conducted and sources evaluated for this purpose. Although reliable figures are certainly needed in order to accurately ascertain risks, the methodology adopted does enable a well-founded assessment to be made. This can be summarised as follows:

[1] Federal Council, *Federal Council report on virtual currencies in response to the Schwaab (13.3687) and Weibel (13.4070) postulates, 25 June 2014*, p. 20f.
[2] CGMF, *Risk of money laundering and terrorist financing posed by crypto assets and crowdfunding*, October 2018, p. 4.
[3] CGMF, *2nd National report on the risks of money laundering and terrorist financing in Switzerland*, October 2021, p. 53.
[4] For information on the mandate and composition of the CGMF, see State Secretariat for International Finance (SIF), *Mandate of the Interdepartmental coordinating group on combating money laundering and the financing of terrorism*, approved by the Federal Council Decree of 17 November 2021.
[5] VAs or VA-derived income managed, taxed or settled by them, or VA-related financial flows entering or leaving the Swiss financial centre.

First of all, the VA sector has experienced strong growth at both global and national levels since 2018. While total VA market capitalisation accounted for less than 1% of global gross domestic product (GDP) in 2018, at its recent peak in 2021, it had already reached 2.7%.[6] Even if these figures are partly due to volatile price fluctuations, the use of VAs has clearly risen sharply in recent years. It is estimated that in 2023, around 420 million people worldwide, or over 4% of the world's population, have owned VAs.[7] This strong increase has also been observed in Switzerland. Various surveys in Switzerland found that in 2020 between 7-10% of respondents had purchased VAs, while in 2022 this figure stood at between 18-20%.[8] However, VA financial flows still remain relatively manageable compared with other financial flows. While the global annual transaction volume of all VAs peaked at USD 15.8 trillion (2021), the global daily volume of over-the-counter foreign exchange transactions, for example, stood at USD 7.5 trillion (April 2022), which is a completely different order of magnitude.[9]

Secondly, reports from various countries, supranational organisations and blockchain analytics companies clearly show that the criminal use of VAs has increased and diversified globally since 2018. The threats posed by money laundering are no longer limited to predicate offences relating to cybercrime and 'crypto-specific' crimes.[10] In the meantime, threats are also coming from a wide variety of offline crimes, including the most serious forms of white-collar crime, and ultimately VAs are also being used by professional money laundering networks.[11] In addition, the use of VAs for certain crimes, especially ransomware attacks and online investment fraud, is now widespread and has become the rule rather than the exception.

Thirdly, the number of VASP FIs domiciled in Switzerland has grown exponentially since 2018: back then, there were fewer than ten FIs that engage in VASP activities; by the end of 2022, there were at least 204. Furthermore, an increasing number of Swiss FIs *without* VASP activities have points of contact with the VA sector (e.g. through the business activities of their clients and the transactions carried out). Given the general expansion of these points of contact as well as the observed increase in the criminal use of VAs, the Swiss financial centre as a whole is now more vulnerable to the misuse of VAs for ML/TF purposes.

Fourthly, there appears to be confirmation of this in the significant increase in the number of VA-related SARs submitted to the Money Laundering Reporting Office Switzerland (MROS): For Switzerland, the risk analysis published in 2018 indicated that Swiss authorities had not yet identified a single case where VAs were used to finance terrorist activities and only a few cases of money laundering involving these new technologies.[12] Today, this conclusion is outdated. Compared to 2018, the Money Laundering Reporting Office Switzerland (MROS) receives SARs relating to

[6] Financial Stability Board (FSB), *FSB Chair's letter to G20 Finance Ministers and Central Bank Governors*, March 2018, p. 2. According to the Financial Stability Board, market capitalisation of VAs surged 350% to USD 2.6 trillion in 2021; see Financial Stability Board (FSB), *Assessment of Risks to Financial Stability from Crypto-assets*, February 2022, p. 1. According to World Bank estimates, global GDP reached USD 96.1 trillion in 2021; see World Bank, *GDP (current US$) – World*, last checked in May 2023.
[7] Triple-A, *Global Cryptocurrency Ownership Data*, last checked in May 2023.
[8] Moneyland, *Wie legen Schweizer ihr Geld an?*, 22 April 2020. Moneyland, *So investieren Schweizerinnen and Schweizer ihr Geld*, 19 July 2022. A number of similarly structured surveys report the same trend, with only minor percentage point variations, e.g.: Migros Bank, *Kryptowährungen bei jüngeren Generationen beliebter als Gold*, 27 February 2020. Handelszeitung, *Krypto lockt: Studie zeigt grosses Interesse in der Schweiz*, 22 June 2021.
[9] For information on global transaction volumes for all VAs, see Chainalysis, *The Crypto Crime Report 2022*, February 2022, p. 3. For information on the global trading volume for over-the-counter foreign exchange transactions, see Bank for International Settlements (BIS), *OTC foreign exchange turnover in April 2022*, October 2022.
[10] For example, initial coin offerings (ICOs) and other fraudulent investment schemes or the use of VAs in various money mule schemes.
[11] Europol Spotlight, *Cryptocurrencies – Tracing the Evolution of Criminal Finances*, December 2021, p. 2.
[12] CGMF, *Risk of money laundering and terrorist financing posed by crypto assets and crowdfunding*, October 2018, p. 4.

the use of VAs for money laundering or terrorist financing purposes on a daily basis. Nearly 10% of all SARs submitted to MROS between 2020 and 2022 related to VAs, with this share already reaching 13.8% in 2022.

In order to address the developments summarised here and bring the VA sector in compliance with international standards, various amendments have been made to substantive law in Switzerland since 2018 (see Section 4.4). Some of these amendments are even more stringent than the Recommendations formulated by the Financial Action Task Force (FATF). However, there are specific implementation challenges that impact the effectiveness of Switzerland's AML/CFT arsenal in this sector:

First of all, the ability to detect money laundering and terrorist financing through VAs in Switzerland depends heavily on the reporting behaviour of FIs that engage in VASP activities. Available figures, however, seem to indicate that they are much less likely to file a SAR than FIs *without* VASP activities. There are currently over 204 FIs with VASP activities in Switzerland but only 24 have filed SARs since 2020. In contrast, MROS received of 118 FIs *without* VASP activities at least one VA-related SAR during the same period.

Secondly, one of the distinctive features of the VA sector is that related service providers, business activities, persons and transactions are highly international in nature. One of the biggest challenges in this area is the fact that most countries have not or not yet applied FATF Recommendations to the VA sector, including in particular compliance with the Travel Rule (see Section 4.3.2). Compared to other countries, Switzerland was very quick to transpose the Travel Rule into its existing legislation. Nevertheless, VASPs domiciled abroad are vulnerable to being misused as a gateway enabling criminal assets (in VAs or fiat currency) to enter the legitimate financial circuit. It is also important to realise that these VAs are always just one transaction, or one second, away from ending up in Switzerland. Therefore, failure on the part of third countries to apply FATF Recommendations to the VA sector also increases the risk that Switzerland's financial system will be exploited for money laundering and terrorist financing purposes. This circumstance requires greater vigilance from financial intermediaries. All FIs – with or without VASP activities – are vulnerable to being misused as recipients of incriminated assets from these countries by means of indirect transfers.

Thirdly, Swiss law enforcement agencies in particular – but also other agencies and offices involved in ML/TF countermeasures – face specific challenges in the VA sector. Roughly half of them have already started to pool more personnel, knowledge and technical resources to meet these challenges.

Fourthly, the co-existence of different payment processing systems has always posed a risk from an AML/CFT standpoint. This risk has reached a new dimension with the co-existence of fiat and VA payment processing systems, which are fundamentally different. Consequently, data and information on the respective systems are structured, stored and made available in different ways. In addition, several possible payment flows also exist simultaneously for individual VAs, some of which offer a high degree of anonymity.[13] The simultaneity of different payment processing systems makes it much more difficult for individual actors, such as a financial intermediary or

[13] The oldest cryptocurrency Bitcoin helps to illustrate this: Transactions can either be 'on-chain' or 'off-chain'. In the first case, the transactions are processed directly on a source blockchain network to which the cryptocurrency belongs (i.e. referred to as the mainnet, the base layer or layer 1). In the second case, transactions are processed using a layer 2 scaling solution instead. Examples include a payment channel protocol built on top of the base layer (e.g. the Lightning Network in the case of the Bitcoin mainnet); a two-way blockchain bridge connecting the mainnet to a sidechain; a platform enabling different coins to be exchanged with one another (coin swap) or using a statechain to exchange private keys instead of coins.

a law enforcement agency, to see the big picture. Criminals take advantage of this to launder illegally gained assets and cover their tracks. This problem has become more acute since it only takes a few seconds to electronically transfer fiat currency and VAs worldwide and because it also only takes a few seconds for users to withdraw VAs from financial intermediaries and transfer them to privately controlled wallets. These two factors, speed and the lack of electronic borders, thus make it difficult to gain a comprehensive overview of the situation.

The risk landscape in the VA sector has changed in recent years and the use of cryptocurrencies for money laundering and terrorist financing purposes has increased. It is highly unlikely that VAs will disappear from the scene in the near future. At the same time, it is difficult to measure the related money laundering and terrorist financing risks. 15 years after the emergence of the oldest VA (Bitcoin), no reliable consolidated data exist on the size and shape of the VA sector worldwide or in Switzerland or on the fiat and VA financial flows associated with it. Accordingly, there is no means of determining what proportion of these financial flows may have a criminal origin. As explained in this report, Switzerland does not have any provisions specifying the responsibility for collecting such figures in the sense of a national monitoring.

While there was for a certain time some justification for the lack of national monitoring based on the argument that the VA hype would soon disappear, the absence of national monitoring has now become a risk in itself in view of rapid developments in the VA sector. Reliable figures on the actual size of the VA sector and the criminal use of VAs in Switzerland would facilitate an assessment to which extent the (suspected) cases already detected are representative for operations in the Swiss VA sector and which recommendations for amending the AML/CTF dispositive seem appropriate.

At the same time, recent successes in freezing and confiscating incriminated VAs show that there are significant opportunities and previously unimagined AML/CFT possibilities in the VA sector. The inherent transparency of most VAs can be used by financial intermediaries and law enforcement agencies to immediately detect suspicious activities and track VA financial flows. In the context of combating ML/TF, the VA sector thus offers a decisive advantage over traditional payment systems – provided the necessary resources and expertise are available.

4. Framework

This chapter is intended to clarify the legal and economic status of virtual assets (VAs) at both national and international level. It explains the terms 'virtual asset' and 'virtual asset service provider' as defined by the FATF and compares these terms with the ones used in Swiss legislation and official publications. For an overview of which individuals and services are covered by these definitions the basic aspects and distinctions of the VA ecosystem and their interaction with the traditional financial sector are illustrated. The relevant regulatory developments at international and national level since 2018 are also examined in more detail, including in particular the current status of implementation of the FATF Recommendations regarding VAs and VASPs.[14] Finally, despite the limited availability of data, we seek to provide as accurate a description as possible of the current structure of the VA sector and the use of VAs in Switzerland.

4.1 Virtual currencies, virtual assets and virtual asset service providers

The Federal Council report on virtual currencies was published in June 2014 in response to the Schwaab and Weibel postulates. This report defines the term virtual currency as follows: 'A virtual currency is a digital representation of a value which can be traded on the Internet and although it takes on the role of money – it can be used as a means of payment for real goods and services – it is not accepted as legal tender anywhere. These currencies have their own denominations. They differ from e-money in that they are not based on a currency with legal tender status. Virtual currencies exist only as a digital code and therefore do not have a physical counterpart for example in the form of coins or notes. Given their tradability, virtual currencies should be classified as an asset.'[15]

In October 2018 the Financial Action Task Force (FATF)[16] gave its first definition of 'virtual assets' (VAs) and 'virtual asset service providers' (VASPs) – to draw a distinction with the previously used term 'virtual currency'.[17] The new definitions were added to FATF Recommendation No 15 ('New technologies') in order to clarify the requirements placed on these new forms of assets and providers:

> 'A virtual asset is a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations.'.[18]

[14] For documentation of regulatory developments in connection with VAs and VASPs in Switzerland up to and including 2018, see CGMF, *Risk of money laundering and terrorist financing posed by crypto assets and crowdfunding*, October 2018.
[15] Federal Council, *Federal Council report on virtual currencies in response to the Schwaab (13.3687) and Weibel (13.4070) postulates, 25 June 2014*, p. 7f.
[16] The FATF is the main point of reference for international standards aimed at countering money laundering and terrorist financing.
[17] FATF, *Outcomes FATF Plenary, 17-19 October 2018*, October 2018. Other key FATF publications on this topic that confirm these developments: FATF, *Guidance for a Risk-Based Approach to Virtual Currencies*, June 2015. FATF, *Guidance to a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, June 2019, p. 4. FATF, *The FATF Recommendations*, February 2023, p. 140.
[18] FATF, *The FATF Recommendations*, February 2023, p. 135.

The FATF also defined the term 'virtual asset service provider' (VASP) as follows:

> 'Virtual asset service provider' means any natural or legal person who is not covered elsewhere under the Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person:
> i. exchange between virtual assets and fiat currencies;
> ii. exchange between one or more forms of virtual assets;
> iii. transfer of virtual assets;
> iv. safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and
> v. participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.'.[19]

With the incorporation into the Federal Council's Anti-Money Laundering Ordinance (AMLO)[20] on 1 January 2016, the term 'virtual currency' was included for the first time in a legal decree in Switzerland. Meanwhile, the CGMF used the terms 'virtual currency' and 'cryptocurrency' synonymously in its risk analyses published in 2018 and defined an additional generic term with the word 'crypto asset':

> 'A crypto asset is commonly understood to be a digital representation of a value that can be digitally traded on a blockchain and can be used for the purpose of payment (payment function), use (usage function) or investment (investment function).'[21]

The use of this generic term was forward-looking in that it covers not only cryptocurrencies in the classical sense, but also, for example, newly emerging phenomena such as non-fungible tokens (NFTs, see Section 6.2). However, the definition did include the indication that these can be traded on a blockchain.[22] Various countries also use different terms such as 'digital currencies' or 'digital assets' and define and use these terms differently.

For its part, the Swiss Financial Market Supervisory Authority (FINMA) considers the term used in Switzerland ('virtual currencies') to be synonymous with the term used by the FATF ('virtual assets'). Thus, for example, FINMA's assessment of NFTs is based on their economic purpose rather than on their technical features. Whereas the main question is, what kind of right the NFT represents. In the present report, virtual currencies are used interchangeably with virtual assets (VA).

[19] FATF, *The FATF Recommendations*, February 2023, p. 135.
[20] SR 955.01 – *Ordinance of 11 November 2015 on Combating Money Laundering and Terrorist Financing* (Anti-Money Laundering Ordinance, AMLO), Art. 4 para. 2 let. a., status as of 1 January 2016.
[21] CGMF, *Risk of money laundering and terrorist financing posed by crypto assets and crowdfunding*, October 2018, p. 8.
[22] Blockchain technology is one of several possible distributed ledger technologies (DLTs), which is the umbrella category for data structures that span multiple computers and locations. Thus, cryptocurrencies or NFTs based on distributed ledger technologies other than blockchain technology are theoretically possible (and in some cases already exist).

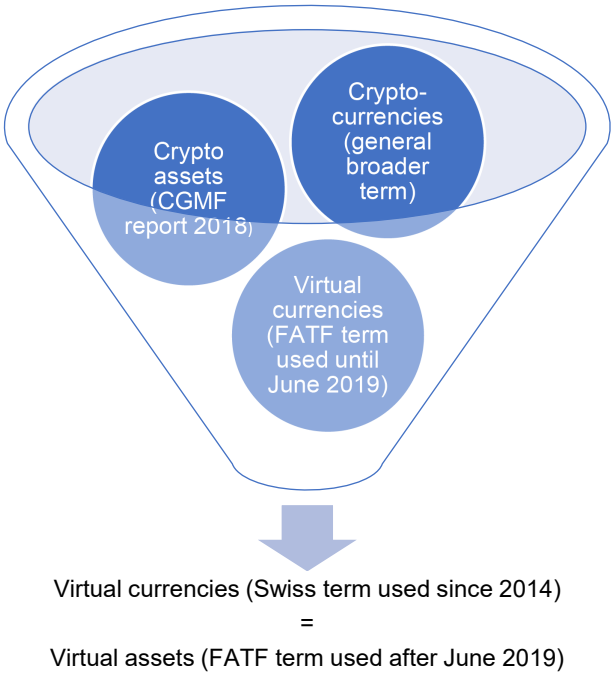

Figure 1: The synonymous terms 'virtual currencies' (CH) and 'virtual assets' (FATF) are legally defined generic terms and include, for example, NFTs.

4.2 VA ecosystem

Various models are used to describe the VA ecosystem and to categorise activities involving VAs. These models differ depending on the area of focus and perspective adopted. The model presented here considers the VA ecosystem from a value creation perspective, from the moment a VA is created to the moment it is used for a specific service. Examples of financial intermediation (within the meaning of the Anti-Money Laundering Act) in this value chain are provided. In addition, the interactions between these FIs and VA ecosystem actors in relation to the possible financial flows (whether it be in fiat currency or in VAs) are shown. Given the rapid developments in the VA sector, it should be noted that neither the classifications nor the examples given are exhaustive. Depending on the situation, individual categories or services may also overlap.

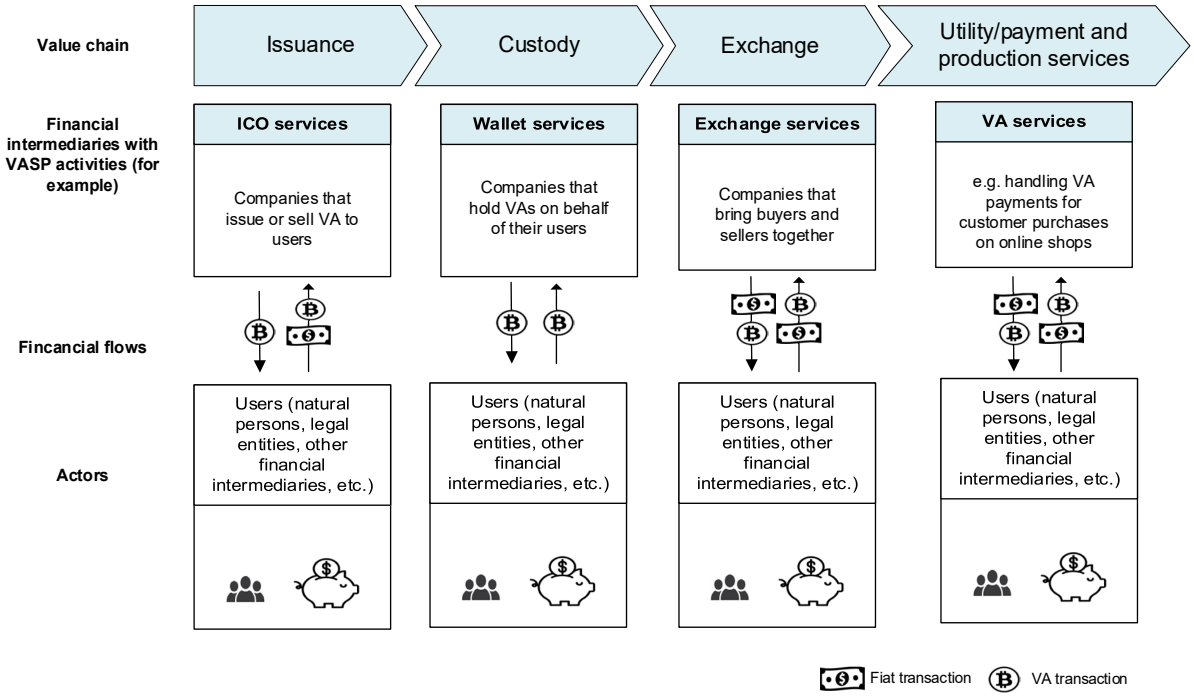

Figure 2: Illustration of a typical VA value chain and the associated financial intermediation

There are also different models used around the world to categorise VAs on the basis of their respective characteristics. Here, too, it should be noted that these categories may overlap and the placing of VAs into certain categories often depends on multiple factors, such as technological progress or the respective regulatory framework in each country.

Model 1: Categorisation based on purpose and/or technical features	Model 2: Categorisation based on legal status	Categorisation based on function (see Section 4.4.3)
• **Fungible** (e.g. Bitcoin or Ethereum) vs**. non-fungible token** (e.g. Bored Ape Yacht Club tokens) • **Uncollateralised VAs** (e.g. Bitcoin or Ethereum) vs. **collateralised VAs** (e.g. stablecoins such as DAI or USDT) • **Proof-of-Work** (e.g. Bitcoin or Monero) vs. **Proof-of-Stake** (e.g. Ethereum or Tezos) • **Pseudonymous** (e.g. Bitcoin or Litecoin) **vs. Anonymous** (e.g. Monero or Zcash) • **Cryptocurrencies** (e.g. Bitcoin or Litecoin) vs. **Smart contract platforms** (e.g. Ethereum or Binance Smart Chain)	• **Regulated** vs. **unregulated VAs** (varies by jurisdiction) • **Prohibited** vs. **permitted VAs** (varies by jurisdiction) • VAs as **official legal tender** (e.g. Bitcoin in El Salvador) vs. **VAs used as an unofficial means of payment** (e.g. Monero on Darknet markets)	• **Payment token** • **Utility token** • **Asset token** • **Hybrid token** (tokens that combine features, e.g. payment *and* utility token, or asset, utility *and* payment token)

Figure 3: Different models used to categorise Vas

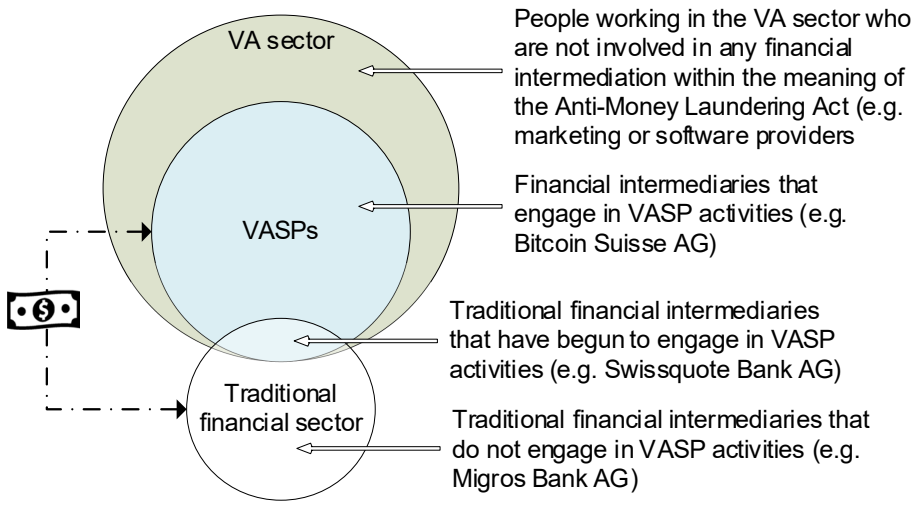

Figure 4: Differences and interaction between FIs that engage or do not engage in VASP activities

The VA sector includes all business activities involving VAs. Not all of these activities fall within the scope of financial intermediation as defined in the Anti-Money Laundering Act (see Section 4.6.1 and 4.6.2). This report focuses on financial intermediaries whose business activities bring them in contact with the VA sector, regardless of whether they carry out VASP activities directly or not. The business activities of traditional FIs without VASP activities can also be related to VAs – for example, when a traditional financial intermediary without VASP activities executes a bank transfer to a VA exchange on behalf of its client or when it provides a business account to a financial intermediary with VASP activities. It should also be noted that not all business activities of financial intermediaries with VASP activities involve VAs. For example, some FIs with VASP activities also offer traditional financial services that are unrelated to VAs.[23]

Infobox 1

Blurring boundaries between FIs with and without VASP activities

From the perspective of combating money laundering, its predicate offences and terrorist financing, the distinction between FIs with and without VASP activities seems irrelevant in the medium to long term. There are several reasons for this.
First of all, the progressive integration of VAs means that traditional financial intermediaries are also increasingly offering services in the VA sector. This development can already be observed and is likely to continue. Secondly, the SARs filed by traditional financial intermediaries show a rising number of points of contact with the VA sector. Thirdly, the growth of the VA sector has prompted FIs without VASP activities to develop business models in which they themselves do not engage in VASP activities, but the business model itself is explicitly geared to the VA sector (e.g. providing business and payment processing accounts in fiat to FIs with VASP activities, which then trigger payments in VAs on the platforms of FIs with VASP activities), see Vulnerability 6 in Section 7.5.1).
In tracking suspicious financial flows, the distinction between fiat and VA forms is ultimately a matter of semantics. The line between these two categories of financial intermediaries is already blurred today. Further growth in the VA sector and an intensification of business activities and points of contact between FIs with and without VASP activities may lead to a further merging of these categories. The distinction could only be important, particularly from

[23] For example, offering clients the possibility of opening a brokerage account.

an AML/CFT perspective, to determine which forms of financial flows (VAs or fiat) need to be taken into account for the analysis and prosecution of suspicious transactions.[24]

4.3 International AML/CFT standards applicable within the VA sector

Since 2018, the global VA sector has expanded significantly. On the one hand, there is now widespread acceptance of VAs, also in the traditional finance sector. At the same time, however, the VA sector has drawn increased scrutiny from national and international regulators, law enforcement agencies, Financial Intelligence Units (FIUs), and the private sector (e.g. blockchain analytics companies). The result has been greater attention to ML/TF issues in the VA sector and capacity building. At the same time, the Financial Action Task Force (FATF) has begun to systematically apply its recommendations to the VA sector, publishing a large number of overviews and guidance documents, which are discussed at length below.

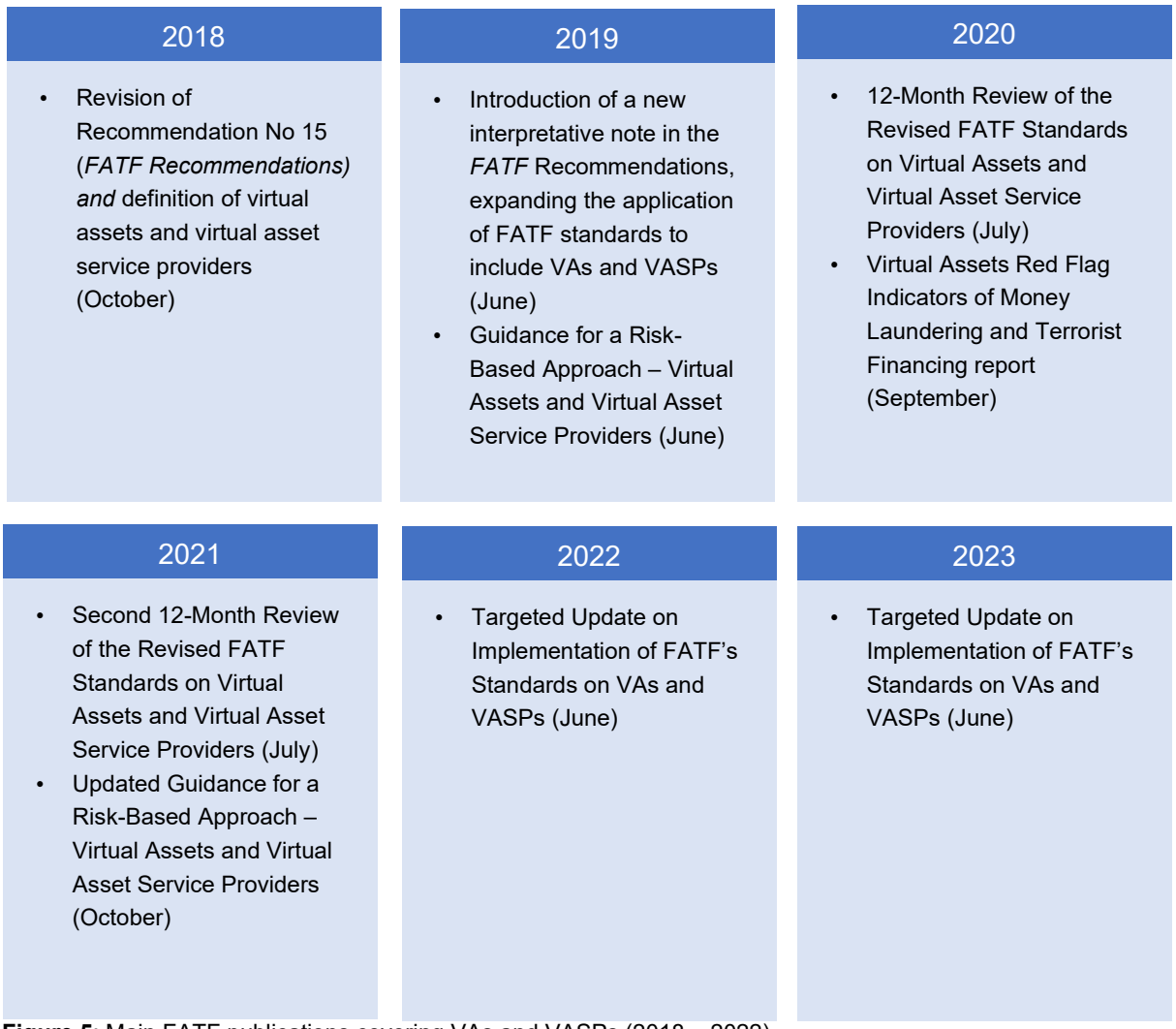

Figure 5: Main FATF publications covering VAs and VASPs (2018 – 2022)

[24] Basel Institute on Governance, Europol, *Seizing the Opportunity: 5 recommendations for crypto-assets-related crime and money laundering*, 2022, p. 1f.

4.4 Travel Rule, stablecoins and decentralised finance

The definitions of 'virtual asset' and 'virtual asset service provider' were established in October 2018 and added to FATF Recommendation No 15 ('New technologies'). This can be seen as the beginning of intensive work at FATF level on this subject.[25] The corresponding interpretative note was adopted in June 2019, providing an explanation of how Recommendations No 10 to 21 should be implemented by VASPs.[26] Implementation of the Travel Rule, which is already well established in conventional payment traffic, was the most important requirement: from now on, all VA transfers between VASPs (e.g. bank transfers) must include information about the sender and recipient. This is done to ensure that the receiving VASP can check the name of the sender and the accuracy of the recipient's information.

	FATF Travel Rule (R. 16)
Sender details	• Name • Account number • Transaction reference number • Address / Date and place of birth / client number / national ID number
Recipient details	• Name • Account number
Minimum threshold	• EUR 1,000 / USD 1,000

Figure 6: Information that must be shared during payment transactions, including VA transactions between VASPs

In June 2019, the FATF published its 'Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers' in response to the 'drastic change in the financial industry' brought on by the VA sector.[27] This guide is intended to show how VAs and VASPs fall within the scope of FATF Recommendations and how these Recommendations can be implemented by national authorities.

Then, in June 2020, the FATF issued a report on stablecoins.[28] Stablecoin projects are designed to limit the price volatility typically associated with VAs by backing the token with specific underlying assets, such as fiat currencies, commodities, real estate or securities. For example, a token can represent a title to one Swiss franc, or to one gram of gold, or to one share in a real estate portfolio or to a given amount of a commodity. The FATF noted that stablecoins share many of the potential ML/TF risks generally associated with VAs: their potential anonymity through transfer via non-custodial wallets, their global reach, and their suitability for the concealment phase in the money laundering process.[29] These characteristics create vulnerabilities in terms of money laundering and terrorist financing. Accordingly, the FATF called on its member countries to prioritise implementation of FATF standards for VAs

[25] FATF, *Outcomes FATF Plenary, 17-19 October 2018*, October 2018.
[26] FATF, *The FATF Recommendations*, February 2023, p. 140.
[27] FATF, *Guidance to a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, June 2019.
[28] FATF, *FATF Report to the G20 Finance Ministers and Central Bank Governors on So-called Stablecoins*, June 2020.
[29] A non-custodial wallet enables user self-storage of VAs, with no third-party access, see Glossary.

and VASPs. The FATF also called on the G20 countries to lead by example in this respect.[30] Subsequently, in September 2020, the FATF published a list of 'red flag indicators' for FIs that engage in VASP activities to help them identify suspicious activities and transactions.[31]

The FATF adopted its standard on virtual asset service providers (VASP) in June 2019 and updated its guidance at the end of 2021. This was done to address unresolved issues and respond to new developments in the VA sector, in particular the newly created DeFi sector.[32] According to the FATF, VAs and VASPs should be defined very broadly, so that DeFi platforms can also be included. This is particularly the case if such platforms are centralised somewhat. This would include, for example, the ability of platform developers to control or intervene in various ways.[33] Consequently, DeFi platforms could be subject to the same due diligence and reporting obligations as other financial intermediaries. This approach poses AML/CFT risks, as future developments in the VA sector could aim at making VA services even more anonymous and decentralised (see Section 6.2.1). At the same time, however, it would ensure that natural persons and legal entities exerting actual control or sufficient influence over a DeFi platform or a DeFi protocol would not be able to hide behind the term 'DeFi' to evade responsibility and disregard their due diligence and reporting obligations.

Vulnerability 1

Diminishing importance of financial intermediation in the VA sector poses challenges to existing AML/CFT regulatory approaches (identified in 2023)

Due to their technical design, VAs generally function as a transnational, barrier-free network for moving assets without regard to territorial borders or the identity of the sender and recipient. The *peer-to-peer* (P2P) architecture of these networks implies that they are basically organised in a decentralised way and their users can participate in an anonymous or pseudonymous form. The establishment of such P2P networks seems to be a lasting trend. No financial intermediaries in the traditional sense are needed to move VAs in these networks. Nevertheless, these have so far played an important role in the VA sector, mostly as on/off ramps enabling the exchange of fiat currency and VAs. Various scenarios are imaginable that could reduce the currently essential role of financial intermediaries in the digital exchange of assets. For example, the growing popularity of VAs and stablecoins in particular, coupled with their increasing worldwide acceptance as a means of payment, could in the medium to long term reduce the need to store VAs with a financial intermediary or even to exchange them for fiat currency at all. At present, most stablecoins are still issued by companies from the VA sector. However, there are already stablecoins backed by decentralised autonomous organisations (DAOs) whose legal status is still unclear in most countries. The ML/TF regulatory approaches adopted by the FATF, as well as those used by Switzerland in particular, are based on the central role of financial intermediaries and their compliance with due diligence and reporting obligations. If this ceases to be the case, regulating the VA sector and curtailing ML/TF risks will become more difficult.[34]

[30] FATF, *FATF Report to the G20 Finance Ministers and Central Bank Governors on So-called Stablecoins*, June 2020, p. 2 – 4.
[31] FATF, *Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing*, September 2020.
[32] Decentralised finance (DeFi) enables users to gain direct access to various VA financial instruments, such as VA trading pairs or derivatives, without having to go through a traditional financial intermediary, see Section 6.2.1.
[33] FATF, *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, October 2021, p. 27 – 36.
[34] See Swiss Financial Market Supervisory Authority (FINMA), *2022 Risk Monitor* (in German), November 2022, p. 19. FATF, *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, October 2021, p. 18f.

4.5 International implementation of the Travel Rule stagnating

In June 2022 and June 2023, the FATF published a report on the global implementation of the Travel Rule, with each sobering results.[35] For the year 2023, most of the countries surveyed (73 out of 135)[36] indicated that they had not yet taken any steps to implement the Travel Rule. Only 35 of the 135 countries had adopted *Travel Rule* legislation as of March 2023 and 27 were in the process of enacting legislation. However, only about one-fifth of this group stated they had begun actual implementation and oversight measures. The FATF concluded that this gap made VAs and VASPs vulnerable to abuse and that there was an urgent need to accelerate the implementation and enforcement of the Travel Rule.[37] Both the Financial Stability Board (FSB) of the Bank for International Settlements (BIS) and the FATF warned of the risk of regulatory arbitrage: the greater the national differences in the regulation of the VA sector, the more likely it is that criminal actors will exploit these differences by relocating their activities to countries where supervision is less developed or even inadequate. In addition, FIs that engage in VASP activities in those countries that do not implement the Travel Rule for VA transactions find themselves in an advantageous position, as they do not have to devote resources to counter money laundering and terrorist financing. The efforts of those countries and VASP FIs that comply with the Travel Rule could be undermined as parts of the sector could migrate to countries that do not implement the Travel Rule. This would lead to even greater ML/TF risks for the VA sector worldwide – including in Switzerland.[38]

However, since the FATF's survey in March 2023, various countries, including the EU and Singapore,[39] have been aligning themselves with Swiss implementation of the Travel Rule, which prohibits the transfer of VAs to non-identified non-custodial wallets. The EU's revised Transfer of Funds Regulation (TFR) contains specific provisions for the transfer of VAs between VASPs and non-custodial wallets. Accordingly, the requirements of this Regulation should apply to all transfers including transfers of crypto-assets to or from non-custodial wallets as long as there is a VASP or other financial intermediary (e.g. obliged entity) involved in the transfer (see Recital (38) TFR). For crypto asset transfers to or from non-custodial wallets, the financial intermediaries on both sides of the transaction (i.e. sender and recipient) must collect the required information on both the sender and the recipient. In the case of a transfer of an amount exceeding EUR 1,000 that is sent or received on behalf of a client of a crypto-asset service provider to or from a self-hosted address, that crypto-asset service provider should verify whether that self-hosted address is effectively owned or controlled by that client (see Recital (39) in conjunction with Art. 14 para. 5 and Art. 16 para. 2 TFR).[40] In Singapore, transactions with non-custodial wallets are not subject to the requirements of the Travel Rule, but should be considered and treated as posing greater ML/TF risks. The payment service provider should therefore apply enhanced risk mitigating factors.[41]

Moreover, since the March 2023 survey, the EU has passed legislation creating a legal framework for VASPs and enforcement of the Travel Rule. The MiCA Regulation of the European Union (Markets in Crypto Assets Regulation) harmonises VA regulation within the

---

[35] FATF, *Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers*, June 2022. FATF, *Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers*, June 2023.
[36] Excl. countries that prohibit VASPs.
[37] Ibid. (2023), p.16-17.
[38] Financial Stability Institute, *Supervising cryptoassets for anti-money laundering*, April 2021, p. 19f. FATF, *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, June 2019, p. 9.
[39] For information about implementation of the Travel Rule in Singapore, see Monetary Authority of Singapore, *Guidelines to Notice PSN02 on Prevention of Money Laundering and Countering the Financing of Terrorism - Digital Payment Token Service*, March 2020.
[40] Official Journal of the European Union, *Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849, OJ L 150*, 9 June 2023.
[41] See *Guidelines to Notice PSN02 on Prevention of Money Laundering and Countering the Financing of Terrorism - Digital Payment Token Service*, March 2020, p. 41 f.

EU and is expected to come into force in 2024.[42] This will bring the number of countries that have adopted laws or regulations on Travel Rule implementation to 58.

Vulnerability 2

Inadequate and unequal international implementation and enforcement of the Travel Rule in the VA sector (identified in 2023)

While technological and economic developments in the VA sector occur rapidly, regulatory developments do not seem to be keeping pace. As early as 2018, the FATF explicitly recommended that the Travel Rule be applied to VA transactions, nearly ten years after the world's first Bitcoin transaction. It is currently not known when all FATF countries will implement the Travel Rule to VA transactions. And this failure to implement the Travel Rule, and corresponding lack of enforcement, increases the likelihood that VAs of criminal origin will be injected into the legal financial system through numerous possible channels – whether it be in the form of fiat currency or VAs. This state of affairs exposes all FIs (with or without VASP activities) to a greater risk of acting as a conduit or end point for financial flows derived from criminal activities (see Vulnerability 6 in Section 7.5.1). In addition, FIs that engage in VASP activities in those countries that do not implement the Travel Rule for VA transactions find themselves in an advantageous position, as they do not have to devote resources to counter money laundering and terrorist financing. The efforts of those countries and VASP FIs that comply with the Travel Rule could be undermined as a result as market share could migrate to countries that do not implement the Travel Rule. This would lead to even greater ML/TF risks for the VA sector worldwide – including in Switzerland.

4.6 National legal framework

Since 2018, new regulations have been introduced in Switzerland that implement FATF Recommendations for the VA sector. In some cases, Swiss regulations are more stringent than those of other countries. In Switzerland, the existing ML/TF regulatory framework has been expanded to include virtual currencies (or VAs) as well as FIs with VASP activities (or VASPs). All financial intermediation activities involving VAs thus fall within the scope of the Anti-Money Laundering Act (AMLA). The Swiss Financial Market Supervisory Authority (FINMA) has clarified its practice and interpretations in several publications. Swiss financial market legislation is principle-based and follows the notion of technology neutrality. The only key consideration is whether the regulation serves its intended purpose – namely to reduce the risk of money laundering – regardless of whether market participants offer their services in analogue or digital form.[43] In 2020, in due course of Switzerland's Enhanced Follow-up Process, the FATF considered that Swiss implementation of Recommendation No 15 and the application of Swiss money laundering regulations to VAs and VASPs were largely compliant.[44] The following sections provide an overview of the Swiss legal framework applicable to VAs and VASPs, assess the level of compliance with international standards, and summarise the key changes made in relation to AML/CFT.

[42] European Parliament, *Crypto-assets: green light to new rules for tracing transfers in the EU*, April 2023.
[43] See Swiss Financial Market Supervisory Authority (FINMA), *2016 Annual Report*, March 2017, p. 26.
[44] FATF, *Anti-money laundering and counter-terrorist financing measures - Switzerland, Enhanced Follow-up Report & 2nd Technical Compliance Re-Rating*, January 2020, p. 7 – 8.

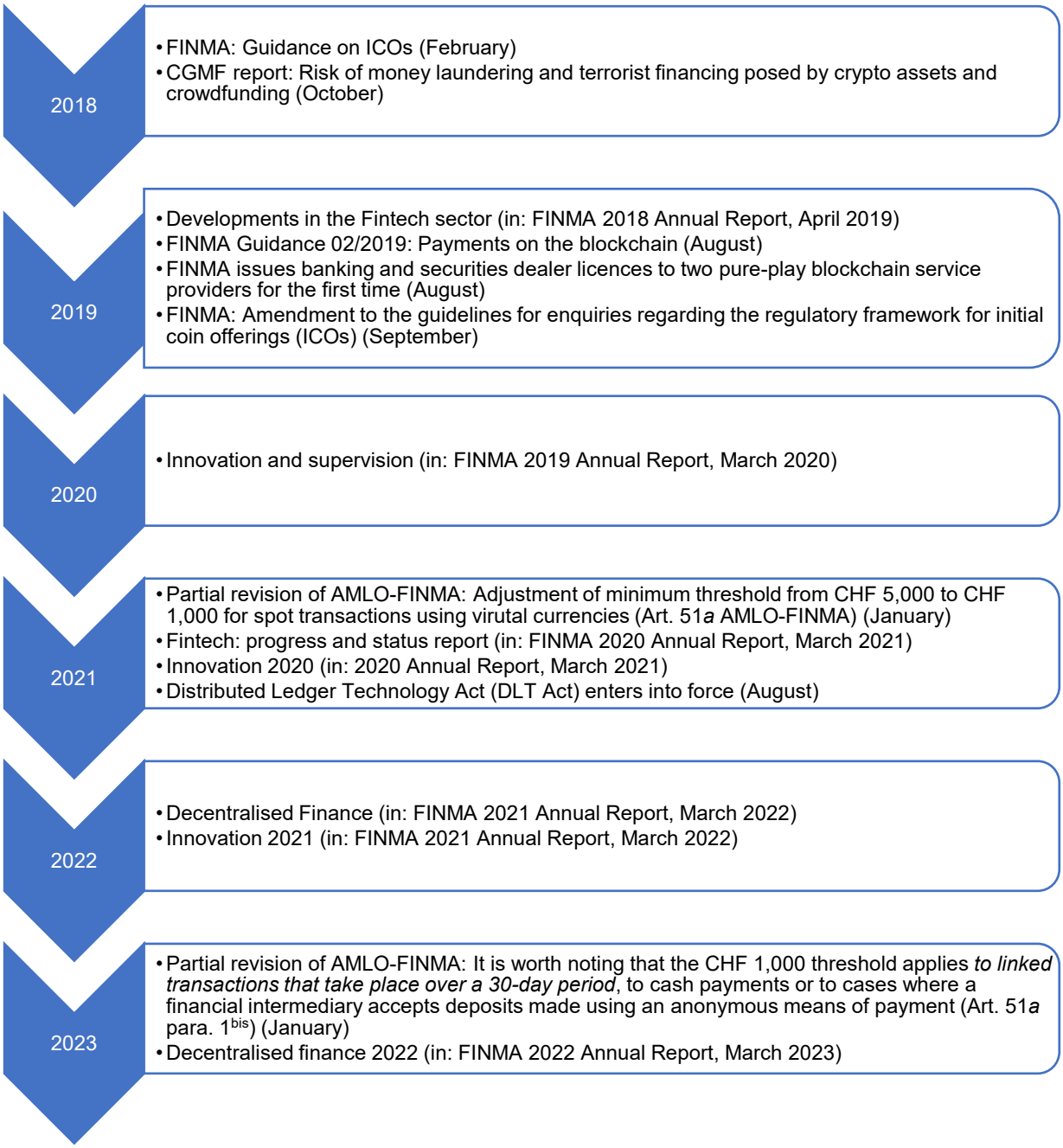

Figure 7: Regulatory developments and relevant official publications in Switzerland on VAs and VASPs (2018 - 2022)

4.6.1 AML/CFT supervision of FIs in Switzerland

Anti-money laundering efforts rest on two main pillars. First, Article 305bis of Swiss Criminal Code (SCC) establishes money laundering as a prosecutable criminal offence. Secondly, the Anti-Money Laundering Act (AMLA) places due diligence and reporting obligations on financial intermediaries and brokers with regard to their clients. Article 2 paras 2 and 3 AMLA establishes who qualifies as a financial intermediary in Switzerland.[45]

[45] SR 955.0 – *Federal Act of 10 October 1997 on Combating Money Laundering and Terrorist Financing in the Financial Sector*, (Anti-Money Laundering Act, AMLA), status as of 23 January 2023.

In the case of banks, brokerage firms, insurance companies and financial institutions subject to the Collective Investment Schemes Act, FINMA directly monitors compliance with these obligations as part of its regular supervisory activities. Audit firms, and, increasingly FINMA itself, conduct on-site audits every year to verify compliance with regulations.

Independent asset managers and trustees are subject to supervision by supervisory organisations, which are themselves authorised and supervised by FINMA. Persons and companies in the parabanking sector (e.g. credit and leasing companies, credit card companies, payment service providers, currency exchange dealers) are also subject to the provisions of the Anti-Money Laundering Act. This latter group is required to join a self-regulatory organisation (SRO) approved and supervised by FINMA for the purpose of monitoring compliance with due diligence and reporting obligations. SROs must monitor whether their affiliated members comply with AML obligations. The specific audit can be carried out by the SROs themselves or by appointed audit firms.

Other supervisory authorities oversee financial intermediaries under AMLA that operate in specific sectors: Gambling houses under the Federal Act of 29 September 2017 on Gambling (GamblA)[46] are supervised by the Federal Gaming Board (FGB); trade assayers and group companies under Article 42bis of the Federal Act of 20 June 1933 on the Control of the Trade in Precious Metals and Precious Metal Articles (PMCA)[47] are supervised by the Central Office for Precious Metals Control (ZEMK); the organisers of major gambling operations under GamblA are supervised by the Intercantonal Gaming Board (GESPA).

4.6.2 Overview of VA services and their subordination to the AMLA

If a given VA service falls within the scope of the AMLA, service providers are subject to various due diligence obligations.

Category of services	Subordination to the AMLA
Token emission (ICOs, tokenisation, etc.)	Subject to AMLA provisions if the tokens issued through an initial coin offering (ICO) can be equated with a means of payment (payment tokens)
Custodial wallet providers	In all cases subject to AMLA provisions
Non-custodial wallet providers	Subject to AMLA provisions if providers retain a certain level of control or intervention capabilities (e.g. multisignature wallets[48] or if they use applications for the secure storage of private keys, even if these can only be decrypted by the client, see Section 4.4.6)
Online currency exchange platforms	Like conventional currency exchange platforms, subject to AMLA provisions

[46] SR 935.51 – *Federal Act of 29 September 2017 on Gambling* (Gambling Act, GamblA), status as of 1 January 2021.
[47] SR 941.31 – *Federal Act on the Control of the Trade in Precious Metals and Precious Metal Articles* (Precious Metals Control Act, PMCA), status as of 1 January 2023.
[48] See Glossary.

Currency exchange offices and cashpoints (incl. VA-ATMs)	Like conventional currency exchange platforms, subject to AMLA provisions
Centralised trading platforms	In all cases subject to AMLA provisions
Decentralised trading platforms & DeFi applications	If, from an economic standpoint, authorisation is required in order to carry out a given financial market activity, FINMA assumes that such a licence is required even in the case where a new type of technical or legal implementation exists (economic-based criterion).
Miners	Outside the scope of AMLA provisions

Figure 8: VA service categories falling within or outside the scope of the Anti-Money Laundering Act (regulatory changes since the 2018 risk analysis are highlighted in red)[49]

4.6.3 ICO guidelines

In 2018, FINMA published its G*uidance on initial coin offerings* (ICOs).[50] In an ICO, investors transfer funds to the ICO organiser. In exchange, they receive blockchain-based coins or tokens, which are either minted on a newly developed blockchain or are generated on an existing blockchain via a smart contract and stored in a decentralised manner.[51] FINMA draws a distinction between payment tokens, utility tokens and asset tokens.[52] This distinction has helped to clarify which activities of ICOs are considered as financial intermediation and are thus subject to AMLA provisions, namely when the tokens issued in these fundraising operations can be equated with payment tokens.[53] Any natural person or legal entity that acts as a financial intermediary and is therefore subject to the AMLA must either have a supervisory licence from FINMA (e.g. banking licence, securities dealer licence) or join a self-regulatory organisation (SRO) in order to carry out these activities in Switzerland.

Infobox 2

Token categories used by the Swiss Financial Market Supervisory Authority (FINMA)[54]

Payment tokens: This category refers to 'cryptocurrencies' in the purest sense, which are defined as tokens that are actually or intended by the organiser to be accepted as a means of payment for the purchase of goods or services or are intended to be used for the transfer of money and value. These tokens do not confer any rights against the issuer.

Utility tokens: FINMA defines this category as tokens that are intended to provide access to a digital utility or service provided on or using a blockchain infrastructure.

[49] See table from 2018 in: CGMF, *Risk of money laundering and terrorist financing posed by crypto assets and crowdfunding*, October 2018, p. 39f.
[50] Swiss Financial Market Supervisory Authority (FINMA), *Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs)*, February 2018.
[51] Ibid., p. 1.
[52] Hybrid tokens also exist.
[53] Ibid., p. 6 – 7.
[54] Ibid., p. 2 – 3.

Asset tokens: This category includes tokens that represent underlying assets. In particular, such tokens may represent a debt claim against the issuer or a membership entitlement within the meaning of company law. In the case of asset tokens, for example, a promise is made that the holder will receive a proportion of future company earnings or future capital flows. Based on its economic function, the token thus represents in particular a share, a bond or a derivative financial instrument. The category of asset tokens can also include tokens that are intended to make physical assets tradable on the blockchain.

These token categories are not always clear-cut. Asset and utility tokens can also fall into the category of payment tokens (referred to as '**hybrid tokens**'). In such cases, the token may cumulatively qualify as securities and a means of payment. As soon as a token, for example an NFT, is actually used as a means of payment, it is considered to be a payment token (substance over form). The due diligence requirements for financial intermediaries apply when accepting, storing, investing or transferring these tokens. Payment tokens are also covered by the Travel Rule and Art. 10 AMLO-FINMA.

4.6.4 Interpretation of Travel Rule in Switzerland

One challenge in combating money laundering and terrorist financing is the ability to effectively monitor compliance with the regulatory framework when transactions are processed on a blockchain network. The regular monitoring principles aimed at countering money laundering also apply to such transactions. In this context, FINMA stated in its Guidance 02/2019 'Payments on the blockchain' that, in line with the principle of technological neutrality, it also applies the current Swiss regulations on the transmission of information in payment transactions to the blockchain area.[55] With regard to the application of AML regulations, no simplifications are envisaged compared to traditional payment transactions.

Article 10 AMLO-FINMA requires FIs to transmit identifying information about the sender and recipient whenever a transfer order is given, irrespective of whether the transaction involves fiat currencies or VAs. This enables the financial intermediary receiving the transfer to verify for example, whether the sender's name is on a sanctions list. It also allows the financial intermediary to check whether the recipient's information is correct and, if not, whether the payment should be sent back to the sender. AMLO-FINMA thus complies with the FATF's revised standards adopted in 2019, which require VASPs to comply with the preventive measures set out in FATF Recommendations 10 to 21, including the *Travel Rule*.

Financial intermediaries with VASP activities may therefore only send VAs to the external wallets of their own, already identified clients and may only receive VAs from such wallets. If data on the sender and recipient cannot be reliably transmitted through the respective payment system, FIs are not permitted to accept VAs from clients of other institutions or send VAs to clients of other institutions.

[55] Swiss Financial Market Supervisory Authority (FINMA), *Guidance 02/2019 - Payments on the blockchain*, August 2019.

	Art. 10 AMLO-FINMA & FINMA Guidance 02/2019	FATF Travel Rule INR 15 para. 7b
Sender details	• Name • Account number • Transaction reference number • Address (or date and place of birth / client number or national ID number)	• Name • Account number • Transaction reference number • Address / date and place of birth / client number / national ID number
Recipient details	• Name • Account number (if there is no account number, transaction reference number.)	• Name • Account number
Minimum threshold	CHF 0.-	EUR 1,000 / USD 1,000
Applicable to transactions involving non-custodial wallets	Yes, see FINMA Guidance 02/2019	No

Figure 9: Implementation of the Travel Rule in Switzerland

4.6.5 Stablecoins and decentralised finance

FINMA observed an increase in the number of stablecoin projects in 2019. In September 2019, a supplement to the guidelines was published to provide guidance on how stablecoins should be assessed under Swiss supervisory legislation.[56]

FINMA also applies the principle of technology neutrality to the regulatory treatment of stablecoins. FINMA focuses on the economic function and purpose of a token (substance over form) and takes into account both the tried and tested valuation decisions (same risks, same rules) and the specific circumstances of individual cases. Stablecoins are divided into case groups according to the type of underlying asset. These case groups (linkage to currencies, commodities, real estate or securities) share the common trait that they are almost always subject to the Anti-Money Laundering Act. This is due to the fact that they are usually meant to serve as a means of payment for stablecoins. When a supervised institution issues stablecoins on an open-access trading platform such as the Ethereum blockchain, it is important to take into account the heightened money laundering and reputational risks. Because the system is open, once the stablecoin has been issued, the issuing institution has only one means of control left, namely when the stablecoin is redeemed for the underlying value. As a result, the due diligence obligations under the Anti-Money Laundering Act can only be met for the first and last person to hold the stablecoin. Anyone who buys or sells the stablecoin on the open platform in between is outside the control of the issuing institution. As FINMA has noted, this can lead to reputational damage for the institution concerned and for the Swiss financial market as a whole.

[56] Swiss Financial Market Supervisory Authority (FINMA), *Supplement to the guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs)*, September 2019.

To address these risks, the issuance of stablecoins by supervised institutions requires contractual and, where appropriate, technological transfer restrictions. Accordingly, all persons holding stablecoins must be sufficiently identified by the issuing institution or by appropriately supervised distribution partners in order to comply with the due diligence obligations provided for under the Anti-Money Laundering Act for all stablecoin transactions. This is a technology-neutral application of the ban on bearer savings accounts (Art. 5 CDB 20).[57]

For DeFi applications, FINMA applies existing financial market rules, without regard to any specific technology or process. If a DeFi application offers the same service with the same associated risks as a similar service provided by traditional financial market intermediaries, then FINMA will apply the same rules. If, from an economic standpoint, a DeFi application carries out a financial market activity that is subject to authorisation, then FINMA also considers that authorisation is required even if the activity takes place using a new form of technical or legal implementation. Accordingly, AML provisions must also be adhered to.[58] FINMA is closely monitoring the trend towards greater development and use of DeFi applications. This is particularly the case when FINMA-supervised entities use or intend to use DeFi applications. FINMA applies the proven principles of 'substance over form' and 'same risks, same rules' to such cases and always decides on the basis of the actual economic circumstances.[59]

4.6.6 DLT Act

On 25 September 2020, the Swiss Parliament adopted the Federal Act on the Adaptation of Federal Legislation to Developments in Digital Ledger Technology.[60] Thus, ten existing Federal Acts were amended, including the Anti-Money Laundering Act (AMLA). One important change was the broadening of the scope of application of the AMLA. For example, Art. 2 para. 2 let. d^{quater} of the AMLA defines DLT trading facilities as financial intermediaries (trading facilities for DLT securities under Article 73a FinMIA[61]). In addition, the Financial Market Infrastructure Ordinance (FinMIO[62]) stipulates that a DLT trading facility cannot accept DLT securities and other assets that could significantly complicate implementation of AMLA compliance obligations (e.g. privacy coins, see Glossary) or compromise the stability and integrity of the financial system.

In addition, the Anti-Money Laundering Ordinance (AMLO) defines a service as a payment transaction if the financial intermediary 'assists in the transfer of virtual currencies to a third party, if it has a continuing business relationship with the contracting party or if it holds virtual currencies on behalf of the contracting party, and it does not provide the service exclusively to adequately supervised financial intermediaries'.[63] This means that wallet providers and decentralised trading platforms are now also considered financial intermediaries under the AMLA if these providers – as interpreted by the FATF – have certain control or intervention options with regard to such platforms or wallets.

---

[57] Swiss Bankers Association (SBA), *Agreement on the Swiss banks' code of conduct with regard to the exercise of due diligence (CBD 20)*, 2020.
[58] Swiss Financial Market Supervisory Authority (FINMA), *2021 Annual Report*, March 2022, p. 20.
[59] Swiss Financial Market Supervisory Authority (FINMA), *2022 Annual Report*, March 2023, p. 21.
[60] Federal Gazette BBl 2020 7801, *Federal Act on the Adaptation of Federal Legislation to Developments in Digital Ledger Technology* (in German), October 2020.
[61] SR 958.1 – *Federal Act of 19 June 2015 on Financial Market Infrastructures and Market Conduct in Securities and Derivatives Trading* (Financial Market Infrastructure Act, FinMIA).
[62] SR 958.11 – *Ordinance of 25 November 2015 on Financial Market Infrastructures and Market Conduct in Securities and Derivatives Trading* (Financial Market Infrastructure Ordinance, FinMIO).
[63] Anti-Money Laundering Ordinance, AMLO, Art. 4 paras 1 and 1^{bis}, status as of 1 August 2021. Excerpt: Federal Department of Finance (FDF): *Explanatory Report for Consultation on the Federal Council Ordinance on Adaptation of Federal Law to Developments in Digital Ledger Technology (in German)*, October 2020, p. 15.

This applies, for example, to trading platforms that do not have access to the private key of their clients, but are able to transfer the virtual currencies via smart contract and can confirm, release or block the orders or otherwise exercise control over the smart contract. Also included are, for example, wallet providers that have access to a key and require the transaction to be signed before it can be carried out successfully (multisig wallet). Services for the secure storage of private keys may also be included, even if the latter are encrypted and must always be decrypted by the client. The risks with such wallets, which are neither pure custodial nor pure non-custodial wallets, are that the origin of the virtual currencies can be concealed by moving them between such wallets and within address structures. The changes were justified by the fact that with such increasingly decentralised models of asset transfer, financial intermediaries no longer have sole control over assets in all business models.[64] Providers of pure non-custodial wallets, which merely make software available on a one-off basis, should still remain outside the scope of the AMLA. The term 'one-off' refers to, for example, developers who merely offer software for download without entering into any business relationship with the user. Also excluded from the scope of AMLA are trading platforms that only bring buyers and sellers together and process transactions on the trading platform without using a smart contract. This is purely an intermediary activity in which there is no involvement in the transfer of the virtual currencies.

In addition, the AMLO was amended stating that the professional issuance of a means of payment constitutes a financial intermediary activity and that virtual currencies are also covered by the Anti-Money Laundering Act, whether they are actually a digital means of payment or are intended by the organiser or issuer to be used as such.[65] This wording has also created more clarity with regard to the AMLA status of VAs issued in the context of initial coin offerings (ICOs). By expanding the meaning of the term 'financial intermediary', Switzerland has implemented what the FATF recommended in its 'Updated guidance on a risk-based approach to virtual assets and virtual asset service providers' to individual countries, namely to interpret the VASP term as broadly as possible.[66]

4.6.7 AML supervision by FINMA and amendments to AMLO-FINMA

At the end of August 2019, FINMA granted two blockchain financial service providers a licence, one as a bank and one as a securities dealer. As is customary for other FIs, various conditions and requirements had to be met in order to ensure the orderly development of the business. During the licensing process, FINMA paid particular attention to crypto-specific risks. Strict criteria and control processes needed to be established to address operational risks. With respect to the safe custody of tokens, the technological infrastructure used by the two applicants was thoroughly tested, with the support of the competent licensing auditors, in order to adequately address the elevated IT and cyber security risks. Other areas of focus included regular monitoring of transactions to counter money laundering, the usual KYC requirements and the mandatory clarifications of transactions.
In recent years, FINMA-supervised institutions have become increasingly active in the crypto space, either already offering crypto services or planning to do so. Based on these findings, in 2021 FINMA analysed and reviewed the planned business activities of banks to determine the level of compliance with money laundering regulations.[67] FINMA also clarified its expectations with regard to the auditing of institutions that operate in the crypto sector. In the summer of

[64] Ibid., p. 7.
[65] Anti-Money Laundering Ordinance, AMLO, Art. 2 para. 3 let. b AMLA in connection with Art. 4 para. 1, let. c AMLO in connection with Art. 4 para. 1bis let. c AMLO, status as of 1 August 2021.
[66] FATF, *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, October 2021, p. 24 – 36, esp. para. 91, p. 35.
[67] Swiss Financial Market Supervisory Authority (FINMA), *2021 Annual Report*, March 2022, p. 32.

2021, the five existing modules[68] used in AML audits were supplemented by a sixth module covering virtual assets (VAs) and virtual asset service providers (VASPs).[69]

Effective 1 January 2021, the threshold for identifying the counterparty in a currency exchange transaction and thus in a non-permanent business relationship was also lowered from CHF 5,000 to CHF 1,000 in line with the requirements of FATF Recommendation No 15 (Art. 51*a* AMLO-FINMA).[70] The adjusted threshold is in line with FATF Recommendations and takes into account heightened risks in this area.[71] This threshold applies not only to individual transactions, but also to transactions considered to be interconnected. The main case of application for the CHF 1,000 threshold is the exchange of money at VA-ATMs. This threshold was adopted by the self-regulatory organisations (SROs) to which VASP FIs are affiliated. FINMA's partially revised Anti-Money Laundering Ordinance, which came into force on 1 January 2023, also specified that the CHF 1,000 threshold applies to cash payments or the receipt of other anonymous means of payment (such as cryptocurrencies or certain prepaid cards) for the sale or purchase of virtual currencies (Art. 51*a* para. 1bis AMLO-FINMA).[72] Financial intermediaries must also take technical precautions to prevent the CHF 1,000 threshold from being exceeded through interlinked transactions taking place within a 30-day period.

4.7 VAs and VASPs in Switzerland

An important methodological aspect in conducting this risk analysis is to gain an overview of the manner and intensity in which VAs are used in Switzerland. This requires the gathering of information on the specific VA services that are offered and used both in Switzerland and worldwide. Information on the intensity of the interaction of the Swiss VA sector with the business and financial sector in Switzerland is also essential.[73]

Since the last sectorial risk analysis on this topic in 2018, the general use of VAs in Switzerland has increased significantly and the Swiss VA sector has grown considerably. However, precise information on the concrete structure of the Swiss VA sector is largely non-existent. Nevertheless, there are clear indications that Switzerland belongs to the group of countries that is in the leading in this area.

Traditionally, the Swiss financial centre plays an important role worldwide as a hub for international financial transactions, especially in the areas of cross-border asset management, global reinsurance business, as a commodity trading hub and commodity trade financing centre, and as the location of Europe's third-largest stock exchange.[74] And finally, Switzerland is one of the leading locations in the VA sector.[75] In the financial sector in particular, a growing

[68] Booking Centres, Rules for Identification, Complex Structures, In-depth Handling of Politically Exposed Persons and Trade Finance.
[69] Swiss Financial Market Supervisory Authority (FINMA), *2021 Annual Report*, March 2022, p. 32.
[70] SR 955.033.0 – *Ordinance of the Swiss Financial Market Supervisory Authority of 3 June 2015 on the Prevention of Money Laundering and the Financing of Terrorism* (Anti-Money Laundering Ordinance-FINMA, AMLO-FINMA), Art. 51*a*, status as of 1 January 2021.
[71] There have also been specific cases in which certain drug trafficking networks made inappropriate use of ATMs in Switzerland to process payment transactions. See, for example, Tages Anzeiger, *Schweizer Online-Drogenversand – «Hippe Kleider, Typ Studentin, und das Täschli voller Drogen»*, 18 March 2021.
[72] Anti-Money Laundering Ordinance-FINMA, AMLO-FINMA, Art. 51*a* para. 1bis, status as of 1 January 2023.
[73] World Bank, *Virtual Assets and Virtual Asset Service Providers ML/TF Risk Assessment Tool*, June 2022, p. 14f.
[74] Federal Council, *Leading worldwide, rooted in Switzerland: Policy for a future-proof Swiss financial centre*, December 2020, p. 5.
[75] State Secretariat for International Finance (SIF), *Factsheet – Blockchain and cryptoassets in the financial sector: Switzerland's pioneering role on the international stage*, January 2022.

VA ecosystem has developed in Switzerland, which, according to figures from the State Secretariat for International Finance (SIF), already includes over 1,000 businesses.[76]

However, the vast majority of companies operating in the VA sector are not financial intermediaries as defined by the Anti-Money Laundering Act. Rather, they provide software, legal or technological consulting or similar services that are in turn used by other companies (including financial intermediaries) within the VA ecosystem (see Figure 4 in Section 4.2). There are also several trade associations that seek to expand and further develop the Swiss VA sector. Moreover, many of the world's most important VAs (in terms of market capitalisation) have established a foundation in Switzerland.[77] Most of these foundations are located in the canton of Zug. In 2022, the canton of Zug experienced a net growth of 25 foundations, with 20 of the new foundations being crypto foundations.[78] As a result of the numerous crypto foundations established, the canton of Zug has the second highest density of foundations per cantonal inhabitant in Switzerland (after the canton of Basel-Stadt).[79] Crypto foundations – often heavily capitalised by the capital gains of the VAs they hold – fund individuals, entities, and projects working to advance the underlying blockchain. For the purposes of this report, the Federal Supervisory Authority for Foundations (FSAF) was unable to provide specific details on the actual number of crypto foundations and their balance sheets.

4.7.1 Information on FIs with VASP activities in Switzerland

The present risk analysis focuses on financial intermediaries as defined in the Anti-Money Laundering Act. Depending on their activities, FIs are either directly subordinated to the Swiss Financial Market Supervisory Authority (FINMA) (e.g. banks) or they are required to join a FINMA-recognised and supervised self-regulatory organisation (SRO) (see Section 4.6.1).

	2018	2020	2022
Number of FIs with VASP activities (FINMA-supervised institutes and SRO members)[80]	At least 5[81]	At least 89	At least 204

Figure 10: Increase in the number of FIs with VASP activities in Switzerland 2018 – 2022

[76] State Secretariat for International Finance (SIF), *Blockchain/DLT*, last checked in May 2023. State Secretariat for International Finance (SIF), *Swiss financial sector: Key figures 2023,* April 2023, p. 13.
[77] For example: Ethereum Foundation, Cardano Foundation, Tezos Foundation, Solana Foundation, Polkadot Foundation, etc.
[78] Center for Philanthropy Studies (CEPS), University of Basel; SwissFoundations, the umbrella organisation for Swiss grant foundations; Center for Foundation Law, University of Zurich, *Der Schweizer Stiftungsreport 2023*, June 2023.
[79] 30.7 foundations per 10,000 inhabitants, see Center for Philanthropy Studies (CEPS), University of Basel; SwissFoundations, the umbrella organisation for Swiss grant foundations; Center for Foundation Law, University of Zurich, *Der Schweizer Stiftungsreport 2022*, May 2022, p. 8.
[80] These assertions are based on information provided by the Swiss Financial Market Supervisory Authority (FINMA) and supplemented on the basis of information available to MROS.
[81] During the present risk analysis, we obtained information showing that there were at least five financial intermediaries pursuing VASP activities in Switzerland in 2018. However, in the second national report on the risks of money laundering and terrorist financing published in 2021, the reported figure for 2018 was only two FIs with VASP activities. See CGMF, *2nd National report on the risks of money laundering and terrorist financing in Switzerland*, October 2021, p. 51.

According to FINMA, there were at least 204 FIs with VASP activities at the end of 2022. Of these, 174 FIs were affiliated with an SRO and 30 institutions were subject to FINMA supervision.[82]

FINMA observed that, in general, most banks are focusing more on the issue of digitalisation. A certain dynamic can be seen in the adaptation or expansion of business models relating to VAs, in the creation of interfaces (*open banking*) and in increased cooperation with insurance companies. Nevertheless, there is still a general reluctance on their part to make strategic adjustments to their business models. The institutions supervised by FINMA are either currently expanding the range of VA services on offer or are moving in this direction. Of the banks and securities dealers currently engaged in VA activities in Switzerland, the main activity is holding tokens on behalf of clients and providing a platform for VA trading, followed by the issuance of products and secured loans.

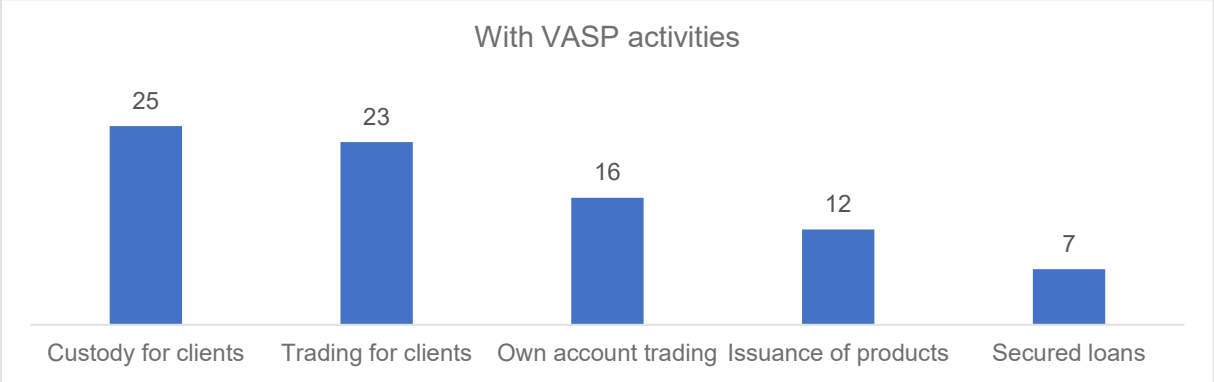

Figure 11: VASP services offered by 30 FINMA-supervised banks and securities firms with crypto activities (end of 2022)[83]

The vast majority of Swiss FIs with VASP activities are affiliated with an SRO. According to the Swiss Financial Market Supervisory Authority (FINMA), these FIs mainly handle exchange transactions (fiat-VA and VA-VA) and provide VA custody services.

The most exhaustive data so far on the business activities of Swiss FIs that engage in VASP activities can be found in the 'Swiss Digital Asset Market Report 2022', a joint publication produced by a number of private players and a university. A total of 81 Swiss-based companies were contacted, 47 of which took part in the survey.[84] In 2021, the 17 companies providing VA trading services reported a combined total trading volume of CHF 41.2 billion.[85] 16 companies surveyed provided their clients with VA custody services. Of these, 11 companies provided figures showing that they held VAs worth over CHF 13.2 billion in custody for their clients at the end of 2021.[86] Since only a fraction of the FIs with VASP activities in Switzerland took part in the survey, it can be assumed that the actual trading volume and the VAs held in custody by all VASP FIs in Switzerland are higher. However, it is still unclear whether the data of these individual VASP FIs can be extrapolated to represent the business activities of all FIs with VASP activities in Switzerland.

[82] According to FINMA, by the end of September 2023, there were already 38 FINMA-supervised FIs engaged in VASP activities.
[83] See Swiss Financial Market Supervisory Authority (FINMA), *2022 Annual Report*, March 2023, p. 23.
[84] Home of Blockchain, *Swiss Digital Asset Market Report 2022*, May 2022, p. 16.
[85] Ibid., p. 25.
[86] Ibid., p. 20.

4.7.2 Information on the use of VAs in Switzerland

Other studies have attempted to quantify cross-border VA financial flows in and out of Switzerland using different calculation methods. The blockchain analytics company Chainalysis, for example, ranked Switzerland 14th out of 154 countries on the 'DeFi Adoption Index' for the year 2021.[87] On the European list of the 'Global Crypto Adoption Index', Switzerland was ranked 6th out of 30 for 2021 and 7th for 2022.[88] According to the authors of the study, over USD 60 billion worth of VAs were transferred from Switzerland to DeFi and CeFi platforms between July 2020 and June 2021.[89]
These figures are roughly in the same order of magnitude as the results of an annual study conducted by the Lucerne University of Applied Sciences and Arts, which provided its own estimate of the global trading volume of transactions conducted from Switzerland on VA platforms, as shown below:[90]

	2020	2021	2022
Centralised VA exchanges (CHF)	92.6 billion	81.2 billion	50.3 billion
Decentralised VA exchanges (CHF)	4 billion	5.1 billion	1.5 billion
Total	**96.6 billion**	**86.3 billion**	**51.8 billion**

Figure 12: Estimated trading volume from Switzerland on VA platforms worldwide (CeFi and DeFi) 2020 – 2022

However, Switzerland's estimated share of global VA trading volume was always below 1% in these years. Even compared with financial flows in other sectors, these figures still seem manageable: the annual trading volume on the Swiss Stock Exchange (SIX), for example, amounted to CHF 1208 billion in 2022.[91] However, it would be wrong to assume that the ML/TF risks in the VA sector in Switzerland are decreasing and manageable based on the annually decreasing and ultimately still manageable figures since 2020. In the same years, the number of SARs submitted in relation to money laundering in Switzerland as well as the sum of VAs stolen through theft or fraud increased significantly (see Section 7.2).

Based on the calculation methods used in the studies mentioned above, the actual figures are probably significantly higher.[92] In addition, these calculations do not take into account fiat financial flows in connection with VA trading transactions. No estimates are available for these financial flows. Nor do the figures indicate which actors (natural persons, legal entities or FIs with VASP activities) contributed to these financial flows and in what proportions. Ultimately, all of the aforementioned studies only provide guesstimates of the size of the Swiss VA sector and show that VA use has now become commonplace in Switzerland.

[87] Chainalysis, *The 2021 Geography of Cryptocurrency Report*, October 2021, p. 55.
[88] Ibid., p. 55. Chainalysis, *The 2022 Geography of Cryptocurrency Report*, September 2022, p. 29.
[89] Chainalysis, *The 2021 Geography of Cryptocurrency Report*, October 2021, p. 55.
[90] For 2020 (data collection period: 01.10.2020-01.09.2021), see Institute of Financial Services Zug IFZ (Lucerne University of Applied Sciences and Arts), *Crypto Assets Study 2021*, p. 17 – 20. For 2021 (data collection period: 01.05.2021-30.04.2022), see Institute of Financial Services Zug IFZ (Lucerne University of Applied Sciences and Arts), *Crypto Assets Study 2022*, p. 12. For 2022 (data collection period: 01.01.2022-31.12.2022), see Institute of Financial Services Zug IFZ (Lucerne University of Applied Sciences and Arts), *Fintech Study 2023*, p. 63.
[91] Cash, *Handelsvolumen an der SIX 2022 rückläufig*, 3 January 2023.
[92] Chainalysis and the Lucerne University of Applied Sciences and Arts both point out that the totals that they calculated are minimum amounts. See Institute of Financial Services Zug IFZ (Lucerne University of Applied Sciences and Arts), *Crypto Assets Study 2021*, p. 17. Chainalysis, *The 2021 Geography of Cryptocurrency Report*, October 2021, p. 5.

The numerous ICOs launched in Switzerland presumably also contributed to an increase in VA-related financial flows. However, the financial flows associated with ICOs can either be in VAs or fiat currency, depending on the project in question. Since 2019, the Swiss Financial Market Supervisory Authority (FINMA) has received over 400 requests for authorisation in connection with the launch of ICOs in Switzerland. The actual number of ICOs conducted is likely to be significantly higher, as these are not mandatory notifications, but enquiries regarding possible subordination under financial market law (see Section 4.6.3).

According to several surveys conducted in Switzerland, VA use has clearly increased in recent years. A survey on Swiss investment behaviour conducted in 2018 showed that 8% of respondents had bought VAs at least once. In 2022, the same survey showed that 18% had already done so.[93] Even if individual surveys of this kind should be treated with caution, taken together they clearly show increased uptake in the use of VAs in Switzerland.[94] However, the results do not provide any information on how often these VA purchases were made via Swiss or foreign financial intermediaries. The survey results are clear, however, with regard to the correlation between previous VA purchases and the age of the respondents: people between the ages of 18 and 49 were the most likely to have already purchased VAs or express an intention to do so in the near future.[95] This is a strong indication that the trend towards increased use of VAs observed in recent years will continue.

The oldest cryptocurrency, Bitcoin, has been available for purchase at all SBB ticket machines in Switzerland since 2016.[96] By the end of 2017, this service had already been used by at least 6,000 people, half of them even on a regular basis.[97] In addition, there are over 60 VA-ATMs in Switzerland run by various Swiss VASP FIs that allow people to buy and even sell Monero, the most important and oldest privacy coin (see Glossary).[98] Since then, some cantons have introduced the possibility of paying taxes using VAs.[99] In March 2022, the City of Lugano announced a partnership with stablecoin provider Tether to accelerate the adoption of blockchain technology as the foundation for transformation of the city's financial infrastructure. Lugano's project will involve over 10,000 local merchants signing up to accept Bitcoin as a means of payment. The aim is also to facilitate the payment of public municipal services using Bitcoin, Tether (USDT) and Lugano's own cryptocurrency LVGA.[100]

As this non-exhaustive list of examples shows, the opportunities to buy and sell VAs in Switzerland or to use them as a means of payment for various services have expanded considerably in recent years. Other examples illustrate that this growth has also been seen in industries that are subject to specific risks of money laundering. For example, numerous businesses – including jewellery and other luxury goods dealers, antique shops, art galleries, and hotel and restaurant establishments – offer the possibility of paying with VAs.[101]

---

[93] Moneyland, *Wie legen Schweizer ihr Geld an?*, 22 April 2020. Moneyland, *So investieren Schweizerinnen and Schweizer ihr Geld*, 19 July 2022.
[94] Other similarly designed surveys deviate by a few percentage points up or down, but show the same trend, e.g.: Migros Bank, *Kryptowährungen bei jüngeren Generationen beliebter als Gold*, February 2020. Handelszeitung, *Krypto lockt: Studie zeigt grosses Interesse in der Schweiz*, June 2021.
[95] Ibid.
[96] Handelszeitung, *6000 Kunden kaufen bei der SBB Bitcoins | Handelszeitung*, 1 November 2017. Swiss Federal Railways (SBB), *Kaufen Sie Ihr Bitcoin Paper Wallet jederzeit an einem SBB Billettautomaten | SBB*, last checked in May 2023.
[97] Ibid.
[98] Coin ATM Radar, *Bitcoin ATM Map*, last checked in May 2023.
[99] Finews, *Tessiner dürfen ihre Steuern jetzt in Bitcoin zahlen*, 7 July 2022. Canton of Zug, *Kanton Zug akzeptiert ab 2021 Kryptowährungen für Steuerzahlungen* (press release), 3 September 2020.
[100] City of Lugano, Tether, *Lugano's Plan B*, last checked in May 2023.
[101] Handelszeitung, *85'000 Händler in der Schweiz können nun Zahlungen mit Bitcoin and Ether annehmen*, 19 August 2021. For a geographical overview, see Coinmap, *Crypto ATMs & merchants of the world*, last checked in May 2023.

It is also possible to use VAs to buy companies and shares thereof in Switzerland.[102] Moreover, it is possible to establish companies using VAs as a contribution in kind (start-up capital). By early 2023, several hundred companies had been established in Switzerland in this way, operating in a wide range of sectors and not necessarily related to VAs or financial services.

Even real estate can be purchased in Switzerland using VAs.[103] The Federal Office for Land Registry and Real Estate Law (FOLR) as well as various cantonal land registry offices, official notary offices and land registry inspectorates consulted confirmed to us that VAs have been used for the purpose of buying real estate in Switzerland.[104] However, there is no specific information on this and with the current legal basis it is not possible to collect this information. Only the individual notary's offices have access to the contractual provisions regarding the means of payment for the purchase of real estate. As for the potential use of VAs in the 21 licensed Swiss casinos and their online gambling platforms, the Federal Gaming Board (FGB) may prohibit certain means of payment such as VAs under Art. 80 para. 3 of the Gambling Ordinance if their use is inconsistent with the objectives of the Federal Gambling Act.[105] So far, two casinos have expressed interest in using VAs. However, according to the FGB, they were not able to propose a procedure that would have satisfied the requirements set out in the Anti-Money Laundering Act. In 2023, the FGB intends to assess whether and under what conditions the use of VAs as a means of payment in Swiss casinos is compatible with the objectives of the Federal Gambling Act. At present, however, VAs are not accepted as a means of payment in gambling houses and casinos.

As Switzerland is the world's largest gold trading hub, recent research has also been conducted to determine whether the use of VAs is common in business transactions involving the trading and processing of gold in Switzerland.[106] The Central Office for Precious Metals Control (ZEMK), which was contacted for the present report, does not have any concrete information regarding the use of VAs by trade inspectors, smelters and purchasers of smelted goods under its supervision (as of May 2023). To date, it is not known whether VAs are used in individual transactions in the international supply chain of raw precious metals received by the major refiners (trade inspectors). It cannot be ruled out that some of the approximately 800–1,000 buyers of smelted goods in Switzerland may actually use VAs in some cases to process their transactions.

[102] See, for example, Aktionariat, *Create a market for your shares*, last checked in May 2023.
[103] See, for example, Bithome, *Buy and Sell Real Estate with Bitcoin or Cryptos*, last checked in May 2023.
[104] In addition to the Federal Office for Land Registry and Real Estate Law (FOLR), we also contacted the Basel-Stadt Cantonal Land Registry and Surveying Office, the Geneva Cantonal Land Registry Office, the Zug Cantonal Land Registry and Geoinformation Office, the Zug Municipal Notary's Office and the Zurich Cantonal Notary's Office.
[105] See SR 935.511 – *Gambling Ordinance of 7 November 2018* (Gambling Ordinance, GamblO), status as of 1 January 2021.
[106] Switzerland is a major player in the global precious metals trade, handling up to two-thirds of the world's gold trade. In smelting, Switzerland accounts for around 40 per cent of global capacity. Of the global industry leaders, a large proportion have concentrated their activities in Switzerland. See CGMF, *1st National report on the risks of money laundering and terrorist financing*, June 2015, p. 99.

5. Actors, methodology and data used

This chapter explains the methodology used for the present risk analysis of the VA sector, describes the various categories of actors involved and provides an overview of the data and information gathered.

5.1 Methodology

Risk analyses are iterative processes based on a continuous review of the risk landscape. Fresh insights and more accurate assessments are made possible through repeated risk analyses and comparison of previous results and assessments with the latest ones. These, in turn, can then be fed into subsequent analyses. This iteration can improve the accuracy and relevance of the results.

The method used in the present report to analyse ML/TF risks is in line with international recommendations on national risk analyses.[107] Risk is assessed by identifying threats and vulnerabilities as well as risk mitigating factors.

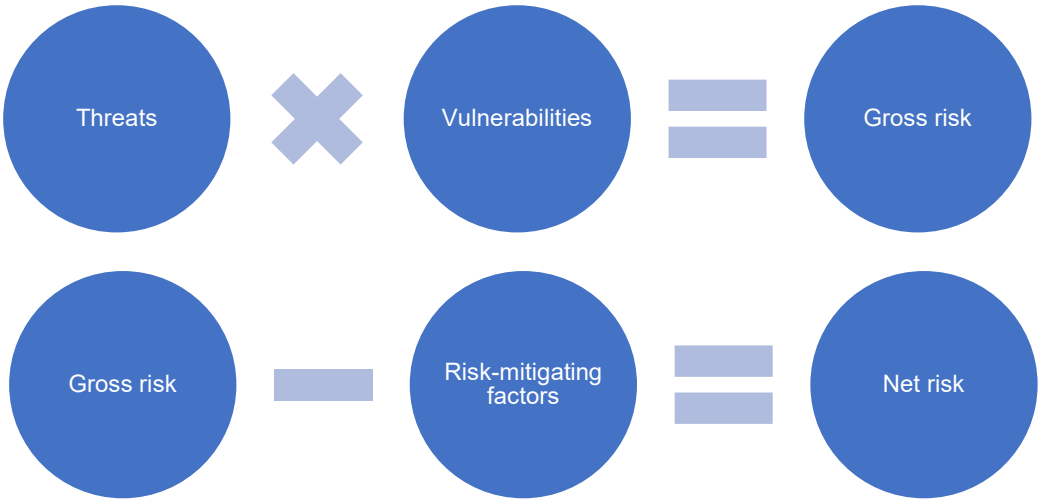

Figure 13: Diagram illustrating the methodology used to evaluate ML/TF risks.

Threats refer to specific risks and threats associated with money laundering and terrorist financing activities. These risks may be associated with specific products or services or with predicate offences to money laundering. An example of a threat associated with specific products or services is the facilitation of anonymous payment processing, which can make it easier for criminals to launder funds from illicit activities. One example of a threat associated with predicate offences to money laundering is the illegal arms trade. When a criminal organisation illegally sells weapons, the risk of laundering and terrorist financing increases, as the criminal organisation will then seek to launder illegally obtained proceeds from the sale of these weapons or use these funds to finance terrorist attacks.

[107] See FATF, *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, October 2021. World Bank, *Virtual Assets and Virtual Asset Service Providers ML/TF Risk Assessment Tool*, June 2022.

Vulnerabilities on the other hand, refer to weaknesses in an organisation or system that can be exploited by criminals for money laundering or terrorist financing activities. Such vulnerabilities might include, for example, inadequate legislation on the supervision of financial intermediaries, or poorly regulated internal business processes of financial intermediaries (e.g. KYC procedures to identify clients and their activities).

Overall, threats and vulnerabilities can both contribute to heightened risk of money laundering and terrorist financing.

Risk-mitigating factors are those factors that minimise the risk of money laundering and terrorist financing, such as when financial intermediaries develop internal control processes to closely monitor clients and their activities.

Gross and net risk: Gross risk refers to the risk that exists without taking into account the effectiveness of risk mitigating factors. Net risk, on the other hand, refers to the risk remaining after risk mitigation factors are in place. The aim is to reduce the net risk to an acceptable level. If the remaining risk is still considered unacceptable, a risk analysis should be conducted to recommend how further risk mitigating factors should be designed and implemented to minimise the net risk.

Threats and vulnerabilities in connection with VAs were already largely identified in the sector risk analysis conducted in 2018 as well as in the national risk analysis performed in 2021.[108] Given the significant changes that have occurred in the VA sector since 2018, the present report considers whether the assessments made back then remain valid and whether any new threats and vulnerabilities have emerged. As was done in the 2018 sector report, all changes in threats and vulnerabilities as well as identified risk mitigating factors are presented at the end of the report (see Chapter 8).

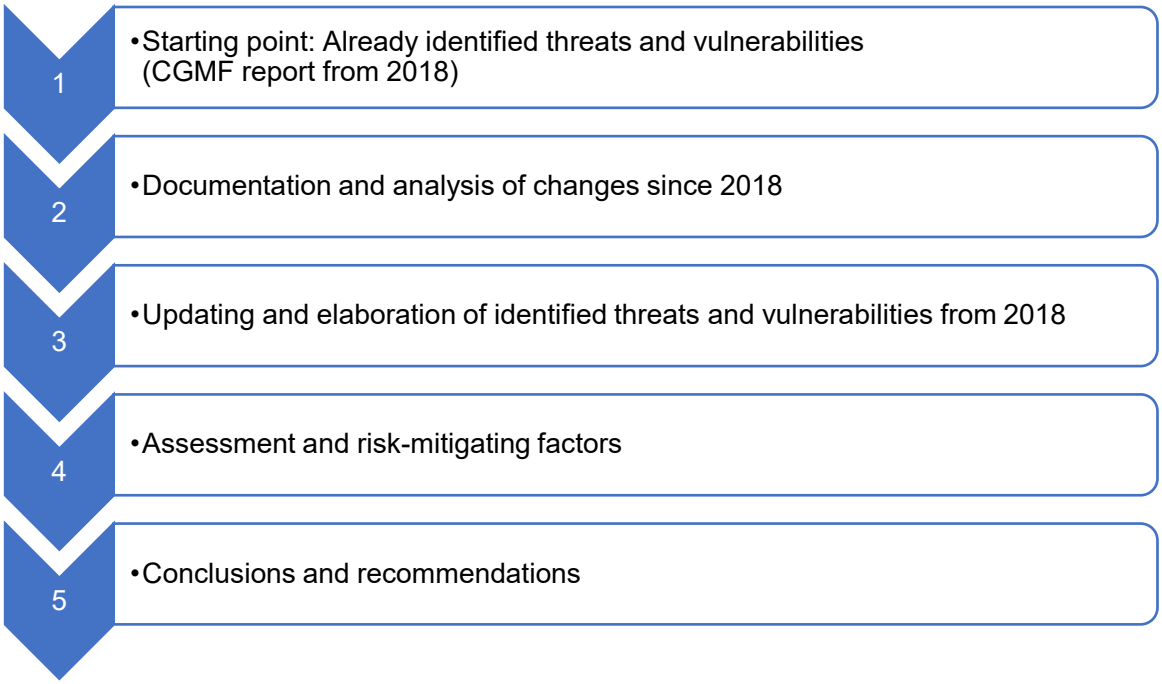

Figure 14: Simplified illustration of the steps involved in preparing the present ML/TF risk analysis

[108] CGMF, *Risk of money laundering and terrorist financing posed by crypto assets and crowdfunding*, October 2018. CGMF, *Second national report on risks of money laundering and terrorist financing*, October 2021, p. 51 – 53.

5.2 Actors and used data

The Money Laundering Reporting Office Switzerland (MROS) was given the lead in preparing this risk analysis. MROS is Switzerland's Financial Intelligence Unit (FIU). It receives and analyses suspicious activity reports (SARs) from financial intermediaries whenever there is a suspected connection to money laundering and terrorist financing. MROS decides whether the information received should be forwarded to a Swiss law enforcement agency. MROS thus plays a key role in Switzerland's AML/CFT system. Various offices and authorities having potential exposure to this topic took part in the risk analysis and provided information, data and expert opinions:

- Selected cantonal land registry offices, official notary offices and land registry inspectorates
- Selected cantonal tax authorities
- Federal Office of Justice (FOJ)
- Federal Office of Police (FEDPOL)
- Office of the Attorney General of Switzerland (OAG)
- Federal Criminal Police Directorate (FCP)
- Swiss Financial Market Supervisory Authority (FINMA)
- Federal Gaming Board (FGB)
- Federal Tax Administration (FTA)
- Federal Supervisory Authority for Foundations (FSAF)
- Federal Office for Land Registry and Real Estate Law (FOLR)
- Central Office for Precious Metals Control (ZEMK)
- Cantonal public prosecutors
- Cantonal and municipal police departments
- Federal Intelligence Service (FIS)
- National Cyber Security Centre (NCSC)
- State Secretariat for International Finance (SIF)

Methodological approaches and best practices of international organisations such as the FATF or the World Bank are crucial when conducting an ML/TF risk analysis. According to World Bank and FATF methodologies, accurate data collection and analysis are essential for effective and tiered risk assessment.[109] In particular, different FIs that engage in VASP activities may pose higher or lower risk depending on a variety of factors, including products, services, clients, geography, business models and the effectiveness of the compliance programme used by these financial intermediaries. Consequently, countries should collect and analyse information on the number and type of FIs with VASP activities, the services they offer and their business activities. The availability of accurate and comprehensive data makes it possible to precisely identify and assess risks during analysis and develop mitigating measures.

In the case of the present risk analysis, however, the widespread lack of data and information on specific services and activities, especially in the Swiss VA sector, poses a methodological challenge. The lack of information on the services offered and the intensity of these business activities makes it more difficult to conduct a detailed risk assessment for individual business models (e.g. custody of VAs for clients, exchange of fiat currency into VAs).

In order to overcome the lack of data and still provide a sound risk assessment, this risk analysis was conducted using a combination of available data sources, collaborative approaches with relevant domestic and foreign authorities, and estimates. By applying proven

[109] FATF, *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, October 2021, p. 11. World Bank, *Virtual Assets and Virtual Asset Service Providers ML/TF Risk Assessment Tool*, June 2022, p. 14f.

methodologies of the World Bank and the FATF, adapted to the specific circumstances of the Swiss VA sector, the ML/TF risks could be adequately assessed despite the limited data available.

An overview of the general intensity of the use of VAs and VA (financial) services offered in Switzerland were gained from various surveys, press reports, specialised studies on the Swiss VA sector and other available sources (including reports on the international context that included information about Switzerland). Information on the use of VAs for criminal purposes in Switzerland in general and for ML/TF purposes in particular was taken from the annual reports of the Federal Office of Police (fedpol), the reports of the National Cyber Security Centre (NCSC) and other publicly available sources such as official crime statistics or news reports.

In addition, non-public sources and databases were examined to draw conclusions regarding the criminal use of VAs in Switzerland in general, as well as their use for ML/TF purposes in particular. At federal level, we considered previous investigations conducted by the Office of the Attorney General of Switzerland and the Federal Criminal Police Directorate, which indicated that VAs were being used for criminal purposes in general and for ML/TF purposes in particular. These investigations related to serious felonies that therefore fall under the authority of the Confederation. At cantonal level, the intercantonal database PICSEL (*Plateforme d'Information de la Criminalité Sérielle En Ligne*) was consulted. This is a centralised database containing online records of incident and damage reports relating to cybercrime cases. The aim is to make it easier for law enforcement agencies to prioritise and coordinate their efforts to crack down on cybercrime.[110] Among other things, records of the number of incidents and associated damage amounts are kept in this database. PICSEL data only provide a partial overview, however, as less than half of the cantons actively manage the database. Despite this, our analysis of the VA-related reports in the database reveals certain digital crime trends in the theft and misappropriation of VAs in Switzerland.

The main non-public source used for this risk analysis were the SARs submitted to the Money Laundering Reporting Office Switzerland (MROS) as well as other data available to MROS. Information gleaned from these SARs, from the international sharing of information and from other databases available to MROS can provide specific indications of the suspected use of VAs for ML/TF purposes in Switzerland. Taken as a whole, an evaluation of the information available to MROS enables common characteristics and typologies to be identified. At a higher level, this information also helps to answer the question of how representative the facts known to MROS are for the Swiss VA sector as a whole. Such an assessment of the extent of ML/TF activities in the VA sector in Switzerland ultimately helps to reveal specific vulnerabilities that may explain blind spots with regard to certain ML/TF phenomena in the VA sector.[111] In addition, during our analysis, information was shared with law enforcement experts[112] and various supervisory authorities.[113] This feedback, based on qualitative and partly quantitative data, allowed us to identify certain trends in the use of VAs for criminal purposes in general and for ML/TF purposes in particular. We were then able to draw general conclusions regarding current opportunities and challenges that Swiss law enforcement agencies face when dealing with criminal offences involving the use of VAs. In addition to gaining further insights, these discussions also helped to shed light on current opportunities and challenges in the VA sector

[110] The database has been operational since April 2021 and is currently being used by nine cantons: Aargau, Fribourg, Geneva, Grisons, Jura, Neuchâtel, Ticino, Vaud and Valais. At least one more canton will join soon (last updated May 2023).
[111] The dark figure is the ratio between the number of crimes actually committed and the number of cases registered in official crime statistics ('bright field').
[112] Among other partners, information was shared with employees within the Digital Crime Investigation Support Network (NEDIK) as well as with cantonal public prosecutors and police authorities.
[113] For example, with the Swiss Financial Market Supervisory Authority (FINMA), the Federal Supervisory Authority for Foundations (FSAF), the Federal Gaming Board (FGB) and the Central Office for Precious Metals Control (ZEMK).

for the various agencies and authorities involved in countering ML/TF. More specifically, we contacted those authorities that, based on the information at our disposal, have already gained extensive experience in this area.

In order to take stock of the global VA risk landscape, risk analyses from other countries as well as annual reports from foreign reporting offices and supervisory authorities were used. The latter also contain information on trends and developments that could influence risks in the Swiss VA sector. The reports published by international organisations and bodies (e.g. the FATF) as well as by private companies (e.g. those involved in blockchain analytics) are also suitable for this purpose. Such reports contain key information and figures on detected cases and patterns as well as already identified ML/TF risk areas in the VA sector. In addition to providing as complete a picture as possible of the global VA risk landscape, the above-mentioned sources can also be used to identify threats and vulnerabilities that are highly likely to exist in Switzerland.

Finally, it is important to emphasise the fact that the amount of data available is insufficient to precisely quantify the identified threats and vulnerabilities or to determine the net risks of specific financial intermediary activities in the VA sector (e.g. fiat-VA exchange, VA custody on behalf of clients). Without reliable figures (e.g. transaction volume, total value of VAs held in custody, number and origin of clients), there is no way to verify whether and to what extent the identified threats, vulnerabilities and risk mitigating factors influence the ML/TF risks associated with these business activities. It is also not possible to assess the extent to which the (suspected) cases already detected in specific business activities are representative enough to be extrapolated.

6. Global risk landscape

Many of the threats and vulnerabilities that arise as a result of VAs being misused for ML/TF purposes relate either to the technological nature of VAs or to the global character of the VA sector. They therefore affect all countries likewise– not just Switzerland. [114] For this reason, this chapter discusses the global context in which the use of VAs isembedded.. The focus is on the global landscape in the VA sector and the main changes that have taken place in this area since the last sector risk analysis in 2018.

6.1 Current global outlook

Since 2018, the use of VA has increased considerably worldwide, resulting in the corresponding expansion of the VA sector. Between spring 2020 and the end of 2021, the VA sector found itself in an upswing phase. Total market capitalisation of all VAs rose from around USD 830 billion in 2018 to roughly USD 2.4 trillion in May 2021.[115] According to estimates, the number of individual users of VAs nearly tripled from 35 million to over 100 million between 2018 and 2020.[116]

The VA sector received a high f media and political attention and attracted many new players. For example, the announcements of individual countries to accept Bitcoin as legal tender or even to hold it as a reserve currency drew a lot of attention during this period.[117] In addition, well-known companies announced their intention to partially convert their cash reserves into Bitcoin.[118] Several major global banks, asset managers and payment service providers also announced their intention to include VA custody and VA investment products in their range of services.[119]

Despite the price collapse of VAs in 2021, the use of VA did not diminish. At the end of 2022, and thus at a time when the crypto sector was in a downward trend, the crypto exchange Coinbase alone recorded over 103 million verified clients, compared to 56 million in April 2021.[120] Some studies predict that by 2030, over 10% of the world's population, or up to one billion people, will be using VAs.[121]

Alongside the growth of users, there seems to also have been a consolidation on the supply side of centralised VA services, as a few of large VA exchanges managed to expand their market share.[122] In view of these developments, blockchain analytics company Chainalysis warned in February 2021 that these companies will need to increase compliance scrutiny of their financial flows, clients and counterparties more carefully in order to avoid jeopardising their position in the market and minimise the corresponding ML/TF risks.[123] And as it so happened, several major FIs with VASP activities received hefty fines in the United States and

[114] CGMF, *Risk of money laundering and terrorist financing posed by crypto assets and crowdfunding*, October 2018, p. 36.
[115] CoinMarketCap, *Global Cryptocurrency Market Charts*, last checked in May 2023.
[116] Cambridge Centre For Alternative Finance (CCAF), *3rd Global Cryptoasset Benchmark Study*, September 2020, p. 12.
[117] BBC News, *Why the Central African Republic adopted Bitcoin*, 6 June 2022. New York Times, *In Global First, El Salvador Adopts Bitcoin as Currency*, 7 September 2021.
[118] Bloomberg, *Tesla Trails Only MicroStrategy in Treasury Bitcoin Allocation*, 8 February 2021.
[119] New York Times, *Banks Tried to Kill Crypto and Failed. Now They're Embracing It (Slowly)*, 1 November 2021.
[120] See Curry David, *Coinbase Revenue and Usage Statistics (2023)*, 28 March 2023.
[121] Finews, *1 Milliarde Krypto-Nutzer bis ins Jahr 2030*, 25 July 2022. Nasdaq, *Blockware Estimates 10% Global Bitcoin Adoption By 2030: Report*, 9 June 2022.
[122] Chainalysis, *Cryptocurrency Exchanges in 2021*, November 2021, p. 3 – 10. Barron's, *The Cryptocurrency Crash Could Lead to a Wave of M&A*, 23 June
[123] Chainalysis, *The 2021 Crypto Crime Report*, February 2021, p. 111.

in Europe of up to a hundred million in the respective currency, mainly because they had not taken adequate precautions against the risk of money laundering and/or had neglected to submit SARs.[124] Investigations revealed, for example, that these financial intermediaries had facilitated transactions involving ransomware groups, darknet markets and sanctioned individuals, entities or addresses.[125] The EU's Markets in Crypto-Assets Regulation (MiCA) is worth mentioning here. Expected to come into force in 2024, MiCA will harmonise the VA regulatory framework within the EU.[126] Since roughly the beginning of 2022, FIs with VASP activities have had to contend with more stringent measures by regulatory and law enforcement agencies at international level than was the case just a few years ago.[127]

6.2 Global changes in the sector 2018 – 2023

Compared to 2018, the global VA sector has changed fundamentally both in size and scope. Based on reports published by international organisations and blockchain analytics companies, the sector has seen three changes in the last five years. First, decentralised finance (DeFi) and the resulting popularity of non-fungible tokens (NFTs) have created a new business area in the VA sector; second, the emergence of this business area has greatly increased the use of stablecoins; and third, the use of VAs has become more geographically diversified from a global standpoint. These developments have created new ML/TF risks, which will be summarised in the following section.

6.2.1 Greater reach and heightened risks

With the DeFi sector (decentralised finance), a completely new area of VA financial services has emerged. DeFi relies principally on smart contracts rather than traditional financial intermediation (TradFi resp. traditional finance, or CeFi resp. centralised finance) to conduct business. Decentralised finance refers to a group of financial applications and services built on a decentralised blockchain platform. Unlike with traditional financial services, users have access to services (e.g. loans, investment products or payment processing) on these platforms without having to register and identify themselves. This is due to the fact that the transactions carried out through these platforms are not executed by a financial intermediary, but rather by the underlying code – the smart contract.

In 2021, the on-chain transaction volume of all decentralised VA exchanges (DEX, resp. decentralised exchange) was consistently higher than that of all centralised VA exchanges (CEX, or centralised exchange).[128] One reason for the growing popularity of DeFi is the simplified and cheaper access to these financial services. The use of DeFi platforms requires only internet access and a VA wallet. Unlike CeFi platforms, users do not have to register or

[124] Financial Crimes Enforcement Network (FinCEN), *FinCEN Announces $100 Million Enforcement Action Against Unregistered Futures Commission Merchant BitMEX for Willful Violations of the Bank Secrecy Act*, 10 August 2021. Monroe Brian, *FinCEN, OFAC fine crypto exchange Bittrex nearly $30 million on AML, sanctions failings, missed SARs, links to darknet markets, mixers, ransomware gangs*, 11 October 2022. New York Times, *Coinbase Reaches $100 Million Settlement With New York Regulators*, 4 January 2023. Reuters, *Dutch central bank fines cryptocurrency exchange Coinbase 3.3 mln euros*, 26 January 2023. Reuters, *Dutch central bank fines Binance 3.3 million euros*, 18 July 2022

[125] Ibid.

[126] European Parliament, *Crypto-assets: green light to new rules for tracing transfers in the EU*, April 2023.

[127] See, for example: New York Times, *Government Cracks Down on Crypto Industry With Flurry of Actions*, 18 February 2023. Europol, *Bitzlato: senior management arrested*, 23 January 2023. Chainalysis, *OFAC Sanctions Hydra Following Law Enforcement Shutdown of the Darknet Market, As Well As Russian Exchange Garantex*, 5 April 2022, Chainalysis, *The 2023 Crypto Crime Report*, February 2023, p. 12.

[128] Chainalysis, *DeFi-Driven Speculation Pushes Decentralized Exchanges' On-Chain Transaction Volumes Past Centralized Platforms*, 6 June 2022.

go through a KYC process, so they remain unidentified.[129] Since these platforms run on smart contracts or software, there is no central entity to stop transactions, freeze accounts or submit SARs in relation to money laundering. As a result, there are effectively no contact persons on such platforms for regulators or law enforcement agencies. Likewise, due to the absence of a financial intermediary (or a VASP), the VAs that users deposit on DeFi platforms fundamentally remain under their control. However, this control is only 'guaranteed' if it is programmed into the underlying smart contract.

As it turns out, vulnerabilities in these smart contracts – some even deliberately built in – gave rise to a number of spectacular hacks and rug pulls where VAs deposited on the platforms in question were siphoned off and vanished. In 2020, blockchain analytics reports put the VAs stolen as a result of hacks of DeFi platforms at around USD 162 million. By 2022, this figure had risen to a total of USD 3.1 billion.[130] With the growth of the DeFi sector, new lucrative opportunities have thus arisen for criminals to steal VAs on a massive scale. However, the stolen VAs must also be laundered afterwards. This, in turn, has increased the demand for techniques to launder stolen VAs – and boosted the potential profits of those who sell or offer such techniques. The vast majority of DeFi platforms issue their own tokens, for example, giving holders of these tokens the right to earn a share of the transaction fees generated on the platform. Significantly, the VAs pilfered from DeFi hacks were primarily laundered via other DeFi platforms, i.e. exchanged into other VAs. It is estimated that in 2021 and 2022 nearly half of the cryptocurrencies stolen in each of these years flowed to DeFi platforms, which clearly shows how vulnerable such platforms are to being misused for money laundering purposes.[131]

Threat 1

Security gaps in the underlying VA technologies (identified in 2018, threat level increased in 2023)[132]

The sector risk analysis of 2018 already considered security gaps in VA technologies and the laundering of illegally acquired VAs as threats. Both of these threats seem to have increased, firstly as a result of the significant expansion of DeFi and secondly due to the numerous hacks, scams and rug pulls in this sector. While it is true that security gaps in VA technology have not become more serious compared to 2018, the number of VAs is now many times higher than it was in 2018. Thus, security gaps have become more numerous as a result.

The functionality of most DeFi services depends on the availability of stablecoins. And this has been the main reason for the boom in the DeFi sector in recent years. Between 2018 and 2022, the share of stablecoins in global VA transaction volume increased from just under 10% to around 45%.[133] In addition to the demand for stablecoins from DeFi applications, this increase has been driven by the growing use of stablecoins in emerging markets, where stablecoins are frequently used for international transfers and for personal savings, based on research by blockchain analytics company Chainalysis.[134] In this respect, stablecoins provide indirect global access to currencies such as the USD or EUR, which has greatly expanded the reach of VAs and their number of users. Stablecoins and VAs with smart contract functionality

[129] KYC stands for 'Know Your Customer' and refers to the process used by financial intermediaries to verify the identity of customers, assess and monitor customer risk, and prevent illegal activities such as money laundering. See Glossary.
[130] Chainalysis, *The 2023 Crypto Crime Report*, February 2023, p. 58.
[131] Ibid., p. 61. Chainalysis, *The Crypto Crime Report 2022*, February 2022, p. 74.
[132] See CGMF, *Risk of money laundering and terrorist financing posed by crypto assets and crowdfunding*, October 2018, p. 22 – 24.
[133] Chainalysis, *The Crypto Crime Report 2022*, February 2022, p. 9.
[134] See Chainalysis, *The State of Web3*, June 2022, p. 3.

(especially Ethereum) – the two key drivers of DeFi applications – together accounted for nearly 90% of the total VA transaction volume in 2022. [135]

With the media frenzy around the buzzwords 'metaverse' and 'Web3' (essentially a blockchain-based World Wide Web), there has also been a lot of hype surrounding NFTs. NFT stands for 'non-fungible token' and refers to uniquely identifiable VAs that have unique features and are stored on a blockchain.[136] NFTs can represent various digital media such as artwork, music, videos and games and are often considered collectibles. Ownership rights over an NFT, i.e., which VA address is authorised to transfer or sell a particular NFT, are cryptographically recorded on the corresponding blockchain. Unlike traditional art trading, NFT artworks can be traded directly between sender and recipient without the need for a financial intermediary or other central entity (e.g. an expert certifying the authenticity of a Picasso painting) to verify the authenticity or record the change of ownership.

The three terms 'Metaverse', 'Web3' and 'NFTs' are ultimately elements that can be associated with the growing DeFi sector. Behind these buzzwords lies the vision (or to some extent already the reality) of new business areas emerging in the VA sector, attracting new users and also bringing previously external business areas such as art, music, gaming or sports into the sphere of influence of the VA sector. In 2021, billions were spent on NFTs, which can be explained by the popularity of various metaverse projects and the promotion of NFTs by celebrities and companies.[137] According to the blockchain analytics company Elliptic, confirmed cases of money laundering involving NFTs have been rare so far.[138] Since 2017, a total of USD 8 million in VAs have been laundered via NFT-based platforms, which is only a fraction of the total NFT-related trading activity. However, this total is based only on identified cases of money laundering and should therefore be taken as a minimum figure.[139] Like other DeFi projects, NFT platforms are vulnerable to hacks, scams and rug pulls. According to Elliptic, between July 2021 and July 2022, over USD 100 million worth of NFTs were stolen through various scams.[140] NFTs may also be misused for ML/TF purposes, especially for trade-based money laundering or for validating the origin of assets, as NFT valuations are subjective and there are no set pricing standards.[141] However, the appeal of NFTs for ML/TF purposes is relatively low at present, as NFTs are among the most transparent of VAs: The full price history of practically every NFT can be viewed at the addresses of its former owners. In contrast, there are established and anonymous techniques to launder VAs (e.g. privacy coins or crypto mixers, see Infobox 4 in Section 7.4.1). Consequently, the current incentive for money launderers to switch to NFTs is arguably low.[142] If the popularity of NFTs and hence the new VA business areas mentioned earlier continue to grow, the reach of the VA sector will also expand accordingly. Similarly, the potential avenues for criminals to misuse NFTs for ML/TF purposes will multiply.

6.2.2 Geographical diversification in the use of Vas

In the meantime, VAs seem to be used by a wide variety of people for a wide variety of purposes. Although reliable figures are not available, there are estimates of how much the

[135] Chainalysis, *DeFi-Driven Speculation Pushes Decentralized Exchanges' On-Chain Transaction Volumes Past Centralized Platforms*, 6 June 2022.
[136] A specific NFT *never* corresponds to another NFT because it is uniquely identifiable.
[137] Elliptic, *NFTs and Financial Crime*, August 2022, p. 5.
[138] Ibid., p. 4.
[139] For example, according to Elliptic, another USD 328.6 million in VAs sent to NFT platforms came from services (e.g. mixing services) designed to obfuscate the origin and authors of the transaction. This in itself could indicate that the sums were derived from criminal activity. See ibid., p. 4.
[140] Ibid., p. 4 and p. 12 – 35.
[141] Elliptic, *NFTs and Financial Crime*, August 2022, p. 77 – 79.
[142] Ibid., p. 79.

general use of VAs has grown in recent years for individual regions across the globe: Of the top 20 countries on the 'Global Crypto Adoption Index' maintained by the blockchain analytics company Chainalysis, only two high-income economies are listed, namely the United States and the United Kingdom.[143] In contrast, half of the top 20 countries were in the lower income bracket (Vietnam, Philippines, Ukraine, India, Pakistan, Nigeria, Morocco, Nepal, Kenya and Indonesia) and eight upper middle-income countries (Brazil, Thailand, Russia, China, Turkey, Argentina, Colombia and Ecuador).

The fact that VAs are now used worldwide by all kinds of people for various legitimate purposes makes it generally more difficult to identify and combat ML/TF risks. The misuse of VAs can now take place in a wide variety of sectors and through diverse channels, making the detection of specific risks more difficult.

Vulnerability 3

Lack of resources and capacity at the institutions involved in combating ML/TF in view of the rapid developments in the VA sector (identified in 2023)

The rapid development of the global VA sector requires these changes to be closely monitored worldwide by the authorities and international organisations involved in AML/CFT efforts. Only in this way will it be possible to ensure the proper monitoring and regulation of the sector, taking into account the constant changes and innovations, to minimise ML/TF risks. It is therefore essential that authorities and international organisations have the necessary resources and capacities to do so. This includes, for example, reaching consensus on the collection, analysis and provision of data on the economic and technological development of the sector, providing personnel with the necessary training and ensuring close cooperation between the authorities involved at national and international level. Globally, resources and capacities do not appear to be allocated adequately. There seem to be major differences both between and within countries in terms of the availability of resources and capacities, as well as in terms of the general level of knowledge and political attention devoted to ML/TF risks. However, even there has been greater political scrutiny of changes taking place in the VA sector (see Section 6.3), the reaction time of the authorities and organisations involved in AML/CFT efforts is sluggish compared to the dynamic developments in the sector. The resulting inability to adequately assess the development of ML/TF risks and take corresponding action to minimise these risks will continue for as long as this lag persists.

6.3 Criminal use of VAs draws political attention

Evidence of increased criminal use of VAs can be found in various reports by international organisations and national authorities. On a broader level, this is also a reflection of the greater overall attention given by supervisory and law enforcement agencies to ML/TF risks in the VA sector. Several FIU annual reports and risk analyses of various countries warn of the risk of VAs being increasingly misused for money laundering and terrorist financing purposes. Most of these sources highlight the appeal of VAs for such activities, pointing to the speed of VA transactions, the encryption techniques used, and the cross-border, internet-based transmission channels, which make monitoring and tracing difficult, if not impossible.[144]

[143] Chainalysis, *The 2022 Geography of Cryptocurrency Report*, September 2022, p. 7.

[144] Financial Intelligence Unit (Germany), *2019 Annual Report*, June 2020, p. 33. Financial Crimes Enforcement Network (FinCEN), *Advisory on Illicit Activity Involving Convertible Virtual Currency*, May 2019, p. 1 – 2.

Several FIUs have noted that the number of SARs relating to VAs has risen in recent years.[145] Several published national risk assessments (NRAs) warn of increased ML/TF risks and a significant potential for misuse.[146] For example, the national risk analysis carried out by Estonia – which is home to a significant number of all VASPs worldwide – showed that most of the VASPs located there have inadequate control over their money laundering and terrorist financing risks. Nearly 75% of Estonia's more than 250 VASPs did not file a single SAR in 2021, while investigations showed that they significantly neglected their due diligence obligations during that time.[147]

According to the FATF, VA-related crimes primarily focus on money laundering offences or predicate offences to money laundering, although criminals also used VAs to evade financial sanctions or raise funds to support terrorism. The types of crimes reported by the various FATF countries included, in particular, trafficking in narcotics and other goods (e.g. firearms), fraud, tax evasion, cybercrime, distribution of child porn, human trafficking, evasion of economic sanctions, and terrorist financing. The most common crimes observed, it said, were in the area of drug trafficking; either through sales conducted directly in VAs or through the use of VAs for money laundering purposes. The second most common type of misuse is related to fraud, ransomware and extortion. In addition, professional money laundering networks are increasingly using VAs as a means of laundering assets.[148]

Infobox 3

Ransomware: VAs drawing greater attention from policymakers

Ransomware is a type of malicious software (malware) that is used to block access to data or systems by encrypting them. The attackers then demand a ransom from the victims to restore the data or access. The global incidence of ransomware attacks has increased significantly in recent years. The attackers almost always demand that their victims pay the ransom in VAs.[149] The use of VAs in ransomware attacks makes it easier for technically skilled attackers to both conceal their identity and mask the flow of funds. Compared to traditional payment transactions, VAs offer the advantage that – as long as they remain in a non-custodial wallet – they cannot be frozen or confiscated by third parties.

In recent years, policymakers have become more aware of the problems surrounding the use of VAs, in part because ransomware attacks across the globe have now spread to key economic or infrastructurally important institutions and large financial players. [150] Ransomware is therefore now seen by many countries not only as a significant cyber threat, but also as a national security risk.[151]

---

[145] Financial Intelligence Unit (Germany), *2019 Annual Report*, June 2020, p. 46. Financial Intelligence Unit (Germany), *2021 Annual Report*, August 2022, p. 48. Financial Intelligence Unit (Netherlands), *Annual Review 2019*, June 2020, p. 13. Financial Intelligence Unit (Netherlands), *Annual Review 2021*, June 2022, p. 7 and p. 27. Financial Intelligence Unit (Estonia), *Yearbook 2019*, 2020, p. 29. Financial Intelligence Unit (Liechtenstein), *2020 Annual Report*, March 2021, p. 5. Financial Intelligence Unit (Liechtenstein), *2021 Annual Report*, April 2022, p. 6. See also Vedrenne Gabriel, *In Europe, Suspicious Payments Triple Thanks to VASPs, Cryptocurrency*, 25 October 2022.

[146] HM Treasury, *National risk assessment of money laundering and terrorist financing 2020*, December 2020, p. 70. Advisory Board for the Fight Against Money Laundering and Terrorist Financing (COLB), *Analyse nationale des risques de blanchiment de capitaux et de financement du terrorisme en France*, September 2019, p. 65. State Financial Service of Ukraine, *Report on the National Risk Assessment*, 2019, p. 78 – 80. Government of the Grand Duchy of Luxembourg, *ML/TF Vertical Risk Assessment: Virtual Asset Service Providers*, December 2020, p. 3 – 4.

[147] Financial Intelligence Unit (Estonia), *The Risks related to Virtual Asset Service Providers in Estonia*, January 2022, p. 5.

[148] FATF, *Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing*, September 2020, p. 4.

[149] FATF, *Countering Ransomware Financing*, March 2023, p. 6.

[150] Prestige Business, *Cyber-Attacken in der Schweiz nehmen auch 2023 zu*, , 3 May 2023.

[151] CNET, *Ransomware rises as a national security threat as bigger targets fall*, 18 October 2021.

According to blockchain analytics company Chainalysis, the total amount of VAs sent to known ransomware addresses more than quadrupled between 2019 and 2020.[152] It is interesting to note that half of all VAs sent from known ransomware addresses to FIs with VASP activities offering VA-fiat exchange (referred to as fiat off-ramps) were transferred to only 21 addresses, suggesting that the laundering of proceeds from ransomware attacks is highly concentrated and organised.[153]

In Switzerland, the National Cyber Security Centre (NCSC) receives reports of cyber incidents from the public and the business community. The NCSC analyses these reports and provides the reporting parties with an assessment of the incident and recommended action steps. According to the NCSC, it is very difficult to determine where VAs extorted from ransomware attacks flow to and who the actual recipients of these payments are. One of the reasons for this is that ransomware has now developed into a service (ransomware as a service) that can be rented or sold on the Darknet to clients who do not need to have any IT knowledge themselves. This development increases the complexity of revenues streams, thus making it more difficult to track and trace them. So far, the NCSC has not collected any data on the number and amount of ransom payments. However, it assumes that many cases where ransom was paid are not even reported to the NCSC.

In December 2022, the Federal Council announced its intention to introduce a reporting obligation in the event of cyberattacks on critical infrastructures.[154] The corresponding bill establishes the legal basis for the requirement that operators of critical infrastructures report cyberattacks. It also sets out the tasks of the National Cyber Security Centre (NCSC), which will serve as the central point of contact for the reporting of cyberattacks.

Threat 2

Ransomware and malware (identified in 2018, threat level increased in 2023)[155]
The sector report published in 2018 had already drawn attention to the fact that VAs had become an instrument of choice for hackers in ransomware attacks. Compared to 2018, ransomware cases have reached unprecedented levels in terms of number, amount of VAs seized, and the risks they pose to private and government infrastructures. The threat level has increased as a result.

Threat 3

VAs as a means of payment for illegal goods and services (identified in 2018, threat level increased in 2023)[156]

Also in 2023, VAs have become the preferred means of payment for illegal goods and services over the internet, e.g. for buying and selling narcotics, stolen credit card information on the Darknet, or even ransomware or other malware software.[157] Sales volumes on Darknet markets have doubled from around USD 750 million in 2018 to USD 1.5 billion today.[158]

[152] Chainalysis, *The 2023 Crypto Crime Report*, February 2023, p. 27.
[153] Ibid., p. 50.
[154] BBl 2023 84 – *Botschaft zur Änderung des Informationssicherheitsgesetzes* (introducing reporting requirements in the event of cyberattacks on critical infrastructures) dated 2 December 2022, 18 January 2023
[155] CGMF, *Risk of money laundering and terrorist financing posed by crypto assets and crowdfunding*, October 2018, p. 26.
[156] CGMF, *Risk of money laundering and terrorist financing posed by crypto assets and crowdfunding*, October 2018, p. 28 – 30.
[157] Chainalysis, *The 2023 Crypto Crime Report*, February 2023, p. 71 – 84.
[158] Ibid., p. 71. Chainalysis, *The Crypto Crime Report 2022*, February 2022, p. 100.

In Switzerland, too, there are known cases where VAs were also used as a means of payment for the organised sale of narcotics.[159] The recognition of risks in this area led to an adjustment of the clarification threshold for virtual currency transactions from CHF 5,000 to CHF 1,000 (Art. 51*a* AMLO-FINMA).

It is still unclear to what extent the use of VAs as a means of payment for illegal goods and services has increased in relation to the general growth of the VA sector. However, the fact that VAs are used more frequently and more diversely as a means of payment for such purposes is well documented. As a result, the threat level has increased.

6.4 Estimates of global ML/TF-relevant financial flows in the VA sector

No reliable figures on ML/TF-relevant financial flows in the VA sector exist at present. In most cases, the only basis for quantitative insights into the use of VAs for ML/TF purposes are estimates made by blockchain analytics companies. This is also one of the reasons why these companies are cited in most FIU annual reports and national risk assessments. The figures produced by these companies only provide a rough idea of the magnitude, and should therefore be viewed with caution for a number of reasons.

First of all, the general term 'crypto crime' used by various blockchain analytics companies is not clearly defined and there is no indication of what crimes and payments fall into this category. Likewise, the 'crypto crime' term does not enable one to determine what actions would qualify as predicate offences to money laundering under Swiss legislation. In its February 2022 'Crypto Crime Report', Chainalysis at least clarified that the figures presented referred only to purely 'cryptocurrency-native crime', such as sales on Darknet markets or ransomware attacks. It is more difficult to determine how much cash from 'offline crime', such as traditional drug trafficking, is converted into cryptocurrency for money laundering purposes.

Secondly, it is unclear whether the share of crypto crime in the annual volume of VA transactions can be compared with illegal financial flows in other sectors. Thirdly, in some cases, such figures were subsequently revised upwards to a large extent.[160] A fourth consideration has to do with the fact that criminal activities, and the associated VA addresses, have to have already been detected beforehand. Experience shows that the reports mainly include analyses of cybercrime (ransomware, hacks, phishing, investment scams, etc.) as well as illegal trade in goods and services on Darknet markets. It seems clear that in the absence of external indications of their criminal relevance (media reports or known VA addresses), the analytical tools used by these companies are not likely to detect payments relating to trade-based money laundering, corruption, human trafficking or terrorist financing, for example.

And fifth, these analyses exclude all off-chain transactions, which are estimated to be at least ten times larger in volume than on-chain transactions.[161] In this respect, their analyses and figures reflect only a tiny fraction of the actual VA transactions taking place. Finally, it is also unclear whether a decrease in the proportion of detected criminal transactions reflects a general decrease in the risk of crime in the VA sector, or whether, conversely, as the VA sector has matured, criminals have increasingly resorted to using sophisticated obfuscation techniques – for example, using non-traceable privacy coins, crypto mixers and decentralised exchanges.

[159] See, for example, article published in Tages Anzeiger, Schweizer Online-Drogenversand – «Hippe Kleider, Typ Studentin, and das Täschli voller Drogen», 18 March 2021.
[160] McGuire, Michael, *Into the Web of Profit. Understanding the Growth of the Cybercrime Economy*, April 2018, p. 4. Chainalysis, *The 2020 Crypto Crime Report*, February 2022, p.4.
[161] See Jimenez, Alison, , 11 January 2022.

Despite these uncertainties, the increase in VA financial flows linked to criminal activity is generally undisputed. Chainalysis estimated that the global total of all VAs received from known addresses with a criminal background exceeded USD 20 billion in 2022, compared to USD 8 billion in 2020.[162] Conversely, these addresses transferred VAs worth around USD 23.8 billion in 2022.[163] This represents an increase of 68% compared to 2021, with roughly USD 14.2 billion.[164] Over half of the value of these VAs flowed to the large VA trading exchanges. However, the corresponding account holders at these trading exchanges were over-the-counter (OTC) brokers. These are VASP FIs that use the platforms of the large trading exchanges in order to provide their services ('nested services', see Infobox 4 in Section 7.4.1). Nevertheless, this figure should raise eyebrows, as the large trading exchanges are the places where VAs can be converted into fiat currency and thus enter the traditional financial system. Large trading exchanges are also the most likely to have dedicated compliance departments that can report these transactions and take action against the users concerned.

At the same time, it is important to put these totals into perspective, as the share of VA transactions that are known to be of criminal nature (including money laundering and terrorist financing), is actually declining as a percentage of total VA transactions. Depending on the source, this share ranges between 0.24% (2022) and 3.3% (2019).[165] In comparison, the UN estimates the amount of money laundered worldwide in a given year to be 2–5% of global GDP.[166] However, despite increasing risks, national risk analyses and similar reports stress the fact that the use of VAs for money laundering purposes is still far below that of fiat currency and more traditional methods.[167]

There are several explanations for the nominal increase in the total volume of VA transactions of a possible criminal nature and the simultaneous decrease in this share of the total VA transaction volume in percentage terms. Many VA thefts occurred during the upswing in VA prices, so the value of stolen VAs also increased on its own, so to speak. Conversely, the relative decrease could be explained by the increasing regulation of the big 'players' who have moved to scrutinise their clients more closely and use blockchain analytics tools to monitor their transactions. In any case, it would be surprising and alarming if, with the spectacular growth of the VA sector, there had been a proportional increase in criminal use.

In the area of ‘crypto crime’, money laundering seems to play the key role as a criminal offence: VAs unlawfully obtained from hacks, ransomware attacks, scams, sales of child porn or narcotics via the Darknet must be laundered at some point, assuming that they return to the legal circuit. In October 2022 alone, even after the significant drop in VA prices, VAs worth USD 718 million were stolen in the course of 11 hacks on DeFi platforms.[168] In 2022, the total amount of VAs obtained through hacks was estimated at USD 3.8 billion.[169]

---

[162] Chainalysis, *2023 Crypto Crime Trends: Illicit Cryptocurrency Volumes Reach All-Time Highs Amid Surge in Sanctions Designations and Hacking*, 12 January 2023.
[163] Chainalysis, *Crypto Money Laundering: Four Exchange Deposit Addresses Received Over $1 Billion in Illicit Funds in 2022*, 26 January 2023.
[164] Ibid.
[165] Chainalysis, *2023 Crypto Crime Trends: Illicit Cryptocurrency Volumes Reach All-Time Highs Amid Surge in Sanctions Designations and Hacking*, 12 January 2023. Ciphertrace, *Cryptocurrency crime and anti-money laundering*, June 2022, p. 5. TRM Labs, *Ensuring Responsible Development of Digital Assets; Request for Comment*, November 2022.
[166] United Nations Office on Drugs and Crime (UNODC), *Money Laundering*, last checked in May 2023.
[167] As a case in point: Department of the Treasury (USA), *National Money Laundering Risk Assessment*, February 2022, p. 41. Europol Spotlight, *Cryptocurrencies – Tracing the Evolution of Criminal Finances*, December 2021, p. 2.
[168] Finews, *Chainalysis: Crypto Hacks Reach Record $3 Billion*, 13 October 2022.
[169] Chainalysis, *The 2023 Crypto Crime Report*, February 2023, p. 56.

Threat 4

Laundering of VAs of criminal origin (in fiat money) (identified in 2018, threat level increased in 2023)[170]

Since 2018, criminals have exploited multiple security vulnerabilities in VA protocols and platforms and illegally obtained billions of dollars in VAs. In order to inject these illicit assets back into the legal financial circuit, these billions need to be laundered. Consequently, compared to 2018, the demand for opportunities to launder illegally obtained VAs has also increased significantly. Compared to 2018, individual FIs with VASP activities are at greater risk of being used to launder these VAs.

Hacks of CeFi and DeFi platforms, moreover, appear to be carried out not only by 'ordinary' hackers, but also by state actors for proliferation financing purposes. According to several published reports by the Panel of Experts to the UN Security Council Sanctions Committee on North Korea, revenues from such hacks are used to support North Korea's weapons of mass destruction and ballistic missile programmes.[171] According to other reports, VA theft now constitutes one of North Korea's main sources of revenue, with up to one-third of funding for its missile programme being obtained through these channels.[172] For 2022, Chainalysis attributed USD 1.7 billion in VAs to hacker groups linked to North Korea.[173] This sum is equivalent to more than 10% of North Korea's gross domestic product.[174] In April 2023, the Financial Action Task Force's Virtual Assets Contact Group (VACG), referring directly to North Korea, stressed the urgent need for countries worldwide to implement FATF standards as the risk of VAs being misused for money laundering, terrorist financing and proliferation financing was increasing. [175]

An important change in the criminal use of VAs observed by Europol is that the use of VA is no longer limited to cybercrime activities, but has now expanded to include all types of crimes requiring the transfer of monetary value.[176] The types of crimes reported by FATF countries illustrate the variety of ways in which VAs are used by a broad range of actors and for a wide variety of criminal purposes.

Similarly, VAs appear to be misused by criminal organisations to launder the proceeds of their 'offline activities'. In 2021, Italian authorities seized over EUR 80 million that a faction of the Sicilian Cosa Nostra is believed to have laundered through a Malta licensed and self-controlled sports betting website.[177] The same money laundering scheme is also said to have been used by other criminal organisations such as the Calabrian 'Ndrangheta, the Naples-based Camorra, but also by Romanian and Chinese organised crime groups.[178] According to Malta's

[170] CGMF, *Risk of money laundering and terrorist financing posed by crypto assets and crowdfunding*, October 2018, p. 26f. The threat was titled 'Laundering of illegally acquired crypto assets' in the 2018 CGMF report on cryptocurrencies. Since then, this threat has been renamed 'Laundering of VAs of criminal origin (in fiat money)' in order to more clearly distinguish it from the threat 'Laundering of fiat money of criminal origin (in VAs)'.
[171] United Nations Security Council, *S/2022/668 Midterm report of the 1718 Panel of Experts*, September 2022, p. 75 – 78. United Nations Security Council, *S/2022/132 Report of the 1718 Panel of Experts*, March 2022, p. 80. United Nations Security Council, *S/2021/211 final report of the Panel of Experts*, March 2021, p. 56f.
[172] Financial Times, *How North Korea became a crypto crime hub*, 14 November 2022. Chainalysis, *North Korean Hackers Have Prolific Year as Their Unlaundered Cryptocurrency Holdings Reach All-time High*, 13 January 2022. Coindesk, *'Ship-to-Ship' Trade and Other Secrets of North Korea's Illicit $1.5B Crypto Stash*, 7 April 2020.
[173] Chainalysis, *The 2023 Crypto Crime Report*, February 2023, p. 60.
[174] In 2021, the GDP of North Korea was around USD 16.4 billion. See United Nations Data Retrieval System, *Democratic People's Republic of Korea*, last checked in May 2023.
[175] FATF, *Press Release - Virtual Assets Contact Group (VACG)*, 14 April 2023.
[176] Europol Spotlight, *Cryptocurrencies – Tracing the Evolution of Criminal Finances*, December 2021, p. 2.
[177] Organized Crime & Corruption Reporting Project (OCCRP), *Italian Mafia Bets on Illegal Online Gambling*, 4 March 2021. Süddeutsche Zeitung, *Wieso die Mafia Fan von Maltas Online-Casinos ist*, 18 December 2022.
[178] L'avvenire di Calabria, *Boom delle scommesse online, ma per la Dia c'è l'ombra dei clan*,, 23 January 2020.

own national risk analysis on VAs, online casinos in Malta pose considerable ML/TF risks.[179] Malta is home to around 10% of the world's gambling operators.[180] The tax revenues generated from these activities accounted for around 12% of Malta's gross domestic product in 2019.[181] Deposits and withdrawals made via e-wallets, which typically also enable VA transactions, accounted for around 10–15% of sales volumes from 2019 to 2021.[182] There are also several publicly known cases where VAs were misused to pay bribes, to finance Al-Qaeda and ISIS terrorist operations and were used by South American drug cartels for money laundering purposes.[183]

The VA sector has strongly grown in size and reach globally since 2018. Significantly more people around the world appear to be using VAs. It remains unclear how much the criminal use of VAs has grown alongside it. The above estimates should therefore be regarded as minimum figures. However, the rising number of SARs submitted in relation to money laundering in the various countries suggests that the use of VAs for ML/TF purposes in particular is suspected more frequently than it was a few years ago. However, this could also be due to increased regulation and heightened VASP awareness. Based on reports from several countries, supranational organisations and blockchain analytics companies, it is clear that there has been a general increase in the criminal use of VAs.

In addition, criminal use of VAs seems to have become more diversified. VAs have long since ceased to be limited to cybercrime activities; they now also appear in connection with a wide variety of 'offline' offences. However, consolidated figures on this are unavailable, which makes it difficult to estimate how often illegally acquired assets from these 'traditional' criminal activities have been laundered using VAs. Detecting these transactions remains a major challenge for blockchain analytics companies and VASPs. For this reason, the number of unreported cases in this area is likely to be significant.

Threat 5

Laundering of fiat money of criminal origin (in VAs) (identified in 2018, unchanged in 2023)[184]

In the 2018 sector report, two risks associated with the use of VAs for money laundering purposes were identified: the first was the laundering of VAs of criminal origin (e.g. hacking into a VA exchange) and second the laundering of fiat money of criminal origin. For the first risk, specific blockchain analytics data indicate that this risk has increased since 2018 (see Risk 4 in Section 6.4). For the second risk, there are no consolidated figures enablings to determine whether the situation has improved or worsened. Individual observations on the use of VAs by criminal organisations for money laundering purposes nevertheless indicate that this risk has at the very least not diminished. The level of risk remains unchanged.

[179] National Coordinating Committee on Combating Money Laundering and Funding of Terrorism (Malta), *Key Results of the Sectoral Risk Assessment on Virtual Financial Assets*, February 2020, p. 12.
[180] Forbes, *Scandals And Mafia Allegations May Force Malta To Reconsider Its Reliance On Online Betting*, 13 March 2021.
[181] Ibid.
[182] Malta Gaming Authority, *Annual Report 2021*, September 2022, p. 79. Forbes, *Scandals And Mafia Allegations May Force Malta To Reconsider Its Reliance On Online Betting*, 13 March 2021.
[183] See Stalinsky Steven, *The Coming Storm – Terrorists Using Cryptocurrency*, 21 August 2019. Department of Justice (USA), *Two Chinese Intelligence Officers Charged with Obstruction of Justice in Scheme to Bribe U.S. Government Employee and Steal Documents Related to the Federal Prosecution of a PRC-Based Company*, 24 October 2022. Chainalysis, *The Crypto Crime Report 2022*, February 2022, p. 93 – 98. AP News, *Mexican cartels turn to bitcoin, internet, e-commerce*, 10 March 2022. Europol, *Underground drug-money bank laundering EUR 180 million liquidated by law enforcement*, 13 April 2023.
[184] CGMF, *Risk of money laundering and terrorist financing posed by crypto assets and crowdfunding*, October 2018, p. 30f. Note: The original section title used in the 2018 publication 'Investment of funds of criminal origin in crypto assets' has been reformulated for greater clarity to 'Laundering of fiat money of criminal origin (in VAs)'.

7. Risk trends for Switzerland

The threats posed by VAs, and the related vulnerabilities that Switzerland faces, were previously identified in the 2018 report on ML/TF risks in the VA sector. There, the various threats were divided into two main categories: those inherent in the use of VA technologies and those arising from the fraudulent use of VAs.[185]

Threats inherent in VA technologies	**Threats** of fraudulent use of VAs	Switzerland's **vulnerabilities** to ML/TF risks through the use of Vas
1. Transaction anonymity and difficult identification of beneficial owners 2. Security weaknesses in the underlying VA technologies 3. Threats in connection with the novelty effect and users' inexperience 4. Malware and ransomware 5. Laundering of VAs of criminal origins VAs (in fiat money)	1. Terrorist financing using VAs 2. VAs as a means of payment for illegal goods and services 3. VA use for phishing 4. Laundering of FIAT money of criminal origins (in VAs)	1. Vulnerabilities of FIs that carry out VA transactions 2. Difficult suppression of ML/TF in the VA sector

Figure 15: CGMF 2018 report: Threats and vulnerabilities identified in association with VAs[186]

In order to enable a comparison with the 2018 findings, this chapter first outlines the changes that Switzerland has experienced since then with regard to combating ML/TF in the VA sector. This will then serve as a basis for determining the extent to which the threats and vulnerabilities identified in 2018 have evolved or new ones have emerged. Ideally, statistical data on the various phenomena would be required to demonstrate these changes. However, this is very difficult to achieve due to the tremendous lack of data, which is in itself a risk (see Section 7.1). The main datasets used to model the changes in this risk analysis were the SARs submitted to the Money Laundering Reporting Office Switzerland (MROS) and other data available to MROS, most of which came from the exchange of information with foreign reporting offices. This includes the evaluation of spontaneous information and information requests with reference to VA or VASPsthat foreign reporting offices provided to Switzerland. MROS used new evaluation methods from the goAML information system to analyse all the available data

[185] CGMF, *Risk of money laundering and terrorist financing posed by crypto assets and crowdfunding*, October 2018, p. 20 – 36.

[186] Ibid. Note: For greater clarity, the threat referred to in the 2018 report as 'Laundering of illegally acquired crypto assets' has been renamed 'Laundering of illegally acquired VAs (in fiat money)', and the threat 'Investment of funds of criminal origin in crypto assets' has been renamed 'Laundering of illegally acquired fiat money (in VAs)'. In addition, the vulnerability referred to in the 2018 report as 'Financial intermediaries that carry out crypto transactions' has been renamed 'Financial intermediaries that carry out VA-related transactions (in VAs or fiat money)' to reflect the broader scope of this vulnerability (see Vulnerability 6).

in detail (see Section 11.1). These analyses clearly indicate, among other things, a higher frequency of SARs involving VAs since 2020.

In addition, as part of this risk analysis and in response to postulates 22.3017 (*Improve the capabilities of law enforcement to handle cases involving cryptocurrencies*) and 22.3145 (*How well equipped are cantonal law enforcement agencies in the prosecution of cybercrime cases?*), a survey was conducted among the various cantonal (and municipal) police forces and public prosecutors.[187] The survey asked for quantitative information on criminal proceedings already initiated in relation to VAs (e.g. number of proceedings, the offences and amounts involved). Respondents were also asked to provide a qualitative assessment of the challenges and opportunities in the VA sector for the work of law enforcement. Due to the lack of monitoring of VA-related criminal proceedings, only a small minority of the responding law enforcement agencies were able to provide consolidated information. The quantitative results from the survey are therefore fragmentary and of limited relevance. They do not replace the need for a national overview for Switzerland. Nonetheless, the overall findings seem to confirm certain assumptions and trends regarding the criminal use of VAs and the related work of law enforcement agencies (see Sections 7.2 to 7.4). In addition to the survey of law enforcement agencies, in-depth discussions were held with various Swiss law enforcement agencies and supervisory authorities.

Additional quantitative findings were obtained by analysing individual data collections of Swiss law enforcement agencies. In particular, these include PICSEL (intercantonal database of reports of cybercrime) and (preliminary) investigations conducted to date by the Federal Criminal Police, in which the use of VAs was a central element of the case and ultimately led to the opening of proceedings. Together with the survey of cantonal law enforcement agencies, the findings of the Federal Criminal Police proved to be the most informative and are therefore referred to frequently in this chapter. On the basis of the information available to MROS, it was also possible to identify certain 'typologies' which qualitatively illustrate the various possible forms and characteristics of ML/TF activities involving VAs. These typologies, which are mainly based on SARs submitted to MROS between 2020 and 2022, illustrate the diversity of techniques used for money laundering or terrorist financing.

7.1 Lack of data an inherent risk

There is very little data available on the use of VAs in general in Switzerland. The situation is even more acute with regard to the use of VAs for criminal offences, for which there are only a few sets of aggregated statistical data. There is even less quantitative data on the use of VAs specifically for money laundering or terrorist financing. Neither is there a national database of foreign requests for mutual legal assistance in criminal matters relating to VAs. As a result, it is unclear how often such requests are made and what challenges they pose for law enforcement agencies.

The lack of data on VA-related financial flows – which may also include fiat money flows – is not unique to Switzerland. Since payments involving VAs are in general anonymous (or pseudonymous), it is difficult to determine the location of the parties involved, unlike with traditional payment transactions. This makes it more difficult to draw accurate conclusions about the use of VAs in a particular country or region, such as Switzerland. The idea that

[187] See 22.3145 (postulate), *How well equipped are cantonal law enforcement agencies in the prosecution of cybercrime cases?*, submitted by the Security Policy Committee of the National Council on 15 February 2022, and 22.3017 (postulate), *Improve the capabilities of law enforcement to handle cases involving cryptocurrencies*, submitted by National Council member Andri Silberschmidt on 16 March 2022. Both postulates were adopted by the National Council in June 2022. The Federal Department of Justice and Police (FDJP) is responsible for responding to these two postulates.

blockchains are transparent is therefore somewhat of a misconception. Also, estimates of the true volume of VAs can only be approximate, as most VA transactions are 'off-chain' and not registered on the blockchain (i.e. 'on-chain').[188] For example, VASPs often keep all internal transactions off-chain. In addition to the main or base layer of a blockchain, which is publicly visible, there are also the 'layer 2' protocols. These additional layers, which are built on top of the original blockchain, are used to improve scalability and reduce transaction costs. A well-known example of such a protocol is the Lightning Network in the Bitcoin ecosystem. Transactions processed on layer 2 protocols are not directly or fully recorded on the blockchain. As a result, the whole system is more complex and opaque, making it harder to trace the flow of VA funds. It is estimated that only about 10% of all VA transactions are recorded on-chain.[189] As a result, the majority of VA transaction data are stored in the private databases of various firms. Large centralised VA trading exchanges would have a better overview of the global financial flows in VAs, but these data are not made public.

Where off-chain transactions and layer 2 protocols are used, this presents some additional challenges but does not leave law enforcement agencies completely in the dark. Tracing the intricate paths of transactions may take longer and cost more, but is not necessarily impossible. Fundamentally, the system is still transparent, even if the added layers make it more complex. Law enforcement can still uncover criminal activity, but it takes more time and resources and requires a higher level of expertise and investigative tools. The transparency of blockchains is not lost, but it is more difficult to penetrate and requires specific investigative tools.

The exact extent of the use of VAs in individual countries or regions is difficult to assess, as both the International Monetary Fund (IMF) and the European Central Bank (ECB) have noted. Already in 2019, the IMF recommended an international exchange of statistical data on VA transactions and positions to address the lack of data and enable more meaningful macroeconomic assessments.[190] The ECB has also recommended that developments be closely monitored and pointed to the lack of reliable statistics on the actual size of the VA sector and the financial flows associated with VAs.[191] However, these recommendations have not yet been implemented. In 2022 the IMF noted that significant data gaps continue to make it difficult to assess the true extent of VA use in the financial system, which also hampers risk analysis by financial authorities.[192] At present, there appears to be no consensus on how to categorise different types of VAs or on the metrics that individual countries can use to examine economic activity and financial flows in the VA sector, which is essentially global. In addition, the IMF notes that, given the rapid evolution of the VA sector, any sector-specific recommendations are always at risk of becoming quickly outdated.

The lack of reliable data on the VA sector was previously noted in the CGMF's 2018 report 'Risk of money laundering and terrorist financing posed by crypto assets and crowdfunding'[193] and in the '2nd National report on the risks of money laundering and terrorist financing in Switzerland' published in October 2021.[194] This report also finds that there are no reliable figures, particularly for Switzerland.

Enquiries with various Swiss authorities and organisations indicate that there is currently no monitoring that would indicate the growth of the sector, the income and assets in

[188] Jimenez Alison, *3 Misconceptions about Cryptocurrency Crime Estimates*, 11 January 2022.
[189] Von Luckner, Reinhart & Rogoff, *Decrypting New Age International Capital Flows, NBER Working Paper No. 29337*, October 2021, p. 1, footnote 2
[190] International Monetary Fund (IMF), *Treatment of Crypto Assets in Macroeconomic Statistics*, 2019, p. 3.
[191] European Central Bank (ECB), *Understanding the crypto-asset phenomenon, its risks and measurement issues*, May 2019.
[192] International Monetary Fund (IMF), *F.18 Recording of Crypto Assets in Macroeconomic Statistics*, March 2022, p. 40.
[193] CGMF, *Risk of money laundering and terrorist financing posed by crypto assets and crowdfunding*, October 2018, p. 35f.
[194] CGMF, *2nd National report on the risks of money laundering and terrorist financing in Switzerland*, October 2021, p. 52.

cryptocurrencies that are taxed in Switzerland, or the frequency and size of the financial flows entering or leaving the Swiss financial centre in connection with the purchase, sale or custody of VAs. There are currently no plans for such monitoring at the national level.[195] This lack of data has become a significant vulnerability in view of the rapid developments in ML/TF in recent years: unexpected trends in regard to ML/TF could potentially remain undetected for a long period of time.

Vulnerability 4

Insufficient figures and statistics at national and international level (identified in 2023)

Given the rapid developments over the past five years, the lack of comprehensive data at national and international level can prove problematic. Some 15 years have passed since the emergence of Bitcoin, the oldest cryptocurrency. Switzerland and its 'Crypto Valley' have an international reputation as a regulatory safe haven, not least because of the rapid progress that Switzerland has made compared to other countries in creating legal certainty for the crypto industry. At the same time, there is very little data available on overall figures, such as the VA-relevant financial flows entering or leaving the Swiss financial centre. Data from blockchain analytics are not the only source of information on the use of VAs for ML/TF purposes. For example, information from traditional payment transactions, commercial registers, tax records, supervisory authorities and public sources can also be used to assess and strengthen the AML/CFT mechanism in relation to VAs. All the different authorities, stakeholders and other actors involved need this information in order to make informed, coordinated decisions and set the right priorities in their work. This general lack of information increases the risk that unexpected developments will go unnoticed for some time and then suddenly expose Switzerland and other international financial centres to economic and political risks.

7.2 Increased use means increased risk

Parallel to the marked increase in the use of VAs, the risks of ML/TF have also increased, as can be seen from the data provided by MROS and Swiss law enforcement agencies.

Swiss law enforcement agencies and MROS are increasingly confronted with cases involving the use of VAs. Since the beginning of 2020, an increasing volume of information received by MROS from Swiss FIs or foreign Financial Intelligence Units (FIUs) has been 'VA-related',[196] i.e. relating to facts or suspicious transactions in connection with the use of VAs.

A SAR of an FI may be VA-related even if the financial intermediary is not engaged in VASP activities. In the evaluation, an SAR was classified as VA-related if at least one of two scenarios applied:

- If the SAR contained VA-related transactions, i.e. if an SAR contained transactions between the reported accounts and accounts of FIs engaged in VASP activities (reports by FIs not engaged in VASP activities) *or* if the reported transactions were denominated in VAs (reports by FIs engaged in VASP activities).
- Where there was a clear link to VAs based on the facts presented in writing by the reporting financial intermediary, even if no VA-related transactions as defined above could be identified in the reported accounts.

[195] To this end, MROS surveyed the Swiss Financial Market Supervisory Authority (FINMA), the Federal Statistical Office (FSO), the Swiss National Bank (SNB), the State Secretariat for International Finance (SIF), the Federal Tax Administration (FTA) and nine cantonal tax authorities.
[196] See Section 11.1 for a detailed description of the evaluation method.

Not only has there been a significant increase in the number of VA-related SARs, but their share of the total number of SARs filed during this period has also risen significantly.

Sharing of VA-related information with foreign reporting offices has also intensified, as has MROS forwarding of VA-related information to Swiss law enforcement agencies. Since 2020, the law enforcement agencies have also recorded a significant increase in the number of criminal charges and proceedings involving VAs.

7.2.1 Increase in VA-related SARs

In 2020, 5.8% of all SARs were classified as VA-related. By 2022, this proportion had more than doubled to 13.8%. In the entire period from 2020 to 2022, 10% of all SARs were VA-related.

	2020	2021	2022	2020–2022 (total)
SARs (per year)	5,334	5,964	7,639	18,937
VA-related SARs (percentage per year)	312 (5.8%)	499 (8.4%)	1,056 (13.8%)	1,867 (9.9%)

Figure 16: VA-related SARs with respect to total SARs each year

The relevance of this information needs to be seen in perspective. For example, the findings on SARs received on the use of VAs for ML/TF purposes refer only to the SARs *received* from FIs. It remains unclear to what extent the findings drawn from this are representative of the actual use of VAs for ML/TF purposes in Switzerland. In particular, given that VA transactions can be processed directly between users and are therefore not fully classified as financial intermediation – and only then subject to the AMLA – it is likely that a significant number of cases remain unreported.

7.2.2 Intensification of FIU information exchange

Another aspect of the work of MROS is the sharing of information with foreign FIUs. There are two ways in which foreign FIUs can contact MROS: through information requests submitted to MROS from abroad, or through *spontaneous information* which are sent without being requested on the assumption that they might be relevant to Switzerland. This exchange also makes it possible to assess the extent to which the information is VA-related, using the same method as for the SARs.

	2020	2021	2022
FIU information exchanges (spontaneous or upon request)	1,397	1,312	1,557
Of which VA-related	18	42	132
Percentage VA-related	1.3%	3.2%	8.5%

Figure 17: FIU information exchanges related to VAs from 2020 to 2022

Since 2020, the prevalence of VA-related information exchanges with foreign FIUs has increased, albeit to a lesser extent than the volume regarding the SARs received by MROS during this period. By 2022, at least one in twelve foreign information reports received by MROS was VA-related.

7.2.3 Increase in the transmission of VA-related information to law enforcement agencies

MROS analyses the information contained in all SARs received and decides whether information from these reports should be forwarded to a Swiss law enforcement agency. Given the growing number of VA-related SARs, law enforcement agencies, in particular the cantonal public prosecutors of Aargau, Bern, Geneva, Vaud and Zurich as well as the Office of the Attorney General of Switzerland, are increasingly confronted with the transmission of VA-related information. However, it can be seen that almost all cantonal public prosecutors have received VA-related information since 2020 and that this is a growing trend.

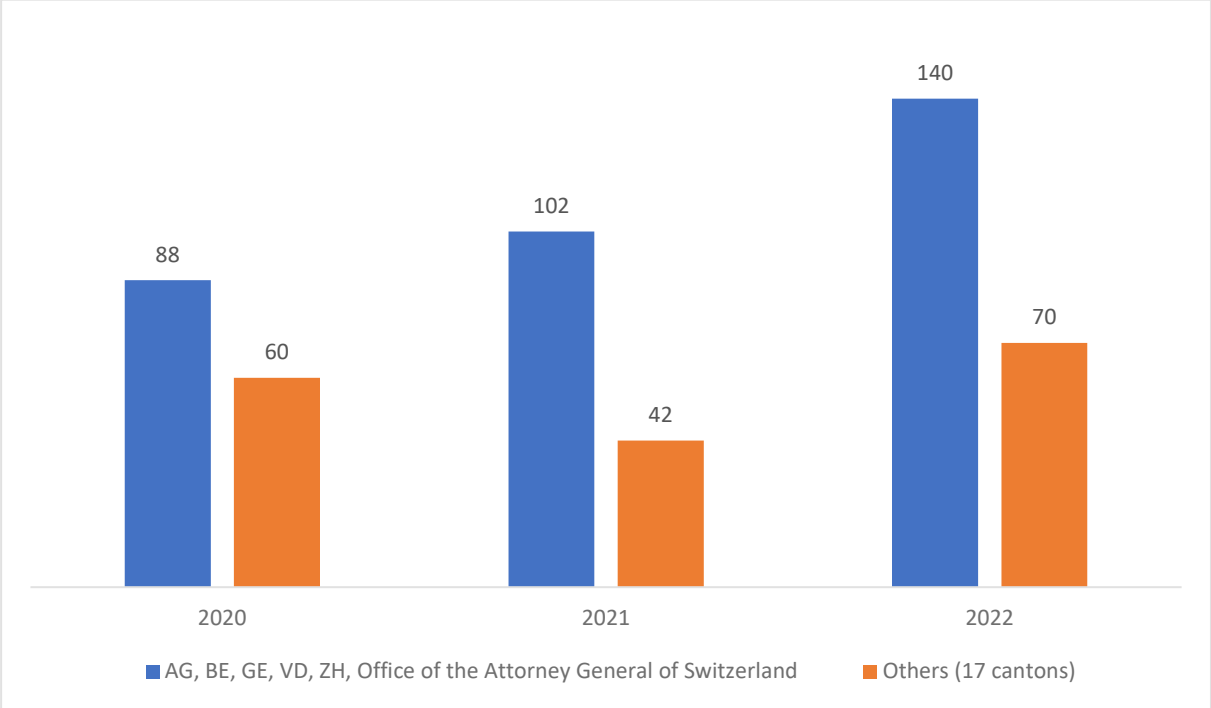

Figure 18: Number of times VA-related information was forwarded to cantonal public prosecutors and the Office of the Attorney General of Switzerland, 2020–2022

7.2.4 Increase in VA-related criminal proceedings

According to the information received, the majority of Swiss police forces and public prosecutors do not systematically record the use of cryptocurrencies in their criminal proceedings, so there is no national overview in this regard. However, between 2020 and 2022, the number of digital crime offences recorded by the police across Switzerland increased by

37% to 33,345 (91 per day).[197] Of these offences, 89% (29,677) were classified as 'cyber-economic crime' and 67% (22,207) under the subcategory 'cyber-fraud'.[198] Based on discussions with various law enforcement experts, it can be assumed that these crimes often involve the use of VAs in one form or another.[199] Some cyber-economic crimes – such as ransomware, extortion and online investment fraud – almost always involve VAs at some stage.[200]

Various surveys and analyses of data from Swiss law enforcement agencies also seem to confirm a significant increase in the number of VA-related criminal proceedings in Switzerland since 2018. Moreover, the surveys also suggest that the sums involved are significant and have been on an upward trend since 2018. Finally, most of the offences that are at the forefront can be classified as cyber-economic crime. This means that these crimes also pose the greatest risk of downstream money laundering related to the criminal use of VAs.

The responses to the survey of Swiss law enforcement agencies seem to confirm this trend.[201] For example, since 2018, seven cantonal public prosecutors have conducted a total of 119 criminal proceedings in which VAs played a key role. More than a third (45) of these criminal proceedings concerned crimes related to money laundering, its predicate offences, organised crime or terrorist financing. Given that only minimal feedback was received, it must be assumed that the actual number of VA-related criminal proceedings since 2018 is significantly higher. In fact, the seven cantonal public prosecutors that responded were the only ones that had any consolidated figures at all. In particular, no data were available from the public prosecutors of some of the more densely populated cantons.

Only six cantonal public prosecutors were able to provide information on the offences involved in these cases. Apart from violations of the Narcotics Act, the offences involved are almost exclusively in the area of cyber-economic crime, most frequently fraud (Art. 146 SCC) and computer fraud (Art. 147 SCC). Only three cantonal public prosecutors were able to provide specific information on the amounts involved in VA-related criminal proceedings. The total amount involved in VA-related criminal proceedings conducted in these three cantons since 2018 was over CHF 130 million (of which, however, over CHF 100 million related to only one case). The annual totals have trended upwards since 2018. Despite the fact that only three cantonal public prosecutors provided details on the amounts involved, additional analyses of data from other cantons paint a similar picture.

This can also be concluded from an analysis of the PICSEL database (*Plateforme d'Information de la Criminalité Sérielle En Ligne*). PICSEL is an intercantonal database for recording criminal complaints involving digital crime. It was set up to centrally record incidents and loss amounts and to help prioritise and coordinate law enforcement efforts in the fight against cybercrime. Criminal complaints filed with the participating cantonal law enforcement agencies in relation to cybercrime are recorded in PICSEL.[202] Criminal complaints are classified by event (e.g. ransomware, online investment fraud, romance scams) and the amount of loss (e.g. cryptocurrency stolen from a wallet, fiat money stolen from an online bank account through phishing or hacking, payment using prepaid cards in the case of ransomware

[197] Earlier figures for digital crime are not available, as these were published for the first time in the 2020 report on police crime statistics. See Federal Statistical Office (FSO), *Police Crime Statistics – 2021 Annual Report (de)*, March 2022, p. 58. Also: Federal Statistical Office (FSO), *Police Crime Statistics – 2022 Annual Report (de)*, March 2023, p. 60.
[198] Ibid. (2022 Annual Report), p. 58 – 60.
[199] This category includes a total of 12 different offences (CEO fraud, fraudulent internet shops, online investment fraud, romance scams, etc.), ibid., p. 60.
[200] See also e.g. National Security Centre (NCSC), *Semi-Annual Report 2022/2 (July–December)*, May 2023, p. 9.
[201] The Federal Criminal Police conducted the survey between February and April 2023 on all cantonal police forces and public prosecutors.
[202] The database has been operational since April 2021 and is currently being used by nine cantons: Aargau, Fribourg, Geneva, Graubünden, Jura, Neuchâtel, Ticino, Vaud and Valais. At least one more canton will join soon (last update May 2023).

attacks). There is also a pilot project similar to PICSEL but which is dedicated exclusively to online investment fraud and involving all Swiss cantons.

The participating cantons use the PICSEL database in different ways. For example, some cantonal law enforcement agencies do not record data on the criminal complaints they receive, but instead use the platform only for research and cooperation with their counterparts in other cantons. Although these data provide only a partial overview, an evaluation effectively demonstrates that there has been an increase in the prevalence of cybercrime cases involving the use or misappropriation of VAs in Switzerland. Compared to other forms of payment, the use and misappropriation of VAs has increased significantly since 2020, not only in absolute terms, but also as a proportion of the total loss amount. Between 2020 and 2021, the amount of financial loss suffered by claimants as a result of VA theft tripled. Compared to 2020, in both 2021 and 2022 there was a significant increase in the volume of stolen VAs as a percentage of the total loss amount of all criminal complaints registered in PICSEL.

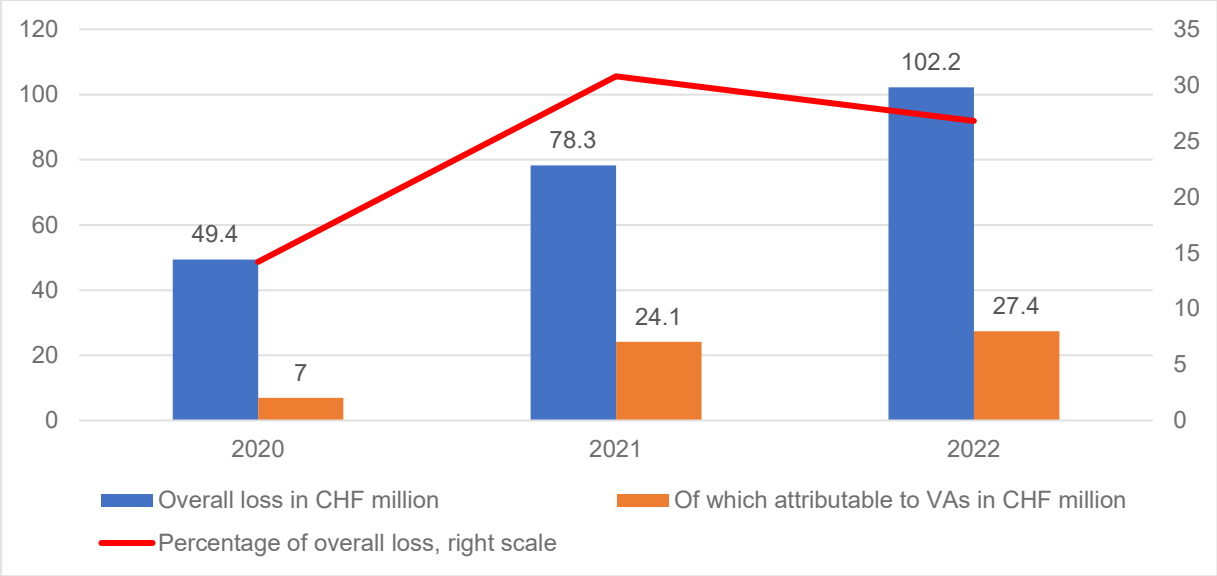

Figure 19: Nominal and percentage increase in VA-related loss amounts from reports filed in PICSEL with respect to 2020

In recent years, the use or misappropriation of VAs in connection with online investment fraud appears to have increased the most. Although it already accounts for around a quarter of the total loss amount in 2020, it rises to more than half of the total loss amount by the end of 2022.

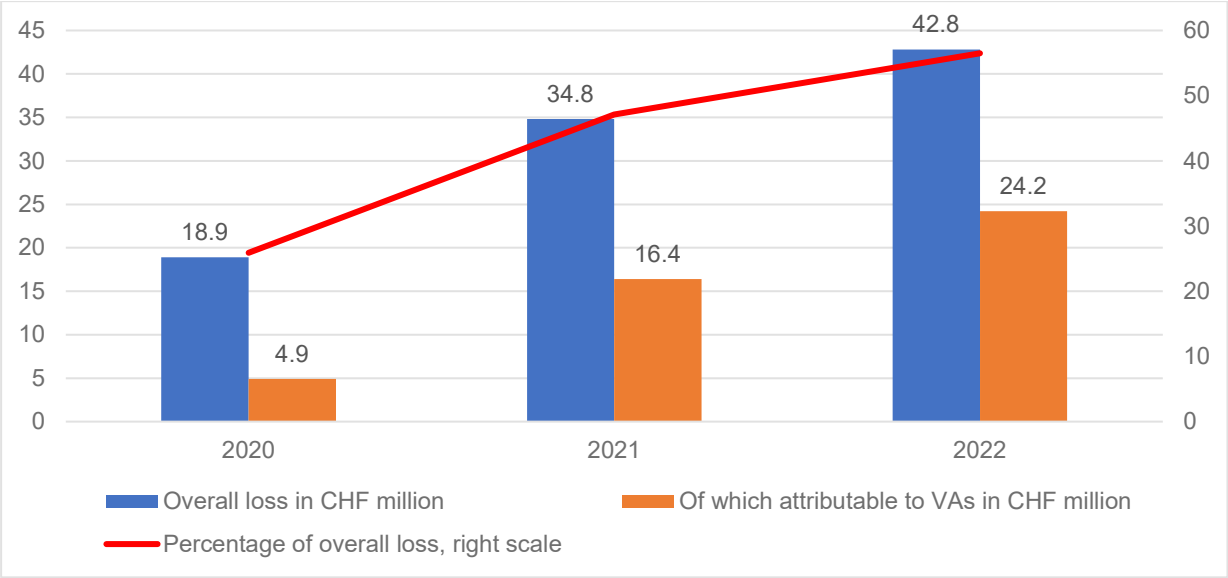

Figure 20: Nominal and percentage increase in VA-related loss amounts related to online investment fraud with respect to 2020

Although it is not possible to make a conclusive assessment on the basis of the figures presented here, it seems clear that the criminal use of VAs in Switzerland has risen since 2018.

According to the law enforcement agencies interviewed, money laundering as a downstream offence was a logical consequence of most of the cases investigated, as VAs obtained through criminal activity have to be laundered at some point. Nevertheless, there does not appear to be any consolidated evidence of downstream money laundering activities in relation to the crimes investigated by law enforcement agencies, whether the proceeds were in fiat money or VAs. However, the there is a lack of substantiated information on these money laundering activities since the investigative focus of law enforcement agencies is usually directed at solving the reported crimes and potentially recovering the victims' stolen funds, while the alleged perpetrators are usually located abroad and their identities cannot be determined in most cases. By using blockchain analytics and contacting foreign FIs engaged in VASP activities, it has been possible to identify isolated indications of VA money laundering networks in Eastern Europe and the Middle and Far East, which is consistent with other research findings.[203]

7.3 Main threats

When submitting an SAR, the reporting FIs inform MROS of the predicate offences they suspect in connection with the persons or accounts reported.[204] Even where the suspected predicate offences do not correspond to the results of the MROS analysis, a quantitative evaluation of suspected predicate offences in VA-related SARs can help to identify potential threats posed by the use of VAs for criminal purposes in general and for ML/TF in particular.

[203] "The leaders of LockBit claim that they primarily use Bitcoin exchanges in Hong Kong and China to launder the proceeds. The view is that China's hostile relationship with the US makes it safer to conduct money laundering operations." See Schurter Daniel, *Das ist die gefährlichste Hackerbande, die auch in der Schweiz wütet*, 23 January 2023.

[204] Note: Reporting FIs may report more than one suspected predicate offence per SAR.

7.3.1 Fraudulent use of VAs as the most serious threat

The number of VA-related SARs was not high in the 2018 risk analysis. The most serious threat identified on the basis of the SARs was related to the issuance of VAs: the majority of cases and suspected predicate offences identified by the reporting FIs related to fraudulent initial coin offerings (ICOs). ICOs continued to be a focus of the supervisory authorities in 2018/19, as indicated in the relevant FINMA guidelines.[205] The SARs submitted to MROS since 2020 are much more diverse in terms of the suspected predicate offences, but the reported cases no longer indicate a particular risk in the area of issuance. Much more frequently, services in connection with the custody or exchange of VAs play a central role in the reported case, which appears suspicious to the FIs and therefore prompts them to submit a corresponding SAR to MROS.

The few SARs received by MROS between 2015 and 2019 from FIs engaged in VASP activities were limited to a small number of suspected predicate offences, in particular fraud, document forgery and computer fraud.[206] These predicate offences were also frequently suspected in the years 2020 to 2022 – even more frequently than average compared to the total number (see Figure 21).

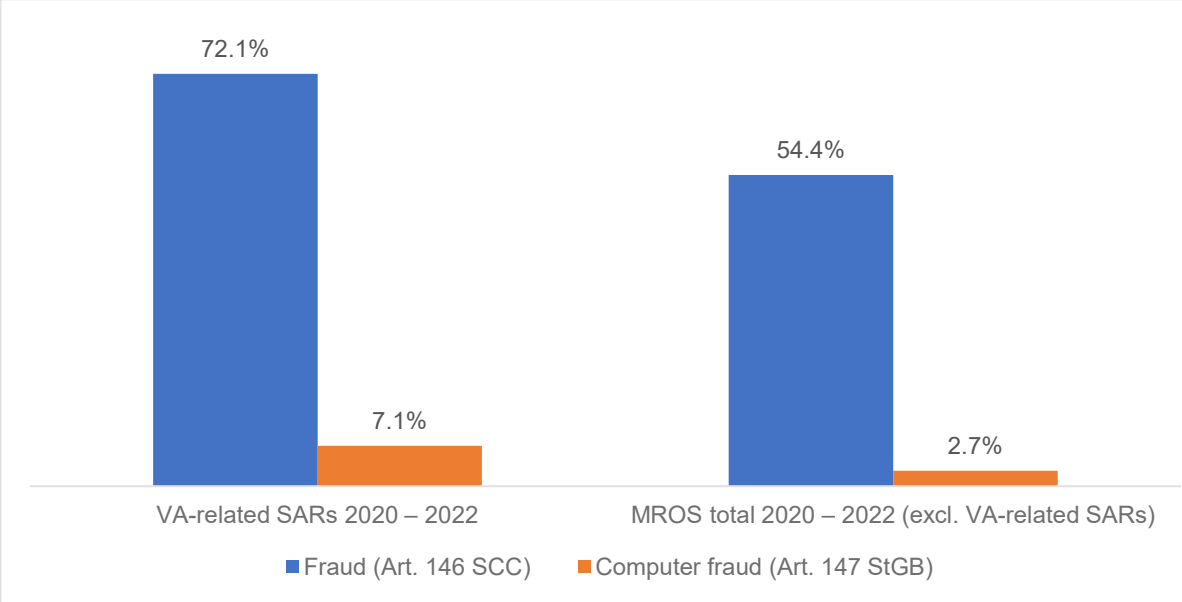

Figure 21: Fraud and computer fraud are suspected as predicate offences in VA-related SARs with a disproportionately high frequency (2020–2022)

It remains unclear whether the over-representation of these two predicate offences is due to the fact that they were actually committed most frequently or whether they were more easily detected and reported by the reporting FIs than other predicate offences. Nevertheless, the fact that these two predicate offences are suspected more often in VA-related SARs than in non-VA-related SARs is consistent with the observations made by FIUs in other countries.[207] On the one hand, the suspected perpetrators seem to take advantage of the ease and speed of switching from VA to fiat money flows (and vice versa) in order to complicate or at least

[205] See Swiss Financial Market Supervisory Authority (FINMA), *Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs), February 2018.* Swiss Financial Market Supervisory Authority (FINMA), *Supplement to the guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs)*, September 2019.

[206] This is consistent with the conclusions of the first CGMF report on VAs in 2018. See CGMF, *Risk of money laundering and terrorist financing posed by crypto assets and crowdfunding*, October 2018, p. 24 – 27.

[207] See e.g. Swedish Police Authority, *The Financial Intelligence Unit Annual Report 2021*, May 2022, p. 15f. Financial Intelligence Unit (Liechtenstein), *Annual Report 2021*, April 2022, p. 11.

delay the tracing of the financial flows from which they benefit. At the same time, they also seek to exploit the vulnerability of VAs to make it more difficult for criminal law enforcement agencies to freeze or seize VAs, usually by transferring VAs to non-custodial wallets. Numerous criminal networks appear to have recognised this vulnerability and are exploiting it for various crimes. VA-related SARs with suspected predicate offences in this area tended to be related to online investment fraud, Ponzi schemes and money mule cases – or a combination of these phenomena. The accounts reported tended to be wire transfer accounts that the account holders knowingly or unknowingly made available to suspected fraudsters.[208] Where computer fraud was also suspected as a predicate offence, it usually involved fraudulently initiated payments (through hacking, social engineering and phishing) transferred from accounts with traditional FIs (domestic or foreign) without VASP activities to accounts with FIs (domestic or foreign) with VASP activities. The aim of the alleged perpetrators appears to have been to convert the victim's fraudulently obtained fiat money on a VASP platform into VAs as quickly as possible and to transfer them to a non-custodial wallet.

Whenever Swiss FIs engaged in VASP activities filed such reports, fraud or computer fraud was suspected as the predicate offence, also in combination with document forgery as the suspected perpetrators often opened a VASP account with stolen or forged identity documents in order to conceal their own identity. In a number of cases, MROS found that although the FIs involved in VASP activities had the identity documents required to open a business relationship, the individuals themselves did not have access to these accounts due to various fraud schemes. However, with a few exceptions, these reports concerned relatively small amounts of just a few hundred or a few thousand Swiss francs.

Threat 6

Threats in connection with the novelty effect and users' inexperience (identified in 2018, upgraded in 2023)[209]

Since 2018, the number of users of VAs has soared. VAs are frequently in the media and investors are, or should be, aware of the risks involved. Nevertheless, the prospect of high returns may cause many people to let their guard down, for example when choosing a financial service provider for their investments or when entering their personal data online. Both MROS information and available law enforcement data suggest that, compared to 2018, many more people are falling victim to VA-related scams that exploit the inexperience of new users. The threat level has therefore increased.

Threat 7

VA use for phishing (identified in 2018, upgraded in 2023)[210]

In some cases, fraud victims are simply persuaded to transfer money by the perpetrators over the phone or by text message. However, phishing is also very common. Compared to 2018, the number of such cases is significantly higher – simply because of the greater use of VAs. The threat level has therefore increased.

[208] Criminals also recruit people online to act as 'money mules', mainly through attractive job offers. Money mules are supposed to transfer criminal money to the perpetrators (who are usually abroad) and make their personal accounts available for this purpose. Anyone involved in such 'business' can be prosecuted for money laundering. See Swiss Crime Prevention, *Money Mules*, last visited in May 2023.
[209] CGMF, *Risk of money laundering and terrorist financing posed by crypto assets and crowdfunding*, October 2018, p. 24 – 26.
[210] Ibid., p. 30.

7.3.2 New threats meaning a wider range of risks

As the number of VA-related SARs has grown over the years, the range of predicate offences suspected by the reporting FIs has also widened.

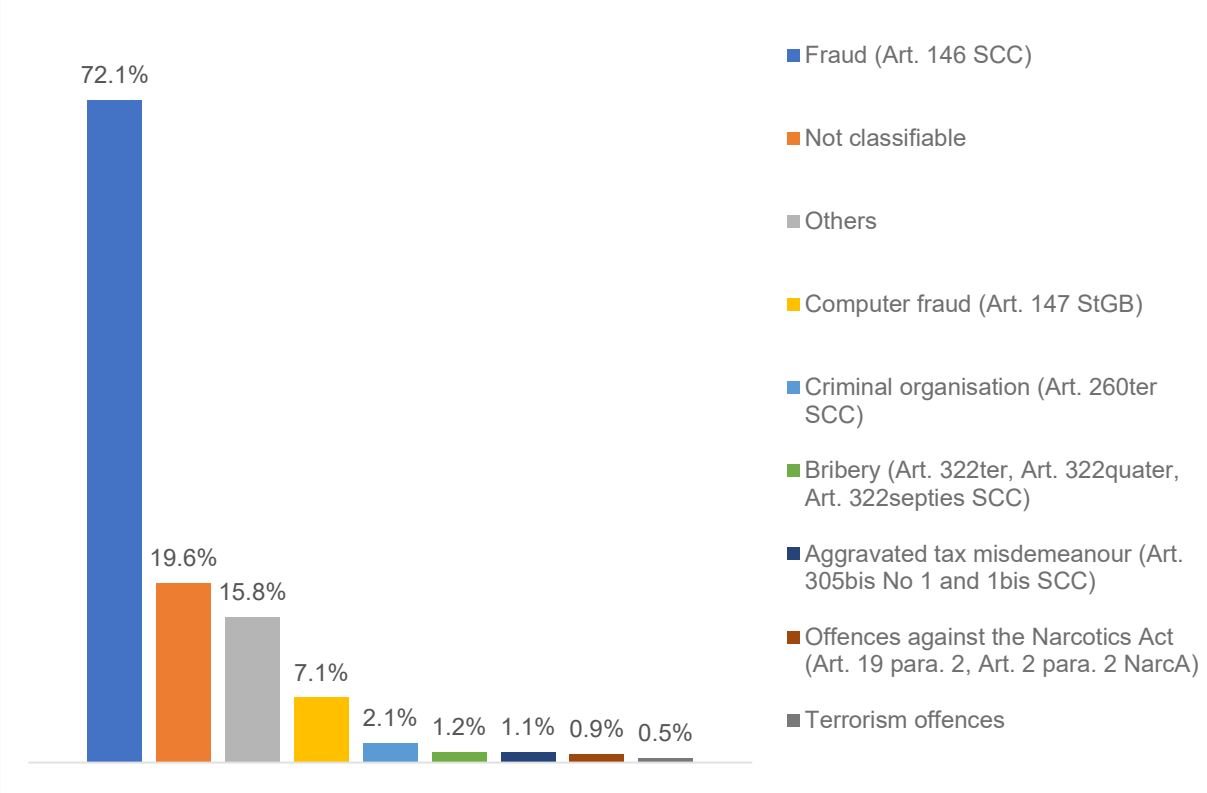

Figure 22: Illustration of the diversity of suspected predicate offences in 1,867 VA-relevant SARs (2020–2022). The predicate offences grouped under 'Other' are listed in Section 11.2 in the Annex.[211]

As shown in Figure 22, although some individual predicate offences are suspected relatively rarely, together they cover a wide range of offences, which also points to a broader criminal use of VAs in payment transactions. For example, the category 'Other' includes almost 30 other predicate offences, suggesting that VAs are now being misused for ML/TF purposes in a wide variety of forms and schemes.[212] Accordingly, the VA-related SARs also included reported facts containing risk indicators that would normally be found in AML/CFT efforts in traditional payment transactions and that point to 'conventional' ML/TF schemes. These include, for example, the involvement of offshore companies in relatively simple commercial transactions (e.g. import of food products), which is unnecessary from a business perspective, or the counterparty's involvement in a complex network of companies whose high transaction volumes were justified by mutual loan agreements (sometimes denominated in VAs) (see Typology 1). This impression is reinforced by analyses conducted by MROS, which often identifies other offences than those predominantly reported by the reporting FIs (e.g. fraud). These tend to be among the more serious forms of crime.

[211] Note: Reporting FIs may suspect several offences and therefore several predicate offences for each SAR submitted. The percentage of suspected predicate offences can therefore be calculated, with the sum of all shares also exceeding 100 per cent. Similarly, offences related to 1.) terrorism financing (Art. 260^{quinquies} SCC) and 2.) Art. 2 of the Federal Act on the Proscription of Al-Qaeda, Islamic State and Associated Organisations are summarised under 'offences in the field of terrorism'.

[212] The complete list of predicate offences suspected in VA-related SARs can be found in Section 11.2 in the Annex.

Typology 1

Network of foreign shell companies buys VAs to allegedly launder fiat money

When opening a business relationship with a foreign company, the reporting financial intermediary noticed that the company's business model and the wording it used were very similar to those of another previously registered corporate client. The financial intermediary then asked the prospective new client for additional documentation on the origin of the funds. The latter provided bank statements and invoices for services allegedly provided. These appeared plausible to the financial intermediary, who proceeded to open the business relationship. In the following days, the new client transferred fiat money from a foreign account to the newly opened account in several transactions, bought VAs with this and immediately transferred them to a non-custodial wallet. In the same month, the reporting financial intermediary received a similar request to open a business relationship from a third company located in the same country as the other two. Again, further documentation on the origin of the funds was requested, but the documentation provided was unsatisfactory. When asked again, the prospective new client did not respond. On closer inspection, the financial intermediary discovered that two of these companies were using the same address. Further anomalies were then found with all three companies in question: some of the client identification forms were not filled in correctly, and the websites looked suspicious, as if they had been set up ad hoc. Further attempts to contact all three companies were unsuccessful. The resulting doubts about the origin of the assets in question prompted the financial intermediary to file a report with MROS.

There were also isolated indications of large-scale drug trafficking and terrorist financing in VA-related reports (see Typology 2).

Typology 2

Suspected terrorist financing with VAs

A financial intermediary offered its customers a crypto ATM service. This service allows Swiss francs to be deposited in an ATM and then exchanged for Bitcoin by the financial intermediary offering the service. For the exchange of Swiss francs into Bitcoin, the financial intermediary partnered with a VA trading exchange in a neighbouring country, which sent the Bitcoin purchased by customers to the Bitcoin address provided by them. This exchange alerted the financial intermediary to the fact that a Bitcoin transaction worth around CHF 100 at the time had been sent from such an address to a Bitcoin address belonging to Al-Qaeda. This Bitcoin address had been the subject of an investigation by a public prosecutor in a third country. In this case, the fact that FIs in the VASP sector are able to track transferred VAs even after they have been handed over to the customer led to the discovery of the suspicious payment. This opens up new possibilities for monitoring VA transactions compared to traditional payment traffic.

The remitter reported to MROS had managed to remain largely anonymous by making the deposit at the crypto ATM, where he only had to provide contact details. However, this information was sufficient for MROS to identify the remitter. Investigations revealed that the individual in question had attracted attention four years earlier by sharing violent jihadist propaganda on social media. In addition to the aforementioned transaction, the transaction analysis identified a further 17 transactions with a total value of around CHF 3,000 to the same Bitcoin address. According to a blockchain analytics tool, the address is said to belong to the Al-Qaeda Bitcoin Transfer Office.

Threat 8

Terrorist financing by means of VAs (identified in 2018, unchanged in 2023)[213]

Since 2018, several VA-related SARs have been submitted to MROS in which the reporting FIs suspected offences related to terrorism.[214] While data from the blockchain analytics company Chainalysis suggest that the amounts sent to known addresses of terrorist organisations have decreased since 2020, it is not clear whether this is actually the case.[215] However, it is well known that in the case of terrorist financing, even small amounts are sufficient to cause significant damage. Overall, there is no evidence of a significant change in the threat situation compared to 2018.

One SAR also provided evidence of the involvement of actors in suspected money laundering activities involving VAs where it can be assumed that these activities were intended to finance the arms programme of a foreign state subject to UN sanctions (see Typology 3).

Typology 3

Suspected proliferation financing with VAs

A Swiss financial intermediary engaged in VASP activities was used to launder cryptocurrencies stolen in a cyberattack on a foreign crypto exchange. The reporting financial intermediary's platform was used by the perpetrator to exchange the stolen cryptocurrencies for another cryptocurrency in order to cover their tracks. According to various experts in the field of blockchain analytics, this attack could be attributed to a group of hackers with links to North Korea.

Threat 9

Proliferation financing by means of VAs (identified in 2023)

According to the information available to MROS, Swiss FIs engaged in VASP activities are also at risk of being misused as hubs for financial flows that serve proliferation financing.

Some of the SARs contained references to international corruption scandals. Politically exposed persons (PEPs) were also identified among the business partners, beneficial owners or counterparties of business relationships reported in VA-related SARs. In other SARs, MROS identified natural persons or legal entities who, according to press reports or information from certain criminal proceedings, were linked to criminal organisations.

An evaluation of 12 VA-related cases that led to investigations by the Federal Criminal Police (FCP) over the past 10 years and ultimately to the opening of proceedings also shows that VAs are not only used for cybercrime offences in Switzerland. The FCP is responsible for investigating all offences that fall under federal jurisdiction. Although the investigated cases

[213] CGMF, *Risk of money laundering and terrorist financing posed by crypto assets and crowdfunding*, October 2018, p. 27 – 28.
[214] The offences relate to 1.) the financing of terrorism (Art. 260^{quinquies} SCC) and 2.) Art. 2 of the Federal Act on the Proscription of Al-Qaeda, Islamic State and Associated Organisations are summarised under 'offences in the field of terrorism'.
[215] Chainalysis, *The 2023 Crypto Crime Report*, February 2023, p. 6.

are relatively few in number and differ in the role of VAs, they all occurred relatively recently, with the oldest of these 12 investigations only dating from 2018.

All of the FCP's investigative departments have by now come across cases involving cryptocurrencies. The scope of the alleged offences once again shows the wide range of possible uses of VAs and the growing diversity of crimes potentially associated with them:

Federal Criminal Police unit involved in the investigation	**Mutual legal assistance, terrorism, international criminal law**	**State protection, criminal organisations**	**White-collar crime**
Offences investigated	• Criminal or terrorist organisation (Art. 260ter SCC) • Federal Act on the Prohibition of Al-Qaeda, Islamic State and Associated Organisations (Art. 2) • Robbery (Art. 140 SCC) • Extortion (Art. 156 SCC) • Misuse of explosives and toxic gases with criminal intent (Art. 224 SCC)	• Counterfeiting money (Art. 240 SCC) • Import, acquisition and storage of counterfeit money (Art. 244 SCC)	• Money laundering (Art. 305bis SCC) • Unauthorised access to data (Art. 143 SCC) • Damage to data (Art. 144bis SCC) • Computer fraud (Art. 147 StGB)
ML methods observed	• Mixing services and privacy wallets • Peel chains • Privacy coins • Chain-hopping • Deliberate use of VASPs with weak or non-existent KYC requirements / use of OTC brokerage services ('nested services')		

Figure 23: Overview of investigations conducted by the Federal Criminal Police in relation to VAs between 2018 and 2022

In its cybercrime investigations, the FCP has observed a recurring theme among the perpetrators: after gaining access to the victim's online bank account through various phishing tactics or Trojans, they make payments to accounts at foreign VASPs, which they have previously opened either in the victim's name (identity theft) or in the name of a previously recruited money mules. The incoming payments are then converted into cryptocurrencies on the VASP platform and, in most cases, immediately transferred to an external wallet. The use of cryptocurrencies thus appears to serve a dual purpose: as a means of laundering funds originally stolen from bank accounts in Switzerland abroad, while at the same time making them more difficult to trace. Conversely, the FCP has also come across a case where a foreign VASP was hacked and the stolen VAs were transferred to a VASP platform in Switzerland to be converted into another cryptocurrency and then immediately transferred out of the platform. Converting one cryptocurrency into another appears to be done for greater concealment, as several different blockchains would have to be analysed for tracing. This tactic, known as chain-hopping, is repeated several times and sometimes combined with other methods of concealment such as mixing, also known as tumbling (see Infobox 4 in Section 7.4.1).

In terrorist financing cases, cryptocurrencies seem to attract both senders and recipients for a variety of reasons. It seems that people who use cryptocurrencies to help finance terrorist organisations assume that their transactions in VAs cannot be traced. At the same time, by publishing their VA addresses on the internet, terrorist organisations can extend their reach and access a much wider potential funding network than if they relied solely on personal contacts for funding. By using non-custodial wallets, these organisations can also protect the cryptocurrency they receive from being frozen and confiscated. The FCP has also observed the same process in cases of ransomware and other forms of extortion.

Finally, the FCP also conducted two investigations into counterfeit money, during which it discovered that cryptocurrencies were being used to buy counterfeit money on the Darknet. In addition to ostensibly 'making' money (e.g. buying a counterfeit fifty euro note for a fraction of its supposed value), this method would provide a means of spending criminally obtained cryptocurrency without having to convert it into fiat via a VASP.

7.3.3 Counterparties and amounts involved

A comparison of the suspected predicate offences and the amounts involved shows that SARs concerning transactions with a high total value (CHF 250,000 or more) cover a wider range of suspected predicate offences (e.g. qualified tax offences, narcotics offences, participation in or support of a criminal organisation) than SARs concerning smaller amounts, where the reporting FIs are more likely to suspect fraud as the predicate offence.

	2020	2021	2022
VA-related SARs from FIs engaged in VASP activities	104	178	143
Of which SARs without VA-related transactions	50	88	75
Of which SARs with VA-related transactions	54	90	68
Total value of VA-related transactions (CHF)	1.8 million	28.5 million	50.5 million
Average value of all VA-related transactions per SAR (CHF)	4,976	32,477	53,618
Median value of all VA-related transactions (CHF)	1,385	3,000	3,500

Figure 24: The amounts involved in SARs from FIs engaged in VASP activities in which suspicious transactions were reported have increased significantly since 2020.

In 2020, MROS received a total of 104 VA-related SARs from FIs engaged in VASP activities. The SARs with VA-related suspicious transactions reported a total value of more than CHF 1.8 million. The average total value reported in each of these SARs was just under CHF 5,000, while the corresponding median value was around CHF 1,385 per SAR. In contrast, FIs engaged in VASP activities reported 178 VA-related SARs in 2021. There were 68 SARs with a total value of CHF 28.5 million, with an average total value per SAR of around CHF 32,477 and a corresponding median at CHF 3,000. In 2022, 143 SARs were submitted to MROS by FIs engaged in VASP activities. In 68 SARs, a direct reference to VAs was established in the transactions, corresponding to a total value of CHF 50.5 million, with an average transaction amount of CHF 53,618 and a median of CHF 3,500. The relatively low median value shows that MROS received a large number of SARs in the years under review involving transactions with a comparatively low total value. The vast majority of these cases involved suspected

fraudulent transfers from accounts held with traditional FIs not engaged in VASP activities to accounts held with FIs engaged in VASP activities. Such cases are often linked to suspected hacking or phishing (computer fraud), where the suspected fraudsters obtain the victims' online banking login details and make a payment from the victim's account to their own. Some of these cases were detected by Swiss FIs engaged in VASP activities because, for example, the fraudsters logged in to different user accounts on the VASP platform using the same IP address, or the same mobile phone number was used for different user accounts and was not registered in the client's country of origin. A recurring pattern was that suspected fraudsters appeared to target cross-border payments in order to complicate or delay the tracing of transaction flows or the freezing and seizing of assets. In such cases, the fiat currency account from which the funds were transferred and the VASP account to which the payment for the purchase of the VAs was made were usually located in different countries. If the account from which the payment was made was held with a Swiss financial intermediary not engaged in VASP activities, the VASP to which the funds were transferred was usually located in another country, and vice versa. If the fraud involved a Swiss financial intermediary engaged in VASP activities, the funds were usually transferred from foreign accounts.

The amounts involved in VA-related SARs from FIs not engaged in VASP activities are significantly lower, as the proportion of VA-related SARs from these FIs *with* VA-related transactions was relatively low. In most cases, the VA-related SARs were identified by certain keywords used by the reporting financial intermediary when describing the facts of the case (e.g. 'Bitcoin' or 'crypto'). Often the reporting FIs referred in general terms to a series of transfers between the reported accounts and those of a VASP, but did not enter the details of the transactions on the electronic form provided, so that they could not be quantified. Many cases were also found where the reporting FIs actually mentioned the relevance to VAs in their written report (e.g. their client was active in the VA sector), but did not recognise the transactional links between the account they reported and the account of a VASP and therefore did not refer to the transactions in question on the electronic form provided.

The figures below should therefore be regarded as an absolute minimum; the actual amounts are likely to be significantly higher.

	2020	2021	2022
VA-related SARs from FIs not engaged in VASP activities	208	321	913
Of which SARs without VA-related transactions	166	258	835
Of which SARs with VA-related transactions	42	63	78
Total value of VA-related transactions (CHF)	1.6 million	15 million	7.4 million

Figure 25: The amounts involved in VA-related SARs from FIs not engaged in VASP activities, 2020–2022

The Swiss financial centre is a world leader in cross-border wealth management for private individuals. The counterparties of the business relationships reported to MROS are therefore often domiciled abroad. At least 46% of the counterparties reported between 2020 and 2022 were either legal entities domiciled abroad or natural persons of foreign nationality (see first bar in Figure 26).

An even higher proportion of international clients can be seen in the SARs of FIs engaged in VASP activities: in at least 69% of these SARs, the reported counterparties were natural persons of foreign nationality or legal entities domiciled abroad. In addition, the reported counterparties were natural persons in 72% of the cases, which seems to indicate that the reporting FIs engaged in VASP activities are primarily active in retail banking.

The counterparties reported in SARs by FIs not engaged in VASP activities are more or less proportional to the MROS total for the last three years in terms of their status (natural persons or legal entities) and origin (nationality for natural persons, domicile for legal entities; see first and second bar in Figure 26). The only clear deviation in the distribution is the relatively high share of natural persons with Swiss nationality as counterparties (33%). There are several plausible reasons for this. For example, in addition to international wealth management, these intermediaries tend to focus on retail clients in Switzerland. Several surveys and studies indicate that Swiss retail clients have increased their use of VAs in recent years – a trend that was probably less pronounced in the cross-border wealth management business of these FIs. Another possible explanation is that the counterparties reported were often suspected money mules or victims of fraud – both patterns are more likely to be found in retail banking than in international wealth management.

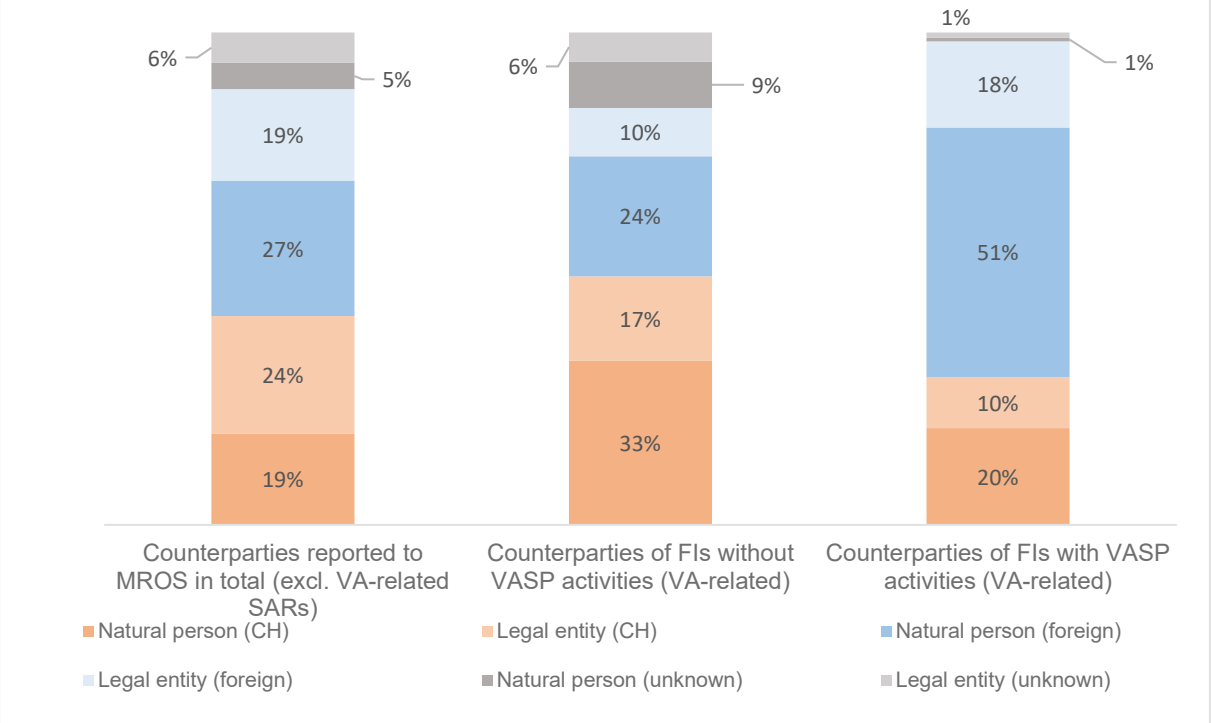

Figure 26: Counterparties reported in the 1,867 VA-related SARs (2020–2022) compared to counterparties reported in all SARs in the same period (minus the 1,867 VA-related SARs). More than half of all reported counterparties of business relationships with FIs engaged in VASP activities are natural persons of foreign nationality.[216]

7.4 Vulnerabilities in regard to law enforcement in the VA sector

VAs present additional opportunities and challenges for law enforcement agencies. In general, the main challenges are related to resources, training, technology and legal aspects. More specifically, there are challenges in tracing VA transactions, identifying the owner of a wallet, seizing a wallet and confiscating the VAs it contains, and gathering information and evidence abroad. Opportunities lie in blockchain analytics and in closer and more streamlined national and international cooperation.

[216] Note: In the case of natural persons with dual nationality, only the first or oldest information stored in the MROS database was taken into account. The higher the number of natural persons with dual nationality among reported counterparties, the less meaningful the chart is with regard to the nationality data of the natural persons.

7.4.1 Solving crimes in the VA sector

VAs give law enforcement agencies the advantage of being able to trace a person's financial activities on the blockchain in real time. In theory, blockchain technology makes it possible to trace both the origin and the destination of VAs. This is particularly important for evidence purposes: for example, if a crime is committed abroad and the funds are laundered in Switzerland. It is crucial to be able to link the act of money laundering to the predicate offence. This can be facilitated with transparent blockchain payments, as in this case the transactions are publicly available.

In order to be able to carry out effective blockchain analytics independently, it is necessary to acquire special tools and knowledge in this area. Several recent international cases in which VAs worth billions of dollars have been seized by law enforcement agencies – even if the related crimes were committed many years ago – demonstrate the value of investing in developing such skills.[217]
A survey of 27 Swiss police authorities shows that more than half of the respondents have at least one tool for performing blockchain analytics (as of the end of April 2023).[218] However, the vast majority of the other half stated that they had indirect access to such tools (see NEDIK in Section 7.4.2). Only two authorities stated that they neither had (indirect) access to tracing tools nor did they intend to acquire such a tool. This shows that the Swiss law enforcement agencies have recognised the need for action in this area and are in the process of acquiring the necessary tools.

However, the majority of the 27 authorities surveyed also indicated that there are significant challenges in using blockchain analytics, particularly in relation to off-chain and layer 2 transactions. On the other hand, parallel to the progress in tracing VA transactions using blockchain analytics tools, concealment techniques have also become more sophisticated (see Vulnerability 10). There have also been cases where blockchain analytics have provided little or no value. Consequently, the challenges in this area will not be overcome by simply acquiring such tools. A high level of expertise, continuous training and further development of analytical tools are necessary for law enforcement agencies to keep up in the race between encryption and decryption techniques.

In the absence of consolidated data from cantonal and municipal police authorities, the Federal Criminal Police (FCP) and MROS were asked which techniques they had encountered in their work to date. These included peel chains, mixers, chain-hopping, privacy coins, wash trading and the use of VASPs with weak or non-existent KYC requirements (see Infobox 4).

Infobox 4

Concealment techniques

Mixing services and privacy wallets: Mixing services, also known as tumblers, can be used to mix VAs 'tainted' by criminal activity with other 'clean' VAs. This is usually done by pooling VAs from different sources for a certain period of time with the aim of making them indistinguishable. Privacy wallets (e.g. Wasabi Wallet) use built-in anonymisation techniques such as CoinJoin to achieve this mixing effect for all VAs stored on them.

[217] Chainalysis, *Crypto Money Laundering: Four Exchange Deposit Addresses Received Over $1 Billion in Illicit Funds in 2022*, 26 January 2023.
[218] Note: In addition to municipal and cantonal police forces, the Swiss Police Institute and Swiss Crime Prevention SCP were also surveyed.

Peel chain: A long series of transactions created by splitting large amounts into smaller amounts at addresses used to disguise the origin or destination of a transaction flow. Given the small amounts of money involved in each transfer, the receipt of such funds on exchanges is less likely to raise alarm.

Privacy coins: Some cryptocurrencies (e.g. Monero) were specifically designed to prevent transactions made with them from being transparent on the blockchain – meaning that transactions cannot be traced.

Chain-hopping involves moving VAs from one blockchain to another – often in rapid succession and multiple iterations, using different blockchains – making them harder to trace.

Wash trading: This technique involves 'selling' VAs to oneself or to accomplices by transferring VAs back and forth between wallets. This artificially creates a transaction history and gives the impression that the VA in question (e.g. a particular NFT or cryptocurrency with low trading volume and low market capitalisation) is more in demand than it actually is, which can also artificially inflate its value. There are several reasons why wash trading of VAs lends itself well to money laundering. For one thing, it can be used to disguise the origin of assets based on a long transaction history. Also, it can be used to increase the plausibility of the origin of the assets or to increase the amount originally involved in the crime.[219]

Use of VASPs with weak or non-existent KYC requirements (mostly 'nested services'): Some platforms are located in jurisdictions that do not fully implement international AML/CFT standards. Many services used by criminals to convert VAs into fiat money (fiat off-ramps) are OTC (over-the-counter) brokers. These use the large VA trading exchanges to tap into the liquidity and trading pairs of the larger service providers. This is why they are also called 'nested services', as the addresses they use can only be assigned to the major venues in the initial stages of investigation. Most OTC brokers are well-known, reputable firms. However, on-chain data obtained by blockchain analytics companies suggest that a small group of them are facilitating the lion's share of money laundering involving the conversion of VAs into fiat money.[220]

If a wallet linked to a criminal activity has been identified and the incriminated VAs are still on the wallet, seizing the VAs on the wallet is also a major challenge. If the VAs associated with the criminal activity are on a custodial wallet, it is possible to access the wallet through the financial intermediary or VASP that manages the wallet and holds the private key. This is subject to law enforcement agencies being able to contact the VASP and also the latter's willingness to cooperate. In several cases investigated by the FCP, it was possible to seize VAs on a custodial wallet.

However, if the VAs in question are on a non-custodial wallet, only the actual owner of the wallet has the private key (or several people in the case of a multisig wallet). In this case, it is much more difficult for law enforcement agencies to access the wallet, seize the VAs and thus prevent possible future transactions. However, a case investigated by the FCP has shown that, in the right circumstances, it is possible to seize VAs even on a non-custodial wallet.

Threat 10

[219] Chainalysis, *Crime and NFTs: Chainalysis Detects Significant Wash Trading and Some NFT Money Laundering In this Emerging Asset Class*, 2 February 2022.
[220] Wired Magazine, *Most Criminal Cryptocurrency Funnels Through Just 5 Exchanges*, 26 January 2023. Europol, *Bitzlato: senior management arrested*, 23 January 2023.

Transaction anonymity and difficult identification of beneficial owners (identified in 2018, unchanged) [221]

The 2018 sector report notes that the risk associated with VAs is similar to that of cash, in terms of anonymity (or pseudonymity). However, the threat posed by VAs is heightened by the transaction speed and mobility enabled by such technology.

Since 2018, the tools used by blockchain analytics companies have become much more efficient and now include, for example, the ability to automatically detect certain concealment techniques and transaction patterns. A number of cases show that using these tools and working with blockchain analytics companies can be fruitful (see Sections 8.2.2 and 8.2.4). At the same time, however, efforts within the crypto community to secure and expand the means of concealment and preservation of anonymity should not be underestimated. The efforts of these two opposing interest groups can be seen as a kind of arms race, the outcome or winner of which remains to be seen. This threat has therefore not changed significantly since 2018.

7.4.2 National and international cooperation

Another challenge of a technological nature – and one of the main reasons for developing the PICSEL database – is the detection of connected cases (series of offences). A survey of Swiss police authorities revealed that there was a degree of support for greater sharing of data and information between themselves in order to identify a series of related offences.

Typology 4

Detection of an organised fraud

A Swiss financial intermediary engaged in VASP activities offers its customers the possibility of purchasing VAs via its app. The VAs can be paid for using credit cards or other electronic means of payment such as Apple Pay or Google Pay. The financial intermediary was contacted by a foreign law enforcement agency and informed that a suspected fraud victim had filed a complaint because his credit card information had been used without his knowledge to purchase VAs on the financial intermediary's platform. The financial intermediary then submitted an SAR to MROS. However, the SAR contained very little information that was useful for MROS to trace and follow up the reported payment flows and to link them to existing information in the MROS database. The enclosed letter from the foreign law enforcement agency contained the name of the alleged fraud victim, but no business relationship had been established with the financial intermediary in that name. The financial intermediary also did not have the full credit card details of the fraud victim, as payment for the VAs supplied by the financial intermediary was made indirectly via a payment processor. He was only able to provide MROS with the first six and last four digits of the credit card used. The reporting financial intermediary also had little information about his 'client', who was obviously not the same person as the foreign fraud victim. With no customer details (name, address, date of birth, etc.), the financial intermediary could only tell MROS from which IP address and with which mobile phone model the suspected fraudster had logged into the financial intermediary's app. Immediately after the amount was debited from the victim's credit card, the VAs purchased were transferred to a VA address over which the financial intermediary had no control and could therefore not block (non-custodial wallet). The analysis carried out by MROS

[221] CGMF, *Risk of money laundering and terrorist financing posed by crypto assets and crowdfunding*, October 2018, p. 21 – 22.

on the basis of information from other SARs from the same financial intermediary showed that various allegedly fraudulent transactions reported to MROS in different SARs ended up at the same destination address after several intermediate stops, which is a strong indication of an organised fraud scheme.

In fact, during the period under review, MROS received numerous SARs with similar facts as described in the above typology. The alleged victims of fraud were almost exclusively domiciled abroad. The common denominator of all these SARs was that the FIs had almost no information about the reported business relationships.[222] Secondly, the individual SARs concerned reported transactions of negligible value. It is obvious that SARs with such similar circumstances are indicative of larger, organised fraud schemes, especially when MROS identifies concealment techniques when tracing the suspected stolen assets. Drawing correlations between the content of seemingly unrelated cases requires considerable resources, for example by using tracing tools or by exchanging information with foreign authorities, and is a major challenge for both MROS in its analytical work and for law enforcement agencies in their investigations. The individual SARs or criminal charges often contain little or no relevant information that could help in the investigation of the suspected perpetrators. The transactions reported are also usually of low value, which can result in foreign FIUs taking a long time to respond to information requests, as these requests are not prioritised. Such organised fraud schemes designed to steal and launder VAs are very hard to detect, which places law enforcement in a very vulnerable position.

In addition to the intercantonal database PICSEL, which can be used to draw correlations between individual cases to form an overall picture, Switzerland also has the Network for Investigative Support in the Fight against Cybercrime (NEDIK), which is used to pool specialist resources. Individual cantonal police forces also use the NEDIK framework to provide services for use by all police forces in the country. Regular meetings on VAs are held within NEDIK to ensure the exchange of information and to set standards in this area. Smaller cantons with few resources can request administrative assistance from the federal government or expert cantons in the same way as other special tools. According to the information gathered, some large cantons, such as Zurich, have invested resources in developing their skills and tools to carry out cybercrime analysis on their own behalf or for requesting authorities. The specialised investigators have also networked with other VA specialists around the world. For example, law enforcement agencies are connected internationally through various networks and can share information and coordinate investigations through Interpol or Europol.

Another possibility is the exchange of information between national money laundering reporting bodies, for example within the framework of the Egmont Group of Financial Intelligence Units. As Switzerland's Financial Intelligence Unit (FIU), MROS receives valuable information and requests from its partner authorities abroad in connection with the use of VAs for ML/TF purposes with a connection to Switzerland. If necessary, it can forward this information for intelligence purposes to other authorities and agencies in Switzerland involved in combating ML/TF. Similarly, MROS sends spontaneous information and requests for information to the FIUs of other countries, partly for its own analytical purposes, but also on behalf of other Swiss authorities. The exchange platforms mentioned above have given rise to a number of projects and products, such as catalogues containing information on FIs engaged in VASP activities in different countries, or best practice guidelines for law enforcement agencies in investigating VAs and contacting FIs engaged in VASP activities abroad.

In this context, discussions with law enforcement agencies at the cantonal and federal levels have revealed that in several cases VAs on platforms of foreign FIs engaged in VASP activities have been successfully frozen and returned to the victims. In some cases, this was done by

[222] For example, personal information about the specific users of the app as well as on the accounts from which the deposited funds used to purchase VAs originated.

means of international legal assistance and in other cases by means of the Budapest Convention (see Infobox 5).

Infobox 5

The Budapest Convention

The Convention of 23 November 2001 on Cybercrime ('Budapest Convention') is an international convention to combat cybercrime. It was adopted by the Council of Europe in 2001 and now has 65 signatories, including most European countries, the United States and Japan.
The Budapest Convention entered into force for Switzerland in 2012.[223] Law enforcement agencies can use the Budapest Convention to access electronic evidence held abroad, including data stored by private companies, without going through the channels of mutual legal assistance.

For example, Article 32 of the Convention provides for cross-border access to stored computer data under certain conditions. This includes data relating to business relationships with FIs engaged in VASP activities and domiciled in the signatory states. In this way, for example, it can be quickly established in whose name an account is held with a foreign financial intermediary engaged in VASP activities, who the beneficial owner is, or what transactions have been carried out through this account at what time. Since money laundering and terrorist financing through VAs is often transnational in nature, with transactions taking place in a matter of seconds, the Convention can speed up the work of law enforcement agencies, leading to higher clearance rates and more freezing and seizing of VAs. This is an advantage over traditional investigations, the success of which depends on the response time of foreign authorities in executing international mutual legal assistance requests and on the time limits for banks to withhold financial documents, which vary widely from one jurisdiction to another.

The Budapest Convention was referred to in the CGMF's 2018 sector report, although at that time there was limited information on the possibility of cross-border access to electronic evidence.[224] According to the information gathered for this risk analysis, Swiss law enforcement agencies have had mixed experiences with the application of the Budapest Convention. Some law enforcement agencies seem to have had positive experiences. Others point out that cooperation with private companies abroad is difficult and that it is impossible to predict on a case-by-case basis whether they will authorise or refuse the transfer of data and may still refer the matter to the mutual assistance channel, thereby wasting valuable investigative time. Some companies would take an alternative route and hand over the data – but only for 'intelligence' purposes rather than as evidence. This means that the data can be used for further investigation (but not as evidence) until it is obtained in a second step through international mutual legal assistance.

Vulnerability 5

Difficult suppression of ML/TF in the VA sector (identified in 2018, unchanged in 2023)[225]

The fundamental anonymity or pseudonymity in the operation of VAs, the decentralisation of their architecture, especially in the area of DeFi and DAOs, and the pronounced international interconnectedness of business relationships in the area of VAs make it difficult for law enforcement agencies to identify and contact the appropriate counterparts to obtain

[223] SR 0.311.43 – *Convention of 23 November 2001 on Cybercrime*, status as of 14 September 2020.
[224] CGMF, *Risk of money laundering and terrorist financing posed by crypto assets and crowdfunding*, October 2018, p. 40 – 41.
[225] CGMF, *Risk of money laundering and terrorist financing posed by crypto assets and crowdfunding*, October 2018, p. 34 – 35.

information relevant to their investigations or proceedings. When contacts are identified, they are usually not located in the same country as the corresponding law enforcement agency. If the relevant information cannot be obtained by virtue of the Budapest Convention, law enforcement agencies must request it through international mutual legal assistance. This is usually time-consuming, which is already a challenge for law enforcement agencies in non-VA-related investigations and proceedings related to tracing of financial flows. This challenge is even bigger for VA transactions, which, compared to traditional payment transactions, take place in seconds across multiple blockchains, FIs, decentralised platforms and national borders. This makes it more difficult to solve crimes in general and to combat money laundering and terrorist financing in particular.

There also appear to be significant differences in the level of knowledge of VAs among law enforcement agencies, both internationally and within countries. While some authorities invested early in knowledge and capacity building and are now equipped with the necessary tools to solve crimes, others have no such experience. This makes national and international cooperation more difficult, in terms of communication and also investigative and procedural aspects. As a result, the inconsistencies or even absence of regulatory approaches around the world, coupled with the different emphasis and prioritisation of cases in VA matters, increases the risk of regulatory arbitrage by criminals who deliberately exploit regulatory loopholes to make it more difficult to detect or prosecute their activities.

7.4.3 Legal precedent

According to the research carried out for this risk analysis, there do not appear to be any legally binding court decisions in Switzerland, either at federal or cantonal level, relating to money laundering and the use of VAs. Such rulings could provide details on the conditions under which their use constitutes a money laundering offence. Only one decision of the Federal Criminal Court in December 2022 provides more information in this respect. This concerned an appeal by an individual rejected by the Federal Criminal Court to prevent the Geneva public prosecutor from transferring his bank records to another European country in the context of international mutual legal assistance. A law enforcement agency in the country in question had accused this person (and others) of, among other things, tax evasion and gang-related money laundering. The ruling states (translated from French): "The conversion of money into cryptocurrencies or [note: other acts] constitutes an act that may hinder the identification of the source, the tracing or the confiscation of assets within the meaning of Art. 305bis SCC".[226] Therefore, in the view of the Federal Criminal Court, the mere exchange of fiat money into VAs is sufficient to constitute the offence of money laundering.

7.5 Vulnerabilities in financial intermediation in connection with Vas

The extent to which FIs are vulnerable to being exploited for money laundering or terrorist financing purposes can be mitigated to a certain extent, for example, through appropriate supervision. The vast majority of Swiss FIs engaged in VASP activities (174) are affiliated to a self-regulatory organisation (SRO), which then supervises them, while banks and investment firms engaged in VASP activities (around 30) are directly supervised by FINMA.[227]
Consolidated information on the specific supervision of FIs with VASP activities by the various SROs could not be made available. However, an exchange of information between MROS and an SRO in 2021 showed that its affiliated members engaged in VASP activities are subject to

[226] RR.2022.45, *Arrêt du 20 décembre 2022*, Judgment of the Federal Criminal Court, Bellinzona, 21 December 2022.
[227] As at end-2022.

stricter supervision rules than the other members. For example, members engaged in VASP activities are audited within a maximum of six months (instead of the usual 12 months) after joining the SRO. Audits of compliance with the provisions of the AMLA are carried out either by the SROs themselves or by audit firms accredited by the SROs.

Typology 5

Swiss public limited company with an SRO licence acquired by anonymous buyers with VAs

A Swiss financial intermediary engaged in VASP activities reported a business relationship with a Swiss corporate client that appears to specialise in setting up Swiss companies and providing fiduciary services. On its website, the client advertised its services of setting up companies in Switzerland for foreign individuals and taking charge of all the administrative work, such as designing a company website, company logo, company brochure, business cards, c/o letterboxes and a fully equipped office space 'at short notice'. For an additional fee, they also offered postal addresses without the 'c/o' – apparently to avoid the impression that the companies they set up were shell companies. Employees of the corporate client also advertised on social networks their assistance in obtaining an SRO licence.

The corporate client in question opened a business relationship with the reporting financial intermediary, allegedly in order to be able to offer its client the possibility to pay in cryptocurrencies. At some point after opening the business relationship, the reporting financial intermediary became aware of three incoming payments from an unknown crypto address, arriving within a few minutes of each other and totalling a medium six-figure sum (in Swiss Francs). However, each of the three payments was slightly below the threshold up to which the reporting financial intermediary allowed such payments to be made. This seemed suspicious to the reporting financial intermediary ('smurfing'), so he contacted the client and enquired about the economic background of the incoming transactions. The client replied that these payments were linked to the sale of one of his companies. To demonstrate the plausibility of the transactions, the client presented the financial intermediary with a contract of sale which showed that the client had sold 100% of the shares in a Swiss company to two buyers (although the client had redacted the buyers' names). When asked why the payment had been split in three, the client explained that the buyers wanted to be able to stagger payment of the invoice if necessary and thereby choose favourable exchange rates. This did not seem plausible to the reporting financial intermediary, given that the payments were received within minutes of each other, and on this basis he submitted an SAR to MROS. The company sold was itself affiliated to an SRO and thus an FI regulated in Switzerland.

This was therefore a case of a Swiss financial intermediary being sold to anonymous purchasers by means of VAs.

Threat 11

Travel Rule is not applied to merchant accounts of Swiss FIs engaged in VASP activities (identified in 2023)

In Switzerland, natural persons and legal entities may accept VAs as a means of payment for the services they provide. Swiss FIs engaged in VASP activities offer merchant accounts to legal entities domiciled in Switzerland. According to the website of a Swiss financial intermediary engaged in VASP activities, such legal entities can use these accounts to receive VA payments. Compliance with due diligence and reporting obligations is the responsibility of the Swiss financial intermediary offering these merchant accounts. In contrast to the provisions of the Travel Rule, the Swiss financial intermediary engaged in VASP activities does not

appear to obtain information about the sender of the VAs in advance (see Figure 9 in Section 4.6.4). This increases the risk that such services will be used by Swiss legal entities to launder VAs, particularly in connection with trade-based money laundering. MROS is also aware of cases where the thresholds for VA transaction were exceeded by means of smurfing.

Like the SROs, FINMA also uses audit firms to conduct risk-oriented audits of the institutions it supervises in accordance with the Anti-Money Laundering Act. In the summer of 2021, FINMA issued its guidelines to audit companies responsible for conducting audits of FINMA-supervised FIs that engage in VASP activities. These audit firms use a specific VA/VASP audit module when conducting their audits of FINMA-supervised FIs that engage in VASP activities.

FINMA also examined how several financial service providers under its supervision verify the beneficial ownership of the non-custodial wallet(s) created by their clients. One common solution is for the financial intermediary to agree in advance with its client the amount (e.g. a micropayment) and the time at which a transfer will be made. A second solution is for the client to send a unique message on the blockchain within a certain period of time. This has to be done when the first transfer is made. The address can then be placed on a 'white list', which eliminates the need to check subsequent transfers with the same address. This procedure is then repeated at regular intervals determined by the FI (e.g. whenever higher-risk transactions take place on the non-custodial wallet or if there is any doubt regarding power of disposal with regard to the non-custodial wallet). For transactions where the counterparty is a service provider with collective wallets, these procedures are not technically feasible. In such cases, FINMA accepts verification of the power of disposal by means of a screenshot: the receiving financial intermediary requests a screenshot of the transaction specified by the client. The document provided serves as proof that the client has power of disposal over the account debited by the VASP.[228] Time-boxing is a new addition to the range of verification methods. This involves the customer transferring an amount directly to a preceding micro-transaction. Customers have to pre-announce the transaction and the desired amount, after which the financial intermediary provides them with the address and a short time window (time box). The agreed transaction can be executed within this time window. Proof of power of disposal is provided by checking that these requirements are met. Another new approach is to have clients log in to the wallet in the presence of employees of the financial intermediary. Provided that the process is adequately documented, this measure also meets the requirements of FINMA Guidance 02/2019 'Payments on the blockchain'.

Business models based on blockchain technology still attract significant investor interest. Unscrupulous market participants continue to take advantage of this and launch offerings, often attracting customers through an online presence. Typically, they try to dupe investors into investing in cryptocurrencies by presenting non-existent companies and products. If FINMA becomes aware of such market participants, it adds them to its warning list and thus alerts investors. It also coordinates these activities with domestic law enforcement agencies and foreign supervisory authorities.

FINMA has also paid close attention to ICOs in the area of FinTech. Given the early stage of many ICOs, there may be numerous uncertainties regarding the projects to be financed and implemented. FINMA cannot rule out the possibility that ICO activities may be carried out with fraudulent intent. FINMA will not tolerate fraudulent or abusive behaviour or circumvention of the regulatory framework and will take the necessary enforcement measures if required.

In total, it conducted investigations into around 60 ICOs, more than half of which were concluded. FINMA identified violations of the Anti-Money Laundering Act (AMLA) in more than ten ICOs and brought criminal charges against those responsible. Eight further cases resulted in entries on FINMA's warning list. Enforcement proceedings were ultimately initiated against

[228] Swiss Financial Market Supervisory Authority (FINMA), *Annual Report 2020*, March 2021, p. 43 – 44.

three companies, one of which has already been concluded. One of the companies against which proceedings were initiated had ignored FINMA's previous assessment when responding to subordination enquiries. In addition, FINMA ordered a number of companies to take measures to restore legal compliance. These measures included the repayment of unlawfully received public deposits under the Banking Act and removal of the word 'bank' or the withdrawal of advertisements with non-existing FINMA licences. There has been a noticeable trend towards offering 'stablecoins', which in particular raises questions regarding the application of the AMLA, the Banking Act and the Collective Investment Schemes Act.

In addition to market activity in the area of ICOs, FINMA also noted an increasing involvement of Swiss providers in secondary market-related financial services in the crypto area. These included trading and custody of tokens, as well as the operation of trading venues and related support activities. The Enforcement Division has conducted investigations against a number of these providers in recent years. In the case of one provider of token trading and custody services, FINMA identified violations of the Banking Act and the Stock Exchange Act, ordered a series of measures to restore compliance with the law and filed criminal charges. FINMA also opened enforcement proceedings against a money transfer service between cryptocurrency trading venues and their clients for the unlawful acceptance of public deposits. In another case, it opened enforcement proceedings for illegal securities trading with tokens. In May 2023, FINMA shut down several coin providers and concluded proceedings against a foundation active in the crypto sector and its founder, finding that they had committed serious violations of supervisory law. Bankruptcy proceedings had already been opened against the foundation in March 2023. FINMA has issued a cease-and-desist order against the founder of the foundation. This will be published on its website for a period of five years.[229] Overall, FINMA has observed an increasing number of fraudulent websites in connection with VA services that purport to offer their clients investments in cryptocurrencies without using the funds paid in for the intended purpose. Where possible, FINMA warns against such offers on its warning list.
In the area of illegal gambling, the Federal Gaming Board (FGB), as the supervisory authority for casinos, dealt with two cases in 2019 in which a VA machine was stationed in a gambling establishment for the purpose of paying winnings to players. In one case, a complaint was filed, but the case is still pending. In the other case, it could not be proven to the satisfaction of the law that the VA machine found was actually used to pay out winnings or who the operator of the illegal platform was. The FGB assumes that VAs could become a popular means of payment in connection with illegal gambling offers in Switzerland.

[229] Swiss Financial Market Supervisory Authority (FINMA), *FINMA concludes proceedings against crypto platform and its founder*, May 2023.

7.5.1 Reporting FIs

The analysis of VA-related SARs for the years 2020 to 2022 shows that the reporting behaviour of the FIs varies considerably depending on whether or not they carry out VASP activities.

	2020		2021		2022		2020–2022 (total)	
VA-related SARs	312		499		1,056		1,867	
	VASP	**No VASP**	**VASP**	**No VASP**	**VASP**	**No VASP**	**VASP**	**No VASP**
Number of reporting FIs	12	40	19	57	12	93	24	118
Number of VA-related SARs	104	208	178	321	143	913	425	1,442

Figure 27: VA-related SARs and their share of the total volume of SARs (2020–2022), broken down by activity of the financial intermediary (VASP or not).

It is noteworthy that 1,442 (77%) of the 1,867 SARs received during the reporting period came from a total of 118 different FIs *not* engaged in VASP activities.

These were generally SARs in which the financial intermediary drew the attention of MROS to suspicious transactions between the reported accounts and the accounts of FIs engaged in VASP activities in Switzerland or abroad. The number of VA-related SARs received from these FIs has steadily increased since 2020.

Typology 6

VA-related SAR from an FI not engaged in VASP activities

A bank submitted an SAR concerning a business relationship with a natural person. Over a period of several months, the individual received several credit payments from different bank accounts, all in the name of different natural persons. The incoming payments from these third parties were immediately transferred from the reported account to the account of a foreign VA exchange.
The reporting financial intermediary suspected that the third parties who had transferred money to the reported account were probably victims of fraud. The reported counterparty had presumably acted as a money mule by making his account available, for a fee, to unknown persons involved in the fraud. The reported counterparty then forwarded these fiat money amounts to the VA exchange, where they were exchanged for VAs and transferred to non-custodial wallets, which were presumably controlled by the unknown perpetrators.

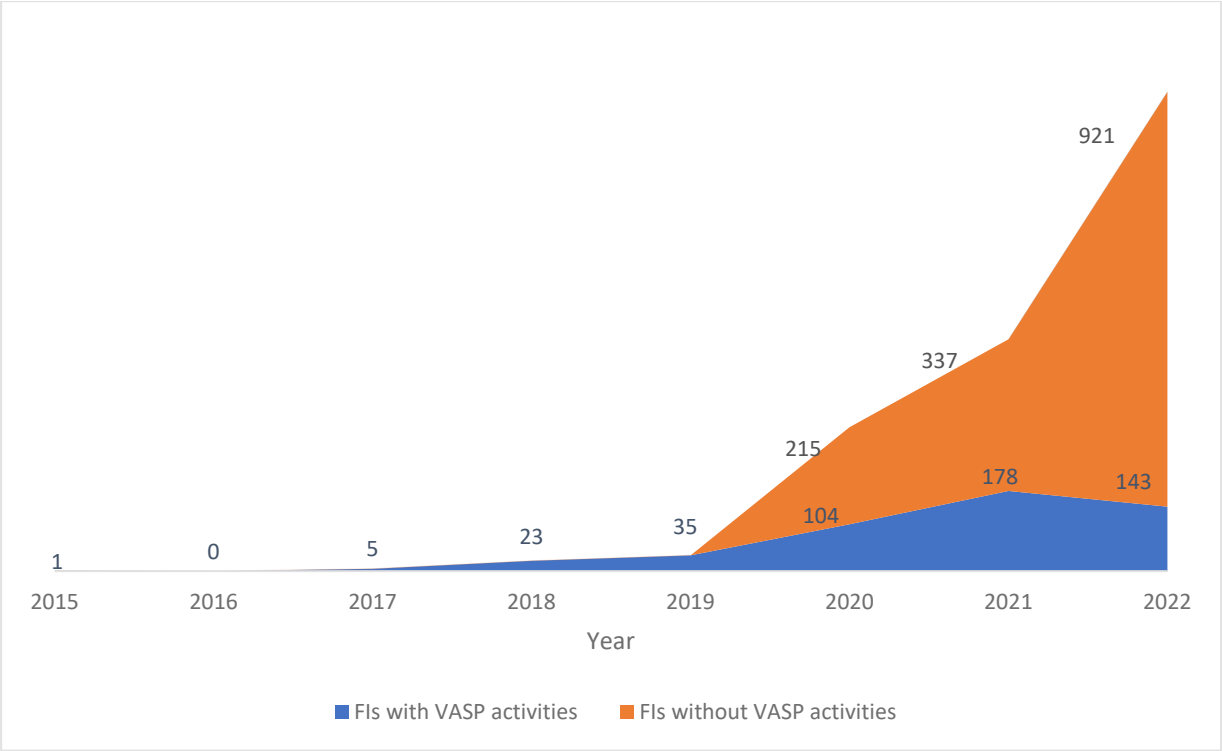

Figure 28: VA-related SARs from FIs not engaged in VASP activities have increased more since 2020 than those from FIs engaged in VASP activities.[230]

It appears that, due to the growth of the VA sector, the increasing general use of VAs and the greater interconnectedness of FIs with and without VA activities, the vulnerability of FIs to being exploited for ML/TF purposes in connection with the use of VAs is no longer primarily limited to FIs actively engaged in VA activities. This is evidenced by the high number of VA-related SARs from FIs without VA activities. For example, an analysis of these SARs shows that the accounts held with these FIs are used for flow-through transactions that begin or end with a transfer to or from a fiat account of a VA exchange, or to park suspicious assets that have previously been exchanged from VAs into fiat money with an FI engaged in VASP activities. Given the widespread use and mainstreaming of the VA sector, FIs without VASP activities are significantly more vulnerable than in 2018 to being misused for ML/TF purposes through VAs, even if they do not engage in VASP activities. Such cases have become more frequent and the sums involved are significantly higher. Moreover, these FIs often rely on external experts in blockchain analytics to determine the plausibility of the economic background of the fiat money held in their accounts, which was previously exchanged into fiat money by other VA providers.[231] MROS is aware of cases that explicitly show that these expert opinions can only provide a certain degree of 'certainty' with regard to the plausibility of the origin of the assets. If non-VASP FIs are not in a position to independently understand and assess the level of plausibility checks, they may be exposed to money laundering risks. They must be aware that this risk is transferred to them, especially – but not only – if companies[232] issue such expert opinions and earn money in some way by referring clients to non-VASP FIs.

[230] Note: For the period prior to 2020, only SARs from FIs engaged in VASP activities were counted, see Section 11.1.1 in the Annex.
[231] See e.g. Gotham City, *L'enquête sur les pirates allemands de Movie2k passe par Genève*,, , No 278, 26 January 2023.
[232] These may be FIs with VASP activities, who receive fees for converting VAs into fiat money, or non-FIs who are paid by the latter for providing expert opinions and/or for referring clients to FIs without VASP activities.

Vulnerability 6

Financial intermediaries carrying out VA-related transactions (in VAs or fiat) (identified in 2018, upgraded in 2023)[233]

The 2018 sector report noted the vulnerability of "FIs involved in crypto asset transactions" to money laundering and terrorist financing risks.[234] Even with strict adherence to the due diligence obligations, the effectiveness of these measures is inherently limited by the fact that crypto transactions are transnational and conducted through service providers registered in many different jurisdictions. For example, online exchange platforms registered in Switzerland are often instructed to exchange cryptocurrencies by foreign custodial wallet providers acting on behalf of their customers. In such cases, the Swiss platform does not have access to the customer's KYC data on the foreign platform for which it is executing the exchange and therefore does not know the customer's identity.

Since 2018, MROS has received numerous SARs from FIs that are not engaged in VASP activities and have identified suspicious transactions to or from domestic or foreign VASP platforms on the accounts they manage. In addition, MROS became aware of several cases in which Swiss FIs not engaged in VASP activities provided foreign FIs engaged in VASP activities with business accounts through which fiat transactions were processed in connection with the purchase or sale of assets on foreign VASP platforms. In this context, the Swiss FIs often appear to be unable to clarify the economic background of the assets transferred through their accounts or to determine the beneficial ownership of these assets. This is because only the foreign financial intermediary, and not the Swiss financial intermediary, has information on the transactions carried out via this account and the persons involved. The Swiss financial intermediary is therefore dependent on the foreign financial intermediary's compliance with its due diligence and reporting requirements and cannot itself ensure that no clients with increased risks or transactions with an uncertain economic background are processed through its accounts.

MROS is aware of several cases in which the provision of such business accounts by the account-holding bank in Switzerland was misused to process payments in connection with alleged criminal offences committed abroad. In some cases, it was even the business clients of a Swiss financial intermediary or the foreign FIs themselves engaged in VASP activities who were accused in criminal proceedings abroad. The fact that the account-holding financial intermediary in Switzerland is insufficiently informed about the transactions it is handling increases the ML/TF risks associated with such business arrangements.
These developments are a further indication of the blurred line between the business activities of FIs engaged in VASP activities and those that are not (see Infobox 1 in Section 4.2). Ultimately, this means that *all* FIs – whether engaged in VASP activities or not – are vulnerable to the risk of being exploited as a transit or destination point for illicit VA-related financial flows – in VAs or fiat.

Between January 2020 and the end of 2022, MROS received more than three times as many VA-related SARs from FIs not engaged in VASP activities (1,442) as from those engaged in VASP activities (425). The number of SARs from FIs engaged in VASP activities also increased, but not as much or as steadily as from FIs not engaged in VASP activities – despite the increasing number of FIs engaged in VASP activities and the presumably increasing volume of their business.

[233] CGMF, *Risk of money laundering and terrorist financing posed by crypto assets and crowdfunding*, October 2018, p. 34 – 35.
[234] Ibid., p. 34.

It is striking that more individual FIs not engaged in VASP activities submitted VA-related SARs than FIs engaged in VASP activities. While 118 different non-VASP FIs submitted at least one VA-related SAR between January 2020 and December 2022, only 24 different VASP FIs did so during the same period.[235] Moreover, more than three quarters of these SARs (329 out of 425 from FIs engaged in VASP activities) came from the same four FIs engaged in VASP activities. These four FIs engaged in VASP activities submitted an SAR on a regular basis, while 20 FIs engaged in VASP activities submitted SARs sporadically.

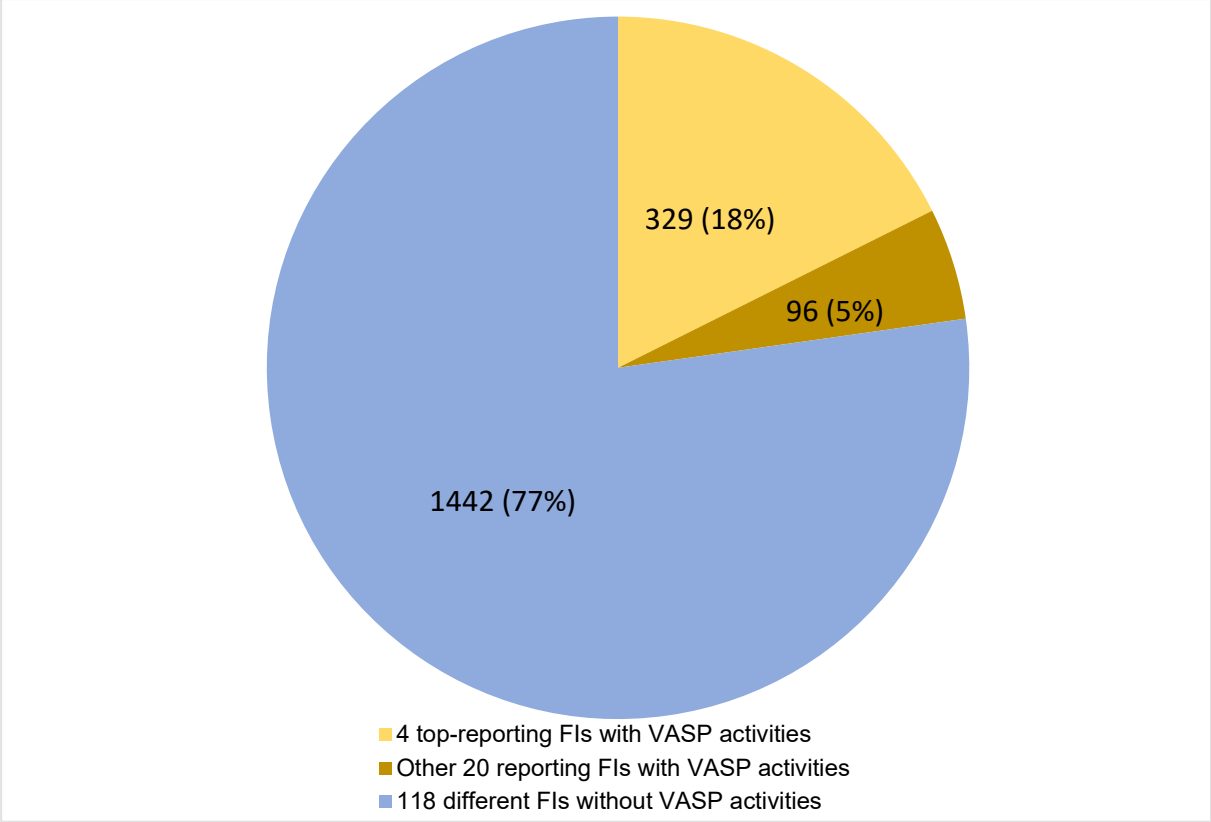

Figure 29. Reporting FIs behind the 1,867 VA-related SARs in 2020–2022. Surprisingly, FIs engaged in VASP activities submitted significantly fewer VA-related SARs than those not engaged in VASP activities.

Vulnerability 7

Absence of SARs from FIs engaged in VASP activities (identified in 2023)

As at the end of 2022, there were at least 204 FIs engaged in VASP activities in Switzerland, either under the direct supervision of FINMA or affiliated to self-regulatory organisations. Between January 2020 and the end of December 2022, 180 of them did not submit a single SAR to MROS. The vast majority of these FIs are affiliated to a self-regulatory organisation. However, in the absence of quantitative data on the services provided and the VA assets under management by Swiss FIs engaged in VASP activities, it is not possible to say with any precision whether the absence of SARs from the overwhelming majority of these FIs is due to their failure to comply with due diligence and reporting obligations or simply to a lack of business activity. However, given the growth of the VA sector in Switzerland and the apparent proliferation of related business activities of FIs engaged in VASP activities, it would appear that MROS is not receiving all the SARs from FIs engaged in VASP activities that it should.

[235] It should be noted that the VA-related SARs submitted by FIs engaged in VASP activities do not necessarily represent *all* of the SARs submitted by these FIs during this period, as some FIs engaged in VASP activities also submitted SARs in connection with other business activities of these FIs that were not related to VAs or VASPs (see Section 4.2).

7.5.2 Factors giving rise to suspicion

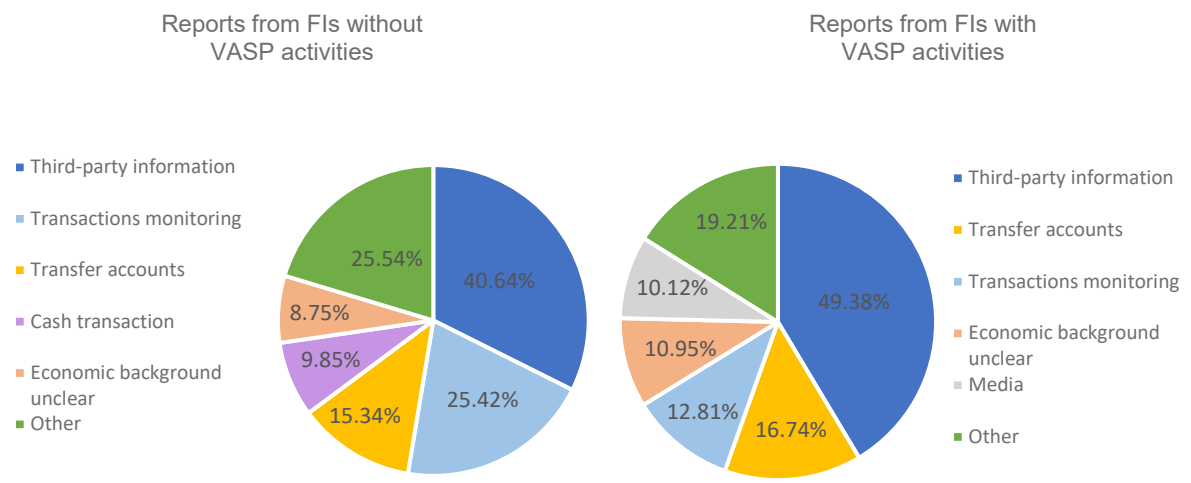

Figure 30: The factors giving rise to suspicion differ according to whether the SAR was filed by an FI with or without VASP activities. Financial intermediaries not engaged in VASP activities were significantly more likely to file an SAR based on their internal transactions monitoring, while FIs engaged in VASP activities were significantly more likely to file an SAR based on information received from third parties.

The incidence of FIs engaged in VASP activities making independent findings on the basis of their transaction monitoring and submitting a VA-related SAR was rather low compared to the incidence of VA-related SARs submitted by FIs not engaged in VASP activities (12.8% for FIs engaged in VASP activities compared to 25.4% for FIs not engaged in VASP activities).

In almost half (49.4%) of the SARs from FIs engaged in VASP activities, the SAR was based on one of the following: a transfer recall from a third-party bank regarding fraudulently initiated payments, a contact from a foreign law enforcement agency or a disclosure order from a Swiss law enforcement agency (summarised below under the term 'third-party information'). In the case of SARs from FIs not engaged in VASP activities, third-party information was much less frequently cited as a reason for submitting an SAR (40.6%). The percentage is high for both types of FIs and seems to reflect a general problem in the area of FIs. However, it appears that intermediaries engaged in VASP activities rely significantly more on this third-party information to detect suspicious transactions.

The SARs of FIs engaged in VASP activities also show that they have frequently been contacted directly by foreign law enforcement agencies (mainly the public prosecutor in Germany) requesting certain information about a business relationship conducted with them – for example, the name of the account holder who was the recipient of a fraudulent payment.

Vulnerability 8

The reporting behaviour of FIs engaged in VASP activities often appears to be reactionary and not based on proactive investigation (identified in 2023).

When submitting SARs, the reporting FIs describe in writing the circumstances of the suspicious activity and the reasons for submitting the SAR. In this context, MROS observed differences between FIs with and without VASP activities with regard to their detection systems, which should account for different sources and grounds for suspicion.

Reporting FIs engaged in VASP activities were more likely than those not engaged in VASP activities to first become aware of suspicious transactions through external information that prompted them to submit an SAR. According to those VASP activities, the most common factor arousing suspicion in the SARs they submitted between 2020 and 2022 was information from third parties (49.4% of SARs submitted by FIs with VASP activities). The reasons given by these FIs for becoming aware of the reported business relationship were: transfer recalls from third-party banks in connection with fraudulent payments, direct contact by suspected fraud victims or their legal representatives, requests from foreign law enforcement agencies, or disclosure orders from Swiss law enforcement agencies. In contrast, information from third parties led to the filing of a report in only 40.7% of VA-related SARs from FIs not engaged in VASP activities.

In the VA-related SARs from FIs without VASP activities, transaction monitoring was cited as a factor giving rise to suspicion twice as often (25.4%) as in SARs from those not engaged in VASP activities (12.8%). Financial intermediaries with VASP activities thus appear to have difficulties in identifying suspicious transactions and processes on the basis of their monitoring and in clarifying their economic background on their own initiative. This does not seem to be unique to Switzerland: an exchange of information with the FIU of Liechtenstein revealed that they too have observed a more reactionary reporting behaviour on the part of FIs engaged in VASP activities. This also leads to the assumption that some FIs with VASP activities have a significant lack of information on payments suspected of being related to money laundering. If these transactions are not identified as suspicious and reportable on the basis of internal investigations or external information, they do not result in an SAR being submitted to MROS.

8. Stocktake and risk-mitigating factors

So far, this report has reassessed and expanded on the threats and vulnerabilities identified in 2018 in light of the significant changes and developments in the VA sector. This chapter now takes stock of the various threats in the form of a summary.
As in the 2018 sector report, this stocktake only presents the changes in threats and vulnerabilities as an overview of the total exposure. This is followed by a list of the risk-mitigating factors identified. The lack of available data makes it impossible to examine and quantify the net risks associated with financial intermediation in the VA sector in Switzerland (see Section 5.2). These figures would be necessary to establish a risk-weighted ranking of the business activities based on their intensity and scope, which could then be used to examine the extent to which each business activity is affected by the threats and vulnerabilities identified and influenced by the risk-mitigating factors.

8.1 Stocktake of the risk analysis

Of the nine threats and two vulnerabilities identified in 2018, none have eased or diminished in any way over the last five years. On the contrary, most of them have increased (7 out of 11), while three threats and one vulnerability have remained unchanged. In addition, two threats and six vulnerabilities have been newly identified as part of this risk analysis.

	Threats	2018	2023
1	Security gaps in the underlying VA technologies	Identified	Increased
2	Ransomware and malware	Identified	Increased
3	VAs as a means of payment for illegal goods and services	Identified	Increased
4	Laundering of illegally acquired VAs (in fiat money)	Identified	Increased
5	Laundering of illegally acquired fiat money (in VAs)	Identified	Unchanged
6	Threats in connection with the novelty effect and users' inexperience	Identified	Increased
7	VA use for phishing	Identified	Increased
8	Terrorist financing using VAs	Identified	Unchanged
9	Proliferation financing by means of VAs		Identified
10	Transaction anonymity and difficult identification of beneficial owners	Identified	Unchanged
11	Travel Rule is not applied to merchant accounts of Swiss FIs engaged in VASP activities		Identified

Figure 31: Overview of the threats identified and how they have changed since 2018

	Vulnerabilities	2018	2023
1	Trend towards decreasing importance of financial intermediation in the VA sector poses a challenge to existing ML/TF regulation		Identified
2	Inadequate and unequal international implementation and enforcement of the travel rule in the VA sector		Identified
3	Lack of resources and capacity on the part of the institutions involved in countering ML/TF in view of the rapid developments in the VA sector		Identified
4	Insufficient figures and statistics at national and international level		Identified
5	Difficult suppression of ML/TF in the VA sector	Identified	Unchanged
6	Financial intermediaries that carry out crypto transactions (in VAs or fiat money)	Identified	Increased
7	Absence of SARs from FIs engaged in VASP activities		Identified
8	The reporting behaviour of FIs engaged in VASP activities often appears to be reactionary and not based on proactive investigations		Identified

Figure 32: Overview of the vulnerabilities identified and how they have changed since 2018

8.2 Risk-mitigating factors

Although VAs pose considerable threats and have equally significant vulnerabilities, there are several factors that can mitigate the risk and thus reduce the impact of the threats and vulnerabilities. Most of these factors have been mentioned earlier in this report and are summarised below. Some of them operate at a global level while others are specific to Switzerland; any differences between the two levels are highlighted.

	Risk-mitigating factors
1	Increased FATF focus and greater political attention
2	Increased international cooperation is already yielding results
3	Consolidation and higher levels of compliance maturity among the big players
4	Fundamental transparency of most blockchains
5	Oversight and implementation of the Travel Rule in Switzerland
6	Broad definition of financial intermediation in the DLT Act

Figure 33: Overview of the risk-mitigating factors identified

8.2.1 Increased FATF focus and greater political attention

Internationally, the ongoing implementation of the FATF's VA-specific recommendations can be seen as a risk-mitigating factor. The FATF appears to be closely monitoring country implementation and regularly publishes guidance and reports on the status of implementation of the VA-specific recommendations.

Greater attention from the FATF and the international governmental community increases the pressure on countries and firms in the VA sector to comply with international AML/CFT rules. This may encourage more widespread implementation of such measures, thereby reducing the risk of VAs being used for ML/TF purposes. Subsequently, such increased attention may also lead to better identification and monitoring of suspicious activities and transactions, also helping to minimise the risk of ML/TF in relation to VAs. For example, the implementation of the Travel Rule will increase the transparency of financial flows between the accounts of FIs engaged in VASP activities and align the benchmark for monitoring due diligence compliance for centralised VA services with that for SWIFT payments. A broad definition of 'VASP' in line with FATF Recommendation No 15 also ensures that the AML/CFT rules that already apply to traditional FIs also apply to VAs. For example, FIs engaged in VASP activities are required to know the identity of their clients, report suspicious transactions and implement effective risk management. More comprehensive global regulation and supervision of FIs engaged in VASP activities can ensure that they are better able to detect and prevent the use of VAs for ML/TF purposes, thereby reducing the ML/TF risk.

8.2.2 Increased international cooperation is already yielding results

Increased international cooperation at various levels in the VA sector, such as between national regulators, law enforcement agencies and FIUs, and also between law enforcement agencies and private companies, can help to reduce ML/TF risks in the VA sector. Some successes have already been achieved, for example in tracing, freezing and seizing VAs, by improving the authorities' knowledge of VAs, sharing information on suspicious cases more quickly and effectively, and intensifying cooperation with businesses in relation to blockchain analytics.[236] By sharing best practices and experiences, different countries and institutions can learn from each other and improve their measures. This, in turn, can also help reducing the risk if it means that ML/TF activities related to VAs are identified and prosecuted more quickly. Finally, enhanced cooperation can help to identify and address remaining gaps and weaknesses in the regulatory architecture, thereby improving regulation and supervision in general. Closer cooperation also promotes harmonisation in the implementation of international standards and can thus improve the impact of AML/CFT measures in the VA sector.[237]

8.2.3 Consolidation and higher levels of compliance maturity among the big players

Global consolidation on the supply side of the VA sector, resulting in a smaller number of large, centralised VA trading exchanges with more mature compliance departments, can help reduce ML/TF risks in the VA sector. Fewer, but larger and better regulated VASPs will lead to less risk and enable better control and monitoring of the residual risk. In addition, larger VASPs

[236] For details about seizures of several billion US dollars in cryptocurrency in 2022, see Chainalysis, *The 2022 Crypto Crime Report*, February 2022, p. 23.
[237] Basel Institute On Governance and Europol, *Seizing the opportunity: 5 recommendations for crypto assets-related crime and money laundering*, 2022, p. 4 – 5.

tend to be better able to invest in compliance departments and transaction monitoring technology, which in turn can increase the likelihood of preventing illegal activities related to VAs. Regulators can also interact more effectively with a smaller number of larger VASPs to enforce regulatory and monitoring standards. This makes it easier to monitor compliance with AML/CFT standards and take action in the event of non-compliance. Finally, the consolidation of the VASP sector may also make it faster to identify and stop the use of VASPs for ML/TF purposes, since there will be fewer places where these activities can take place.

8.2.4 Fundamental transparency of most blockchains

The fundamental transparency of blockchains currently offers opportunities to monitor financial flows in the VA sector that are not possible with traditional payments.[238] Some blockchain analytics solutions can link digital information to people and events in the analogue world, providing unprecedented opportunities for in-depth analysis. However, the quality of these evaluations will always depend on the quality of the underlying data from the analogue world. No common standards have yet been established. These solutions capitalise on two key factors. First, VA transactions are usually publicly visible. This makes it easier to detect and monitor suspicious activity and, in turn, to identify and trace cash flows in real time. This is not possible in traditional payment transactions. Secondly, by providing a permanent and immutable log of transactions, unlike traditional payments, blockchain can also help to reduce the general risks of fraud and counterfeiting in the medium to long term, as once transactions have been made, they can be publicly verified and cannot be altered. As DeFi protocols are typically based on public blockchains, there may be greater transparency. However, some DeFi applications make it difficult or impossible to trace transactions, either intentionally (e.g. mixers, tumblers, privacy wallets) or as a side-effect of their functionality (cross-chain bridges, lending pools, automated market makers). Although every transaction within a DeFi protocol is recorded in real time on the blockchain and is publicly visible, it may not be possible to trace and attribute it, depending on the circumstances. This means that there are also significant money laundering and terrorist financing risks in the DeFi sector, as most users are anonymous. There are still challenges in identifying and monitoring suspicious transactions, especially with the use of anonymisation technologies. However, a growing number of companies and research facilities are now specialising in blockchain data analytics, developing advanced tools and technologies to analyse VA transactions and identify suspicious activities. This can help regulators and law enforcement to detect and prosecute cases of money laundering or terrorist financing. There have already been numerous cases where regulators and law enforcement have been able to detect ML/TF cases, freeze and seize VAs and, thanks in particular to blockchain analytics, link the criminal acts to the perpetrators and prosecute them. CeFi platforms, on the other hand, are based on centralised databases and systems that are not transparent. Access to the data therefore depends on the operator's willingness to cooperate, which can make it difficult to monitor and analyse transactions.

8.2.5 Oversight and implementation of the Travel Rule in Switzerland

In view of the considerable threat that money laundering poses to Switzerland, FINMA attaches high priority to money laundering in general, but also in relation to VASPs. FINMA has therefore introduced various supervisory and monitoring measures and conducts investigations and enforcement proceedings in the event of serious offences.

[238] Ibid., p. 3.

Since the emergence of cryptocurrency activities in the financial markets, Switzerland has applied the existing AML/CFT legal framework to certain cryptocurrencies as well as to specific VASPs considered by FINMA as equivalent to traditional FIs. Within this legal framework, all financial intermediation activities related to cryptocurrencies are subject to the Anti-Money Laundering Act (AMLA). This includes, in particular, services for exchange between cryptocurrencies and fiat currencies and/or between one or more cryptocurrencies, all activities in connection with the transfer, custody and/or management of cryptocurrencies, or keys or other means of enabling control over cryptocurrencies. For more information, see the October 2021 national report on the risks of money laundering and terrorist financing in Switzerland.[239]

In addition, since the introduction of the amended AMLO-FINMA on 1 January 2021, all Swiss FIs engaged in VASP activities must identify the counterparty in transactions with VAs if a transaction or several such transactions that appear to be linked reaches or exceeds the amount of CHF 1,000 where these transactions do not constitute transfers of money and securities and no permanent business relationship is associated with them. Together with the requirements set out in Art. 10 AMLO-FINMA (Disclosures in payment orders), Switzerland thus imposes a greater obligation on its FIs engaged in VASP activities than the FATF Travel Rule, as this regulation is also applied in Switzerland with regard to payments between custodial and non-custodial wallets. If properly implemented, VA inflows and outflows on client accounts of Swiss FIs engaged in VASP activities are currently only possible to and from non-custodial wallets of which the clients concerned are the beneficial owners. This strengthens the FIs' defences against ML/TF. However, the ability to identify the actual beneficial owner of assets in a non-custodial wallet and the origin of those assets remains limited by the technological aspects of VAs. These capabilities are also limited for fiat currencies and other assets in the traditional financial sector. If the FATF recommendations are implemented globally, there will be significantly less scope for anonymising or pseudonymising transactions in the future, at least for transactions between custodian wallets, as FIs engaged in VASP activities will exchange the details of the payer and payee.

8.2.6 Broad definition of financial intermediation in the DLT Act

With the Federal Act on the Adaptation of Federal Law to Developments in Distributed Ledger Technology (DLT Act) and the associated general ordinance, the concept of financial intermediary will in future be expanded in such a way that the power of disposal over assets is not the sole criterion for falling within the scope of the AMLA as an FI. The widening of the definition of financial intermediary is in line with the latest FATF recommendations to interpret the concept of financial intermediary as broadly as necessary so as to avoid loopholes in the ML/TF defence mechanism.[240] In the Swiss VA sector, anyone who "assists in transferring virtual currencies to a third party, provided that it maintains a permanent business relationship with the contractual party or that it exercises power of disposal over virtual currencies on behalf of the contractual party, and it does not provide the service exclusively to appropriately supervised FIs" is now considered an FI.[241] Providers of pure non-custodial wallets, which "merely provide software on a one-off basis", are still not subject to the AMLA.[242] However, it remains to be seen to what extent the distinction between a permanent business relationship and the one-time provision of software is practicable and effective over time as a distinguishing criterion in regard to VAs.

[239] See Section 3.8, p. 38, Innovations in the area of virtual assets (VA) and virtual asset service providers (VASPs), CGMF, *2nd National report on the risks of money laundering and terrorist financing in Switzerland*, October 2021.
[240] See FATF, *Public consultation on FATF draft guidance on a risk-based approach to virtual assets and virtual asset service providers*, March 2021, p. 29 – 30.
[241] See Federal Department of Finance (FDF): *Federal Council Ordinance on the Adaptation of Federal Law to Developments in Distributed Ledger Technology: Explanatory Report for Consultation (in German)*, October 2020.
[242] Ibid.

9. Conclusions and recommendations

In 2018 the CGMF published its first sector-specific risk analysis on the present topic. The threats and vulnerabilities associated with VAs in relation to money laundering and terrorist financing in Switzerland were classified in that report as 'significant'.[243] At the same time it was noted that MROS had received only a handful of SARs in this context and that no reliable statistical data could yet be derived from them. Since 2018, however, the risk landscape has significantly changed, and MROS now receives SARs related to VAs or VASPs on a *daily* basis. Moreover, the influence and significance of VAs has fundamentally changed since 2018. In particular, four key developments can be identified.

First, the number of FIs engaged in VASP activities in Switzerland has increased tremendously, from fewer than 10 in 2018 to at least 204 by the end of 2022. What little information is available on these FIs suggests that their activities have intensified in recent years. By the end of 2021, FIs with VASP activities in Switzerland were managing assets totalling at least a two-digit billion amount.

Secondly, the overall use of VAs in Switzerland has increased significantly over the last five years, as demonstrated by various studies and surveys. More and more people regard VAs as a legitimate means of payment. At the same time, the options for using VAs as a means of payment have also become more diverse and prevalent. As the VA sector increasingly converges with the traditional financial sector, for example through the integration of VAs into established payment platforms, the number of shops and service providers in Switzerland accepting VAs as a means of payment is likely to have grown.

Thirdly, both the criminal use of VAs and breaches of supervisory law in Switzerland have become more prevalent. Swiss law enforcement agencies are facing a growing number of cases involving VAs. Although there are no comprehensive data in this respect, the available data show a nominal and percentage increase in the loss amounts attributable to VAs, which was at least in the region of a two-digit million amount for Switzerland in 2022. However, it appears that the criminal use of VAs has not only risen, but also broadened and diversified. On the one hand, the use of VAs is now at least common in certain crimes, if not an essential part of a successful outcome from the perpetrator's point of view – for example, to receive the ransom money extorted in ransomware attacks. While until a few years ago almost all VA financial flows were denominated in Bitcoin, criminals have adapted their strategies and now use different VAs as needed, including stablecoins, NFTs and, in particular, privacy coins, which are more difficult for law enforcement tools to trace. This is a growing challenge facing law enforcement. In addition, threats are no longer limited to predicate cybercrime offences and 'crypto-specific' crimes. As a result, the range of cases that have been brought to the attention of various law enforcement agencies and MROS and in which the use of VAs can be observed has also expanded. The threats now also come from a wide range of 'offline' crimes, including the most serious forms of white-collar crime and ultimately also the use of VAs by professional money laundering networks and state actors. Various VA-related SARs received by MROS revealed links to politically exposed persons (PEPs), international corruption scandals, transnational organised crime groups and state actors. The potential of VAs for money laundering, terrorist financing and the financing of proliferation has apparently been recognised, which is why they are now widely used for financial crime. FINMA, too, has observed an increase in the number of cases and has highlighted the risks associated with VA/VASPs in its numerous publications and clarified its supervisory expectations. It has also conducted various investigations and enforcement proceedings in this context.

[243] CGMF, *National Risk Assessment: Risk of money laundering and terrorist financing posed by crypto assets and crowdfunding*, October 2018, p. 4.

Fourthly, the sharp rise in VA-related SARs submitted to MROS since 2020 shows that FIs in Switzerland are also increasingly identifying suspicious, ML/TF-related transactions on their accounts in connection with the use of VAs. Already in 2022, almost 14% of the SARs submitted to MROS were related to VAs.

As a result of these four developments, the threats and vulnerabilities identified in the 2018 risk analysis have increased in number and also widened in scope. None of the nine threats and two vulnerabilities identified in that report have decreased over the last five years. On the contrary, most of them have increased (7 out of 11), while three threats and one vulnerability remain unchanged. In addition, two threats and six vulnerabilities have been newly identified as part of this risk analysis. This report clearly shows that, due to their increased importance and the ML/TF risks they pose, VAs require greater scrutiny by the competent authorities in their AML/CFT efforts.

The VA sector is a highly dynamic and rapidly evolving environment. The new technological possibilities opened up by VA present both opportunities and risks for AML/CFT efforts. These are primarily related to the characteristics of VAs and can significantly alter the risk landscape, depending on the direction of future developments.

VAs exist as a parallel payment system to traditional payment transactions, enabling fast international transfers. As VAs and traditional payments are rapidly converging, the number of touchpoints and intersections between both systems is growing. This brings with it risks related to money laundering and terrorist financing. For one thing, law enforcement agencies and all the authorities and institutions entrusted with supervision now face an increased burden in investigating and tracing transactions, as several separate payment systems now have to be investigated. Not only does this require additional expertise, it can also complicate existing investigative processes and increase the number of steps and resources required. Second, the growing integration of VAs with traditional payment transactions makes it easier for criminals to access and use both payment systems. There is a risk that these parties will add another tool to their repertoire of money laundering techniques. They may also combine the use of VAs with traditional concealment techniques or make more use of VAs in already high-risk sectors to make it even more difficult to detect suspicious activity. Third, the growing number of points of contact and intersection between the two payment systems increases the vulnerability of all FIs (with or without VASP activities) to being misused as a transit or end point for illicit VA-related financial flows (in VAs or fiat). This vulnerability is exacerbated if FATF Recommendation No 16 (Travel Rule) is not implemented in all countries.

Nevertheless, the global volume of VA financial flows is still relatively small compared to other financial flows. Therefore, compared to other sectors, the ML/TF risks in the VA sector are still relatively low. Successful concealment of VA financial flows also requires a deep understanding of how VAs work. It is likely that the number of experts in this field is still limited and that most of their activities are limited to cybercrime and 'crypto-specific' crimes such as rug pulls, phishing for wallet data and hacks of VASPs. However, there is clear potential for VAs to enable a 'wider audience' to conceal money flows – for example, professional money launderers with roots in the traditional financial sector or transnational organised crime groups with funds of illicit origin from the 'offline' sector. This trend is already evident in some areas and requires greater awareness of the risks involved. The increased acceptance of VAs for payments, even of large amounts, combined with the rapid convergence of the VA and traditional financial sectors, could lead to increased ML/TF risks in both sectors in the medium to long term.

In any case, the growth of the VA sector is already affecting a significant part of the economic and financial sector and requires the attention of a wide range of stakeholders, including FIs, supervisory and law enforcement agencies and other bodies and actors involved in AML/CFT efforts. The present report identifies shortcomings in some areas and highlights the importance of developing knowledge and resources.

Inadequate resources and capacity can hamper cooperation between AML/CFT actors, both nationally and internationally, especially when they do not have the same level of knowledge and comparable skills in VA investigation and analysis. This can severely delay the identification and prosecution of VA-related ML/TF cases, even if they are not that difficult to detect. This problem already exists at the national level but is exacerbated at the international level, as the investigation of VA-related ML/TF cases almost always depends on well-functioning international cooperation between FIUs, law enforcement and other authorities. A weak link in this chain may be enough to seriously delay or impede the cross-border investigation of ML/TF cases. As a result, there is currently a risk in Switzerland (as in other countries) that some of the actors involved in AML/CFT efforts may not be sufficiently capable to detect and prosecute VA-related ML/TF cases under criminal or supervisory law, because they are not adequately equipped for these new challenges and do not have sufficient resources in this area.

The regulation of the Swiss VA sector is robust by international standards, and previous FATF recommendations for the VA sector have always been implemented promptly. However, in addition to the mostly global threats and vulnerabilities, this report has identified certain country-specific problem areas. Most of these can be attributed to the lack of reliable data for the Swiss VA sector.

Several factors help to mitigate the risks associated with VAs. First, international cooperation in VA investigations has already achieved some success in terms of increased tracing, freezing and confiscation of VAs, demonstrating that if the relevant authorities have sufficient resources, it is possible for them to effectively combat ML/TF in the VA sector. Second, the trend towards consolidation of providers in the VA sector has contributed to an increase in the compliance maturity of the major players. Third, the inherent transparency of most blockchains offers unique opportunities to trace financial flows in a way that is not possible with traditional payment systems. The use of blockchain analytics tools may make it easier to identify and track suspicious activity. Fourth, Switzerland has been early and transparent in communicating and implementing an applicable legal framework and supervisory expectations in the context of VA/VASPs. In particular, the FATF Travel Rule has been consistently implemented by including payments to and from non-custodial wallets, which improves the control and traceability of transactions. Finally, the broadening of the definition of financial intermediation has helped to extend the scope of the Anti-Money Laundering Act to a wider range of actors, thereby closing gaps in AML/CFT defences.

Based on the threats and vulnerabilities identified in this risk analysis, the CGMF proposes the following four measures to strengthen the current system:

1. **Improve data and knowledge on the VA sector in Switzerland**
   In order to accurately identify, understand and assess the ML/TF risks associated with VAs and to develop appropriate measures, data on the VA sector and the criminal use of VAs in Switzerland are essential. This includes information on the size, activities and focus of the sector as well as data on the number of procedures, the offences investigated and the amounts involved. This is crucial in order to effectively counter money laundering and terrorist financing and protect the integrity of the financial centre. The lack of comprehensive national and international data and information not only hampers an overall risk assessment but can also result in failure to identify developments and take the necessary measures before it is too late. Therefore, the key indicators for the sector should be compiled on a regular and comprehensive basis.

2. **Encourage proactive reporting by FIs with VASP activities**
   The figures for SARs submitted to MROS show that less than a quarter of all VA-related SARs in the period 2020–2022 originated from FIs with VASP activities. It should be

noted that a large proportion of these SARs were submitted by just four FIs with VASP activities. In total, only 24 FIs with VASP activities submitted at least one SAR in the period mentioned, although there were already more than 204 FIs with VASP activities in Switzerland at the end of 2022. Analysis of the SARs received from FIs with VASP activities reveals a somewhat reactive reporting behaviour in the sector. The supervisory authorities and institutions should therefore share the findings of this risk analysis with FIs engaged in VASP activities under their supervision and call for a more proactive reporting behaviour, for example by regularly reviewing the compliance and monitoring measures of these FIs.

3. **Provide sufficient capacity and resources to combat ML/TF in the VA sector**
   To meet the challenges of combating ML/TF in the VA sector, enhanced cooperation between competent authorities is required. Available figures and data show that the use of VAs for criminal purposes is increasing in frequency and diversity. In addition, techniques for the criminal use of VAs are constantly evolving. The development of knowledge, skills and resources is therefore a key aspect of the AML/CFT defence mechanism. In addition to the law enforcement agencies' own investigative tools (e.g. blockchain analytics), the most effective means include national and international cooperation, judicial and police mutual legal assistance with their foreign counterparts and the Budapest Convention. However, the effectiveness of these tools depends on the level of knowledge, resources and skills of the relevant stakeholders. The various authorities involved in the fight against ML/TF in Switzerland must therefore be provided with sufficient resources and capacity to effectively combat money laundering and terrorist financing in the VA sector.

4. **Strengthen international cooperation**
   Switzerland continues to work at the international level to combat criminal risks in the financial sector. This commitment is crucial and can help to reduce ML/TF risks in regard to VAs. Switzerland will continue to make a special effort to ensure that the standards that have been developed internationally in this area are rapidly implemented. Many of the threats and vulnerabilities posed by VAs affect all countries likewise, including Switzerland. Given the transnational nature of risks in the VA sector, the most important measures to minimise them must therefore be coordinated at the international level.

10. Publications

22.3017 (postulate), *Improve the capabilities of law enforcement to handle cases involving cryptocurrencies* (de/fr/it), submitted by National Council member Andri Silberschmidt on 16 March 2022.

22.3145 (postulate), *How well equipped are cantonal law enforcement agencies in the prosecution of cybercrime cases?* (de/fr/it), submitted by the Security Policy Committee of the National Council on 15 February 2022.

Aktionariat, *Create a market for your shares*, accessed in May 2023.

AP News, *Mexican cartels turn to bitcoin, internet, e-commerce*, 10 March 2022.

Bank for International Settlements (BIS), *OTC foreign exchange turnover in April 2022*, October 2022.

Barron's, *The Cryptocurrency Crash Could Lead to a Wave of M&A*, 23 June 2022.

Basel Institute On Governance, Europol, *Seizing the Opportunity: 5 recommendations for crypto-assets-related crime and money laundering*, 2022.

BBC News, *Why the Central African Republic adopted Bitcoin*, 6 June 2022.

BBI 2023 84 – *Dispatch on the amendment of the Information Security Act* (Introduction of a reporting obligation for cyberattacks on critical infrastructures) of 2 December 2022 (de/fr/it), January 2023.

Bithome, *Buy and Sell Real Estate with Bitcoin or Cryptos*, accessed in May 2023.

Bloomberg, *Tesla Trails Only MicroStrategy in Treasury Bitcoin Allocation*, 8 February 2021.

Cambridge Centre For Alternative Finance (CCAF), *3rd Global Cryptoasset Benchmark Study*, September 2020.

Canton of Zug*Kanton Zug akzeptiert ab 2021 Kryptowährungen für Steuerzahlungen* (press release), 3 September 2020.

Cash, *Handelsvolumen an der SIX 2022 rückläufig*, 3 January 2023.

Center for Philanthropy Studies (CEPS), University of Basel – SwissFoundations, Association of Swiss grant-making foundations – Center for Foundation Law, University of Zurich, *The Swiss Foundation Report 2022* (de/fr), May 2022.

Center for Philanthropy Studies (CEPS), University of Basel – SwissFoundations, Association of Swiss grant-making foundations – Center for Foundation Law, University of Zurich, *The Swiss Foundation Report 2023* (de/fr), June 2023.

CGMF, *First national report on money laundering and terrorist financing risks*, June 2015.

CGMF, *Risk of money laundering and terrorist financing posed by crypto assets and crowdfunding*, October 2018.

CGMF, *Second national report on risks of money laundering and terrorist financing*, October 2021.

Chainalysis, *2023 Crypto Crime Trends: Illicit Cryptocurrency Volumes Reach All-Time Highs Amid Surge in Sanctions Designations and Hacking*, 12 January 2023.

Chainalysis, *Crime and NFTs: Chainalysis Detects Significant Wash Trading and Some NFT Money Laundering In this Emerging Asset Class*, 2 February 2022.

Chainalysis, *Crypto Money Laundering: Four Exchange Deposit Addresses Received Over $1 Billion in Illicit Funds in 2022*, 26 January 2023.

Chainalysis, *Cryptocurrency Exchanges in 2021*, November 2021.

Chainalysis, *DeFi-Driven Speculation Pushes Decentralized Exchanges' On-Chain Transaction Volumes Past Centralized Platforms*, 6 June 2022.

Chainalysis, *North Korean Hackers Have Prolific Year as Their Unlaundered Cryptocurrency Holdings Reach All-time High*, 13 January 2022.

Chainalysis, *OFAC Sanctions Hydra Following Law Enforcement Shutdown of the Darknet Market, As Well As Russian Exchange Garantex*, 5 April 2022.

Chainalysis, *The 2020 State of Crypto Crime*, January 2020.

Chainalysis, *The 2021 Crypto Crime Report*, February 2021.

Chainalysis, *The 2021 Geography of Cryptocurrency Report*, October 2021.

Chainalysis, *The 2022 Geography of Cryptocurrency Report*, September 2022.

Chainalysis, *The 2023 Crypto Crime Report*, February 2023.

Chainalysis, *The Crypto Crime Report 2022*, February 2022.

Chainalysis, *The State of Web3*, June 2022.

Ciphertrace, *Cryptocurrency crime and anti-money laundering*, June 2022.

City of Lugano, Tether, *Lugano's Plan B*, accessed in May 2023.

CNET, *Ransomware rises as a national security threat as bigger targets fall*, 18 October 2021.

Coin ATM Radar, *Bitcoin ATM Map*, accessed in May 2023.

Coindesk, *'Ship-to-Ship' Trade and Other Secrets of North Korea's Illicit $1.5B Crypto Stash*, 7 April 2020.

Coinmap, *Crypto ATMs & merchants of the world*, accessed in May 2023.

CoinMarketCap, *Global Cryptocurrency Market Charts*, accessed in May 2023.

COLB – French Advisory Board for the Fight Against Money Laundering and Terrorist Financing, *National risk assessment of money laundering and terrorist financing in France* (fr), September 2019.

Curry, David, *Coinbase Revenue and Usage Statistics (2023)*, 28 March 2023.

Department of Justice (USA), *Two Chinese Intelligence Officers Charged with Obstruction of Justice in Scheme to Bribe U.S. Government Employee and Steal Documents Related to the Federal Prosecution of a PRC-Based Company*, 24 October 2022.

Department of the Treasury (USA), *National Money Laundering Risk Assessment*, February 2022.

Elliptic, *NFTs and Financial Crime*, August 2022.

European Central Bank (ECB), *Understanding the crypto-asset phenomenon, its risks and measurement issues*, May 2019.

European Parliament, *Crypto-assets: green light to new rules for tracing transfers in the EU*, April 2023.

Europol Spotlight, *Cryptocurrencies – Tracing the Evolution of Criminal Finances*, December 2021.

Europol, *Bitzlato: senior management arrested*, 23 January 2023.

Europol, *Underground drug-money bank laundering EUR 180 million liquidated by law enforcement*, 13 April 2023.

FATF, *Anti-money laundering and counter-terrorist financing measures - Switzerland, Enhanced Follow-up Report & 2nd Technical Compliance Re-Rating*, January 2020.

FATF, *Countering Ransomware Financing*, March 2023.

FATF, *FATF Report to the G20 Finance Ministers and Central Bank Governors on So-called Stablecoins*, June 2020.

FATF, *Guidance for a Risk-Based Approach to Virtual Currencies*, June 2015.

FATF, *Guidance to a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, June 2019.

FATF, *Outcomes FATF Plenary, 17-19 October 2018*, October 2018.

FATF, *Press Release – Virtual Assets Contact Group (VACG)*, 14 April 2023.

FATF, *Public consultation on FATF draft guidance on a risk-based approach to virtual assets and virtual asset service providers*, March 2021.

FATF, *Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers*, June 2022.

FATF, *Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers*, June 2023.

FATF, *The FATF Recommendations*, February 2023.

FATF, *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers,* October 2021.

FATF, *Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing*, September 2020.

FATF, *Virtual Currencies. Key Definitions and Potential AML/CFT Risks*, June 2014,

Federal Council, *Federal Council report on virtual currencies in response to the Schwaab (13.3687) and Weibel (13.4070) postulates, 25 June 2014* (de).

Federal Council, *Leading worldwide, rooted in Switzerland: Policy for a future-proof Swiss financial centre*, December 2020.

Federal Department of Finance (FDF), *Federal Council Ordinance on the Adaptation of Federal Law to Developments in Distributed Ledger Technology: Explanatory Report for Consultation* (de), October 2020.

Federal Gazette BBl 2020 7801, *Federal Act on Explanatory Report for Consultation on Federal Council Ordinance on Adaptation of Federal Legislation to Developments in Digital Ledger Technology* (de/fr/it), October 2020.

Federal Statistical Office (FSO), *Police Crime Statistics – 2021 Annual Report (de/fr/it)*, March 2022.

Federal Statistical Office (FSO), *Police Crime Statistics – 2022 Annual Report (de/fr/it)*, March 2023.

Financial Crimes Enforcement Network (FinCEN), *Advisory on Illicit Activity Involving Convertible Virtual Currency*, May 2019, p. 1 – 2.

Financial Crimes Enforcement Network (FinCEN), *FinCEN Announces $100 Million Enforcement Action Against Unregistered Futures Commission Merchant BitMEX for Willful Violations of the Bank Secrecy Act*, 10 August 2021.

Financial Intelligence Unit (Estonia), *The Risks related to Virtual Asset Service Providers in Estonia*, January 2022.

Financial Intelligence Unit (Estonia), *Yearbook 2019*, 2020.

Financial Intelligence Unit (Germany), *2021 Annual Report*, August 2022.

Financial Intelligence Unit (Germany), *Annual Report 2019*, June 2020.

Financial Intelligence Unit (Liechtenstein), *Annual Report 2020*, March 2021.

Financial Intelligence Unit (Liechtenstein), *Annual Report 2021*, April 2022.

Financial Intelligence Unit (Netherlands), *Annual Review 2019*, June 2020.

Financial Intelligence Unit (Netherlands), *Annual Review 2021*, June 2022.

Financial Stability Board (FSB), *Assessment of Risks to Financial Stability from Crypto-assets*, February 2022.

Financial Stability Board (FSB), *FSB Chair's letter to G20 Finance Ministers and Central Bank Governors*, March 2018.

Financial Stability Institute, *Supervising cryptoassets for anti-money laundering*, April 2021.

Financial Times, *How North Korea became a crypto crime hub*, 14 November 2022.

Finews, *1 Milliarde Krypto-Nutzer bis ins Jahr 2030*, 25 July 2022.

Finews, *Chainalysis: Crypto Hacks Reach Record $3 Billion*, 13 October 2022.

Finews, *EU erhält europaweite Krypto-Regulierung*, 21 April 2023.

Finews, *Tessiner dürfen ihre Steuern jetzt in Bitcoin zahlen*, 7 July 2022.

Forbes, *Scandals And Mafia Allegations May Force Malta To Reconsider Its Reliance On Online Betting*, 13 March 2021.

Gotham City, *L'enquête sur les pirates allemands de Movie2k passe par Genève*, No 278, 26 January 2023.

Government Of The Grand Duchy Of Luxembourg, *ML/TF Vertical Risk Assessment: Virtual Asset Service Providers*, December 2020.

Handelszeitung, *6000 Kunden kaufen bei der SBB Bitcoins | Handelszeitung*, 1 November 2017.

Handelszeitung, *85'000 Händler in der Schweiz können nun Zahlungen mit Bitcoin und Ether annehmen*, 19 August 2021.

Handelszeitung, *Krypto lockt: Studie zeigt grosses Interesse in der Schweiz*, 22 June 2021.

HM Treasury, *National risk assessment of money laundering and terrorist financing 2020*, December 2020.

Home of Blockchain, *Swiss Digital Asset Market Report 2022*, May 2022

Institute of Financial Services Zug IFZ (Lucerne University of Applied Sciences and Arts), *Crypto Assets Study 2021*.

Institute of Financial Services Zug IFZ (Lucerne University of Applied Sciences and Arts), *Crypto Assets Study 2022*.

Institute of Financial Services Zug IFZ (Lucerne University of Applied Sciences and Arts), *Fintech Study 2023*.

International Monetary Fund (IMF), *F.18 Recording of Crypto Assets in Macroeconomic Statistics*, March 2022

International Monetary Fund (IMF), *Treatment of Crypto Assets in Macroeconomic Statistics*, 2019.

Jimenez, Alison, *3 Misconceptions about Cryptocurrency Crime Estimates*, 11 January 2022.

L'avvenire di Calabria, Boom delle scommesse online, ma per la Dia c'è l'ombra dei clan, 23 January 2020.

Malta Gaming Authority, *2021 Annual Report*, September 2022.

McGuire, Michael, *Into the Web of Profit. Understanding the Growth of the Cybercrime Economy*, April 2018.

Migros Bank, *Kryptowährungen bei jüngeren Generationen beliebter als Gold*, 27 February 2020.

Monetary Authority of Singapore, *Guidelines to Notice PSN02 on Prevention of Money Laundering and Countering the Financing of Terrorism - Digital Payment Token Service*, March 2020.

Money Laundering Reporting Office Switzerland (MROS), *Annual Report 2020*, May 2021.

Moneyland, *So investieren Schweizerinnen und Schweizer ihr Geld*, 19 July 2022.

Moneyland, *Wie legen Schweizer ihr Geld an?*, 22 April 2020.

Monroe, Brian, *FinCEN, OFAC fine crypto exchange Bittrex nearly $30 million on AML, sanctions failings, missed SARs, links to darknet markets, mixers, ransomware gangs*, 11 October 2022.

Nasdaq, *Blockware Estimates 10% Global Bitcoin Adoption By 2030: Report*, 9 June 2022.

National Coordinating Committee on Combating Money Laundering and Funding of Terrorism (Malta), *Key Results of the Sectoral Risk Assessment on Virtual Financial Assets*, February 2020.

National Cyber Security Centre (NCSC), *Semi-Annual Report 2022/II (July–December)*, May 2023.

New York Times, *Banks Tried to Kill Crypto and Failed. Now They're Embracing It (Slowly)*, 1 November 2021.

New York Times, *Coinbase Reaches $100 Million Settlement With New York Regulators*, 4 January 2023.

New York Times, *Government Cracks Down on Crypto Industry With Flurry of Actions*, 18 February 2023.

New York Times, *In Global First, El Salvador Adopts Bitcoin as Currency*, 7 September 2021.

Official Journal of the European Union, *Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849, OJ L 150*, 9 June 2023.

Organized Crime & Corruption Reporting Project (OCCRP), *Italian Mafia Bets on Illegal Online Gambling*, 4 March 2021.

Prestige Business, *Cyber-Attacken in der Schweiz nehmen auch 2023 zu*, 3 May 2023.

Reuters, *Crypto exchange Bittrex to pay $29-mln penalty to U.S. Treasury Department*, 11 October 2022.

Reuters, *Dutch central bank fines Binance 3.3 million euros*, 18 July 2022.

Reuters, *Dutch central bank fines cryptocurrency exchange Coinbase 3.3 mln euros*, 26 January 2023.

RR.2022.45, *Arrêt du 20 décembre 2022 – Cour des plaintes*, Judgment of the Federal Criminal Court, Bellinzona, 21 December 2022.

Schurter, Daniel, *Das ist die gefährlichste Hackerbande, die auch in der Schweiz wütet*, 23 January 2023.

Schweizer Radio und Fernsehen (SRF), *Die Schweiz tut sich schwer mit Gesetzesverschärfungen zum Gold*, 10 May 2022.

SR 0.311.43 – *Convention of 23 November 2001 on Cybercrime* (de/fr/it), status as of 14 September 2020.

SR 935.51 – *Federal Act on Gambling* (Gambling Act, GamblA) (de/fr/it), status as of 1 January 2021.

SR 935.511 – *Gambling Ordinance* (GamblO) (de/fr/it), status as of 1 January 2021.

SR 941.31 – *Federal Act on the Control of the Trade in Precious Metals and Precious Metal Articles* (Precious Metals Control Act, PMCA), status as of 1 January 2023.

SR 955.0 – *Federal Act of 10 October 1997 on Combating Money Laundering and Terrorist Financing in the Financial Sector*, (Anti-Money Laundering Act, AMLA), status as of 23 January 2023.

SR 955.01 – *Ordinance on Combating Money Laundering and Terrorist Financing* (Anti-Money Laundering Ordinance, AMLO), status as of 1 January 2016.

SR 955.01 – *Ordinance on Combating Money Laundering and Terrorist Financing* (Anti-Money Laundering Ordinance, AMLO), status as of 1 August 2021.

SR 955.033.0 – *Ordinance of the Swiss Financial Market Supervisory Authority on Combating Money Laundering and Terrorist Financing* (Anti-Money Laundering Ordinance FINMA, AMLO-FINMA), status as of 1 January 2021.

SR 958.1 – *Federal Act of 19 June 2015 on Financial Market Infrastructures and Market Conduct in Securities and Derivatives Trading* (Financial Market Infrastructure Act, FinMIA).

SR 958.11 – *Ordinance on Financial Market Infrastructures and Market Conduct in Securities and Derivatives Trading* (Financial Market Infrastructure Ordinance, FinMIO).

Stalinsky, Steven, *The Coming Storm – Terrorists Using Cryptocurrency*, 21 August 2019.

State Financial Service of Ukraine, *Report on the National Risk Assessment*, 2019.

State Secretariat for International Finance (SIF), *Blockchain/DLT*, accessed in May 2023.

State Secretariat for International Finance (SIF), *Factsheet - Blockchain and cryptoassets in the financial sector: Switzerland's pioneering role on the international stage*, January 2022.

State Secretariat for International Finance (SIF), *Mandate of the Interdepartmental coordinating group on combating money laundering and the financing of terrorism* (de), approved by the Federal Council Decree of 17 November 2021.

State Secretariat for International Finance (SIF), *Swiss financial sector, Key figures 2023,* April 2023.

Süddeutsche Zeitung, *Wieso die Mafia Fan von Maltas Online-Casinos ist*, 18 December 2022.

Swedish Police Authority, *The Financial Intelligence Unit Annual Report 2021*, May 2022.

Swiss Bankers Association (SBA), *Agreement on the Swiss banks' code of conduct with regard to the exercise of due diligence (CBD 20)*, 2020.

Swiss Crime Prevention, *Money Mules* (de/fr/it), accessed in May 2023.

Swiss Federal Railways (SBB), *Buy a Bitcoin paper wallet*, accessed in May 2023.

Swiss Financial Market Supervisory Authority (FINMA), *2016 Annual Report*, March 2017.

Swiss Financial Market Supervisory Authority (FINMA), *Annual Report 2020*, March 2021.

Swiss Financial Market Supervisory Authority (FINMA), *Annual Report 2021*, March 2022.

Swiss Financial Market Supervisory Authority (FINMA), *Annual Report 2022*, March 2023.

Swiss Financial Market Supervisory Authority (FINMA), *FINMA concludes proceedings against crypto platform and its founder*, May 2023.

Swiss Financial Market Supervisory Authority (FINMA), *Guidance 02/2019 – Payments on the blockchain*, August 2019.

Swiss Financial Market Supervisory Authority (FINMA), *Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs)*, February 2018.

Swiss Financial Market Supervisory Authority (FINMA), *Risk Monitor 2022*, November 2022.

Swiss Financial Market Supervisory Authority (FINMA), *Supplement to the guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs)*, September 2019.

Swiss Foundations, *Der Schweizer Stiftungsreport*, CEPS Forschung und Praxis. Vol. 30 June 2023.

Swissinfo, *Gold sourcing and Switzerland in focus at the Human Rights Council*, 3 October 2022.

Tages Anzeiger, *Schweizer Online-Drogenversand – Hippe Kleider, Typ Studentin, und das Täschli voller Drogen*, 18 March 2021.

Triple-A, *Global Cryptocurrency Ownership Data*, accessed in May 2023.

TRM Labs, *Ensuring Responsible Development of Digital Assets; Request for Comment*, November 2022.

United Nations Data Retrieval System, *Democratic People's Republic of Korea*, accessed in May 2023.

United Nations Office on Drugs and Crime (UNODC), *Money Laundering*, accessed in May 2023.

United Nations Security Council, *S/2021/211 final report of the Panel of Experts*, March 2021.

United Nations Security Council, *S/2022/132 Report of the 1718 Panel of Experts*, March 2022.

United Nations Security Council, *S/2022/668 Midterm report of the 1718 Panel of Experts*, September 2022.

Vedrenne, Gabriel, *In Europe, Suspicious Payments Triple Thanks to VASPs, Cryptocurrency*, 25 October 2022.

Von Luckner, Reinhart & Rogoff, *Decrypting New Age International Capital Flows, NBER Working Paper No. 29337*, October 2021, p. 1, footnote 2

Wired Magazine, *Most Criminal Cryptocurrency Funnels Through Just 5 Exchanges*, 26 January 2023.

World Bank, *GDP (current US$) – World*, accessed in May 2023.

World Bank, *Virtual Assets and Virtual Asset Service Providers ML/TF Risk Assessment Tool*, June 2022.

11. Annex

11.1 MROS methodology for analysis of suspicious activity reports

The introduction of the goAML system has opened up new possibilities for MROS to analyse the data it receives from FIs, domestic authorities and foreign Financial Intelligence Units. The data are now stored in a relational data processing system and can be analysed more in-depth using various retrieval procedures. MROS has successfully applied this new methodology in the context of this report. A simplified description is given below.

For the results of the analysis of SARs presented in Chapter 7, an analysis was conducted to determine which of the SARs submitted in the years 2020 to 2022 were 'VA-related'. To be classified as VA-related, an SAR had to meet at least one of the following criteria:

1. Identification of relevant SARs based on transaction, account and account-holder details: The SAR had to show transactions between the accounts specified in the SAR and accounts (unambiguously identified by MROS) of Swiss or foreign FIs with VASP activities. By definition, this includes SARs submitted by Swiss FIs with VASP activities, provided that these SARs contain suspicious transactions or facts involving VAs.[244] On the other hand, it also includes SARs from FIs *without* VASP activities whose reported transactions involve an FI (unambiguously identified by MROS) with VASP activities in Switzerland or abroad as one of the transaction counterparties (recipient or sender).

2. Identification of relevant SARs based on a list of VA-specific keywords:[245] Each SAR submitted to MROS contains a written description of the facts provided by the reporting financial intermediary. This had to contain at least one of at least 50 keywords (e.g. 'Bitcoin', 'crypto') in order to be added to the set of SARs earmarked for further in-depth analysis. Care was taken to ensure that SARs identified by way of keywords were only classified as VA-related if they did not generate false positives (e.g. FIAT as a car brand or 'mining' in the sense of ore mining).

For the years 2020 to 2022, a total of 1,867 SARs met at least one of these criteria. This is a conservative estimate: there may actually be more VA-related reports among the 18,937 SARs received during that period. For one thing, it is possible that other SARs contained transactions between the accounts indicated in the SAR and accounts of Swiss or foreign FIs with VASP activities but that these transactions were not reported by the FIs[246] or that these accounts were not known to MROS, so the corresponding SARs could not be identified. Secondly, it is possible that an SAR did in fact have a connection with VAs or VASPs but that this was not identified by way of the keyword search. The applied keyword method can only identify those SARs in which the reporting financial intermediary had already established a connection with VAs and explicitly mentioned this in the written facts, enabling it to be identified using the keyword list. Furthermore, additional information requested by MROS to analyse the report (in accordance with Art. 11a AMLA) was not taken into account in the analysis. The specified number of SARs related to money laundering is therefore a minimum estimate.

The sample obtained using this method was then categorised according to whether the SAR was submitted by an FI with or without VASP activities, as this would determine which forms

[244] SARs from FIs with VASP activities are not necessarily VA-related, as some of these FIs also offer conventional financial services unrelated to VAs. See Figure 4 in Section 4.2.
[245] The keywords were identified and collected by MROS in the preparation of this risk analysis. All the keywords were used in different languages (English, German, Italian, French) and with different spellings for the text search.
[246] As required by MROS, the SARs submitted to MROS generally contain structured details on those transactions deemed suspicious by the financial intermediary.

of financial flows and different typologies could be identified. In the SARs from FIs without VASP activities, the financial flows were in fiat form only, whereas SARs from FIs with VASP activities could include both fiat and VA transactions. It should also be noted that the SARs submitted by FIs with VASP activities do not necessarily comprise all SARs submitted by these FIs, as they may have also submitted SARs unrelated to VAs or VASPs, particularly if these FIs (e.g. banks) also offer their clients traditional financial services unrelated to VAs (see Figure 4 in Section 4.2). The 1,867 reports were analysed both quantitatively and qualitatively using a list of evaluation indicators. The focus was on the information about the reporting FIs, the predicate offences suspected by the reporting financial intermediary, the elements giving rise to suspicion, the counterparties reported, the financial flows identified and the amounts involved.

11.1.1 SARs from FIs with VASP activities before 2020

Although the present risk analysis focuses primarily on the period after 2020, the number of SARs received by MROS from FIs with VASP activities was also analysed for the years 2015 to 2019. This gives an insight into the increase in the number of SARs and the reporting behaviour of these FIs over a longer period of time.

However, some clarifications are needed when comparing the figures for the period from 2020 with those of previous years. Prior to 2020, MROS counted a single reported business relationship as an individual SAR. With the introduction of the goAML system at the end of 2019, the way in which SARs received by MROS are counted was changed.[247] It is now possible to report several business relationships simultaneously in a single SAR, i.e. if they are reported by the reporting financial intermediary in the same context or on the basis of one and the same suspicious circumstance. Since 1 January 2020, MROS has therefore been counting the number of SARs rather than the number of reported business relationships. This makes it difficult to compare the figures up to and including 2019 with those from 2020 onwards. To make this comparison in the present analysis, the 185 business relationships reported between 2015 and 2019 were examined and several of them were counted together as one SAR if they were reported by the same financial intermediary, at the same time and under the same circumstances.[248] Using this method, the 185 business relationships were grouped into 53 SARs.

11.2 Details for specific illustrations

Figure 22, Section 7.3.2
The 'Others' category comprises the following other predicate offences suspected by reporting FIs:

- Foreign Nationals and Integration Act (Art. 116 para. 3, Art. 118 para. 3 FNIA)
- Banking Act (Art. 47 para. 1bis BankA)
- Gambling Act (Art. 130 para. 2 GamblA)
- Theft (Art. 139 SCC)
- Import, acquisition and storage of counterfeit money (Art. 244 para. 2 SCC)
- Extortion (Art. 156 SCC)
- Counterfeiting money (Art. 240 para. 1 SCC)

[247] Money Laundering Reporting Office Switzerland (MROS), *Annual Report 2020*, May 2021, p. 16.
[248] For example, more than 100 of these 185 business relationships were reported to MROS by the same financial intermediary on the basis of the same suspicious transactions.

- Goods Control Act (Art. 14 para. 2 GCA)
- Therapeutic Products Act (Art. 86 para. 2 TPA)
- Exploitation of insider information or price manipulation (Art. 154 para. 2, Art. 155 para. 2 FinMIA)
- Bankruptcy and debt collection felonies or misdemeanours (Art. 163 No 1, Art. 164 No 1, Art. 165, Art. 171 para. 1 SCC)
- Fraud in respect of payments and services (Art. 14 para. 4 ACLA, Art. 51 NESA)
- Murder (Art. 112 SCC)
- Sexual offences (Art. 187 No 1, Art. 189, Art. 190, Art. 191, Art. 195, Art. 197 para. 4 SCC)
- Other offences
- Sport Promotion Act (Art. 22 para. 2 and 3 SpoPA)
- Unauthorised access to data (Art. 143 SCC)
- Misconduct in public office (Art. 314 SCC)
- Criminal mismanagement (Art. 158 No 1 and 2 SCC)
- Federal Copyright Act (Art. 67 para. 2, Art. 69 para. 2 CopA)
- Document forgery (Art. 251 No 1, Art. 253, Art. 254, Art. 317 No 1 SCC)
- Felonies and misdemeanours against the state (Art. 265, Art. 266bis, Art. 266b, Art. 267 No 1 and 2, Art. 271 No 1 para. 4, No 2 and No 3 SCC)
- Offences against the Embargo Act (Art. 9 para. 2 EmbA)
- Misappropriation (Art. 138 SCC)
- Intentional homicide (Art. 111 SCC)
- Counterfeiting of goods (Art. 155 para. 2 SCC)
- Other punishable offences against property (Art. 140, Art. 144bis No 2, Art. 148, Art. 157, Art. 160 SCC