2024

SECTORAL ASSESSMENT FOR VIRTUAL ASSET SERVICE PROVIDERS IN ROMANIA

www.onpcsb.ro

CONTENTS

The National Office for Prevention and Control of Money Laundering (FIU Romania)

+40 213 155 207

onpcsb@opcsb.ro

22 Tudor Vladimirescu Boulevard, Green Gate building, 7th floor, 5th District, Bucharest, Romania

Definitions and keywords

CRYPTO-ASSETS	Forms of digital value, that use cryptography to secure transactions and control the creation of additional units (cryptocurrencies, various types of tokens, NFTs, etc.).
CRYPTOCURRENCY	A distinct sub-category of cryptoassets, a type of digital, virtual, non-bankable currency used as a means of payment (e.g. Bitcoin, Ethereum, Ripple, Avalanche). Cryptocurrencies have their own blockchain and use cryptography to secure transactions and control the generation of new units.
FATF (FINANCIAL ACTION TASK FORCE)	International body that sets global standards to prevent money laundering and terrorist financing.
TF (TERRORIST FINANCING)	The act of providing funds to support terrorist activities or terrorist organizations.
ML (MONEY LAUNDERING)	The process by which funds obtained from illegal activities are transformed into legitimate assets.
VASP (VIRTUAL ASSETS SERVICE PROVIDER)	Providers of services related to virtual assets (cryptocurrencies) and include exchanges, digital wallet providers, financial intermediaries and other entities that offer crypto-asset management and transfer services. These entities operate in accordance with the relevant regulations in force

I

Introduction

1.1. Purpose of the evaluation

The risk assessment of the virtual asset service provider (VASP) sector aims to analyze the significant opportunities and risks associated with this sector, particularly in the context of money laundering (ML) and terrorist financing (TF). The rapid development of this sector, both globally and in Romania, requires a detailed assessment of specific vulnerabilities in order to implement appropriate supervisory and compliance measures.

In October 2018, the Financial Action Task Force (FATF), the international developer of standards to combat ML/TF, adopted a new standard and issued guidance on the regulation and supervision of virtual assets (VA) and virtual assets service providers (VASPs). The FATF recommends countries to identify, assess and understand ML/TF risks, develop and implement a national risk-based regime. Recommendation 15 as amended by the FATF requires that the sector be regulated for ML/TF purposes, i.e. VASPs must be licensed or registered and be subject to effective monitoring or oversight systems [1].

[1] FATF - Updated Guidance for a Risk-Based Approach – Virtual Assets and Virtual Asset Service Providers - October 2021

Although some jurisdictions have introduced regulations, overall implementation is relatively weak and compliance lags behind most other financial sectors. Based on 98 mutual evaluation and follow-up reports, about 75% of jurisdictions are only partially or not compliant with FATF requirements. FATF's March 2023 survey found that 34% of respondents had not conducted a risk assessment on VA and VASP, citing lack of reliable data and limited guidance as the main challenges [2].

In September 2022, the National Office for Preventing and Combating Money Laundering, in collaboration with the National Bank of Romania, the Financial Supervisory Authority, the Ministry of Justice, the Ministry of Internal Affairs, the Prosecutor's Office of the High Court of Cassation and Justice and the Romanian Intelligence Service, prepared the first report on the National Assessment of Money Laundering and Terrorist Financing Risks. This report covered the period 2018-2020 and highlighted the fact that the economic sector in which cryptocurrency service providers operate presents a high level of risk, characterized by the anonymity of transactions, their speed and the lack of limitations on the volume of funds transferred.

According to the National Risk Assessment, the case analysis identified 52 situations where cryptocurrencies were used to launder criminal proceeds. The most common associated crimes were corruption, cybercrime, fraud, phishing and skimming fraud, and tax evasion. External inflows were found to be the main mechanism through which the proceeds of these crimes were introduced into the banking system, while external transfers and cash withdrawals were the main methods of externalizing the laundered money.

Based on the FATF recommendations and the findings of the National Risk Assessment, the Committee of Experts for the Evaluation of Anti-Money Laundering and Counter-Terrorist Financing Measures (Moneyval) highlighted in its May 2023 peer review report that the Romanian authorities have initiated some important steps towards the regulation and supervision of virtual asset service providers (VASPs). However, a comprehensive risk assessment of virtual asset (VA) and VASP activities has not yet been conducted and the requirements for VASPs are currently limited to exchanges and wallet holders.

This sectoral assessment aims to analyze in detail the risks associated with VASPs activities in Romania, taking into account existing national legislation, international regulations, the findings of the National Risk Assessment and the findings of the Moneyval Report (2023), which emphasized the need to conduct a comprehensive risk assessment.

[2] FATF - Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers – June 2023

This report will contain recommendations and mitigation measures, and specific actions will be monitored and evaluated in line with national and European regulatory developments, including the implementation of the MiCA Regulation and other applicable regulations by the end of 2024.

1.2. Objectives of the evaluation

The objectives of the sectoral risk assessment of the risks associated with the activities of virtual asset service providers (VASPs) are essential to ensure a comprehensive understanding of the challenges and opportunities presented by this emerging sector. In this context, the assessment aims to identify and assess specific money laundering (ML) and terrorist financing (TF) risks, taking into account the latest international standards set by the Financial Action Task Force (FATF), the European Commission's 2022 Supranational Risk Assessment (SNRA), the findings of the National Risk Assessment (NRA), and the Moneyval Report (2023).

A central objective is to link VASP's specific risks to those highlighted in the Supranational Risk Assessment. This linkage will allow for a more informed approach, taking into account the risk and vulnerability measures identified at both national and international levels. The assessment will take into account all relevant factors, including the types of services and products offered, customer risks, as well as geographic factors influencing VASP's activity in Romania.

Another important aspect is the adjustment of regulatory measures. The assessment aims to develop tailored regulatory measures based on the risks identified, ensuring effective alignment with international best practice. This fine-tuning will include the formulation of specific recommendations to address the risks, in particular with regard to activities that allow business relationships without the physical presence of the customer and anonymous transactions or transactions under pseudonyms.

Another key objective is to propose appropriate risk mitigation measures. This will include identifying strong digital identity solutions to counter anonymized transactions and ensuring an effective customer identification and verification system. The assessment will also consider the risks associated with the use of crypto-ATMs, which can provide a gateway for criminals to introduce illicit funds into the crypto ecosystem.

In addition, the evaluation will contribute to the development of a system of continuous monitoring and assessment of risks, together with the effectiveness of regulatory and counter ML/TF measures.

This monitoring will take into account developments in the VASP sector and the future implementation of the MiCA Regulation, thus ensuring a dynamic and adaptable regulatory framework.

Finally, the assessment will promote awareness and education among virtual asset service providers and their users, aiming to increase awareness of the associated risks and measures to prevent ML/TF, thus contributing to a safer and more transparent environment. By realizing these objectives, the sectoral assessment aims to contribute to the construction of an effective regulatory and monitoring framework, which responds to the current and future challenges of the VASP sector in Romania, aligning with international standards and EU requirements

1.3. The risk assessment methodology

The methodology used to assess the risks in the sector of virtual currency and fiat currency exchange service providers (VASPs) in Romania has been developed in compliance with the FATF international recommendations and the internationally adopted methodologies for combating money laundering and terrorist financing. FATF recommends countries to conduct risk assessments in each sector subject to these requirements, with the aim of identifying, assessing and understanding the associated risks, and adopting proportionate preventive measures.

The risk assessment process for the VASP sector was structured in several key steps, including data collection and analysis, identification of relevant sources of information, and assessment of the risks associated with money laundering and terrorist financing. The main steps of the process included the analysis of the general context of the VASP sector, which considered the number of active entities, the volume of transactions and the level of adoption of crypto-assets at national level, as well as the identification of key characteristics specific to the VASP sector, including risks, threats, vulnerabilities, likelihood of adverse events and their consequences.

The research of national and international sources of information, the adaptation of data collection modules to the specific national context, the formulation of requests to the authorities involved and the collection of information from the sector entities through tools such as questionnaires addressed to the VASP sector, requests to the relevant competent authorities, statistical sheets on the profile of users, as well as the analysis of cases of misuse of VASP services, were essential steps in the realization of the sector assessment.

The committee responsible for the sectoral assessment of VASPs, appointed at the level of the National Office for the Prevention and Combating of Money Laundering, managed the collection, analysis and interpretation of data from national and international sources, ensuring that the methodology complied with international standards. The risk assessment of the VASP sector in Romania included a detailed analysis of the geographic, economic and legal context to understand the size, characteristics and specific vulnerabilities of the sector.

The evaluation also covered the analysis of money laundering cases independent of other crimes, the sources of funds from domestic and international illegal activities associated with the VASP sector, and how the proceeds of predicate offences enter the financial system through this sector. The link with other economic sectors with which VASPs interact was also assessed.

The report summarizes the risk assessment associated with the VASP sector, highlighting the main money laundering and terrorist financing risks, describing the vulnerabilities identified, the overall level of risk exposure and the effectiveness of the management measures in place. This summary provides a clear picture of the state of compliance and the sector's ability to prevent and combat money laundering and terrorist financing activities, providing recommendations for improving supervision, collaboration and implementation of AML/CFT policies in line with international standards.

1.4. Sources of data and information

Information plays an essential role in the development of a sector assessment, having a direct impact on the quality and final results. An important step in assessing the risks associated with the virtual asset service provider sector in Romania was the use of effective tools and procedures to identify relevant sources of information and collect both quantitative and qualitative data. In order to obtain a clear picture of money laundering and terrorist financing risks, information from a variety of sources was exploited. Among these, the information provided by entities in the VASP sector was particularly valuable, as operators in this field have practical experience in ML/TF prevention and counter-measures. Working with these entities has provided relevant insights into the risks and challenges facing the sector.

VASP sector entities were a primary source of information, given their expertise and knowledge in preventing and combating money laundering and terrorist financing. Data collection from these entities was carried out through questionnaires, designed to obtain specific information on the typologies of activity, perceived risks and compliance measures implemented. These questionnaires allowed a detailed assessment of how VASPs manage their risks and react to identified threats, providing a solid basis for further analysis.

Collaboration with competent law enforcement authorities has also been essential. They provided relevant statistical data, including information on cases associated with this sector. This data, together with observations on typologies and trends in ML/TF prevention work, helped to provide a clear picture of the existing risks and the interventions needed.

The National Office for the Prevention and Combating of Money Laundering (NOPCML) played a central role in the assessment process, being responsible for receiving and analyzing suspicious transaction reports. The information provided from the NOPCML database was crucial in identifying threats and vulnerabilities in the VASP sector, as well as uncovering emerging trends that could affect this area.

In addition to these domestic sources, information from international organizations and specialized bodies such as FATF, MONEYVAL has been integrated. These provided valuable studies and reports on ML/TF typologies, promoting international standards relevant to the VASP sector. Also, the European Commission's 2022 supranational risk assessments (SNRAs) provided an important reference framework for national analysis.

The National ML/TF Risk Assessment Report, published in 2022, was another foundational source of information, providing data and findings relevant to the VASP sector. In addition, the guide developed by the National Office for Preventing and Combating Money Laundering included suspicious indicators and money laundering typologies in the cryptoassets field, providing a useful tool for understanding specific risks.

The results of the surveillance activities carried out by the National Office for the Prevention and Combating of Money Laundering complemented the analysis, providing a clear view on compliance and possible vulnerabilities in the sector. Credible open sources have also been used to complement information obtained from more formal sources, thus ensuring a more informed assessment.

The data collection tools had a significant impact on the assessment process, facilitating the identification of risk management priorities. These included establishing areas of focus for assessment, analyzing the general context of the VASP sector, and identifying key characteristics relevant for ML/TF risk assessment. This involved a detailed examination of the associated threats and vulnerabilities, as well as the likelihood of negative events.

The collection of relevant data and information was a crucial activity to complete the evaluation. This included researching national and international sources of information, adapting the data collection modules to the specific national context, formulating requests to the authorities involved and collecting information from sector entities through these tools. In addition, the analysis of the responses received from law enforcement and other relevant competent authorities involved, including the NOPCML, ensured a rigorous and informed risk assessment.

In the context of the relatively small size of the VASP sector in Romania, the data collected was not limited to a small number of known cases. The assessment was designed to capture emerging trends, vulnerabilities and wider threats, including those that have not yet manifested themselves clearly in the country. A comparison of the misuse of VASP services in Romania with those in other jurisdictions was also undertaken to gain a deeper understanding of global trends and cross-border risks. This approach included the integration of information from reliable international sources such as other countries' sector reports and specific studies on the risks associated with the VASP sector. This was a necessity, especially in the context that Romania did not have sufficient domestic cases to build a solid basis for analysis.

1.5. Structure of the report

Introduction

The purpose of this chapter is to outline the general framework for assessing the risks associated with money laundering and terrorist financing, in line with the international standards set by the Financial Action Task Force (FATF) and specific national requirements. It highlights the fundamental purpose of the assessment, which is to identify and analyze the risks inherent to the VASP sector, essential for the formulation of effective prevention policies. The assessment methodology is detailed, providing a description of the process used to collect and analyze data. The sources of information included are varied, encompassing reporting entities, regulators, law enforcement agencies, the National Office for the Prevention and Combating of Money Laundering, as well as relevant open sources and guidelines.

VASP Sector Profile

This chapter is devoted to exploring the profile of the VASP sector, starting with a clear definition of the sector and its fundamental role in the national economy. The economic importance of the sector is analyzed, highlighting its significant contributions. Contextual factors influencing the evolution of the sector are also examined, including global trends and emerging regulations. The relevant legal framework is detailed, highlighting existing national regulations as well as the new harmonized legal framework at EU level.

ML/TF Risk Assessment

This chapter focuses on VASP sector-specific ML/TF risk assessment. Various typologies of associated risks are presented, drawing on statistical data and reports produced by international institutions. The risk assessment based on customer characteristics is carried out by means of questionnaires and analysis from international reports. The risks associated with the products and services offered by VASPs are also examined, based on information collected from the entities through questionnaires. The chapter concludes with a detailed analysis of external and internal threats, highlighting the vulnerabilities of the sector to various forms of financial crime.

Threats and Vulnerabilities

This chapter investigates in depth the typologies of money laundering that occur within the VASP sector, drawing on national and international guidelines and resources. It addresses the magnitude and nature of the terrorist financing phenomenon, highlighting the implications for national and international security. Vulnerability analysis of the VASP sector is undertaken through an examination of the linkages with other economic sectors, identifying synergies and risks associated with them.

Risk Management

This chapter discusses measures to prevent and mitigate the risks of ML/TF, based on regulations set by national and European legislation. Response strategies and risk management are analyzed in detail, highlighting ways in which the VASP sector can adopt effective compliance practices. The criteria for risk profiling are discussed, including the development of a risk matrix indicating the level of risk associated with the VASP sector in Romania.

Conclusions and Recommendations

The final chapter summarizes the main findings of the assessment, highlighting the significant risks identified within the VASP sector. It formulates a series of concrete recommendations for authorities and entities in the sector, aimed at supporting the implementation of effective measures to prevent and combat ML/TF. These recommendations are based on previous analysis and findings with the objective of strengthening the integrity and security of the financial sector as a whole.

II

Sector profile

Assessing the VASP sector in Romania involves a comprehensive analysis of the geographical, economic and legal context in order to understand both the size and the vulnerabilities of this sector. Romania's strategic position in South-Eastern Europe and its status as a member state of the European Union facilitate significant cross-border flows, which, while offering economic opportunities, increase the risk of exposure to money laundering and terrorist financing.

ÎIn recent years, the adoption of crypto-assets has grown considerably, underpinned by a growing public interest in these digital assets. This is reflected in the growing number of installed crypto-ATMs and a significant increase in online searches related to cryptocurrencies.

In this context, the assessment of the VASP sector will examine its role, its economic importance and the applicable legal framework in order to identify the risks of ML/TF and the measures needed to manage them at national level.

2.1. Definition and role of the VASP sector

The sector of providers of exchange services between virtual currencies and fiat currencies includes a wide range of entities that facilitate the exchange, storage and management of cryptoassets. These entities play a key role in the cryptoassets ecosystem, providing services that enable users to trade and hold virtual currencies.

What is a virtual currency?

„a digital representation of value that is not issued or guaranteed by a central bank or public authority, is not necessarily linked to a legally established currency and does not have the legal status of money or currency, but is accepted by natural or legal persons as a means of exchange and can be transferred, stored and traded electronically" [3]

This definition highlights several key aspects of virtual currencies that differentiate them from traditional fiat currencies. First, virtual currencies are digital representations of value. This means that they have no physical form, such as banknotes or coins, and exist exclusively in the electronic environment.

Another important aspect is that virtual currencies are not issued or guaranteed by a central bank or public authority. Unlike fiat currencies, such as the dollar or the euro, which are issued and backed by governments and central banks, virtual currencies do not have a government guarantor backing their value. This makes them more vulnerable to price fluctuations and market uncertainties. However, because they are not directly linked to a public authority, they can operate independently of traditional financial systems, offering a decentralized alternative.

They also do not have the legal status of a currency. This means that, unlike national currencies which must be compulsorily accepted in transactions within a country (such as the mandatory acceptance of the euro currency in the euro area), virtual currencies have no such legal obligation.

[3] Directive (EU) 2018/843 of the European Parliament and of the Council

However, virtual currencies are voluntarily accepted by many individuals and organizations, both individuals and businesses, as a means of exchange in transactions. This voluntary acceptance has contributed to the increasing use of virtual currencies in international commercial and financial transactions.

Virtual currencies are attractive to users because they can be transferred, stored and traded electronically, eliminating the need for traditional intermediaries such as banks. This facilitates rapid transfers of value between users, regardless of geographical distance or time zone, at low cost compared to traditional bank transfer methods. Virtual currencies have thus become a preferred medium for cross-border transactions and international payments.

What is a digital wallet provider?

„an entity that provides services to securely hold private cryptographic keys on behalf of its customers for holding, storing and transferring virtual currency" [4]

This definition emphasizes the importance of digital wallet providers in the cryptoassets ecosystem, highlighting their central role in protecting users' access to virtual funds. Private cryptographic keys, which are essential for authorization and secure transactions, are managed by these entities. By keeping these keys secure, digital wallet providers not only ensure the security of users, but also help to facilitate fast and efficient transactions.

As the use of cryptoassets expands globally, digital wallet providers are becoming essential pillars of transaction security, with a responsibility t o prevent unauthorized access and cyber-attacks. In the context of anti-money laundering and anti-terrorist financing legal regulations, these providers play a crucial role by implementing rigorous security and KYC measures, helping to prevent abuse and ensuring compliance with applicable legal regulations.

[4] Directive (EU) 2018/843 of the European Parliament and of the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purpose of money laundering or terrorist financing and amending Directives 2009/138/EC and 2013/36/EU

What is the role of VASPs?

Virtual Currency Exchange Service Providers (VASPs) are an essential component of the cryptoassets ecosystem. These entities facilitate the connection between the worlds of virtual currencies and traditional finance, providing the necessary bridge for efficient and secure transactions between the two systems

VASPs are of crucial importance in a booming digital financial system as they allow users to access liquidity by converting cryptoassets into fiat currencies, thus providing flexibility for users, investors and businesses. In addition, VASPs contribute to the security of transactions and funds by managing digital wallets and offering secure custody solutions, protecting users' cryptoassets from cyber risks and fraud. They facilitate a range of services such as:

Exchange between virtual and fiat currencies

VASPs allow users to convert virtual currencies into fiat currencies (such as EUR, USD or RON) and vice versa, providing access to liquidity and connecting digital and traditional financial markets.

Providing and managing digital wallets

VASPs provide custody and management services for digital wallets, ensuring the secure storage of cryptoassets.

Fast transactions and cross-border transfers

VASPs facilitate fast fund transfers between users globally at lower costs than traditional bank transfer methods

Why are VASPs important in the digital economy?

VASPs play a fundamental role in sustaining and expanding the digital economy by facilitating the use of cryptoassets in commercial transactions, investments and financial transfers. They create a link between traditional markets and the emerging cryptoasset-based economy, enabling users to access and use virtual currencies efficiently and securely. The rapid development of the cryptoassets sector has contributed significantly to the diversification of the digital economy.

The rise in cryptocurrency adoption and blockchain use has also generated a wave of new investment from both technology companies and private investors, who see huge potential in the industry. The VASP sector is playing an important role in this process, providing the necessary infrastructure to facilitate the conversion of cryptoassets into fiat currencies and vice versa, so that users can access liquidity and actively participate in digital financial markets.

How VASPs contribute to combating the risks of ML/TF?

VASPs play a key role in combating the risks of money laundering and terrorist financing by implementing strict KYC/CFT compliance regulations. While the VASP sector facilitates fast transfers and can provide a degree of anonymity, these entities are required to implement measures to help prevent cryptoassets from being used for illicit purposes. In order to combat money laundering and terrorism financing risks, VASPs are obliged to adopt and enforce effective know-your-customer mechanisms, to identify and verify the identity of users. These measures are essential to reduce the anonymity of transactions with crypto-assets and to prevent their use to disguise the origin of criminal proceeds.

VASPs must also implement transaction monitoring systems to identify suspicious transactions and report them to the competent authorities. These Suspicious Transaction Reports (STRs) are essential tools in detecting illicit activities and contribute to effective oversight of the sector.

By applying these measures and cooperating with regulators and supervisors, VASPs actively contribute to preventing and combating money laundering and terrorist financing. In this context, compliance with AML/CFT regulations not only reduces ML/TF risks, but also protects the integrity of the digital financial market and its users. Thus, although VASPs are exposed to significant risks by the nature of their activities, the adoption of effective supervisory and preventive mechanisms contributes to reducing the vulnerabilities of the sector and ensuring compliance with legal requirements.

2.2. Economic importance and contextual factors

Romania, located in south-eastern Europe, has a strategic position at the crossroads of important trade and financial routes. This facilitates a high volume of cross-border transactions, especially in trade relations with EU Member States and the Balkan region. Its geographical location gives it access to global markets and international financial flows, but exposes the VASP sector to additional risks, in particular money laundering and terrorist financing through crypto-assets.

Romania has seen a significant increase in interest in cryptoassets in recent years. According to the Crypto-Ready Index report of 2021 [5], Romania ranks 33rd globally in terms of readiness for cryptoasset adoption, but stands out by being in the top 10 countries in the world with the most cryptoasset ATMs.

[5] https://cryptohead.io/research/crypto-ready-index

According to this report, in 2021, a total of 86 crypto ATMs h a v e been identified in Romania, which is equivalent to one ATM for every 157,379 inhabitants. This indicates a growing accessibility to crypto infrastructure, facilitating the use of cryptocurrencies and increasing their integration in the digital economy. This increase in accessibility suggests that the Romanian market is becoming increasingly open to innovations in the cryptoassets sector and reflects a growing public interest in these emerging technologies.

In addition, public interest in crypto-assets has grown significantly, reflected by a 331.3% year-on-year increase in online searches related to cryptocurrencies, suggesting a growing adoption of these technologies among the population. Also, with 7,635 annual Google searches per 100,000 people, Romania is one of the countries with the highest interest in cryptoassets.

Although Romania has one of the world's fastest internet connections i n urban areas, there are major regional disparities in access to digital technologies. In big cities like Bucharest, Cluj-Napoca and Timisoara, access to high-speed internet and digital services is well developed. In contrast, in rural areas, access to internet and digital infrastructure is limited, which affects the uptake of crypto-assets and people's access to this market. This digital divide creates challenges in terms of uniform access to new digital technologies and services, including cryptoassets.

2.3. Applicable legal framework

In Romania, the main legal framework in the context of preventing and combating money laundering and terrorist financing (ML/TF) is regulated by Law no. 129/2019 on preventing and combating money laundering and terrorist financing, as well as amending and supplementing certain normative acts.

Law No 129/2019 on preventing and combating money laundering and terrorist financing was published in the Official Journal of Romania, Part I, on July 18, 2019, its provisions transposed Directive (EU) 2015/849 of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, published in the Official Journal of the European Union on June 5, 2015.

According to national legislation, namely in accordance with the provisions of Art. (1), lit g^1 and $g^2$of Law no. 129/2019 on preventing and combating money laundering and financing terrorism, as well as for amending and supplementing some normative acts, the providers of exchange services between virtual currencies and fiat currencies, as well as the providers of digital wallets are considered as reporting entities, supervised by the National Office for the Prevention and Combating of Money Laundering, respectively they are subject to all the obligations in the context of preventing and combating money laundering and terrorist financing (ML/TF).

Following the adoption of this normative act, in order to ensure effective supervision and monitoring of the categories of reporting entities, it was necessary to identify those that actually carry out activities falling under the Law No 129/2019 for the prevention and combating money laundering and terrorist financing.

In this regard, Government Emergency Ordinance No. 53/2022 was adopted on amending and supplementing Law No. 129/2019 on preventing and combating money laundering and terrorist financing, as well as amending and supplementing some normative acts. Thus, the reporting entities referred to in Art. 5 para. (1) lit. g) - k) of Law no. 129/2019, implicitly the providers of exchange services between virtual currencies and fiat currencies, as well as the providers of digital wallets, of the obligation to notify the Office, exclusively electronically, of the commencement/suspension/termination of the activity falling under this law.

Romania, as a member state of the United Nations and the European Union, has assumed international commitments, in which context we underline that the legally binding acts of these organizations establish the obligation for Member States to adopt certain legislative measures to implement international sanctions established by the United Nations Security Council, based on Art. 41 of the Charter of the United Nations and by the European Union in the framework of the Common Foreign and Security Policy. In this regard, the national framework for the implementation of international sanctions is regulated by Government Emergency Ordinance No. 202/2008 and Government Decision No. 603/2011, legal provisions which impose additional obligations on the regulated entities in relation to the implementation of international sanctions established by the UN and the European Union.

Thus, providers of exchange services between virtual currencies and fiat currencies, as well as digital wallet providers are obliged to identify transactions involving designated persons or entities or assets under sanctions, according to Government Emergency Ordinance no. 202/2008.

Currently, in Romania, market access for virtual currency and fiat currency exchange service providers and digital wallet providers (VASP) is not subject to licensing or authorization, as the entities are incorporated in accordance with the provisions of Law 31/1990 on Companies. However, a legislative project has been initiated and is currently under preparation, which needs to be adapted to the emerging new legal framework.

At the European level, in the context of the regulation of cryptoassets and related service providers, a harmonized legal framework has been created for the first time by the adoption of key pieces of legislation, as follows:

Markets in Crypto Assets Regulation (MiCA):	REGULATION (EU) 2023/1114 OF THE PARLIAMENT REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of May 31, 2023 on crypto-asset markets and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937
TFR Regulation:	REGULATION (EU) 2023/1113 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of May 31, 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849 (recast)

The new common legal framework complements the regulatory framework by specifying additional requirements applicable to VASPs. These regulations impose obligations on transaction transparency, record-keeping and customer identification f o r transactions with virtual assets, thus harmonizing compliance standards across the European Union. The TFR Regulation, applicable from 30 December 2024, introduces a significant change by classifying cryptoasset service providers (VASPs) as financial institutions, thus subject to a set of obligations similar to those applicable to traditional financial institutions. For the purposes of the MiCA Regulation, VASPs will be required to obtain a license or authorization in order to continue to operate in the European market.

This regulation aims to protect investors by increasing transparency and establishing a comprehensive regulatory framework for issuers and service providers of crypto-assets, including ML/TF compliance.

This package closes a loophole in existing EU legislation, ensuring that the current legal framework does not create obstacles to the use of new digital financial instruments, while at the same time aiming to support innovation and the adoption of new financial technologies while providing an adequate level of consumer and investor protection.

- **Under the new regulations, each VASP will be required to hold a license or authorization obtained through a chargeable procedure.**

- **Under the new regulations, entities that provide cryptoassets services in accordance with applicable national law before December 30, 2024 may continue to do so until July 1, 2026 or until they obtain or are denied a MiCA authorization.**

Currently, legislative measures have been initiated at national level to adapt national legislation to the requirements of the EU harmonized regulatory framework, which are essential to ensure a smooth transition to the new legal framework, thus protecting investors and financial stability.

The adoption of the new legal framework, which adapts the national legislation to the European MiCA and TFR regulations, marks an important milestone in the regulation of the crypto-assets sector. These measures help to ensure compliance with ML/TF standards, thus protecting both investors and financial stability, and providing an appropriate framework for innovation and development in the VASP sector in Romania.

III

ML/TF risk assessment

3.1. VASP sector supervision at national level

The National Office for the Prevention and Combating of Money Laundering - FIU Romania - is the competent authority for the supervision of the sector concerning providers of exchange services between virtual and fiat currencies, as well as providers of digital wallets. This institution operates through a systematic approach, centered on risk assessment, with the main objective of protecting the integrity of the financial system. By implementing the national legal rules on the prevention of money laundering and terrorist financing, the aim is to ensure a safe and transparent operating environment for all entities involved.

Monitoring is carried out both through off-site methods and on-site control actions. In off-site activities, supervision shall be performed by analyzing relevant data and information on the reporting entities, using a predefined analytical tool. This analysis allows the assessment of each entity's exposure to the risks of money laundering and terrorist financing, which contributes to a better understanding of their operational context.

As a result of the assessment, within the analytical process, of the degree of exposure to the risk of money laundering and terrorist financing, based on data and information available at the NOPCML level, results are obtained on the basis of which on-site verification and control actions are initiated, which involve direct checks at the premises of the reporting entities, which monitor how the entities in this sector comply with the legal

regulations and apply the necessary measures to prevent illegal activities. At the same time, it is also worth mentioning that the on-site supervision component is also aimed at increasing the level of awareness and compliance of the reporting entities with the legal obligations in the field of preventing and combating money laundering and terrorist financing.

The Office's responsibility to supervise reporting entities, i.e. providers of exchange services between virtual and fiat currencies as well as providers of digital wallets, is based on the national legal framework, which confers specific powers on the Office. Supervision is carried out through a dedicated operational system which constantly assesses the risks associated with the activities of the monitored entities. This analytical process makes it possible to determine the frequency and intensity of surveillance activities, based on the results of the risk assessments.

The supervision activity is performed through an operational system specific to the risk based approach, which involves analytical processes of assessing risk indicators, thus determining the level of exposure to ML/TF risks of the reporting entities. The frequency and intensity of supervisory activity is determined based on the assessments of the National Assessment Report on Money Laundering and Terrorist Financing Risks (2022). Given the small size of the VASP sector in Romania, where according to the 2022 National Risk Assessment (NRA) [6] it was revealed that there are between 5 and 6 active entities, it is essential to focus on the supervision and control methods used by the National Office for the Prevention and Combating of Money Laundering. In 2022, off-site supervisions were conducted for a total of 11 reporting entities in the VASP category, and based on the results obtained, on-site controls were conducted at 2 entities. The purpose of these controls was to assess compliance with legal rules and to identify possible deficiencies in the management of money laundering and terrorist financing risks [7]. The on-site controls carried out by the NOPCML also assessed the "fit and proper " status of the company's senior management, who must have the necessary knowledge, experience and expertise to manage the risks of money laundering and terrorist financing. The results of the controls did not reveal any significant deficiencies, which suggests a reasonable degree of compliance among the supervised entities. However, it is important to note that no actions have been imposed, but a plan of measures has been established to remedy the deficiencies identified. These findings are relevant for the risk assessment but should be interpreted with caution given the small size of the sector and the limited number of controls.

[6] National Risk Assessment Report on Money Laundering and Terrorist Financing - 2022
[7] Activity Report of the National Office for Prevention and Combating Money Laundering - 2022

In addition to this context, it is crucial to emphasize that Law No. 129/2019 on preventing and combating money laundering and terrorist financing was amended in 2020, also regulating providers of exchange services between virtual currencies and fiat currencies, as well as digital wallet providers in the category of reporting entities. This adds an additional layer of complexity to the oversight of the sector as these regulations are relatively new.

The sectoral ML/TF risk assessment for the VASP domain was based on information collected from a total of 10 entities that submitted the requested information in due time to complete the assessment.

Given the small size of the sector, the question arises to what extent the results obtained provide a complete picture of the risks of money laundering and terrorist financing in the VASP sector. Although the supervision carried out by the NOPCML is essential to identify and manage the risks, the small size of the sector and the limited number of controls may lead to a partial assessment of the risks. On-site controls, carried out only on entities considered high risk, reflect only a fraction of the activities in the sector, leaving room for potential undeclared or unidentified risks in lower risk entities or those not directly supervised.

Even in this context, the information obtained from NOPCML supervision is an important benchmark for assessing residual and inherent risks. Even if no major shortcomings have been identified, it is possible that with more controls or in the context of sector expansion, risks may evolve or become more evident. Supervision needs to continue and adapt as the sector grows and becomes more complex, bearing in mind that, from a risk assessment perspective, small size does not automatically mean low risks.

Conclusion

The information obtained from the supervision conducted by the National Office for Prevention and Combating Money Laundering provides a valuable basis for assessing the risks of money laundering and terrorist financing in the VASP sector. However, this information is limited by the small size of the sector and hence the small number of controls performed. It is essential that the risk assessment is a continuous and dynamic process, taking into account the evolution of the sector and possible emerging threats, in order to ensure an effective system to prevent and combat money laundering and terrorist financing.

3.2. The size of the VASP sector in Romania

Currently, access to the Romanian market by providers of virtual currency and fiat currency exchange services and digital wallet providers is not subject to a specific authorization or licensing framework. In the absence of a specific authorization regulation for market access, the notification obligation imposed by Emergency Ordinance 53/2022 serves as a partial mitigating measure. It requires each VASP to inform the National Office for t h e Prevention and Combating of Money Laundering of the commencement, suspension or cessation of activities. Although this requirement allows monitoring of the sector, its effectiveness is limited.

Between 2021 and 2024, the NOPCML received 36 notifications of activity in this sector. Following data collection through questionnaires, it was confirmed that only 12 of the 31 responding entities are carrying out VASP specific activities. The sectoral risk assessment was mainly based on the information received from 10 of them, which provided the necessary data in a timely manner. However, it is possible that there may be other entities operating in this sector in the market, which have not been confirmed in this assessment.

The small size of the VASP sector in Romania, marked by a limited entity base, means that changes in the market are significant and can quickly influence the overall data. Even the registration of a single new entity can change the structure of the sector, impacting risk assessments and risk management measures. For this reason, it is important that the analysis takes into account not only the current state of the sector, but also global trends and the potential for market growth, as the crypto-assets sector is highly dynamic, strongly influenced by technological innovation and emerging regulation at the international level.

	2021 (RON)	**2022 (RON)**	**2023 (RON)**
VASP 1	≈ 8.5 mil.	≈ 12 mil.	≈ 4.5 mil.
VASP 2	≈ 6.5 mil.	≈ 3 mil.	≈ 2 mil.
VASP 3	≈ 1.1 mil.	≈ 1.5 mil.	≈ 1.7 mil.

Top 3 VASPs in Romania according to turnover. Source: Ministry of Finance

According to the financial statements for the years 2021, 2022 and 2023, the fluctuations in the turnover of the main VASPs in Romania in the period 2021-2023 indicate an unstable market, sensitive to economic and regulatory factors. Currently, the turnovers of the main VASPs in Romania also include revenues from activities carried out under CAEN codes that are not specific to the VASP sector. This combination of revenues from different activities reduces clarity on the performance strictly related to the VASP sector, thus complicating the process of monitoring and assessing VASPspecific risks. In order to ensure adequate monitoring and accurate assessment of the associated risks, it is necessary that VASPs only carry out activities falling under a specific CAEN code, without engaging in other economic activities.

Thus, although the VASP sector in Romania is relatively small, with only 12 confirmed entities, its growth potential and international developments call for close monitoring and continuous analysis. Given the rapid pace of development of blockchain technology and the crypto-assets market globally, this sector presents an increased risk of exposure to money laundering and terrorist financing threats. With the adoption of increasingly stringent regulations at the international level, such as the implementation of harmonized legal frameworks at the European Union level, it is essential that risk analysis is carried out dynamically, constantly adapting to new trends and vulnerabilities.

In order to align with these international requirements and to prevent cross-border risks associated with VASP activities, it is necessary to implement a flexible and adaptable regulatory framework, including risk assessment measures as well as effective reporting and control mechanisms. In addition, given the potential growth of this sector, the monitoring of VASP activities needs to be supported by enhanced cooperation between national and international authorities to proactively identify and counter potential vulnerabilities.

Conclusion

Although the size of the VASP sector in Romania is small for the time being, its dynamics promise significant future expansion. This growth potential, coupled with international trends, underlines the importance of a robust risk analysis and risk management framework to ensure compliance with national and international requirements in terms of preventing and combating money laundering and terrorist financing.

3.3. Risks identified in the global context

In assessing the risks associated with the virtual asset service provider sector, various sectoral assessments and international reports have highlighted fundamental risks related to user anonymity, incomplete or ineffective regulation and the use of new decentralized financial technologies.

A major general risk in this sector is customer anonymity, which affects the ability of authorities to detect and prevent money laundering and terrorist financing activities. The FATF's 2023 report highlights that while some jurisdictions have made progress in implementing strict KYC regulations, many VASPs still allow transactions with partial or complete anonymity, which facilitates illicit activities. Platforms that do not implement robust compliance measures face t h e risk of becoming vehicles for laundering criminal proceeds [8].

According to FATF assessments, there is a significant delay in the effective implementation of anti-money laundering and counter-terrorist financing regulations for VASPs globally. Approximately 75% of jurisdictions have not implemented or have partially implemented FATF standards for VASPs, which exposes the sector to significant vulnerabilities related to money laundering and terrorist financing. In many cases, there is a lack of a national risk assessment (NRA) that properly identifies the risks associated with this sector [9].

Peer-to-peer (P2P) transactions are another significant risk, according to the Chainalysis 2024 report. The lack of a centralized intermediary in these transactions makes funds more difficult to trace, which opens up opportunities for cybercriminals to hide the origin of illicit funds. Chainalysis shows that these transactions have become a favored channel for criminal groups, especially entities associated with countries under international sanctions, such as North Korea [10].

In addition, decentralized technologies such as decentralized platforms (DeFi) are seen as a challenge for effective supervision of financial flows. FATF emphasizes that the lack of a centralized point of control and the difficulty of tracking funds in these decentralized ecosystems increase the risk of VASPs being used for money laundering and other illicit activities [11].

[8] FATF (June, 2023) - Targeted Update On Implementation Of The FATF Standards On Virtual Assets And Virtual Asset Service Providers
[9] FATF(2024)-Virtual Assets: Targeted Update on Implementation of the FATF Standards on VAs and VASPs
[10] Chainalysis Crypto Crime Report 2024
[11] FATF (June 2023)-Targeted Update On Implementation Of The Fatf Standards On Virtual Assets And Virtual Asset Service Providers

At the same time, the Moneyval (2023) report on money laundering and terrorist financing risks associated with the VASP sector also highlights the need for major improvements in Member States' compliance with FATF standards in the area of virtual assets and related service providers. The report finds that, although some progress has been made, most Member States still face significant shortcomings in the implementation of preventive measures and effective supervision of the VASP sector. Major challenges include risk assessment, detecting unregistered platforms, improving the quality of suspicious transaction reporting and managing the risks associated with anonymity and decentralized technologies. The report also emphasizes the importance of enhancing international cooperation to combat cross-border crimes related to virtual assets and to increase the effectiveness of anti-money laundering and counter-terrorist financing measures [12].

Recent national assessments of this sector by other EU Member States have highlighted significant risks in the use of VASPs for money laundering activities through the rapid conversion of cryptocurrencies into fiat assets, as well as the risks associated with offramping services. According to Chainalysis, more than 71.7% of illicit funds were converted into fiat currencies through a small number of off-ramping platforms, indicating high vulnerabilities within these entities [10].

Reports on sectoral assessments carried out by various jurisdictions have also emphasized the need for increased international cooperation to combat the risks associated with this sector, given the cross-border nature of VASP transactions and the need for effective oversight of VASP transactions requiring common mechanisms and cooperation tools at a global level.

Conclusion

The risks associated with the VASP sector in the global context include anonymity of transactions, geographical vulnerabilities, the use of new decentralized financial technologies and the concentration of illicit activities around specific platforms. Full implementation of the FATF recommendations and the adoption of stringent regulatory and compliance measures remain essential to mitigate these risks.

[12] Moneyval (2023)-Money Laundering And Terrorist Financing Risks In The World Of Virtual Assets

3.4. Risks identified at national level

Risk identification and analysis of the VASP sector in Romania plays a central role in the national assessment. This analysis is based on the responses provided by VASPs through questionnaires, focusing on four key categories of risks as follows:

CUSTOMER RISK

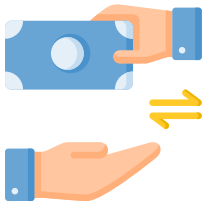
It aims to identify and assess customer typologies, source jurisdictions and complex legal structures that may pose a high risk of money laundering and terrorist financing.

PRODUCTS AND SERVICES RISK

It refers to the risks associated with the types of services offered by VASPs, such as crypto-asset exchange, digital wallets and other products that may facilitate anonymous or difficult to trace transactions

COMPLIANCE RISK

Includes measures and procedures implemented by VASPs t o comply with national and international regulations on the prevention of money laundering and terrorist financing.



TRANSACTIONS RISK

This category looks at the risks associated with financial transactions carried out using crypto-assets, in particular cross-border transactions, which may facilitate anonymous or suspicious transfers.

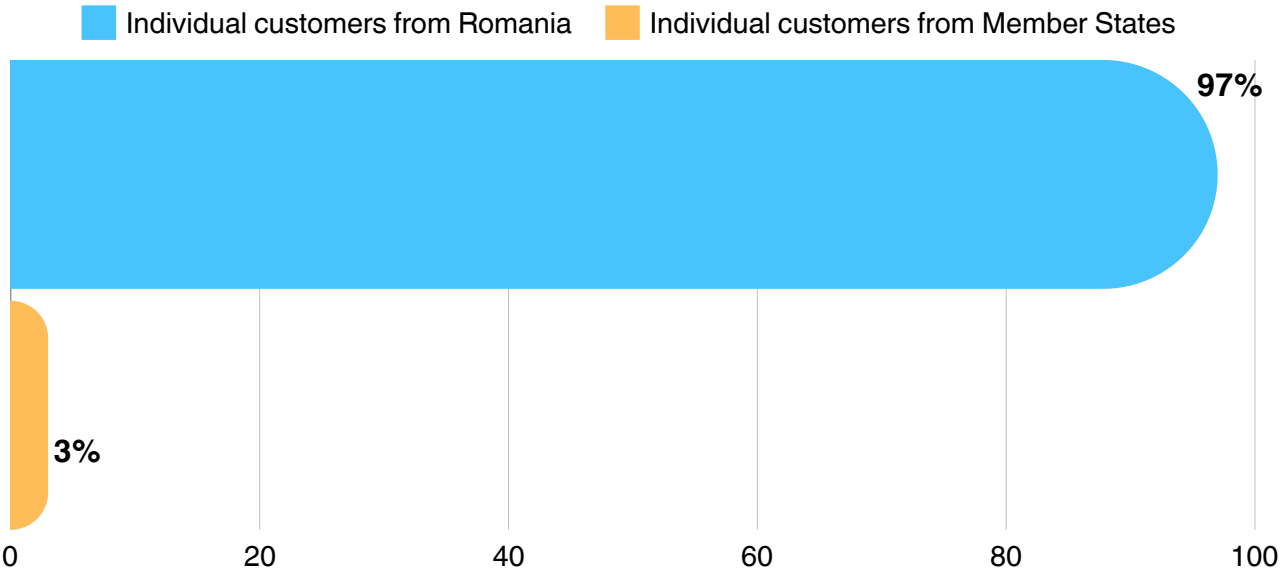
These risk areas are considered critical for identifying vulnerabilities in the sector, as they affect fundamental aspects of VASPs' activities, from customer typology and profile, to regulator y compliance and transaction monitoring. In what follows, we explore each of these risks in more detail, based on data collected through questionnaires, providing a comprehensive picture of the sector's exposure to potential money laundering and terrorist financing threats.

Customer risk

The analysis of customer-related risks in the VASP sector in Romania has highlighted a number of specific risk factors, which are key to understanding the sector's vulnerabilities to money laundering and terrorist financing. The questionnaire responses provided by the VASPs provided significant data on the typology of customers, their jurisdictions of origin and their economic activities. The relevant data and risks are presented below.

All the VASPs that completed the questionnaire indicated that they predominantly operate in Romania. However, for entities that conduct cross-border transactions with customers in other jurisdictions, this issue requires close monitoring, as certain jurisdictions may be more vulnerable to illicit activities due to a lack of strict regulation or lower standards of financial supervision.

The proportion of customers from Romania is significant, representing the majority for all entities (over 97% for most VASPs), according to the figure below. However, there are also customers from the European Union (EU), with a smaller proportion (e.g. between 2% and 3%), and in some cases there is a small proportion of customers from non-EU jurisdictions, in particular countries in the Balkan region and the Republic of Moldova. This indicates a moderate risk due to international transactions, especially in the context of potentially high risk jurisdictions.



Proportion of individual customers of VASPs in Romania

VASPs' responses indicate that the majority of customers are individuals, accounting for over 90% of all customers. This indicates a high risk of frequent small value transactions, which are often used to fragment transfers and avoid reporting, especially in the context of insufficient monitoring. Individuals present a high risk in assessing the source of funds and monitoring transaction behavior.

Corporate clients represent between 0% and 10% of the client portfolio, and some VASPs have indicated that they come from economic sectors considered high risk. An additional risk comes from complex legal structures used by some legal entities to hide the true beneficiaries of transactions.

A significant risk identified in the questionnaires is customers from high-risk jurisdictions, which were mentioned by several VASPs. In general, the share of these customers is low (below 1% for most entities), but they are highly vulnerable to the use of cryptoassets for money laundering or terrorist financing purposes. Examples of high-risk jurisdictions mentioned include non-EU countries in geopolitically unstable regions such as Iran, Afghanistan, North Korea, Syria, Yemen, Burkina Fasso, etc.

Another notable risk is Publicly Exposed Person (PEP) customers. Although the proportion of PEPs among VASP customers is relatively low (less than 1%), they pose a high risk of ML/TF due to potential links to corruption. VASPs have implemented additional measures to verify and monitor these customers as required by law, but the low number of PEP customers does not eliminate the associated risk.

Another category of high-risk customers are legal entities operating in vulnerable economic sectors, according to the National ML/TF Risk Assessment. The questionnaires show that these customers have a minor presence among VASP customers (generally less than 2%), but the activities of these sectors, such as gambling or real estate agencies, increase the risk of cryptoassets being used for illicit activities.

An additional risk is posed by the use of complex legal structures, which has been identified in a small percentage of VASPs' clients (generally less than 0.5%). These structures are often used to hide the real beneficiaries of transactions and can be a red flag for money laundering activities. In cases where VASPs have identified shell companies, they have applied additional due diligence measures and have thoroughly investigated the ownership structure of these entities, thereby reducing the risks associated with illicit financial activities.

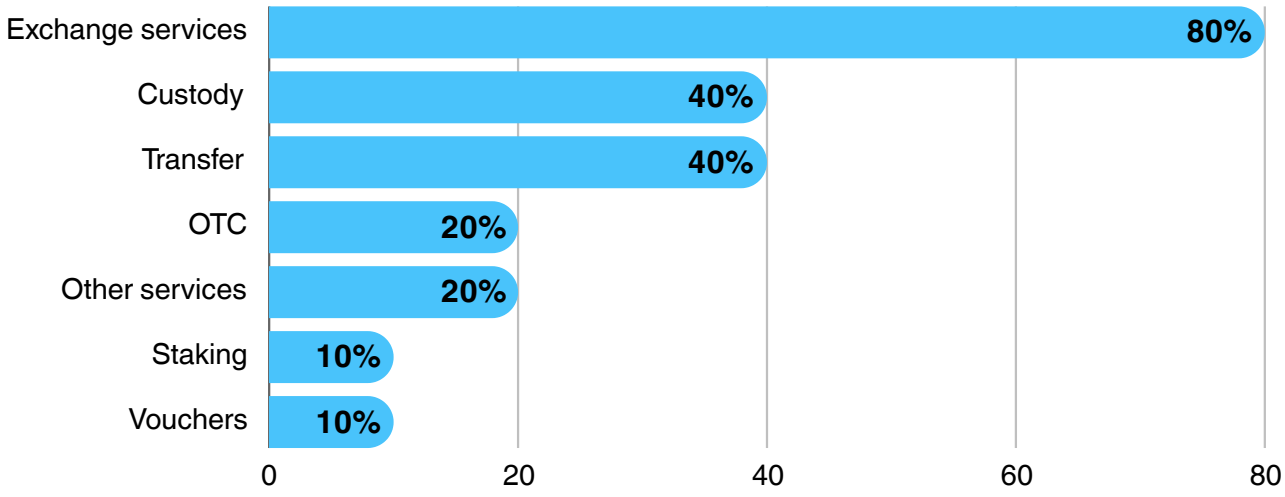
Conclusion

The VASPs' responses to the client questions reveal a number of significant risks, including risks associated with clients from high-risk jurisdictions, PEP clients and those operating in vulnerable economic sectors. Although the majority of clients are from Romania and the EU, there is moderate exposure to cross-border risks and complex legal structures. Strict KYC and due diligence measures need to be continuously applied to reduce vulnerabilities and prevent illicit activities in the VASP sector in Romania.

Products and services risk

Analyzing the risks associated with the products and services offered by VASPs is crucial for understanding the sector's exposure to vulnerabilities related to money laundering and terrorist financing. A detailed analysis of the questionnaire responses indicates that VASPs in Romania offer a diverse range of services, including exchanging between virtual currencies and fiat currencies, providing custody for cryptoassets, and in some cases, OTC services and transactions conducted through cryptoasset ATMs.

According to the data collected and presented in the figure below, 80% of VASPs offer exchange services between virtual currencies and fiat currencies, these being among the most common services.



Percentage distribution of products and services offered by VASPs in Romania

The exchange between virtual currencies and fiat currencies entails a number of vulnerabilities, as it allows for the rapid conversion of digital assets into traditional currencies and vice versa, thus facilitating the possibility of concealing the origin of illicit funds. From this perspective, these VASPs need to apply strict know-your-customer and transaction monitoring measures to prevent their platforms from being used in money laundering schemes.

As for custody services for cryptoassets, only about 30% of entities offer these services. The custody of crypto-assets poses significant risks as it involves holding and managing client funds, which can facilitate unauthorized access or fraudulent activities in the event of inadequate cybersecurity systems.

Also, an important aspect of the risk assessment is related to ATM transactions of cryptoassets. From the data obtained, only a few entities reported the use of ATMs in the period 2021-2024. One of the VASPs indicated operating 85 ATMs in Romania, which is a significant proportion compared to the other entities that either do not have ATMs or reported a low number. For example, another VASP reported the operation of 5 ATMs in Romania and another 6 owned by third parties. These entities are exposed to the risks associated with anonymous or spoofed transactions, especially in the absence of strict KYC controls.

Another entity reported that, although it had operated ATMs in the past, its business was terminated in January 2024, emphasizing that the use of these machines should be closely monitored to prevent their use in suspicious money laundering activities. In addition, there are also VASPs that, although they did not operate ATMs during the period under assessment, provided other related services such as intermediating crypto payments. In terms of know-your-customer measures for ATM transactions, VASPs' responses varied. For example, one VASP operating ATMs applied simplified KYC measures for transactions below RON 15,000, while for transactions above this threshold additional checks were required, including confirming identity by verifying official documents and checking the customer against international sanctions lists.

OTC services are another important category in the analysis of risks associated with products and services offered by VASPs. They were mentioned by about 20% of VASPs indicating that they offer such services. OTC transactions are private transactions between two parties without the use of a public exchange platform. While these services can offer advantages in terms of flexibility and the possibility to handle large volumes of transactions, they present significant risks, in particular in terms of anonymity and avoidance of strict know-yourcustomer measures.

OTC trades are often favored by large investors because they can negotiate more favorable prices outside the open markets. But precisely for this reason, there is a risk that OTC trades may be used to avoid the controls and reporting requirements imposed by ML/TF regulation.

Conclusion

The risk associated with the products and services offered by VASPs is considered to be high, in particular due to the anonymity and complexity of transactions, such as exchanges between virtual currencies and fiat currencies, custody of cryptoassets and the operation of cryptocurrency ATMs. These activities present major ML/TF regulatory compliance challenges. OTC services also contribute to this elevated risk due to the private nature of transactions, which requires stricter monitoring and enforcement of know-your-customer measures

Compliance risk

Compliance risk is a key issue in the work of VASPs, given the stringent requirements imposed by national and international legislation on the prevention of money laundering and terrorist financing.

In this context, regulatory compliance and the application of appropriate know-yourcustomer measures, transaction monitoring and suspicious activity reporting are critical factors in managing compliance risk. Analysis of the data obtained from the questionnaires completed by the VASPs provides a detailed insight into the degree of compliance and the practices implemented by these entities.

The VASPs' responses indicate that the majority of VASPs (80%) had steady revenues from cryptocurrency-related activities over the period 2021-2024, while only 20% had no revenues. Those 20% of VASPs that did not record revenues during this period are either newly established entities or are in the early stages of their activity. This intense economic activity underscores the importance of applying strict compliance measures to prevent risks associated with cryptoassets transactions and the customers involved.

In terms of customer identification procedures, all the VASPs analyzed have implemented such measures, but the methods applied vary. Approximately 20% of the entities use inperson verification, while the majority opt for verification online or through digital platforms. Notably, 70% of VASPs use additional verification for PEP customers and 60% apply additional verification for customers in high-risk jurisdictions. Another key element is the use of artificial intelligence (AI) to verify identity documents - a technology adopted by 70% of entities. This modern approach offers greater efficiency and accuracy in identifying potential risks and ensuring compliance with legal requirements.

More than half of the VASPs surveyed have automated systems in place to monitor and detect suspicious transactions, a key element in managing compliance risk and preventing money laundering and terrorist financing activities. These systems use advanced technologies, such as GBCAS, Chainalysis and other customized solutions, which enable real-time data analysis and rapid identification of unusual or potentially suspicious transactions. Deploying these solutions gives VASPs the ability to set configurable rules, risk scores and automated alerts so that they can identify transactions that exceed certain value thresholds or originate from high-risk jurisdictions.

However, although the systems are available and in use, the number of suspicious transactions reported to the National Office for the Prevention and Combating of Money Laundering remains low. This suggests either that suspicious transactions are rare within these entities or that there is possible under-reporting due to difficulties in identifying and assessing risks. In some cases, VASPs have resorted to custom solutions developed in-house, which include monitoring the frequency of transactions, analyzing customer behavior, and automatically checking crypto addresses against sanction lists.

VASPs that used advanced Software as a Service (SaaS) systems also benefited from additional capabilities such as blockchain data analytics and real-time risk detection. These solutions can play a crucial role in improving the efficiency of compliance systems and increasing the detection of suspicious transactions.

In terms of reporting/notifying authorities other than the NOPCML, this is rare. Only a small proportion of the VASPs mentioned that they have made reports or referrals to authorities such as the Directorate for the Investigation of Organized Crime and Terrorism, the Romanian Police or the National Agency for Tax Administration. The number of reports varies, usually between 0 and 8 cases per year, indicating that exposure to significant risks is limited

The main indicators of suspicion identified by VASPs include transactions not justified by customer activity, frequent transactions to high-risk jurisdictions and customers' refusal to provide the information necessary for compliance. A significant proportion of VASPs also identified PEP-related transactions and transactions that avoid reporting limits by fragmenting transfers.

In terms of know-your-customer measures at cryptocurrency ATMs, about 30% of VASPs operating ATMs apply simplified know-your-customer measures for small-value transactions, generally below RON 15,000. In these cases, checks include confirming the customer's wallet address through advanced blockchain intelligence software that provides fast, accurate and risk-sensitive monitoring of transactions and virtual wallet addresses, as well as checking them against international sanction lists. For higher value transactions, the measures become more complex to ensure compliance and effective risk management.

One cryptoactive ATM operator mentions that for amounts transacted between RON 15,000 and RON 30,000 per day, requires additional checks, such as confirming the phone number with a code sent by SMS. Where transactions exceed the threshold of RON 30,000 per day, KYC measures are intensified. These include both manual and automated verification of identity documents using advanced artificial intelligence-based technologies. The verification process can involve scanning the ID card or passport and performing a realtime video verification where the customer is asked to take a selfie or move their head to confirm that they are the same person as the person in the document presented.

For customers considered higher risk, the measures become even more rigorous. In these cases, home address checks are carried out on the basis of documents such as utility bills or bank statements. Customers are also required to fill in an affidavit confirming that they are the real beneficiaries of the transactions and declaring the source of the funds used. Where necessary, VASP requests additional supporting documentation to verify the origin of the funds.

To prevent possible abuses or attempts to fragment transactions, one operator's ATMs have set a daily limit of RON 48,000 for both buying and selling. If a customer wishes to carry out a transaction exceeding this limit, he/she must contact the VASP to request the lifting of the limit, after further verification of his/her identity. In all cases, customers are asked on-screen whether they are a PEP and whether they are purchasing Bitcoin in their own e-wallet. If customers are PEPs or if the e-wallet does not belong to them, the transaction is automatically declined because the VASP does not accept PEP customers or purchases in foreign wallets.

An important aspect to emphasize in the case of exchanges between virtual currencies and fiat currencies via cryptocurrency ATMs is the extremely risky nature of these services from the ML/FT perspective, due to the use of cash, loopholes in national legislation, as well as the fact that know-your-customer measures are not always applied and in some cases, transactions are monitored manually.

Conclusion

Compliance risk in the VASP sector in Romania is of major importance, as noncompliance can attract significant sanctions or expose platforms to legal and reputational risks. Although most VASPs have implemented compliance measures, including KYC procedures and automated monitoring solutions, challenges remain related to the uniformity of their application, identification and reporting of suspicious activities, caused by insufficient knowledge of ML/TF typologies in the VASP domain. Close monitoring and constant enforcement of preventive measures are essential to ensure the integrity of this growing sector.

Transactions risk

Transaction risk is a key dimension in assessing the vulnerabilities of the VASP sector in Romania, being closely related to the volume, frequency and nature of transactions carried out by entities offering cryptoassets services. Within the analysis, several relevant aspects were highlighted based on the answers received to the questionnaire questions.

In terms of annual trading volume, most VASPs reported a significant volume of crypto-asset trading between 2021-2024. For example, one of the VASPs recorded transactions of more than €133 million in 2021, while other entities reported volumes between several million and tens of millions of euros. This intense activity indicates that the VASPs are actively involved in facilitating crypto-asset transactions and underscores the importance of implementing measures to prevent money laundering and terrorist financing risks. However, there are also entities that have not reported significant activity during this period, either because they were recently established or because they have not been very active.

Nine out of ten VASPs reported that they hold and use bank accounts opened in Romania, thus underlining the integration of most of these entities into the national banking system, with the exception of two VASPs. Thus, for one VASP that had accounts in Romania but from 2022 transferred its banking operations to Lithuania, this decision may be motivated by strategic considerations, such as easier access to international markets or optimizing operational costs, or by seeking a more flexible regulatory framework.

The data collected for the period 2021-2024 shows a slight decrease in the annual number of customers transacting at cryptocurrency ATMs, as reported by VASPs. One notable example is a VASP that saw a sizable increase in 2022, with 1,618 customers, but the number dropped to 1,337 in 2023 and dramatically to just 7 customers in 2024 (as of October). In other cases, some VASPs only started reporting ATM activity in more recent years, while others did not record any ATM transactions at all during the period analyzed.

In terms of transaction volumes, a similar pattern of gradual decrease is observed. For example, one VASP recorded a volume of EUR 3,561,802 in 2021, with a slight increase in 2022 (EUR 3,643,262), but the volume decreased slightly to EUR 3,455,444 in 2023 and EUR 3,146,485 in 2024 (up to October). Another VASP also saw a significant decrease in ATM transaction volume, from EUR 1,501,019 in 2023 to just EUR 4,915 in 2024 (through October). This development reflects a slight decrease in activity at cryptocurrency ATMs, which can be attributed to a variety of factors, including changes in customer behavior and adjustments to industry regulations. Even if the declines are not considerable, current trends indicate a stabilization or even a reduction in activity in some cases, suggesting the need to closely monitor market developments and adapt compliance and operational strategies to respond to the new realities of the cryptoasset industry.

Conclusion

Transaction risk in the VASP sector in Romania reflects a slight decrease in activity, both at ATMs and in overall transaction volumes, according to data collected for the period 2021-2024. Although some VASPs have recorded significant transaction volumes, the overall trend shows a gradual decrease. One of the reasons for this decrease can be considered the development of the cryptoassets market, which, after the peak in 2021, entered a correction phase (cryptoasset price decrease). This decline highlights the importance of continuous monitoring and adapting compliance measures to effectively manage the risks associated with cryptoasset trading in the context of market fluctuations.

3.5. Crime and emerging trends in the VASP sector in Romania

As part of the risk assessment of the VASP sector, data and information representing relevant inputs from law enforcement and other relevant authorities were collected. This input has provided a comprehensive overview of VASP sector typologies, *modus operandi* and identified risks, highlighting vulnerabilities that criminals can exploit at national level.

A small number of money laundering offenses based on predicate offenses associated with the VASP sector have been identified at national level, the complexity of these offenses and the sophisticated techniques used to conceal the funds used make them particularly dangerous. The use of crypto-assets provides criminals with a high degree of anonymity, which complicates the monitoring and tracing of financial flows, especially in cases involving multiple jurisdictions. Global trends indicate an increasing use of VASP platforms for fast and anonymous transfers of funds, often involved in complex layering structures designed to conceal the origin of illicit funds.

Data and information collected from law enforcement agencies indicate that economic, cyber and fraud crimes are the most common illicit activities associated with the VASP sector, highlighting the major risks involved in the use of this sector by criminals. In terms of economic crime and fraud, the VASP sector in Romania is more exposed to Ponzi schemes, investment fraud and fictitious transactions. Criminals use the services offered by VASPs to target fraudulently obtained funds, luring victims with promises of quick and substantial gains from cryptocurrency investments. These funds are then quickly transferred between accounts and cryptocurrency exchange platforms, complicating the process of tracing financial flows and hiding their illicit origin.

Economic fraud schemes in the VASP sector are facilitated by incomplete regulation and weak customer identity verification requirements. Platforms that impose minimal Know Your Customer (KYC) requirements allow criminals to operate with a high degree of anonymity, thus favoring their use for illicit activities. In addition, given the risks associated with crypto ATM transactions, intelligence provided by the authorities has revealed a significant amount of criminal activity.

In the area of cybercrime and cyber attacks, digital wallets and trading platforms are often targeted by phishing and hacking attacks. Criminals use advanced techniques to gain unauthorized access to funds through remote control applications, enabling them to carry out fraudulent transactions on behalf of victims. Ransomware attacks are also a significant threat associated with the VASP sector, with cryptocurrencies being preferred for ransom payments due to the high level of anonymity they offer. Currently, at national level, the competent authorities are managing USD 6,000,000 worth of unavailable virtual currencies, mainly stemming from criminal cases related to cybercrime.

Information gathered from the authorities has also revealed other important trends, including fraud scenarios involving impersonation of employees of trusted public or financial institutions. In these cases, attackers contact users of financial services under the false identity of official representatives, changing their identity to reflect positions of authority. Under the pretext of preventing imminent fraud, they persuade victims to open credit lines and deposit the proceeds into a digital wallet controlled by the attackers, using means of conversion into virtual assets.

Cross-border crime is a significant vulnerability in the VASP sector, given the global and decentralized nature of cryptocurrencies. These characteristics facilitate their use for money laundering and other transnational criminal activities. Criminals frequently use layering and mixing techniques to disguise the origin of illicit funds, which complicates efforts by authorities to trace financial flows and recover these funds. In cross-border transactions, VASPs are often used for complex international operations involving multiple jurisdictions, creating significant challenges for competent authorities in investigating and combating these crimes.

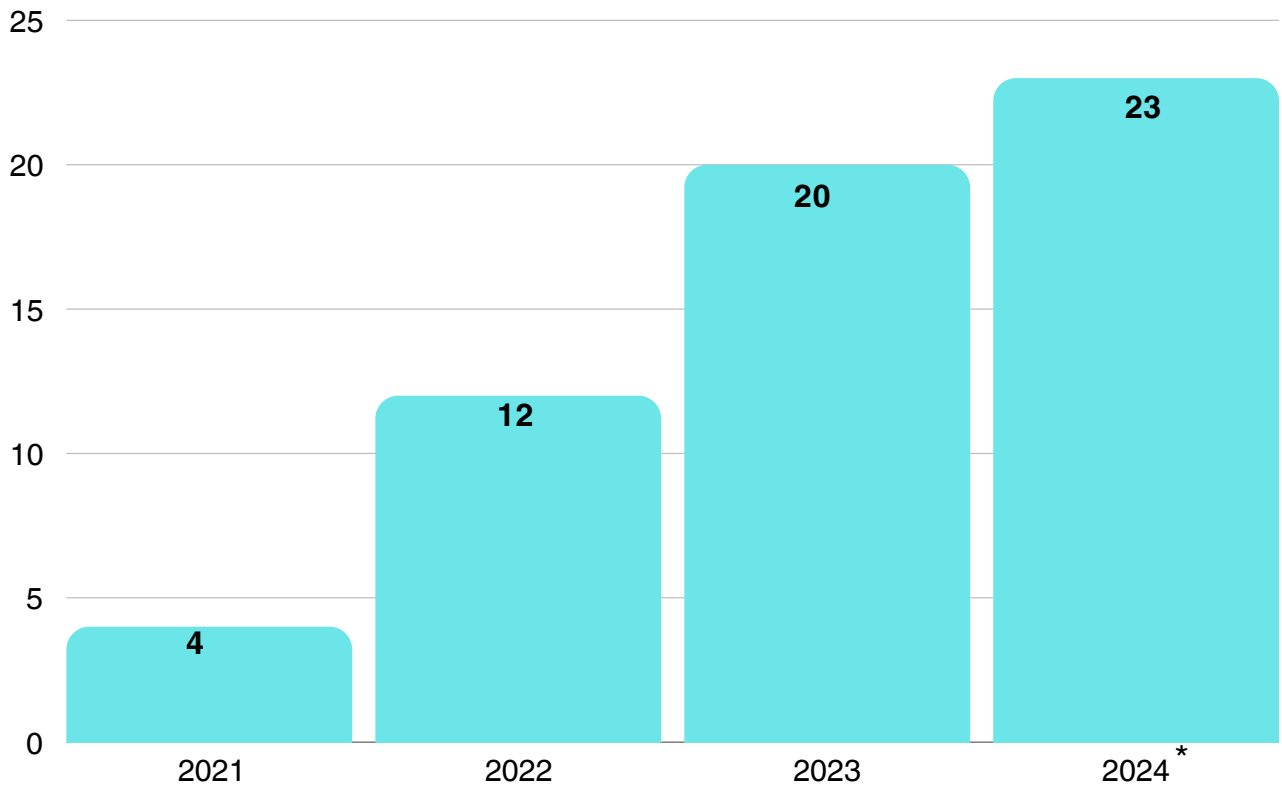
From the information provided by law enforcement agencies, requests for mutual assistance in the investigation of money laundering offenses based on predicate offenses associated with the VASP sector have been highlighted. These requests underline the importance of cooperation with Europol, which facilitates the exchange of information and coordination at international level, thus contributing to the effective fight against cross-border crime. Close cooperation with Europol and other international bodies is essential to overcome the legal and operational challenges involved in investigating complex transactions that cross multiple jurisdictions.

In terms of international cooperation, the NOPCML - FIU Romania has handled a significant number of spontaneous SARs from financial intelligence units in other Member States, which were subsequently forwarded to the competent authorities, thus contributing to the risk management of the VASP sector. At the same time, the NOPCML received requests for information that facilitated international collaboration, strengthening efforts to monitor and combat cross-border crime.

Investment scams in the VASP sector are an important emerging trend. In these schemes, criminals lure investors with the promise of quick and high returns from investments in fake cryptocurrencies and NFTs, presented as legitimate opportunities. Many of these investors are ultimately duped and their funds are quickly diverted into digital wallets controlled by the criminals. These schemes are often amplified by the use of advanced phishing and remote access technologies, allowing criminals to manipulate victims' accounts and transfer funds across multiple jurisdictions, complicating recovery efforts. The use of VASP platforms with incomplete regulations and minimal KYC requirements, provides a high degree of anonymity for such criminals, highlighting the vulnerabilities that this sector presents to this type of fraud.

In the context of the risks associated with the VASP sector, suspicious transaction reports (STRs) submitted by reporting entities are an essential tool in identifying and preventing criminal activity. Between 2021-2024, the N received a significant number of suspicious transaction reports indirectly associated with the VASP sector and 59 STRs from VASPs. Following the suspicious transaction reports received in the period 2021-2024, 10 SARs were disseminated to the Public Prosecutor's Office of the High Court of Cassation and Justice, which also related to transactions with virtual currencies, and 6 criminal cases were filed.

The total of 59 STRs received from VASP entities are broken down as follows:



**by October 2024*

However, VASP sector-specific reporting remains insufficient to provide a complete picture of risks, suggesting the need for more rigorous oversight and development of analytical capabilities.

Crime in the VASP sector is evolving rapidly, fueled by technological innovation and the increasing use of cryptocurrencies and other digital assets. Criminals are constantly adjusting their tactics to exploit existing vulnerabilities. While authorities and the private sector are working to implement stricter oversight and regulatory measures, there is a need to identify more advanced technological solutions to effectively monitor and track transactions and prevent illicit activities.

Another worrying trend is the rise in cryptocurrency investment scams, which are becoming increasingly sophisticated and transnational, making it harder for authorities to combat them. The use of remote control applications complicates the detection and prevention of these crimes, and victims are often manipulated into unwittingly participating in money laundering activities, thus increasing the complexity of investigations and widening the impact on vulnerable populations.

The significant trends identified reflect the use of complex layering schemes and mixing services to disguise the origin of funds. These methods underline the need for closer international collaboration and the development of technological solutions capable of dealing with the increasingly advanced methods used by criminals.

The risk assessment of the VASP sector in Romania reveals a high potential for financial innovation, but at the same time highlights significant vulnerabilities exploited by criminals. Although the number of money laundering cases associated with the sector is low, the complexity and sophistication of these crimes, including the use of concealment techniques such as layering and mixing, create major risks. Cross-border criminality and the global nature of cryptocurrencies complicate authorities' efforts to trace financial flows and recover illicit funds.

To address these emerging risks, strengthened regulation, the use of advanced technological solutions and enhanced international cooperation, in particular with institutions such as Europol, are essential. Limited data and intelligence at national level also underlines the need for more effective reporting mechanisms and more rigorous oversight to provide a comprehensive understanding of the crime phenomenon and protect the integrity of the financial system.

In conclusion, the VASP sector requires increased attention, continuous monitoring and permanent adaptation to new crime trends and risks in order to prevent the exploitation of the criminal phenomenon and to ensure the protection of the national and international financial system.

IV

Identifying threats and vulnerabilities

4.1. Money laundering typologies in the VASP domain

Combating money laundering in the cryptoasset service provider sector is a priority for both authorities and financial institutions, given the anonymity and decentralization of cryptoassets, which facilitates illegal activities. With the growing popularity and use of cryptoassets, regulatory efforts have intensified, imposing stricter know-your-customer and transaction monitoring measures. However, the sector remains vulnerable due to rapid innovation and the diversity of trading platforms and products.

Based on the guide ***"Indicators of suspiciousness and money laundering typologies in the cryptoassets field"***, published by the National Office for Preventing and Combating Money Laundering in 2023, six of the most common money laundering typologies identified in the cryptoassets field have been analyzed. This updated guide provides a clear picture o f how criminal networks use cryptoactive technologies to conduct their illicit activities.

01 Use of non-compliant platforms

Direct money laundering through cryptoasset transactions is the process by which illicit funds are introduced into the crypto environment, transferred through multiple transactions to hide their origin and then converted into clean cryptoassets.

02 Use of money mules in money laundering

The use of money mules in cryptoassets money laundering refers to the involvement of intermediaries in the process of transferring and converting illicit funds in order to conceal the route and final beneficiaries o f these funds.

03 Use of mixers and DeFi platforms to hide tracks

It's a technique used in cryptoassets money laundering, where transactions are scrambled and transferred through decentralized platforms to make it more difficult to identify and trace the origin and destination of funds

04 Use of crypto ATMs to launder money

It is a method by which illicit funds are converted into cryptoassets via crypto ATMs, enabling criminals to obtain "clean" funds in a seemingly legal way and without revealing their identity.

05 Use of NFTs for money laundering purposes

The use of NFTs for money laundering purposes involves the transfer of illicit funds through these unique digital assets, which allow criminals to hide the illicit origin and launder the funds, taking advantage of the special characteristics and the difficulty of tracing associated with them,

06 Use of ICOs to launder money

The use of ICOs for money laundering purposes consists in launching crowdfunding campaigns via cryptoassets, whereby criminals hide the origins of illicit funds and achieve the appearance of legality through crypto investments and transactions.

1. Use of non-compliant platforms

One of the common methods of money laundering through cryptocurrency transactions involves the use of non-compliant exchange platforms. Criminals exploit the vulnerabilities of these platforms, which often do not implement know-your-customer measures and do not comply with regulations in specific jurisdictions

Non-compliant exchange platforms or those that impose minimal KYC requirements provide an environment conducive to money laundering, as they do not ask for detailed information about the identity of customers or the origin of funds. They tend to avoid the application of the rigors of anti-money laundering regulations and KYC standards, thus facilitating the use of anonymous accounts or accounts with minimal identifying information, allowing criminals to conduct transactions without proper verification of their identity and without recording relevant details in order to identify illicit activities. These platforms also do not apply restrictions on transaction volumes and values, thus enabling criminals to conduct large and frequent transactions without attracting the attention of the authorities.

Description of typology

- **an individual obtains cryptoassets through a ransomware attack,** which consists of taking control of victims' computer systems and demanding a ransom in cryptoassets. After obtaining the cryptoassets, the perpetrator seeks to legalize them through complex money laundering schemes, such as successive exchanges on non-compliant platforms, to hide the trail of transactions and make it difficult to trace illicit activities;

- the first step in the money laundering process is to **identify a non-compliant exchange platform and open an anonymous account on it**. By opening an anonymous account, the person avoids providing detailed information about his or her identity, which allows him or her to carry out transactions without being subject to proper identity verification and without leaving a digital trail that could lead to his or her identification. Choosing such a non-compliant platform is essential as it offers a higher degree of anonymity and reduces the risk of detection by authorities or law enforcement agencies;

- once illegally obtained cryptoassets are transferred on this platform, **they will be converted into other digital assets or fiat currencies;**

- **the "dirty" cryptoassets, transformed into other digital assets, will then be exchanged into fiat currency through successive transactions** on both noncompliant and compliant platforms;

- t**he funds resulting from these cryptoactives exchanges will then be transferred to a bank account or withdrawn in cash from a crypto ATM.** Through this step, the criminal attempts to integrate the illegally obtained funds into the traditional financial system or convert them into cash, thereby facilitating their use in legal activities or to avoid detection of illicit transactions. This additional action contributes to creating the appearance of legality of the funds and complicates the tracing of money flows, adding an additional layer of complexity to the process of investigating criminal activities.

Typology-specific indicators

1. The exchange platform used does not comply with anti-money laundering regulations and is often a new start-up;

2. Anonymous accounts are opened without proper checks or know-your-customer measures;

3. There are no limits on transaction amounts or volumes, allowing large transactions without attracting attention;

4. Customers frequently trade on non-compliant platforms that do not apply KYC standards;

5. The exchange platform displays suggestive messages on its website promoting user anonymity and mentioning the acceptance of cash in crypto transactions;

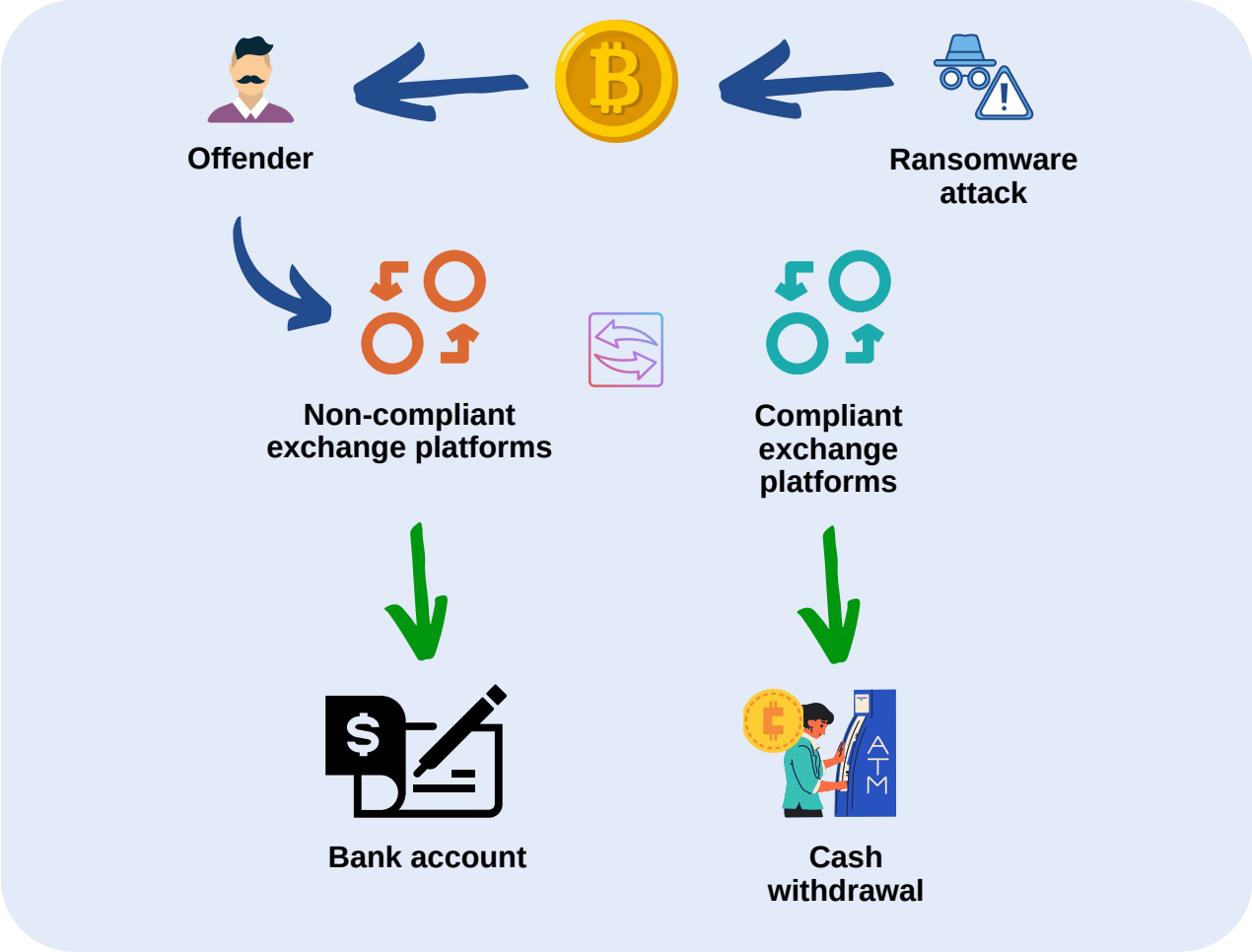
6. The non-compliant exchange platform offers chat services between users, creating an environment conducive to communicating and coordinating illegal transactions and discussing suspicious activity.

7. 7. Involvement of the exchange platform in transactions with illicitly sourced cryptoassets: there is information indicating that the exchange platform is involved in transactions with illicitly sourced crypto-assets. This may be revealed by previous investigations or publicly available information sources.

Practical examples

1. An individual involved in illegal activities, such as drug trafficking or cybercrime, uses a non-compliant exchange platform to launder money. It opens an account without providing detailed information and conducts transactions without strict identity checks, transferring and converting cryptoassets to hide the origin of funds [13].

2. An individual involved in online fraud or phishing uses a non-compliant platform to transfer funds in cryptoassets. It exchanges between anonymous addresses, avoiding strict identity checks and increasing anonymity. It can thus quickly convert its illegally obtained funds, making it difficult for authorities to trace and recover them [14].



[13] Financial Action Task Force (FATF) - Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing, https://www.fatf-gafi.org/en/publications/Methodsandtrends/Virtual-assets-red-flag-indicators.html
[14] Europol, Internet Organised Crime Threat Assessment (IOCTA) 2021, https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2021

2. Use of money mules in money laundering

Money laundering in crypto-assets often involves the use of sophisticated tactics to hide the illicit origins of funds and avoid detection by the authorities. One such typology is the use of money mules.

These individuals become intermediaries in the transfer of illicit funds, thus facilitating their laundering and dispersal via cryptoassets. Money launderers agree to receive illicit funds into their personal accounts or e-wallets, and then follow the criminals' instructions on the transfers and conversions necessary to hide the trail of transactions and disperse the funds in a seemingly legal manner.

By involving money mules in this complex process, criminals can launder their money and benefit from the anonymous and decentralized characteristics of cryptoassets, giving them additional protection against identification and tracking by the authorities.

Description of typology

- recruiting money mules: criminals identify potential money mules through various channels such as online recruitment sites, social media platforms or even personal acquaintances. They are lured by promises of quick and easy wins or offers of "work" in fictitious companies;

- training and involvement of money mules refers to the fact that they are trained and provided with personal and banking information to facilitate the transfer of funds through their accounts, including the creation of cryptoassets accounts and conducting transactions on behalf of criminals;

- fund transfers: money mules transfer illicit funds to cryptocurrency addresses specified by the criminals, using exchange platforms or digital wallets;

- splitting and dissipation of funds: once funds are transferred to cryptoasset addresses, criminals attempt to dissipate and split these funds to increase the difficulty of tracking and identifying them. This may involve conducting multiple and complex transactions between different crypto-asset addresses, commingling funds through mixers, and using other fund dispersal tactics;

- Conversion into fiat currencies: finally, funds converted into crypto-assets can be transferred back into fiat currency in an attempt to break the link with the original illegal activities. To carry out these transfers, criminals may use cryptocurrency-fiat exchange platforms or resort to P2P transactions involving individuals or entities willing to exchange the currency. This complex process makes it difficult to trace the origin and final destination of funds;

- he complicity of money mules: it is important to note that in many cases, money mules may be aware of or even complicit in the illegal activities they are involved in, motivated by profit or manipulated by blackmail or threats.

Typology-specific indicators

1. Relationships with persons known to be involved in criminal activities: the main cause of money launderers' involvement in money laundering is their relationship with the criminals who obtained the funds illegally. These money mules often have connections and acquaintances in the criminal world, which facilitates the money laundering process through them;

2. Unauthorized financial intermediation services: money mules often operate as unauthorized financial intermediaries, offering money transfer and currency conversion services on behalf of criminals. They may act as individuals or may have shell companies through which they carry out their illegal activities;

3. Unusual and atypical financial transactions: money mules carry out financial transactions outside normal business patterns. These transactions may include frequent currency exchanges, rapid and repeated transfers of funds between accounts, and the use of complex ways to hide the traces of financial transfers;

4. Use of multiple bank accounts: Money mules typically use multiple bank accounts to disperse and hide funds. They may have accounts in different jurisdictions and transfer money between these accounts to make it difficult to trace the flow of money and to hide traces of illicit activities;

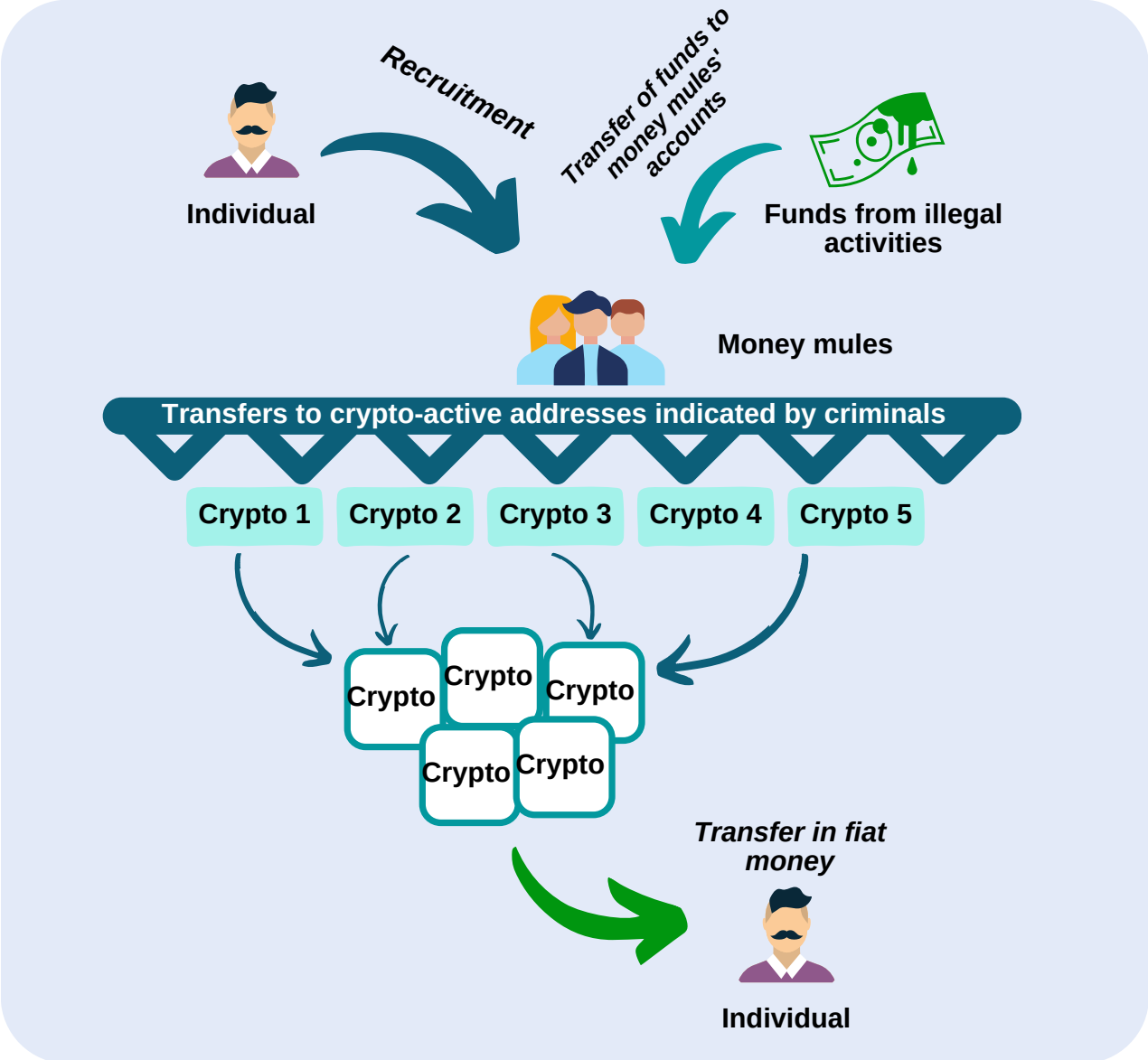
5. Cash transactions: money mules are often involved in cash transactions as they offer a higher level of anonymity and facilitate money laundering through the rapid exchange of cash funds between different people and locations;

6. . Use of transaction structuring schemes: to avoid triggering STRs, money mules may use transaction structuring schemes whereby they divide large amounts of money into smaller transactions to avoid attracting the attention of financial authorities.

Practical examples:

1. An individual is recruited to transfer illicit funds via cryptoassets to a person in another country. He receives precise instructions on the cryptoassets accounts to which he is to make the transfers and receives a portion of the funds as a reward for his services [15];

2. A criminal group uses an extensive network of money mules to transfer funds derived from phishing and online fraud activities into cryptoassets. They use various cryptoassets addresses and blending services to hide the origin of the funds and make it difficult to trace them [16];



[15] Elliptic Typologies Report 2022 Edition, Preventing Financial Crime in Cryptoassets
[16] https://www.fatf-gafi.org/en/publications/Methodsandtrends/Virtual-assets-red-flag-indicators.html;

3. Use of mixers and DeFi platforms to hide tracks

One of the tools used by criminals to cover their tracks and launder illicit funds is the use of mixers and decentralized platforms. Mixers, also known as crypto tumblers, are specialized platforms that allow the mixing of cryptoassets by combining and commingling multiple transactions, making it difficult to trace the origin of funds. These mixers provide a form of anonymity, as it is not possible to identify the exact sources and destinations of transactions.

Description of typology

The use of mixers and decentralized platforms is a common typology in the process of money laundering through cryptoassets. This typology involves the following steps:

- the criminal transfers his cryptoassets into a mixer. It takes the cryptoassets from different users and redistributes them in a way that masks the link between the source and destination addresses. This process usually involves multiple internal transactions and exchanges between different addresses, which further complicates the tracking of funds;

- anonymous transactions and no identity verification: decentralized mixers and platforms offer users the possibility to conduct transactions without having to disclose detailed personal information or undergo rigorous identity verification. This feature offers users an increased level of anonymity and privacy in financial transactions;

- lack of centralized control and storage of funds: decentralized platforms, with no centralized intermediaries and no storage of user funds, provide increased privacy and security. This feature offers users protection, but also gives criminals the opportunity to carry out discretionary transactions without leaving obvious traces;

- mixers and DeFi platforms offer chat services between users, facilitating communication and coordination of illegal transactions. This facilitates the exchange of information about suspicious activity and helps criminals to carry out illegal transactions undetected;

- some platforms may be involved in transactions with illicit cryptoassets. Suggestive messages on the site, such as accepting cash or detailed instructions for bank transfers, may signal possible involvement in illegal activity.

Typology-specific indicators:

- **The use of mixers:** one of the specific indicators is the frequent transfer of cryptocurrencies in a mixer, such as Tornado Cash. Criminals can perform a series of internal transactions and exchanges between multiple different addresses in order to mix cryptoassets and hide the trail of transactions. This complex and repetitive process of transfers and exchanges is designed to make it difficult to investigate and identify the origin or destination of funds;

- **Exchange between different cryptoassets:** another indicator is the exchange of crypto-assets mixed into other digital assets or fiat currency through decentralized platforms. Criminals can use these platforms to convert cryptoassets into other forms of assets, making it more difficult to track transactions;

- **Lack of rigorous KYC:** mixers and decentralized platforms do not impose strict identity verification measures on users. This allows criminals to open anonymous accounts without providing detailed personal information or having their identity properly verified;

- **Suggestive anonymity messages:** these may be displayed on some crypto-asset mixing platforms or on various decentralized platforms, suggesting that users can transact without being detected or tracked. These messages may encourage users to trust the platform and believe that their financial activities will be hidden and shielded from the eye of the authorities. By promoting a sense of anonymity and privacy, these messages can attract the attention of criminals who want to cover their tracks and take advantage of money laundering opportunities without consequences;

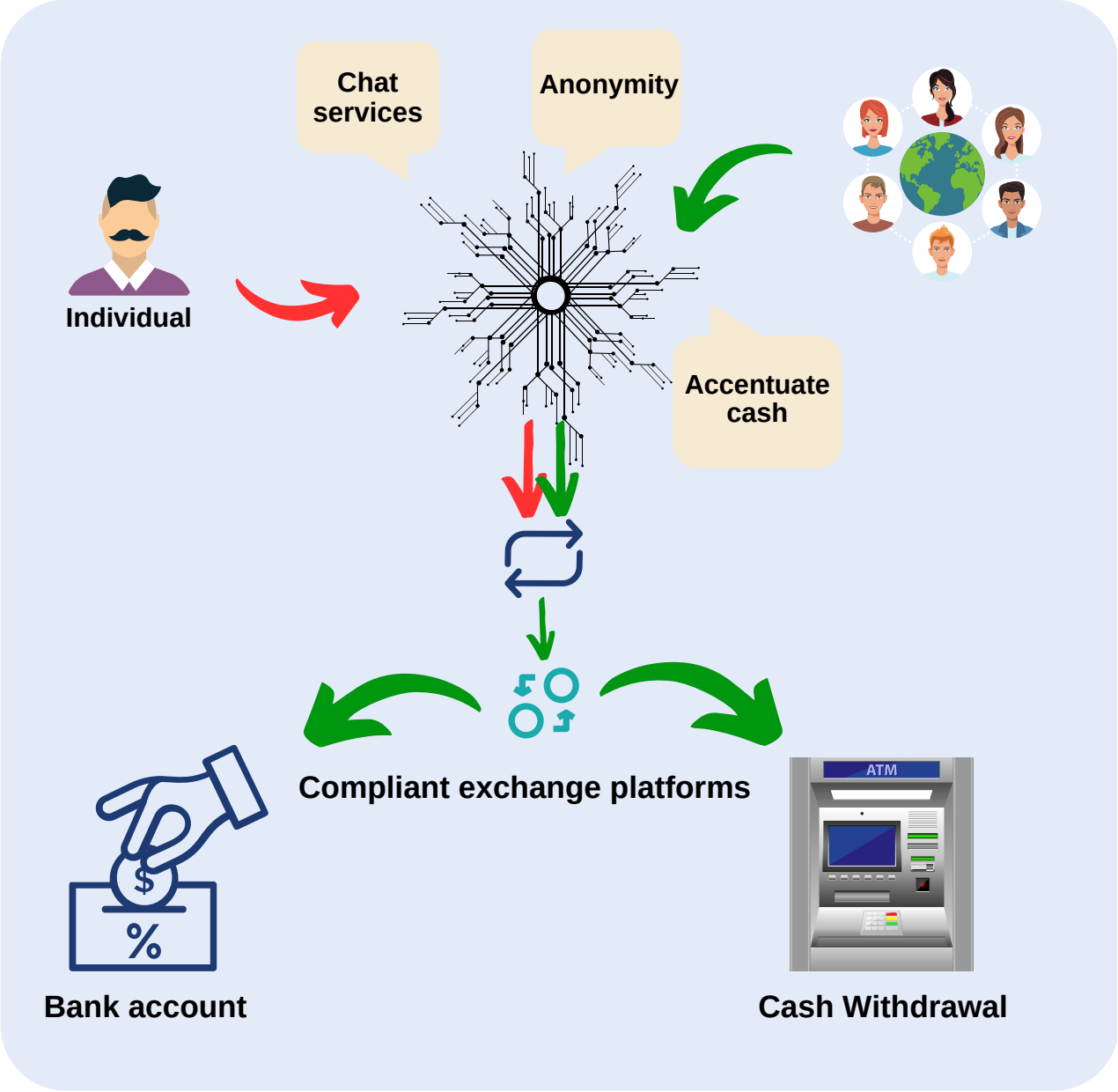
- **Involvement of platforms in illicit transactions:** there are situations where cryptoasset mixing platforms or decentralized platforms are involved in transactions with illicit crypto-assets. This can be evidenced by investigations and relevant information about suspicious activities carried out on these platforms.

Practical examples:

1. Silk Road was an online marketplace known for the illegal trade of drugs and other illicit goods. In this case, users involved in illegal activities used decentralized mixers to shuffle illegally obtained cryptoassets, thus hiding the origin of the funds and making them appear clean [17].

2. AlphaBay was an online marketplace shut down in 2017 by the FBI, known for illegally selling drugs, weapons and other illicit goods. In this case, a criminal group used the decentralized platform to exchange cryptoassets obtained through illegal activities into other digital assets or fiat currency [18].

3. An individual or a criminal group involved in financial crimes, such as bank fraud or tax evasion, uses a blender to mix cryptoassets obtained through these illicit activities. The mixer takes the cryptoassets and mixes them with other funds from legitimate sources, making it difficult to trace and identify specific transactions [19].



[17] United States Department of Justice (DOJ), https://www.justice.gov/usao-sdny/press-release/file/1549821/download;
[18] FBI, https://www.fbi.gov/news/stories/alphabay-takedown;
[19] Europol - "Internet Organised Crime Threat Assessment (IOCTA) 2020" (https://www.europol.europa.eu/iocta-2020).

4. Use of crypto ATMs to launder money

With the rise in popularity of crypto ATMs, they have become an increasingly used solution to buy and sell cryptocurrencies in a convenient and affordable way. However, a significant issue that needs to be addressed relates to the potential money laundering risk associated with the use of these ATMs,

According to a study [20] conducted in 2021, Romania ranks 9th in the world in terms of the reported number of crypto ATMs, with a total of 86 crypto ATMs in operation. This figure indicates a significant presence of these facilities in our country, reflecting the population's increased interest in and need for accessibility to cryptocurrency transactions. However, with the increasing use of crypto ATMs, a number of associated risks are also coming to the fore, particularly in terms of money laundering and misuse of cryptoassets.

Description of typology

The use of crypto ATMs for money laundering is an effective tactic by which criminals try to convert funds derived from illegal activities into cryptocurrencies.

Crypto ATMs are electronic devices that allow users to buy and sell cryptocurrencies, such as Bitcoin, Ethereum or Litecoin, quickly and easily.

With this type of ATM, criminals can carry out anonymous and confidential transactions without having to reveal their identity or go through rigorous verification processes. This feature of crypto ATMs provides criminals with a favorable environment to launder illegally obtained money. They can purchase cryptoassets through these devices using funds derived from illicit activities and then sell or transfer the cryptoassets to other addresses, thus hiding the origins and destinations of the funds.

In addition, crypto ATMs allow cash transactions, making the money laundering process even harder to detect. Criminals can deposit cash into a crypto ATM and receive cryptoassets in return, without the source of the funds being identified or traced. This ability to quickly convert cash into cryptocurrencies facilitates the money laundering process and complicates subsequent investigations by the authorities. As a relatively new and evolving technology, supervisory regulations and procedures may struggle to keep pace with innovations and tactics used by criminals.

[20] https:cryptohead.io/research/cryto-ready-index

Another important aspect of using crypto ATMs for money laundering purposes is that these devices can be located in public or private locations, such as shopping centers, bars, restaurants or even offices. This gives criminals a wide range of locations where they can conduct transactions without raising suspicion. Also, the installation and setup of a crypto ATM does not require special licenses or approvals in many jurisdictions, making it difficult to effectively monitor and regulate these facilities.

Typology-specific indicators:

- **Repeated use of the same crypto ATM for significant cash transactions** may raise questions about the source of funds and the purpose of their use. This may indicate suspicious activity, such as money laundering or financing illegal activities;

- **The crypto ATM is located in high-crime areas** or in a location associated with a front business that may be owned by criminals;

- **Transacting large amounts of money in a short period of time** is a tactic used to fragment and disperse funds. The purpose of this practice is to hide the traces of the transactions and to make it difficult for the authorities to trace and investigate them later;

- **Conducting transactions through crypto ATMs for the purpose of quickly transferring funds between anonymous cryptocurrency addresses.** The use of anonymous cryptocurrencies makes it easier to hide the origin and destination of funds, which may indicate illegal activity;

- **Multiple digital wallets send funds via ATMs** to a single recipient in a short period of time;

- **The use of a large number of cards or digital wallets** to transact with crypto ATMs;

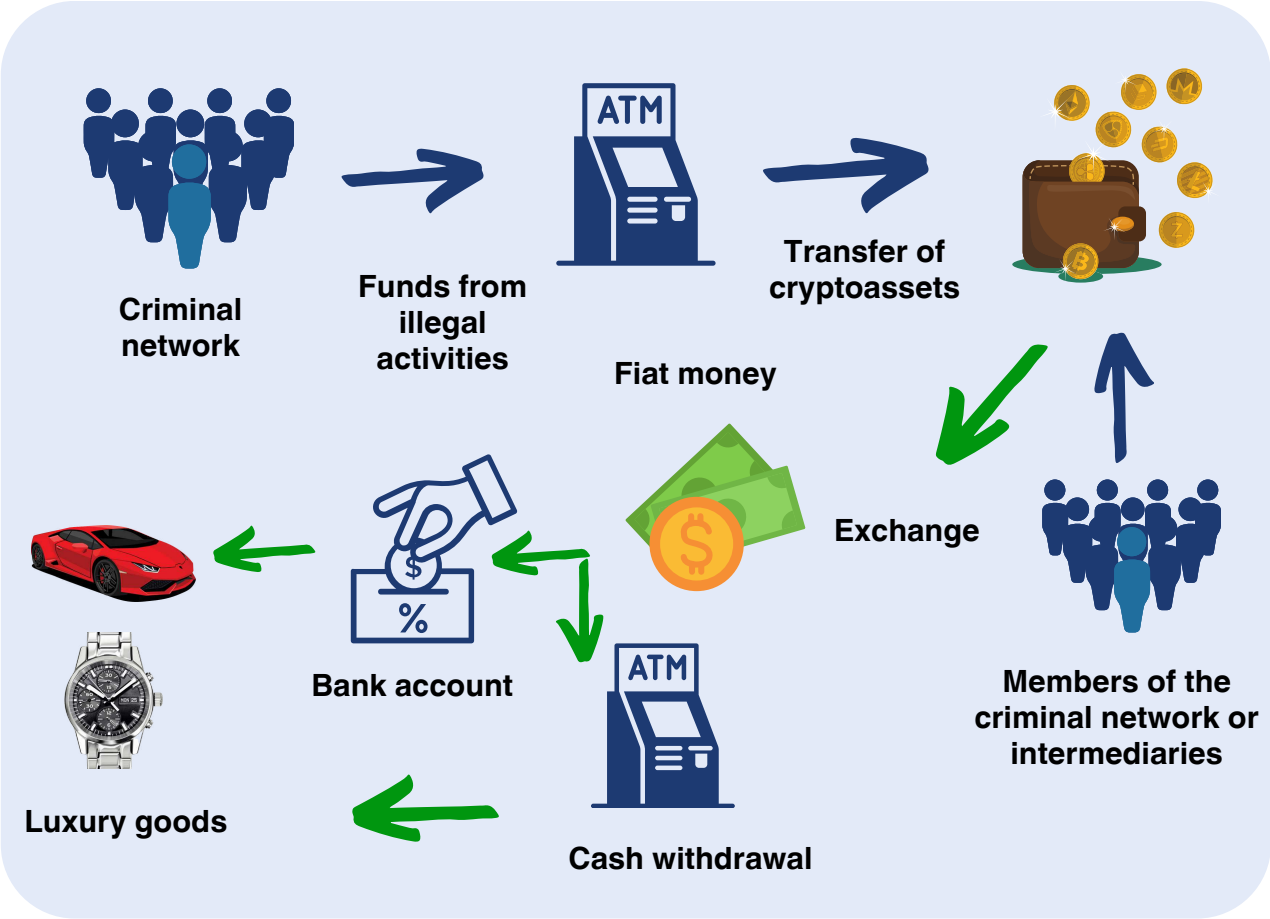
- **Transactions with smaller amounts and very close to the reporting thresholds** set by the financial authorities may raise suspicions of an intention to avoid reporting obligations and to hide financial activities;

- **The use of crypto ATMs to transfer cryptocurrencies** to unauthorized or non-compliant platforms in jurisdictions with weak customer identification rules.

Practical examples:

1. A criminal group is using crypto ATMs located in countries with weak regulations to convert large sums of drug money into cryptocurrencies. This points to a strategy adopted by criminals to hide and launder funds derived from illegal activities by exploiting loopholes in the regulation and oversight practices of these countries [21].

2. An individual conducts repeated buy-sell transactions using crypto ATMs. He adopts a strategy whereby he fragments and disperses funds into different types of cryptocurrencies, thus attempting to make it difficult to track and investigate his transactions [22].



[21] Elliptic Typologies Report 2022 Edition, Preventing Financial Crime in Cryptoassets
[22] Financial Action Task Force (FATF) - Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing, https://www.fatf-gafi.org/en/publications/Methodsandtrends/Virtual-assets-red-flag-indicators.html

5. The use of NFTs for money laundering purposes

NFTs have gained popularity recently, representing ownership of a unique digital asset, such as a digital artwork or video game. As defined by Clifford Change, NFTs are digital tokens created based on blockchain technology, which give the owner the right to own and trade a unique and non-searchable digital object.

However, an unintended consequence of the popularity of NFTs is their use for money laundering purposes. This growth in the use of NFTs raises significant concerns about the integrity and legality of transactions conducted with them. As NFTs allow the tokenization of unique digital assets and even physical assets, there is a risk that these transactions could be used to hide or launder funds derived from illegal activities. Because NFTs are traded online and recorded on the blockchain, the appearance of transparency is present. However, due to the unique and indistinguishable nature of NFTs, identifying the parties involved and tracing the origin of funds becomes difficult.

Description of typology

Money laundering using NFTs can involve several types of schemes and strategies. Here are some examples of money laundering typologies that can be associated with NFTs:

- **Creation and trading of fictitious NFTs:** In this scheme, criminals create false or fictitious NFTs and trade them between their accounts or with the complicity of third parties. The aim is to create the appearance of legitimate transactions and launder the proceeds of illegal activities through these NFTs;

- **Use of real NFTs but purchased with illegally obtained funds:** In this strategy, criminals use funds obtained from illegal activities to purchase real NFTs. These NFTs can then be traded on legal NFT markets, apparently legitimizing the origin of the funds. In this way, criminals try to conceal the illegal transactions and make 'clean' profits through NFTs;

- **Using NFTs for transfers of value: another money laundering strategy through NFTs involves using them to transfer value between different entities or cryptocurrency addresses.** Criminals can purchase NFTs and transfer them between their accounts or to an accomplice to hide money flows and make it difficult to trace transactions;

- **Money laundering through digital art:** an increasingly common tactic is to associate NFT with digital art. Criminals can create or purchase digital artworks and turn them into NFTs, giving them an appearance of uniqueness and value. These NFTs can then be traded on NFT platforms, and the money from these transactions can be considered "clean". This allows criminals to use digital art and NFTs as money laundering tools.

These are just a few examples of the types of money laundering that can be associated with NFTs. It is important to note that these activities can vary in complexity and may involve additional techniques and strategies to conceal illegal transactions and make them difficult for the authorities to trace.

Typology-specific indicators:

- **Transactions in NFTs at extremely high prices may suggest money laundering, masking the true purpose of these operations;**

- **Frequent transfers of NFTs between anonymous addresses** may indicate deliberate attempts to hide transactions and avoid detection of illegal activities;

- **The use of non-compliant exchange platforms for trading in NFTs** may indicate illegal activity and an environment conducive to money laundering, as these platforms may offer a higher degree of anonymity and weaker or non-existent enforcement of compliance measures;

- **The creation of NFTs using anonymous addresses** is a practice where tokens are generated and traded without being associated with verifiable identities. This can be accomplished by using anonymous digital wallets or other services that allow the user's identity to be hidden;

- **Transactions with NFTs in poorly regulated jurisdictions** may indicate doing business in areas with low cryptoassets compliance standards;

- **The use of NFTs as a tool for value transfer between cryptoassets** is a strategy whereby NFTs are used to facilitate the exchange of digital assets between different types of cryptocurrencies or cryptoassets.

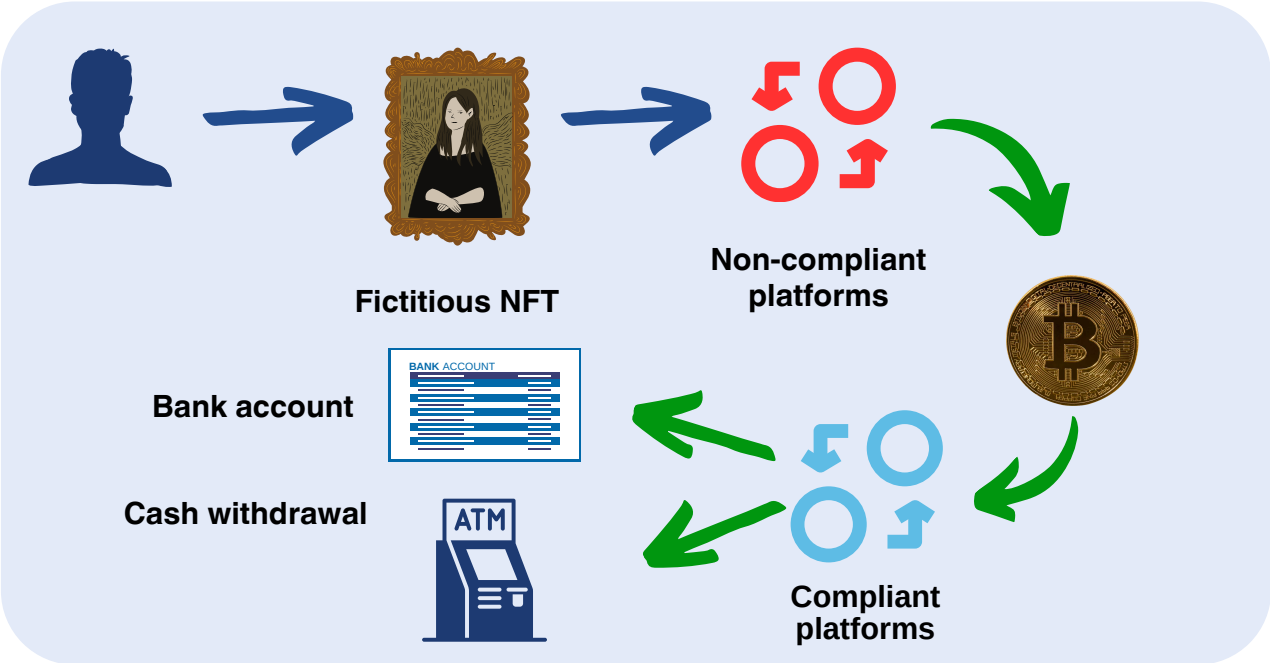
This use of NFTs can be exploited for money laundering purposes, as the transfer of value through NFTs can complicate the tracing of funds and the identification of illegal activities.

Practical examples:

1. An individual who owns an NFT wants to launder a sum of money illegally obtained through it. To make the NFT appear more valuable than it really is, the individual creates several anonymous addresses in his digital wallet. He then carries out fictitious transactions between these addresses, making fake purchases and sales of the NFT at exorbitant prices [23].

Through these rigged transactions, the individual manages to create the appearance of high demand and interest in his NFT. This enables him to attract the attention of legitimate buyers and sell the NFT at a higher price. The amount obtained from this transaction is now considered 'clean' and can be used legally, thus hiding the illicit origin of the funds;

2. A criminal group is using Bitcoin and NFTs to launder illegally obtained money. Thanks to the anonymity provided by the blockchain, Bitcoin transactions are confidential and do not reveal information about buyers and sellers. This allows criminals to purchase digital art or other assets using illegally obtained funds without attracting the attention of the authorities. Bitcoin transactions are immutable, meaning they cannot be refunded or canceled and the origin of the funds remains unknown. Thus, by using NFTs, criminals can conceal the illicit origin of the money and legitimize it through seemingly legal transactions with digital assets [24].



[23]Chainalysis 2022 Crypto Crime Report, https://go.chainalysis.com/2022-Crypto-Crime-Report.html;
[24] NFT money laundering and AML compliance, https://withpersona.com/blog/nfts-and-compliance-what-to-know-about-this-crypto-era-commodity.

6. The use of ICOs to launder money

ICOs (Initial Coin Offerings) are a popular method of cryptocurrency financing, where a new digital currency or token is issued in exchange for investment in projects. However, the use of ICOs can be susceptible to abuse and misuse for money laundering purposes.

The use of ICOs for money laundering purposes is a major concern for financial regulators. This malpractice involves the conversion of funds derived from illegal activities into digital currencies through ICOs in order to integrate them into the legal economy and hide their illicit origin. ICOs thus become an attractive tool for money laundering due to their specific characteristics. It is important to emphasize that money laundering through ICOs is not a widespread practice, but it is essential to identify and understand the risks associated with this typology in order to develop effective measures and solutions to combat this phenomenon.

Description of typology

1. Anonymity: ICOs offer a high degree of anonymity as participants are not required to reveal their full identity during the investment process. This makes identifying and tracking transactions more difficult, allowing money laundering through ICOs;

2. Use of other cryptocurrencies: some ICOs allow investors to purchase tokens using other cryptocurrencies instead of traditional coins. This provides opportunities for money laundering through ICOs, as funds from illegal activities can first be converted into another cryptocurrency and then used to buy tokens in ICOs;

3. Complexity of ICO structures: some ICOs may have complex structures and advanced mechanisms, which may be intentionally used to hide the origin of funds and create a more difficult money laundering process to trace. These structures may involve the use of multiple funding stages, intermediaries or multiple cryptocurrency addresses to complicate further investigation;

4. Poorly regulated jurisdictions: ICOs can benefit from jurisdictions with weak or no anti-money laundering regulations. These jurisdictions provide an enabling environment for ICOs to conduct money laundering, as there are fewer legal restrictions and controls in place to prevent and detect these illicit activities;

5. Use of funds outside ICO projects: some ICOs may be used fraudulently, in the sense that the funds raised are not properly used for the development of the proposed project. Instead, these funds may be diverted to the issuers' personal accounts or other speculative investments, thus contributing to money laundering.

It is important to note that the typology description does not cover all aspects of the use of ICOs for money laundering purposes, as these practices may vary depending on the specific circumstances and strategies used by criminals.

Typology-specific indicators:

- **Large volumes of funds:** the use of ICOs for money laundering purposes can involve significant investments, as large amounts of money can be fragmented and hidden behind the tokens issued in the event. By splitting large sums into small tranches and distributing them across different ICO projects, money launderers can obtain digital tokens in exchange for their money, allowing them to capitalize on the growth potential of these digital assets and obtain seemingly legitimate funds;

- **Use of unauthorized or non-compliant exchange platforms:** money launderers may choose to run ICOs on unauthorized or non-compliant platforms or in jurisdictions with weak customer identification rules to avoid rigorous supervision and scrutiny by the authorities;

- **Use of fund commingling:** money launderers may use advanced fund commingling techniques to make it difficult to trace transactions carried out in ICOs and to hide the links between the cryptocurrency addresses involved. This tactic involves mixing and transferring funds through multiple cryptocurrency addresses in an attempt to create a complex web of transactions that is difficult to trace;

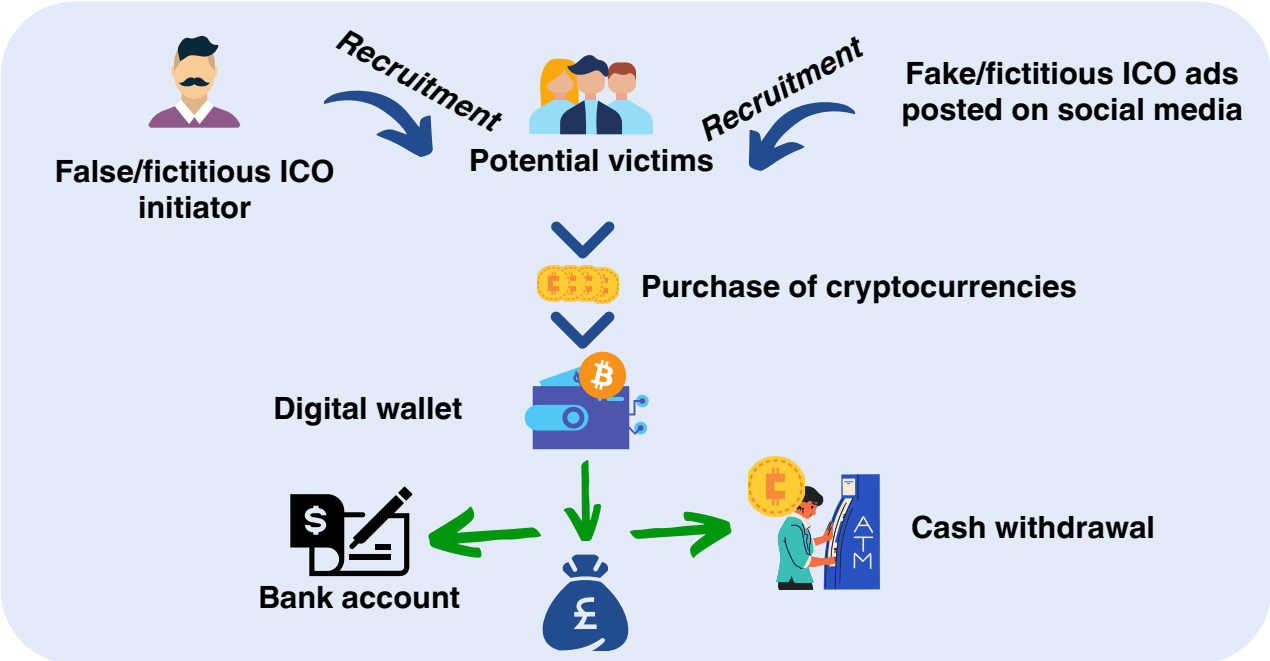
- **Involvement of multiple jurisdictions:** the use of ICOs for money laundering purposes can involve operations in different jurisdictions, complicating cooperation between authorities and the investigation of illegal activities. Money launderers can take advantage of the cross-border nature of cryptocurrencies and ICOs to transfer funds between different countries and jurisdictions with different rules on cryptocurrencies and money laundering;

- **Complexity of transactions:** the use of ICOs for money laundering purposes often involves the transfer of funds between anonymous cryptocurrency addresses, using advanced cryptographic techniques and complex blockchain protocols. This complexity of transactions makes it difficult to trace money flows and identify their origin.

Practical examples:

1. The use of unauthorized or non-compliant platforms: from 2017-2020, the US Securities and Exchange Commission (SEC) issued warnings and brought legal actions against several ICOs that were found to be unauthorized and not in compliance with securities regulations. These legal actions targeted money laundering attempts through ICOs and resulted in financial penalties and bans. The SEC brought charges against Dominic Lacroix and his company, PlexCorps, for promoting and selling securities called PlexCoin over the internet to investors in the U.S. and other countries, making false claims that investments in PlexCoin would yield a 1,354% return in less than 29 days [25].

2. . The use of fund blending in ICOs can be exemplified by the Monero cryptocurrency platform project. As part of the ICO process, Monero has implemented advanced fundmixing techniques to improve the level of transaction confidentiality. This was achieved by using a special protocol called "Ring Confidential Transactions". This protocol groups transactions into a "ring" of digital signatures, making it difficult to trace the origin of transactions. This practice attracted both privacy-minded investors and individuals with illegal intentions who saw Monero as a way to launder money. The commingling of funds increased opacity and made it difficult for the authorities to investigate suspicious transactions [26].



[25] SEC Emergency Action Halts ICO Scam, https://www.sec.gov/news/press-release/2017-219;;
[26] Virtual Asset Red Flag Indicators of Money Laundering and Terrorist Financing, https://ciphertrace.com/virtual-asset-red-flag-indicators-of-money-laundering

4.2. Terrorist financing: magnitude and nature

Terrorist financing is a global security threat that requires a coordinated and concerted approach by national and international authorities. In this context, virtual asset service providers are becoming increasingly visible to terrorist entities due to the specific characteristics of cryptocurrencies, which facilitate rapid financial transfers and avoid scrutiny by authorities. Although the use of cryptocurrencies by terrorist organizations represents a small fraction of illicit transactions in the crypto ecosystem, it remains a constant concern. The seriousness of any funds contributing to terrorism, regardless of the amount, requires the utmost attention from the public and private sector.

According to the National Defense Strategy for the period 2020-2024, the terrorist phenomenon in Romania maintains its conjunctural character, being dependent on developments in the external space. Expressing itself indirectly, through its association with NATO, the EU, the USA and the European states actively involved in the fight against terrorism, Romania remains a target of opportunity for terrorist organizations. Radical Islamist hostile Islamist information campaigns continue to be the main factor fuelling (self-)radicalization processes, which constitute one of the significant security risks in Romania, although without reaching the scale of a phenomenon.

The National Defense Strategy 2020-2024 highlights major trends with the potential to affect and influence the security environment, including cryptocurrencies, blockchain technology, artificial intelligence, machine learning, Internet of Things, big data and quantum technology, which can be used in organized crime, cybercrime, hacktivist, terrorist or extremist activities, as well as in offensive operations coordinated by entities supporting the interests of state actors. The risks of adapting hybrid offensive actions to technological developments are emerging through a continuous diversification of modus operandi and coordinated resources aimed at damaging national interests, including security interests.

What is terrorist financing?

„Collecting or making available, directly or indirectly, funds, whether licit or illicit, with the intention that they should be used or in the knowledge that they are to be used, in whole or in part, to commit terrorist acts or to support a terrorist entity, and is punishable by imprisonment of 5 to 12 years and disqualification from certain rights" [27]

The national legislation has created the necessary framework for inter-institutional consultations, facilitating proper exchange of information and integrated risk analysis in the area of competence. Reporting entities, i.e. providers of virtual currency and fiat currency exchange services, as well as digital wallet providers, are obliged to report suspicious transactions to the National Office for the Prevention and Combating Money Laundering if they know, suspect or have reasonable grounds to suspect terrorist financing activities. Their ability to identify terrorist financing transactions is essential for the documentation of illicit activities.

The NOPCML analyzes and processes the information received, and if there are indications of terrorist financing, it immediately informs the competent authorities in the matter.

The FATF guidelines [28] recommend the adoption of a robust regulatory framework for VASPs, including the obligation to report suspicious transactions and comply with know-your-customer requirements. This is important to prevent the use of cryptocurrencies in terrorist financing activities.

It should be noted that no suspicious transaction reports related to terrorist financing activities were received by the N during the period under evaluation.

The implementation of the new European legal framework will establish clear requirements for the authorization and supervision of VASPs, bringing national legislation in line with international standards and helping to reduce the risks related to terrorist financing.

[27] Law 535/2004 on preventing and combating terrorism
[28] FATF (June 2021) Guidance On Proliferation Financing Risk Assessment And Mitigation

Cryptocurrencies, the main foundation of the services offered by VASPs, have characteristics that make them attractive for illicit activities, including terrorist financing. The relative anonymity of transactions complicates the identification of users, giving malicious actors the opportunity to disguise funds used for terrorist actions. Rapid cross-border transfers substantially reduce authorities' ability to control international financial flows. This lack of uniform global regulation allows terrorists to exploit legislative loopholes between states by using VASPs in less regulated jurisdictions.

Since 2020, Romania has been using a terrorist alert system based on four levels: Low, Cautious, High and Critical [29]. Currently, the alert level is "Cautious", which suggests a low risk of terrorist attack, but with constant monitoring of potential threats. According to the National Defence Strategy 2020-2024 and the National Terrorist Alert System (NTS), Romania does not face a significant terrorist threat, as no terrorist organizations have been identified as active on its territory. However, the latent risk of the use of cryptocurrencies for terrorist financing may increase as these digital assets become more widespread.

The 2024 Chainalysis report highlights that terrorist organizations such as Hezbollah have demonstrated the ability to use cryptocurrencies to expand their traditional financial networks. In June 2023, a concrete example was the seizure of approximately $1.7 million in cryptocurrency linked to Hezbollah through a hawala operator. This situation illustrates the complexity of the terrorist financing infrastructure, which often relies on intermediaries to facilitate fund transfers, making it difficult to estimate terrorist-related activities.

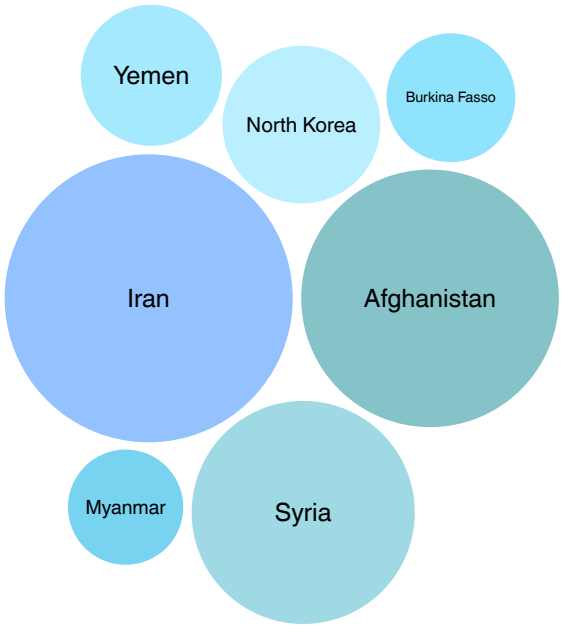
The VASP sector in Romania is in a development phase and is currently not subject to a specific authorization regime. However, this will change with the implementation of the MiCA (Markets in Crypto-Assets) Regulation, which will introduce a clear licensing and oversight framework for virtual asset service providers. Although, there have been no reported cases of terrorist financing through VASPs in Romania, the associated risks will increase as cryptocurrencies become more popular.

Migration and cross-border exposure are other vulnerabilities. Romania, located on a secondary transit route for migrants from the Middle East, North Africa and South Asia, may create an indirect vulnerability. In addition, transactions by VASPs from Romania to high-risk third jurisdictions require increased scrutiny given the rapid expansion of the sector internationally, although no links to such jurisdictions have been identified from the data and intelligence collected.

[29] https://www.sri.ro/sistemul-national-de-alerta-terorista

The volume of sanctions-related transactions is a growing share of total illicit transactions, in part due to the increase in the number of sanctioned entities, but also due to the difficulty of enforcing sanctions against entities in certain regions or decentralized operations.

The 2024 Chainalysis report noted that cryptocurrency flows to sanctioned entities and jurisdictions accounted for 61.5% of total illicit transaction volume in 2023 [30].



Main jurisdictions considered high risk by the VASPs in terms of terrorist financing

From the information collected through the questionnaires, it emerged that 80% of the entities perform checks on international sanction lists to assess the risks associated with their customers' jurisdictions in the context of terrorist financing (TF), which demonstrates an increased attention to managing risks related to customers and sanctioned jurisdictions.

At the same time, only one VASP reported that they had identified cases where, prior to initiating a business relationship or during the monitoring of an existing client, they had discovered clients who were on international sanctions lists.

In this case, the checks carried out through specialized platforms such as Ondato and Google led to the refusal to open business relationships, demonstrating the effectiveness of measures to prevent exposure to FT risks. These measures help to align with international requirements and reduce the risk of involvement in illicit activities.

In conclusion, the risks of terrorist financing in the VASP sector in Romania are low at the moment, but this is due to the early stage of development of the sector and the low level of terrorist threat at national level. However, the inherent characteristics of cryptocurrencies - anonymity, the speed of transfers and the lack of uniform regulation - continue to represent significant risk factors. The Romanian authorities need to implement additional regulations, strengthen supervision and maintain close international cooperation, adopting a proactive attitude and effective preventive measures to prevent the use of the sector for terrorist

[30] Chainalysis Crypto Crime Report 2024

purposes, thus adapting to the new challenges of innovative financial technologies and contributing to the global fight against terrorist financing.

4.3. Analysis of vulnerabilities in association with other economic sectors

The VASP sector in Romania presents a number of significant vulnerabilities, amplified by its interactions with various economic sectors. Its relationships with other sectors create significant risks from the perspective of preventing money laundering and terrorist financing, especially as many of these sectors are already identified as high risk in the 2022 National Risk Assessment. These vulnerabilities stem from the lack of appropriate regulation of crypto-assets and the difficulty in overseeing the anonymous and rapid transactions facilitated by these assets.

The vulnerabilities of the VASP sector are determined by several factors including market structure, ownership specifics, products and activities, geography, customers and transactions, and channels. Vulnerability analysis of the cryptoassets sector is complex and can be performed by considering its interactions and dependencies with other economic sectors.

In the case of the banking sector, this is one of the most highly regulated areas, with strict know-your-customer (KYC) and suspicious transaction reporting (STR) measures. However, interaction with cryptoassets could bring significant challenges, given the anonymity of transactions and the difficulty in identifying the real benefits of cryptoasset transactions. Turning cryptocurrencies into fiat currency through bank accounts poses a considerable risk, given the potential for illicit funds to be integrated into the traditional financial system. Although banks are tightly regulated, the increased use of cryptoassets calls for improved oversight mechanisms and cooperation with VASPs to prevent potential abuses.

E-commerce is another sector where interaction with cryptoassets adds a new level of risk. Online transactions are fast, anonymous and difficult to monitor, making them an ideal vehicle for money laundering. In addition, e-commerce platforms can be used to disguise illicit funds, especially when cryptocurrencies are accepted without proper checks. This anonymity makes supervision and enforcement of measures to prevent money laundering extremely difficult.

The results of the National Risk Assessment (2022) also highlight the vulnerability of the VASP sector in association with other high-risk economic sectors such as real estate, gambling and business consultancy.

These sectors already pose significant money laundering risks and the integration of cryptoassets into these areas only increases the level of exposure to illicit activities.

Analyzing the vulnerability of the crypto-assets sector in association with the gambling sector is a vast topic, given the growing popularity of cryptocurrencies and online gambling platforms. Due to the high volatility of crypto-assets, players could face significant losses quickly and gambling operators could have difficulties in managing financial risks. Cryptoassets also allow anonymity, which can facilitate money laundering and other illicit activities, and the gambling sector, especially online gambling, can be used to launder illegally obtained funds. The conclusion is that the crypto-assets sector, in combination with the gambling sector, presents significant vulnerabilities that require increased attention from both regulators and users. Linking financial, legal and security risks is very important to ensure a safer and more stable environment for all participants. It is essential to have a clear legislative framework and to invest in user education for those trading in this area.

Analiza vulnerabilității sectorului criptoactivelor în asociere cu sectorul jocurilor de noroc este un subiect vast, având în vedere creșterea popularității criptomonedelor și a platformelor de jocuri de noroc online. Din cauza volatilității mari a criptoactivelor, jucătorii s-ar putea confrunta cu pierderi semnificative rapid, iar operatorii de jocuri de noroc ar putea avea dificultăți în gestionarea riscurilor financiare. De asemenea, criptoactivele permit anonimitate, ceea ce poate facilita spălarea de bani și alte activități ilicite, iar sectorul jocurilor de noroc, în special cel online, poate fi utilizat pentru a spăla fonduri obținute din surse ilegale. Concluzia este că sectorul criptoactivelor, în asociere cu sectorul jocurilor de noroc, prezintă vulnerabilități semnificative care necesită o atenție sporită atât din partea reglementatorilor, cât și a utilizatorilor. Corelarea riscurilor financiare, legale și de securitate este foarte importantă pentru a asigura un mediu mai sigur și mai stabil pentru toți participanții. Este esențial să existe un cadru legislativ clar și să se investească în educația utilizatorilor pentru care tranzacționează în acest domeniu.

The link between the VASP sector and the services offered by management and business consultancy professionals is remarkable, as the two fields influence each other on various levels. However, these activities can amplify risks if advice is not properly aligned with legal requirements. As cryptoassets are integrated into traditional financial strategies, risks of non-compliance may arise, particularly in the absence of clear guidelines on the use of cryptoassets in advice. Advisors can bring valuable insights on how these two spheres can work effectively together and suggest ways to integrate cryptoassets into existing financial strategies. Industry vulnerability, in interaction with management and business advisory

services, is a multi-stakeholder issue involving regulation, security, volatility, transparency and ethics. Proactive approaches from advisors can help both investors and companies navigate these challenges, mitigating risks and maximizing opportunities in this evolving sector.

In conclusion, the crypto-assets sector is highly vulnerable due to its interconnectedness with other economic sectors, evolving regulations, volatility and technological risks. It is essential that investors, regulators and other stakeholders are aware of these risks, work together to ensure the proper integration of crypto-assets into the global economy and take effective measures to manage them.

V

Risk Management

5.1. Risk prevention and mitigation measures

Risk prevention and mitigation measures in the VASP sector need to be integrated and well structured in order to respond effectively to identified challenges and vulnerabilities. These measures need to be tailored to the specificities of this sector, taking into account the characteristics of anonymous transactions, the speed and global nature of the virtual asset market and the high exposure to money laundering and terrorist financing risks.

The first essential step for risk prevention in this sector is the development and implementation of clear and effective national policies. These policies need to be coordinated between the authorities involved in the VASP sector and support the development of a sound legislative and regulatory framework. The implementation of the new European legal framework will bring greater clarity and ensure compliance with international standards, in particular with regard to the prevention of money laundering and terrorist financing.

With the introduction of regulations on the authorization of VASPs at national level, a formal oversight and control mechanism will be created. This process will include strict authorization and registration requirements for VASPs, setting clear rules for ML/TF compliance. This will enable continuous monitoring of activities and improve the ability of authorities to identify and combat associated risks, preventing the use of virtual assets for illicit purposes. The MiCA Regulation ensures that all entities offering crypto-asset services in the European Union will be subject to a uniform authorization process, thus increasing transparency and accountability of the sector.

In addition, international collaboration is a key element, facilitating the exchange of information and best practices between EU Member States, in particular in the area of data exchange on virtual asset transactions and suspicious activities.

In order to ensure effective risk prevention, VASPs need to apply stringent know-your-customer (KYC) and extensive due diligence measures, especially for transactions involving high-risk or high-value jurisdictions. Verifying the identity of customers and monitoring their activities are essential to prevent the use of virtual assets for illicit purposes. Continuous monitoring of transactions, using advanced technologies such as blockchain, will enable the automatic detection of suspicious activities and facilitate the prevention and combating of illegal activities. The implementation of "travel rule" requirements, which require the transmission of customer information in cross-border transactions, is central to risk prevention. In addition, operators of trading platforms for crypto-assets need to develop and implement effective risk management mechanisms and put in place rigorous internal controls to prevent fraudulent activities.

Operational oversight and law enforcement are essential for risk prevention. Law enforcement authorities need to work closely with supervisors and other relevant authorities to respond quickly to suspicious activity in the sector. VASPs should implement advanced technological systems to continuously monitor transactions and automatically detect suspicious or high-risk activities. In this context, on-site controls at the premises of the VASPs should be intensified to verify compliance with legal requirements. These measures will ensure constant and effective supervision of the sector.

In conclusion, the application of a risk-based approach and the strengthening of risk prevention and mitigation measures are central elements in the management of the VASP sector as regulated in the new European legal framework, thus complementing the supervisory measures established at national level.

The amendment of the national legal framework and the adoption of measures to implement the new European legal framework is a key element in the prevention and mitigation of risks in the virtual asset sector. These measures will bring national regulations in line with European and international requirements, ensuring more rigorous oversight of VASPs and increasing transparency and accountability in the prevention of money laundering and terrorist financing.

These measures, properly and coherently implemented, will help to increase confidence in the virtual asset market and prevent its misuse for illicit purposes, thereby enhancing market integrity and transparency.

5.2. Response and risk management strategies

The response and risk management strategies in the VASP sector need to be dynamic, integrated and take into account the specificities of VASP transactions. These strategies aim to prevent the risks of money laundering (ML) and terrorist financing (TF) through a risk-based approach and swift and effective response measures that ensure continued compliance with national and international regulations.

The Risk-Based Approach (RBA) is the foundation of the response strategy. Oversight and control of VASP sector entities should be performed based on the risk profile of each entity and transaction. Thus, high-risk entities, such as those that facilitate user anonymity or conduct complex cross-border transactions, should be prioritized in the supervision and control processes. VASPs need to implement extensive due diligence measures, especially for high-risk customers and transactions, including detailed verification of customer identity, continuous monitoring of transactions and collection of additional information about the source of funds and the purpose of transactions. This approach allows efficient allocation of resources to respond quickly to major risks.

In the event of the detection of suspicious transactions or potential security breaches, VASPs must have rapid response plans in place. These plans include measures such as immediate blocking of suspicious transactions, internal investigation of incidents and immediate reporting to the competent authorities. In addition, response strategies should include mechanisms to assess and remediate deficiencies to prevent reoccurrence of incidents and improve long-term compliance. The implementation of such rapid measures is essential to maintain market integrity and prevent the use of virtual assets for illicit purposes.

Cooperation with relevant competent authorities is another key element in effective risk management in the VASP sector. Virtual Asset Service Providers need to work closely with authorities to facilitate the rapid exchange of information on suspicious transactions and to respond promptly to data requests. This cooperation is essential for the application of the travel rule, which requires the transmission of customer information in cross-border transactions, thereby increasing transparency and traceability of transactions.

Developing and implementing effective operational response plans are fundamental to managing cyber threats, fraud and other risks that could compromise the security of virtual asset trading platforms. VASPs must have the ability to respond promptly to cyber-attacks or security incidents, thereby ensuring continuity of operations and the protection of customer data. Constantly updating technology infrastructure and conducting regular security testing will help identify and remediate vulnerabilities.

Continuous monitoring and updating of risk assessments are essential to ensure effective monitoring of VASP activities. Supervisory authorities should conduct regular on-site and offsite controls to monitor compliance with legal requirements and to assess the effectiveness of ML/TF prevention measures. These controls need to be flexible and adapted to new emerging risks, such as new types of illegal transactions involving highly anonymized cryptocurrencies or complex cross-border transactions.

In conclusion, response and risk management strategies in the VASP sector need to be dynamic and well coordinated. The implementation of risk-based measures, rapid response plans, effective collaboration with the authorities and the use of advanced monitoring technologies will ensure the protection of the virtual asset market and compliance with international and European standards, thus contributing to the prevention of the sector from being used for illicit purposes.

5.3. Risk assessment and profiling for the VASP sector

Establishing an appropriate risk profile for Virtual Asset Service Providers (VASPs) in Romania requires a detailed assessment of the risks associated with this sector. Major risks have been identified in relation to customers, products and services offered, transactions conducted, and regulatory compliance. These risks are analyzed in terms of their likelihood to materialize and the impact they may have on the sector in order to determine the overall level of risk and to establish measures.

In the VASP sector in Romania, an important factor contributing to the level of risk is the lack of a strict and clear regulatory framework for the authorization of VASPs. This absence of specific licensing regulations allows VASPs to operate without the necessary oversight of the entire sector and jeopardizes market integrity by exposing VASPs to high risks of money laundering and terrorist financing.

The risks associated with customers in the VASP sector are significant, particularly in the context of anonymous customers or customers from high-risk jurisdictions. There are also risks associated with customers considered as Publicly Exposed Persons (PEPs) and those operating in vulnerable economic sectors. Although the majority of clients are from Romania and the European Union, there is moderate exposure to cross-border risks and complex legal structures. The main vulnerabilities stem from the lack of uniformity in the application of KYC measures and the difficulty in monitoring the activities of high-risk clients. Strict due diligence is essential to prevent illicit activities in this sector.

The likelihood of this risk is considered medium to high, given the sector's exposure to customers in vulnerable jurisdictions. The potential impact is high, as money laundering and terrorist financing activities may seriously affect the integrity of the sector.

The products and services offered by VASPs, in particular cryptocurrencies that facilitate anonymity and exchanges between virtual currencies and fiat currencies, are high risk. These activities are often difficult to monitor and the anonymity offered by cryptocurrencies increases the risk of their use in illegal activities. Over-the-counter (OTC) services, which allow private transactions, also contribute to the high risk in this sector. The difficulty of monitoring transactions and applying due diligence measures for these services complicates compliance with anti-money laundering and countering the financing of terrorism (ML/TF) regulations,

The likelihood of this risk is high because the products and services offered by VASPs, by their very nature, favor anonymity. The impact is also high as these products may facilitate money laundering and terrorist financing in the absence of strict monitoring and regulatory measures. The lack of a clear regulatory framework for the authorization of VASPs compounds these risks, providing a window o f opportunity for illicit activities in this sector.

Anonymous and cross-border trading in the VASP sector is a source of considerable risk. Although recent data show a decrease in transaction volumes between 2021-2024, some VASPs continue to experience significant transaction volumes. Fluctuations in the crypto-asset market influence these transactions, and the anonymity specific to many cross-border transactions adds an additional layer of risk.

The likelihood is medium in the context of the recent downturn in activity, but a high risk remains due to the large volume of transactions that remains in the sector. The impact is high as anonymous and cross-border transactions continue to be a way to transfer illicit funds. Close monitoring of these transactions and constant adaptation of compliance measures are needed to limit these risks.

Compliance risk in the VASP sector in Romania remains a major concern, given the challenges related to the uniform application of ML/TF regulations. Although most VASPs have implemented compliance measures, including KYC procedures and automated monitoring solutions, there are still significant challenges in reporting suspicious activities and applying preventive measures. Insufficient knowledge of ML/TF typologies and the lack of a clear regulatory framework for the authorization of VASPs contribute to these risks.

The likelihood of this risk is medium, due to the efforts made by VASPs to implement compliance measures. However, the impact is high, as non-compliance may entail significant legal sanctions and reputational risks.

Global sector-wide threats in the VASP sector refer to major risks that affect the entire sector internationally, having a significant impact on its integrity and security. These threats are not limited to a single jurisdiction and can affect multiple platforms and entities operating worldwide. Although the European legal framework (MiCA and TFR) will soon be applicable, global risks persist due to the specificity of the crypto-assets market, the digital nature of these assets and the inherent vulnerabilities to cyber-attacks and other illicit activities.

Matrix of risks associated with the VASP sector in Romania

Category	Threats	Vulnerabilities	Probability	Impact	Risk level
Customer risks	Anonymous customers from high-risk jurisdictions	Insufficient KYC measures, crossborder exposure	Medium to high	High	High
Risks related to products and services	Anonymous cryptocurrencies, OTC services and ATMs	Monitoring difficulties, anonymity, lack of authorization	High	High	High
Risks related to transactions	Anonymous cross-border high value or cash transactions via ATMs	Fluctuations in crypto-assets market, increased anonymity	High	High	High
Compliance risks	Insufficient regulations, Non-compliance with ML/TF regulations	Challenges in reporting suspicious activity, lack of authorization	Medium	High	Medium to high
Global threat	Cyber attacks, complex cross-border transactions, spread of DeFi	Difficulty of traceability of anonymous transactions, exposure to non-cooperative jurisdictions	High	High	High
VASP sector risk in Romania: High Risk					

Probability refers to the chance or frequency with which an identified risk may materialize in the VASP sector. It is assessed in terms of the historical frequency of the risk, the vulnerabilities of the sector and the context in which VASPs operate. Probability is categorized into four levels. At a very high probability, the risk is considered unavoidable, frequently arising due to systemic weaknesses or due to the nature of activities in the VASP sector, such as anonymous or cross-border cryptocurrency transactions. A high probability indicates that the risk is very likely to occur under favorable conditions, such as interactions with customers in high-risk jurisdictions. If the likelihood is moderate, there is a medium chance that the risk is likely to occur, usually in specific circumstances, such as fluctuations in the cryptoassets market. At the low probability level, risk is unlikely to occur and only manifests itself in isolated situations, such as minor operational deficiencies.

Impact refers to the severity or consequences that a risk may have on the VASP sector if it materializes. It can include both financial impacts and legal consequences. In the case of a high impact, the risk may have serious consequences on the sector's functioning, financial stability and regulatory compliance, such as non-compliance with ML/TF requirements, which may lead to major sanctions and significant losses. A moderate impact indicates that the risk would affect the functioning of the sector, but to a manageable extent in the medium term, such as temporary deficiencies in the application of KYC measures. If the impact is low, the consequences are minor and manageable with no long-term effects on VASPs, such as minor operational errors with no consequences on the security of funds or compliance.

The risk matrix combines probability and impact to determine the overall level of risk for each category. For example, a risk with high probability and high impact is classified as high, meaning that it requires immediate mitigation measures. Conversely, a risk with low likelihood and moderate impact will be considered medium or low, and can be managed with periodic interventions and less significant resources.

Overall, high risks require urgent interventions and rigorous prevention and mitigation measures, as well as constant monitoring to prevent serious consequences for the sector. Medium-high risks require prompt action and strict prevention measures, but are manageable in the long term. Medium risks are less pressing and can be managed by already existing prevention measures, while low risks can be addressed by minor interventions without having a significant impact on the overall business.

In conclusion, the sectoral assessment of ML/TF risks in the VASP sector in Romania indicates a high risk, due to the anonymity of transactions, the complexity of products and services offered, as well as the compliance and regulatory challenges, emphasizing the need to implement strict monitoring and control measures to prevent the sector from being used for illicit activities.

Conclusions and recommendations

6.1. Summary of main findings

The risk assessment of the VASP sector in Romania highlights several key vulnerabilities and major risks. The adoption of the new legal framework, which will harmonize the national legislation with the European MiCA and TFR regulations, marks an important milestone in the regulation of the crypto-assets sector. This harmonized legal framework will help to ensure that the sector complies with international standards to prevent money laundering and terrorist financing (ML/TF), thereby protecting investors and financial stability, while providing an appropriate framework for innovation and development.

The information obtained through the surveillance conducted by the National Office for Prevention and Combating Money Laundering provides a solid basis for assessing the risks associated with the VASP sector. However, these data are limited by the small size of the sector and the low number of controls carried out, thus underlining the need for risk assessment to be a continuous and dynamic process. This is essential to keep pace with the evolution of the sector and emerging threats, ensuring an effective system to prevent and combat money laundering and terrorist financing.

Globally, the risks associated with the VASP sector are amplified by the anonymity of transactions, geographical vulnerabilities and the use of new decentralized financial technologies. The concentration of illicit activities around specific platforms adds an additional layer of risk. In this context, the full implementation of FATF recommendations and the adoption of stringent regulatory and compliance measures remain essential to mitigate these risks.

Client-related risks are also significant, in particular for clients from high-risk jurisdictions, Publicly Exposed Persons (PEPs) and those operating in vulnerable economic sectors. Although the majority of clients are from Romania and the European Union, there is moderate exposure to cross-border risks and complex legal structures. Strict KYC and due diligence measures remain essential to reduce these vulnerabilities and prevent illicit activities.

In terms of products and services offered by VASPs, the risk is considered high. The anonymity and complexity of transactions, including exchanges between virtual currencies and fiat currencies, custody of cryptoassets, and the operation of cryptocurrency ATMs, pose major challenges in terms of ML/TF regulatory compliance. Over-the-counter (OTC) services also contribute to this elevated risk due to the private nature of the transactions, which require stricter monitoring and rigorous know-your-customer measures.

Compliance risk is also a significant element in the VASP sector in Romania so, although most VASPs have implemented compliance measures, including KYC procedures and automated monitoring solutions, there are still challenges related to the uniformity of application of these measures and the identification and reporting of suspicious activities. Close monitoring and constant enforcement of preventive measures are essential to ensure the integrity of this growing sector.

In terms of transaction-related risk, the data collected for the period 2021-2024 shows a decrease in both crypto-asset ATM activity and overall transaction volume. This decline can be attributed to fluctuations in the crypto-assets market, which, after peaking in 2021, entered a correction phase. Although activity in the sector has declined, the complexity and high value of funds involved in the remaining transactions emphasizes the need for continuous monitoring and strict compliance measures.

Although the number of money laundering cases associated with the sector is low, the complexity and sophistication of these crimes create major risks. Cross-border criminality and the global nature of cryptocurrencies complicate authorities' efforts to track financial flows and recover illicit funds. To address these emerging risks, strengthened regulation, the use of advanced technological solutions and enhanced international cooperation are essential.

The VASP sector in Romania has been assessed as high risk based on the risks identified at national level, but also taking into account global trends and significant cross-border risks. Transaction anonymity, product complexity and exposure to high-risk jurisdictions amplify the sector's vulnerabilities. In addition, the lack of a comprehensive regulatory framework at national level, in particular with regard to the authorization of VASPs, contributes to increased risks. These elements, combined with international risks and the use of cryptoassets in illicit activities, underline the need for strong supervisory and regulatory measures.

6.2. Recommendations for authorities and entities

On the basis of the risks identified in the VASP sector in Romania, it is essential that the authorities and entities involved adopt effective and integrated measures to manage vulnerabilities and prevent the use of this sector for illicit activities. The implementation of a comprehensive regulatory framework, harmonized with European and international requirements, is crucial to strengthen oversight and compliance in this area.

A first necessary step is the urgent adoption of a clear and coherent framework for the authorization of Virtual Asset Service Providers (VASPs). The lack of strict regulation for the authorization of VASPs represents a significant risk. The implementation of European regulations, such as MiCA and TFR, will ensure better control over activities in this sector, reducing the risks of money laundering and terrorist financing (ML/TF).

At the same time, it is recommended that providers of exchange services between virtual and fiat currencies, as well as providers of digital wallets, should be covered under a specific CAEN code, which would facilitate more effective monitoring of activities in this sector and help to manage the risks of money laundering and terrorist financing. Strengthening KYC and due diligence measures is also essential. VASPs need to apply stringent measures in assessing and monitoring their customers, especially those from high-risk jurisdictions and Publicly Exposed Persons (PEPs). This cooperation should include information sharing between supervisors and VASPs to facilitate the identification and mitigation of risks.

Relevant competent authorities need to work closely with VASPs to ensure that KYC measures are implemented consistently and effectively. This cooperation should include information sharing between supervisors and VASPs to facilitate the identification and mitigation of risks.

Given that Romania is among the top 10 countries globally in terms of the number of crypto ATMs (86 machines) and the ML/TF risks associated with cash transactions carried out through them, as well as the lack of consistent application of know-your-customer measures, it is necessary to introduce stricter requirements for verifying the identity of users and monitoring transactions carried out through crypto-ATMs.

In addition, the high risks associated with anonymous and cross-border transactions require the development of advanced monitoring mechanisms. The use of modern technologies, such as automated solutions for monitoring suspicious transactions, the implementation of "travel rule" requirements and the exchange of data between competent authorities in different jurisdictions will be essential to detect suspicious activities quickly. It is also important to strengthen cooperation between VASPs and authorities to ensure compliance with international standards and national regulations.

Cooperation at national level between law enforcement, supervisors and other relevant authorities is essential for effective oversight of the VASP sector and to ensure a rapid and coordinated response to risks. This cooperation may involve information sharing, joint investigation of suspicious transactions and consistent application of sanctions for noncompliance.

Given the cross-border nature of crypto transactions, international cooperation remains essential. Law enforcement, supervisors and other relevant authorities need to continue to work with partners in other countries to detect suspicious activity involving multiple jurisdictions. Improved international information exchange mechanisms, in particular between supervisory and law enforcement authorities, will help prevent money laundering and terrorist financing activities.

Although the NOPCML conducts training sessions for VASP entities, it is important to continuously build compliance capacity. These sessions need to be expanded and constantly updated to reflect new money laundering and terrorist financing typologies, thereby ensuring that VASPs are prepared to react quickly to emerging risks and apply compliance measures in accordance with ML/TF regulations.

In conclusion, in order to mitigate the high risks identified in the VASP sector in Romania, the adoption of a robust legal framework and the implementation of strict prevention and monitoring measures are essential. Effective cooperation at national level between the relevant competent authorities is also vital for effective oversight of the sector. By applying appropriate measures and developing effective monitoring and reporting mechanisms, the VASP sector can be protected from being used for illicit activities, contributing to maintaining financial stability and protecting investors.