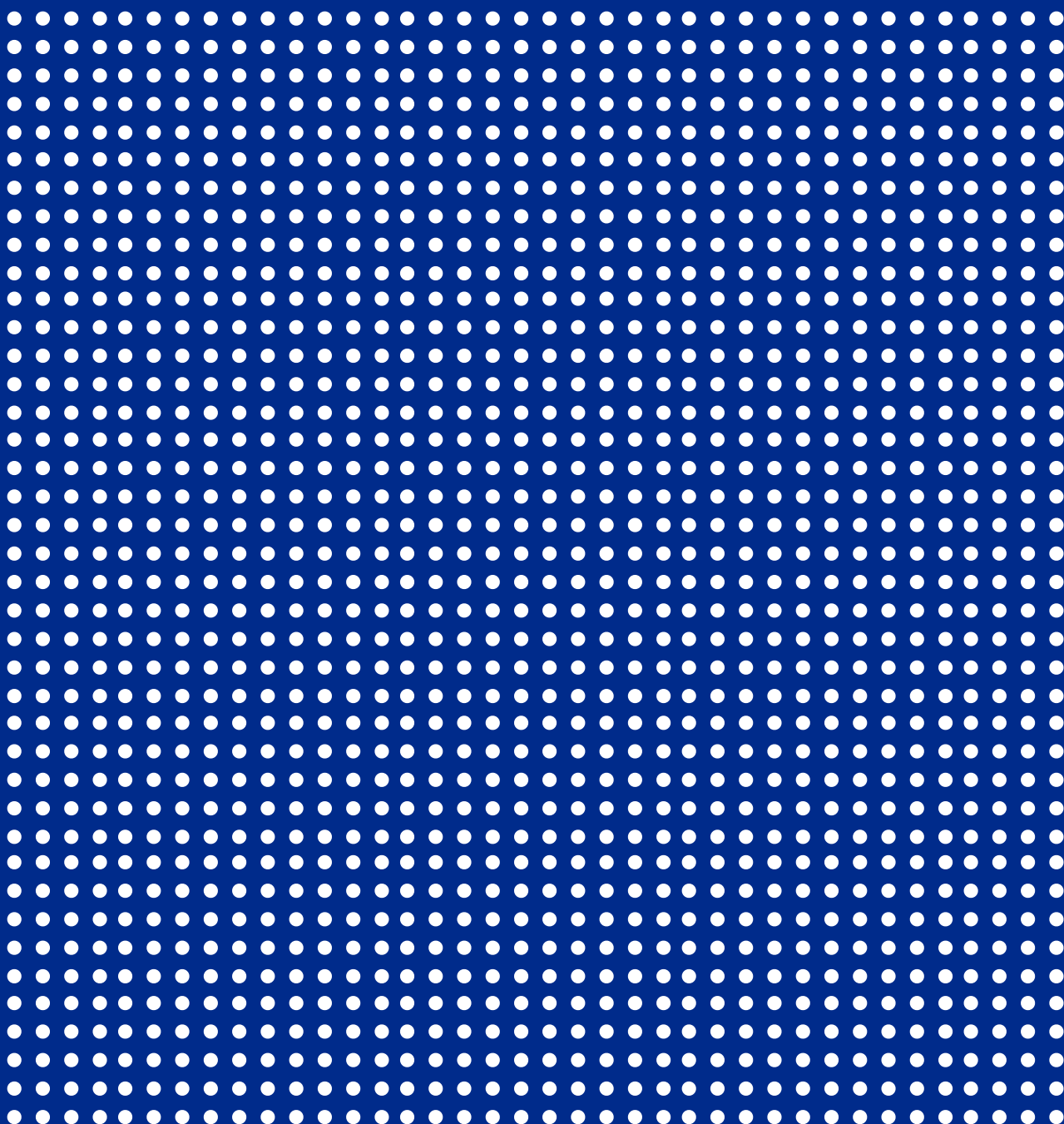


# REPORT



## Money Laundering / Terrorist Financing National Risk Assessment of Virtual Assets and Virtual Asset Service Providers in the Republic of Moldova

December, 2024  
Chisinau

## ***Disclaimer***

*The 2024 Money Laundering (ML) and Terrorism Financing (TF) Risk Assessment of Virtual Assets (VAs) and Virtual Asset Service Providers (VASPs) in the Republic of Moldova was conducted as a self-assessment by Moldovan authorities, with support of the Office of the Co-ordinator of OSCE Economic and Environmental Activities (OCEEA). The assessment utilized the National Risk Assessment Tool for Virtual Assets and Virtual Asset Service Providers developed by the World Bank Group.*

*All data, statistics, and information used in the completion of the VA/VASP ML/TF risk assessment, as well as the resulting analysis, interpretations, conclusions, and outcomes, wholly belong to the Moldovan authorities and do not reflect the views of the World Bank Group or OCEEA.*

# Table of Contents

List of Tables .....	5
List of Figures.....	6
Acronyms.....	7
Executive Summary.....	8
1. Introduction .....	9
1.1. Context of the Republic of Moldova and Scope of the Assessment.....	9
1.2. Objectives .....	10
1.3. The Current State .....	10
1.4. Regulatory Developments and Limitations .....	11
2. Risk Assessment Methodology .....	12
2.1. The Overall NRA Process.....	12
2.2. Risk Assessment Working Group .....	13
2.3. The World Bank VA/VASP ML/TF Risk Assessment Tool.....	13
2.3.1. Identifying Relevant VASP Channels.....	13
2.3.2. Assessing Threats, Vulnerabilities, and Mitigation Measures .....	17
2.4. Data Collection and Analysis.....	19
3. Overview of Global VA and VASP Ecosystems.....	19
3.1. Evolution of VAs/VASPs Ecosystems and ML/TF Risks.....	20
3.2. VA/VASP Global Regulatory Developments.....	23
3.3. Cryptocurrency Activity in Moldova: An Overview from Chainalysis.....	25
3.4. ML/TF Risks Associated with the VAs and VASPs.....	30
4. Survey Responses.....	33
4.1. Law Enforcement Agencies (LEAs) and Intelligence Services' Responses to the VAs/VASPs Survey .....	33
4.2. Regulators Responses to the VA&VASP Questionnaire Survey .....	40
4.3. Private Sector Responses to the VA&VASPs Surveys .....	43
4.3.1. Banking Sector .....	43
4.3.2. Non-bank Payment Service Providers (PSPs).....	47
5. VA/VASP Interaction with Traditional Obligated Entities and Informal Economy in Moldova.....	49
5.1. Formal Sector (TOE) .....	50
5.1.1. Banking Sector .....	50
5.1.2. PSPs.....	52
5.2. Informal Sector: The Underground Economy in Moldova.....	54
5.2.1. Telegram as a Key Hub for Informal VAs Transactions and Activities .....	54
5.2.2. P2P Crypto Trading Platforms.....	57
5.2.3. Exchange Couriers (USDT-FIAT).....	58

5.2.4.	Transnistria Region (Mining Activity) .....	58
6.	Case Studies, Typologies & Emerging Trends.....	59
6.1.	Case Studies & Typologies .....	59
Case 1 -	“Onecoin” Ponzi Scheme (2016).....	59
Case 2 -	Laundering Drug Trafficking Proceeds (2018) .....	59
Case 3 -	“Maxi Capital” Scam (2023) .....	60
Case 4 -	Fake Crypto Trading Platform (2023) .....	60
Case 5 -	Fake Stock Brokers (2023) .....	60
Case 6 -	False Promises of Investment: Scammers Target and Defraud a 68-Year-Old Woman (2023) .....	60
Case 7 -	“Deep Fake” Investment Scam (2024) .....	61
Case 8 -	Illegal Migration Scheme Paid in Cryptocurrencies (2024).....	61
6.2.	Emerging Trends.....	62
Election Interference & Cryptocurrency .....		62
7.	The Risk Assessment.....	64
7.1.	ML/TF Threat Assessment.....	64
7.1.1.	VA Nature and Profile .....	65
7.1.2.	Accessibility to Criminal.....	67
7.1.3.	Source of Funding VA .....	69
7.1.4.	Operational Features of VA .....	70
7.1.5.	Ease of Criminality.....	72
7.1.6.	Economic Impact.....	74
7.2.	ML/TF Inherent Vulnerability Assessment .....	75
7.3.	Mitigation Measures (Low) .....	79
7.4.	Overall ML/TF Risk .....	80
8.	Conclusions .....	80
8.1.	Key Findings.....	80
8.2.	Recommendations.....	82
8.3.	Challenges and Limitations .....	83
9.	Annex .....	84
9.1.	Glossary .....	84
9.2.	Timeline of key events and developments in the VA/VASP Ecosystem and Moldova's specific actions .....	85
9.3.	List of CASPs regulatory authorities in the EU .....	86

## List of Tables

Table 1: The 27 VASP Channels.....	14
Table 2: Definition of the VASPs and Types of Services (according to WB Toolkit).....	14
Table 3: Input Variables for ML/TF Vulnerability Assessment.....	18
Table 4: Mitigation Measures Input Variables.....	18
Table 5: VA/VASP Questionnaire Survey Respondents .....	19
Table 6: Eastern Neighbourhood countries' per capita received, sent and total darknet market revenue engagement (in euros), period: April 2019 - June 2021 .....	22
Table 7: Top Services Related to Cryptocurrency Accessed from Moldova (2024-06).....	28
Table 8: Number of STRs/SARs associated with VA/VASPs reported (2021 – 2024) .....	35
Table 9: No. of cases associated with VA and VASPs by predicate offence, by year (2021 – 2023) .....	37
Table 10: Value of sized VAs by LEAs (2021-2024) .....	39
Table 11: Estimated number of transactions via bank accounts to/from foreign VASPs, for the period 2021 – 2024 .....	45
Table 12: Total number of transactions conducted through special accounts in relation to foreign VASPs (April – August 2024).....	47
Table 13: Estimated number of transactions via PSP accounts to/from foreign VASPs, ....	48
Table 14: Sector interaction with the VASP Channels .....	49
Table 15: Interaction of the PSP Sector and the VAs/VASPs .....	53
Table 16: ML/TF Threat Ratings by Input Variables .....	64
Table 17: Assessed VASP Channels .....	65
Table 18: ML/TF Threat Ratings by VASP Channels .....	75
Table 19: Overall Vulnerability Exposure Summary .....	76
Table 20: Description of the Vulnerability Input Variables according to WB Methodology: .....	77
Table 21: ML/TF Inherent Vulnerability Ratings by VASP Channels .....	79
Table 22: VA/VASP ML/TF threat, inherent vulnerability and residual risk ratings across all VASP channels.....	80
Table 23: Timeline of key events and developments in the VA/VASP Ecosystem and Moldova's Specific Actions .....	86
Table 24: List of CASPs licensing authorities in the EU .....	87

## List of Figures

Figure 1: Input Variables for ML/TF Threat Assessment.....	17
Figure 2: Growth of VAs ecosystem.....	20
Figure 3: Global Crypto Market Capitalization (2014 - 2024) .....	21
Figure 4: Total flows to a selection of Eastern European countries (2023-06 to 2024-06) 25	
Figure 5: Total illicit value received in selected Eastern European countries (2023-06 to 2024-06).....	26
Figure 6: Moldova Illicit Flows by Category (2023-06 to 2024-06) .....	26
Figure 7: Moldova Deposit Frequency Between 2021-06 and 2024-06 .....	27
Figure 8: Moldova Deposit Frequency to Infrastructure as a Service (2021-06 and 2024-06) .....	29
Figure 9: Eastern European DeFi growth by country and category (2022 – 2024) .....	30
Figure 10: Level of Familiarity of LEAs and Intelligence Services with VAs/VASPs .....	33
Figure 11: Number of voluntary income declarations from VAs (2021 – 2023) .....	37
Figure 12: Total declared income from VA (2021 - 2023) .....	37
Figure 13: Total Predicate Offences Associated with VA and VASP (2021-2023), in Percentage.....	38
Figure 14: No. of Predicate Offences Associated with VA and VASPs (2021-2023), by Year .....	38
Figure 15: Total Value of Seized Cryptocurrency Assets by LEAs (2021-2024).....	39
Figure 16: LEAs Perceived Risk for ML/TF associated with VAs/VASPs (%).....	40
Figure 17: Banks perception of ML/TF risks associated to VAs/VASPs (%) .....	44
Figure 18: Estimated number of transactions/amounts via bank accounts to/from foreign VASPs, for the period 2021 – 2024 .....	45
Figure 19: Top Frequently Observed VASPs in Transactions Conducted via Bank Accounts (2021 -2024) .....	46
Figure 20: Estimated number of transactions/amounts via PSPs accounts to/from foreign VASPs, for the period 2021 – 2024 .....	47
Figure 21: Top Frequently Observed VASPs in Transactions Conducted via PSPs Accounts (2021 -2024) .....	48
Figure 22: Crypto Escrow Service on Telegram .....	55
Figure 23: Crypto Exchange Chat on Telegram .....	55
Figure 24: Crypto “Magazin” – Goods for Sale.....	56
Figure 25: Binance App Screenshot - P2P Trading .....	57
Figure 26: Binance P2P Trading Operations .....	58
Figure 27: VA Nature and Profile – Summary of different risk elements .....	65
Figure 28: Accessibility to Criminal – Summary of risk elements .....	67
Figure 29: Total Per Capita Sent/Received in Dark Web Market.....	69
Figure 30: Source of Funding – Summary of risk elements.....	69
Figure 31: Operational Features of VA – Summary of risk elements.....	70
Figure 32: Ease of Criminality – Tax Evasion .....	72
Figure 33: Economic Impact – Summary of risk elements .....	74

## Acronyms

AML	Anti-Money Laundering
CASP/CAPSs	Crypto-Asset Service Provider
CFT	Counter Financing of Terrorism
CNPF	National Commission for Financial Markets
DeFi	Decentralized Finance
DEX	Decentralized Exchange
DLT	Distributed Ledger Technology
DNM	Darknet Marketplace
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
KYC	Know Your Customer
LEA/LEAs	Law Enforcement Agencies
MiCA	EU Markets in Crypto-Assets Regulation
ML	Money Laundering
MONEYVAL	Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism
NBM	National Bank of Moldova
NFT	Non-Fungible Token
NRA	National Risk Assessment
P2P	Peer-to-Peer
PSP	Non-Bank Payment Service Provider
R	FATF Recommendation
SAR	Suspicious Activity Report
STR	Suspicious Transaction Report
TF	Terrorists Financing
TOE	Traditional Obligated Entities
VA/VAs	Virtual Assets
VASP	Virtual Assets Service Providers
WG	Working Group

## Executive Summary

This National Risk Assessment (NRA) provides an in-depth analysis of the emerging money laundering (ML) and terrorist financing (TF) risks associated with virtual assets (VAs) and virtual asset service providers (VASPs) in the Republic of Moldova. With the rapid growth of digital finance globally, Moldova's VA landscape has become increasingly vulnerable to exploitation by criminal groups. This report draws from international standards, FATF recommendations, and local data to assess these risks and proposes regulatory and operational measures to address the challenges identified.

Guided by the FATF Recommendation 15—which mandates that countries identify, assess, and comprehend the ML/TF risks arising from VA activities and VASPs – this report was prepared as a self-assessment by Moldovan authorities with support from the OCEEA, using the World Bank's (WB) NRA tool designed for VAs/VASPs.

The assessment team employed the World Bank's methodology to identify threats and vulnerabilities, evaluate inherent risks, and existing mitigating measures, thereby assessing the residual risks related to VAs/VASPs. Using this approach, the team determined activities requiring evaluation, focusing on six (6) VASP channels related to VA wallet providers, exchanges, and investment providers which were found to interact directly or/and indirectly with Moldova's formal and informal sectors.

Key findings show that Moldova is particularly vulnerable due to its lack of a comprehensive regulatory framework, limited institutional capacity to monitor VA transactions, identify natural or legal persons engaging in illegal VASP activities, and enforce appropriate sanctions. Additionally, Moldova's geographical proximity to conflict zones increases its exposure to ML/TF threats involving VAs.

The findings also identify substantial challenges in addressing risks related to VAs/VASPs. Existing mechanisms to mitigate these risks reveal notable inefficiencies, largely resulting from the country's restrictive legislation and a lack of essential tools for effectively managing identified vulnerabilities. Although there is a general prohibition on VA-related services, this measure is not sufficiently comprehensive and fails to cover the full spectrum of VA-related risks.

Based on the assessment of each input variable provided in the WB NRA tools kit across all the relevant channels, the overall ML/TF residual risk associated to VA/VASP is rated as “**High**” after considering mitigating measures at the time of assessment.

In *Section 8.2*, the WG outlined a list of recommended measures to be taken by the Moldovan authorities to mitigate ML/TF risks related to VAs/VASPs. These recommendations include: strengthening regulatory framework in alignment with EU Directives and FATF standards, focusing on licensing, registration, and the oversight of VASPs; improve international collaboration; and enhance the capacities of LEAs and regulatory authorities by equipping them with the necessary knowledge and experience related to VA activities.

# 1. Introduction

The increasing use of digital currencies, particularly VAs, has reshaped the global financial landscape. These digital representations of value, utilizing decentralized ledger technologies such as blockchain, have generated significant interest due to their ability to enable seamless transactions without the need for traditional financial intermediaries. Among the most well-known of these assets is Bitcoin, which garnered worldwide attention during its unprecedented surge in value at the end of 2017. This rapid rise in Bitcoin's price, alongside other digital currencies, sparked public and media interest and highlighted the potential of VAs to bypass traditional banking systems through their pseudo-anonymous and decentralized nature. While this innovation offers advantages like greater transaction speed and lower costs, it also presents new risks, particularly in the areas of ML/TF.

The lack of regulatory oversight and the anonymity inherent in VA transactions pose significant challenges for authorities in managing ML/TF risks. Recognizing these threats, international bodies such as the FATF have taken steps to address the vulnerabilities associated with VAs. In October 2018, FATF updated its Recommendations to encompass financial activities involving VAs explicitly. This update included new glossary definitions for "virtual asset" and "virtual asset service provider" and an amendment to Recommendation 15. This amended Recommendation mandates the regulation of VASPs for anti-money laundering and counter-financing of terrorism (AML/CFT) purposes. It requires the licensing or registration of VASPs and their adherence to effective systems for AML/CFT supervision or monitoring.

## 1.1. Context of the Republic of Moldova and Scope of the Assessment

For the Republic of Moldova, these international developments have underscored the need to establish a robust framework for assessing and mitigating ML/TF risks associated with VAs/VASPs. According to the Second MONEYVAL Enhanced Follow-up Report, a critical shortcoming in Moldova's compliance with FATF's Recommendation 15 (R.15) is the absence of a comprehensive assessment of the ML/TF risks emerging from VA and VASP activities.<sup>1</sup> This gap in risk assessment could potentially expose the country's financial system to exploitation by illicit actors, undermining efforts to strengthen both national and regional security.

Moldova, like many countries, is at a crossroads in regulating this new and evolving sector. While VAs have potential economic benefits, their misuse for illicit purposes poses significant risks to national security and financial integrity.

To address this issue, the present NRA Report aims to identify and evaluate the specific ML/TF risks posed by the activities of VAs and VASPs within Moldova. This assessment is crucial for understanding the extent of these risks and for implementing effective regulatory and supervisory measures that align with FATF standards. By doing so, Moldova can enhance its resilience against financial crimes and ensure a secure environment for the legitimate use of digital financial services. Furthermore, this NRA will serve as a foundational tool for policymakers and regulatory bodies in developing a tailored approach

---

<sup>1</sup> <https://rm.coe.int/moneyval-2024-4-md-5thround-2ndenhfur/1680b05e46>

to the oversight of VAs and VASPs, fostering a balanced regulatory environment that supports innovation while mitigating risks.

In a rapidly evolving digital financial landscape, this assessment comes at a critical juncture. It reflects Moldova's commitment to aligning with global best practices in AML/CFT, addressing existing vulnerabilities, and building a comprehensive understanding of the risks associated with virtual assets. This proactive approach not only aims to safeguard the integrity of Moldova's financial system but also positions the country as a responsible actor in the global fight against financial crime. As the use of VAs expands, a thorough and forward-looking assessment of their risks is essential for ensuring that Moldova remains well-prepared to address both current and emerging challenges in this field.

## 1.2. Objectives

The NRA on ML/TF risks associated to VAs/VASPs in the Republic of Moldova aims to achieve several key objectives. These objectives are designed to improve the understanding, regulation, and mitigation of ML/TF risks, while promoting a secure and transparent environment for digital financial activities in Moldova. The primary objectives of this assessment include:

- i. **Identifying, assessing and understanding the specific ML/TF risks arising from VA and VASP activities:** This objective is aligned with the FATF's R.15, which requires jurisdictions to develop a clear understanding of the risks associated with virtual asset activities and take appropriate measures to address them.
- ii. **Strengthen the Regulatory Framework:** To support the development and implementation of relevant legislation that incorporates a risk-based approach to prevent ML/TF risks. This approach ensures that preventive measures are commensurate with the level of risks identified, thereby strengthening Moldova's AML/CFT framework in the VA and VASP sector.
- iii. **Mitigate Identified Risks:** To ensure that the ML/TF risks associated with VAs and VASPs are mitigated effectively or contained within an acceptable tolerance threshold. This includes implementing supervision and monitoring mechanisms that help maintain the integrity of Moldova's financial system, strengthening both national and regional security.
- iv. **Resource Allocation and Decision-Making:** To enable effective prioritization and allocation of resources, this assessment is designed to guide actions at both national and sectoral levels to address identified risks, supporting informed decisions on regulatory and supervisory priorities within the VA and VASP sectors.

By achieving these objectives, the NRA seeks to create a comprehensive and adaptive approach to managing ML/TF risks in the digital financial sector, ultimately contributing to Moldova's long-term financial stability and compliance with international standards. This effort is essential for safeguarding the integrity of Moldova's financial system while enabling the country to harness the legitimate benefits of virtual assets in a secure and regulated manner.

## 1.3. The Current State

The regulatory and legal landscape for VAs and VASPs in the Republic of Moldova is in a state of early development. Moldova, like many nations, has not yet established a comprehensive legal framework specifically tailored to regulate the VA/VASPs sector. The

current legislative environment relies primarily on the general provisions of existing AML/CFT legal framework (*Law No. 308/2017 on prevention and combating money laundering and terrorism financing*<sup>2</sup>), which have been updated to address the increasing interest in VAs. While domestic VASP activities and related transactions involving VAs and fiat currencies remain restricted, access to VAs and VASPs is still available through foreign entities, leaving the financial sector vulnerable to ML/TF risks.

The lack of specific regulation in Moldova for VAs and VASPs prompted policymakers to adopt a high-level strategy aimed at minimising the potential misuse of VAs for circumventing international financial sanctions. This policy approach was especially pertinent following heightened risks of sanctions evasion in response to geopolitical shifts, such as the conflict in Ukraine.

Currently, Moldova's regulatory landscape remains restricted, primarily focusing on prohibiting domestic VASP activities and limiting interactions with authorized foreign VASPs<sup>3</sup> under stringent conditions.

#### 1.4. Regulatory Developments and Limitations

Moldova's initial response to VAs emerged as early as 2017 when the National Bank of Moldova (NBM) issued its first warning notice<sup>4</sup> advising entities and natural persons to avoid involvement in virtual currency transactions, highlighting potential exposure to ML/TF risks. In 2018, three additional follow-up notices and clarifications<sup>5</sup> were issued, reiterating the risks associated with VAs and advising citizens to proceed with caution in any VA-related activities.

In October 2021, amendments to Law No. 133 of June 17, 2016, *on the declaration of assets and personal interests* entered into force, expanding the obligations of individuals subject to declaration. Under these amendments, those **subject to declaration are required to report virtual assets, including virtual currencies**, if their value exceeds 10 average monthly salaries in the economy.

Prior to the adoption of the 2023 amendments to the AML/CFT Law, the National Bank issued another circular on October 28, 2022, instructing banks and PSPs to cease any facilitating/intermediating payments from/to their accounts for crypto platforms involved in buying/selling virtual currencies and to cease collaboration with companies engaged in exchanging virtual currencies for fiat currency. The National Bank cited, among other reasons, the obligations outlined in AML/CFT Law No. 308/2017, which require reporting entities to apply due diligence measures based on identified risks.

In response to growing concerns about the misuse of VAs, amendments to the AML/CFT Law No. 308/2017 were enacted on July 1, 2023. These amendments, marked Moldova's

---

<sup>2</sup> State register of legal acts, website: [https://www.legis.md/cautare/getResults?doc\\_id=136906&lang=ro#](https://www.legis.md/cautare/getResults?doc_id=136906&lang=ro#) [last access: 29 October, 2024].

<sup>3</sup> Authorized foreign VASPs that are licensed or registered in other jurisdictions and supervised by foreign regulators.

<sup>4</sup> Bank of Moldova, website: <https://www.bnm.md/ro/content/moneda-virtuala-si-riscuri-asociate>, [last access: 1<sup>st</sup> November, 2024].

<sup>5</sup> Bank of Moldova, website: <https://www.bnm.md/ro/content/bnm-avertizeaza-ca-investitiile-criptovalute-implica-riscuri-inalte> [last access 1<sup>st</sup> November, 2024].

<https://www.bnm.md/ro/content/banca-nationala-atentioneaza-mod-repetat-asupra-riscurilor-de-investi-criptovalute> [last access 1<sup>st</sup> November, 2024].

<https://www.bnm.md/ro/content/clarificarea-pozitiei-de-reglementare-si-autorizare-monedei-virtuale> [last access 1<sup>st</sup> November, 2024].

first attempt to recognize virtual assets and introduce the concept of VASPs within its legislative lexicon. While these changes brought Moldova closer to international standards, the regulatory scope remains limited, primarily due to the lack of specific licensing requirements or a dedicated VASP oversight regime. The law prohibited the activity of providing VA services on the territory of Republic of Moldova. The enforcement and monitoring mechanisms for prohibition are not defined, which hinders its effectiveness and risk mitigation. However, reporting entities (REs) are allowed to facilitate transactions for resident clients with foreign-licensed VASPs, under strict operational conditions and limitations related to clients, accounts and other enhanced measures when facilitating such transactions.

In fact, according to Article 5 (4<sup>1-4</sup>), of the AML/CFT Law No. 308/2017, the REs are required:

- not to open or maintain accounts for non-resident clients to transact with foreign VASPs;
- not to open or maintain accounts for foreign VASPs or to open or maintain accounts at foreign VASPs;
- prohibiting the conduct of occasional transactions for/at foreign VASPs;
- limit activity of local residents only with authorized foreign VASPs and up to a monthly threshold of approximately EUR 2,600 (50,000 MDL).

When providing such services REs are required to apply enhanced due diligence including opening special accounts and the implementation of information technology (IT) solutions for traceability of transactions (Art. 8 (5<sup>1</sup>) – AML/CFT Law No. 308/2017).

Furthermore, in addition to the prohibitions outlined in Article 5, paragraphs (4<sup>1</sup>) – (4<sup>4</sup>) of AML/CFT Law 308/2017, the Article 4, paragraph (11) of the same Law specifies that **conducting activities in breach of these prohibitions is punishable under Article 263, paragraph (9) of the Contravention Code or Article 241, paragraph (1), letter b) of the Criminal Code.**

## 2. Risk Assessment Methodology

### 2.1. The Overall NRA Process

The methodology for this risk assessment is a simplified version of the World Bank's National Risk Assessment Tool that was adopted to the situation and needs of the Republic of Moldova. It is supplemented by open-source data, investigative reports, input from relevant national stakeholders, and expert judgement. The assessment focuses on identifying potential ML/TF threats, and vulnerabilities, related to VAs and VASPs, as well as the effectiveness of existing mitigation measures in Moldova.

The NRA was conducted using both qualitative and quantitative methods:

- **Questionnaire distribution:** Surveys were sent to key stakeholders, including law enforcement agencies, financial sector regulators, and private sector participants (banks and PSPs), as well as foreign FIUs, requesting assistance to reach out to foreign VASPs.
- **Open-source research:** Data was gathered from international reports, news outlets, and online platforms monitoring cryptocurrency trends in the region.

- **Workshops:** Consultation sessions were held with international experts and local institutions to analyse the evolving risks in the virtual asset space.

In assessing risks, the assessment team relied on identifying threats and vulnerabilities for both VA/VASPs, based on analysis of information collected from several sources previously referred to, in addition to the equations included in the assessment tool prepared by the World Bank. This assessment considers the input variables, which represent a set of characteristics and attributes through which threats and vulnerabilities in the activities of VAs and VASPs can be identified primarily from a local perspective, as well as on an international perspective, through the characteristics inherent in VAs that make it global, borderless, and without any restrictions.

## 2.2. Risk Assessment Working Group

To ensure a comprehensive and coordinated approach, Moldova established a Risk Assessment Working Group composed of all relevant competent authorities. **The NRA was led by the Financial Intelligence Unit of the Republic of Moldova (FIU Moldova)**, supported by a working group comprised of representatives from key Law Enforcement Agencies (LEAs) and Regulatory Bodies, including:

- Prosecutor General's Office
- National Investigation Inspectorate
- Border Police
- National Anticorruption Office (Asset Recovery Office)
- Customs Service
- State Tax Service
- Security and Intelligence Service
- National Integrity Authority
- National Bank of Moldova
- National Commission for Financial Markets

Valuable insights were also gathered from the private sector, offering essential data, trends, and perspectives to support the analysis and the formulation of recommendations for this risk assessment.

## 2.3. The World Bank VA/VASP ML/TF Risk Assessment Tool

The risk assessment tool, based on the World Bank's methodology, is designed to assess ML/TF risks within a country's VA/VASP ecosystem. The tool categorizes VASPs into seven (7) types, outlines twelve (12) distinct VASP services, and identifies twenty-seven (27) specific activities or channels (*refer to Table 1*). Each of these categories is evaluated using tailored assessment criteria, allowing for detailed risk profiling at the product, service, and activity levels.

### 2.3.1. Identifying Relevant VASP Channels

The initial step for the WG was to identify relevant VASP channels through which Moldova's Traditional Obligated Entities (TOE) and the informal sector – have the potential to interact with VASPs. This structured framework helps to clarify sector-specific interactions and exposures, providing a comprehensive basis for understanding the ML/TF risks associated with VA/VASPs in Moldova.

Table 1: The 27 VASP Channels

VASPs	Types of Services	Sub-type (Channel)
VIRTUAL ASSET WALLET PROVIDERS	Custodial Services	1. Hot Wallet
	Non-Custodial Services	2. Cold Wallet
VIRTUAL ASSET EXCHANGES	Transfer Services	3. P2P
		4. P2B
	Conversion Services	5. Fiat-to-Virtual 6. Virtual-to-Fiat 7. Virtual-to-Virtual
VIRTUAL ASSET BROKING / PAYMENT PROCESSING	Payment Gateway	8. ATMs
		9. Merchants
		10. Cards
VIRTUAL ASSET MANAGEMENT PROVIDERS	11. Fund Management	
	12. Fund Distribution	
	13. Compliance, Audit & Risk Management	
INITIAL COIN OFFERING (ICO) PROVIDERS	Fund Raising	14. Fiat-to-Virtual 15. Virtual-to-Virtual
	Investment	16. Development of Product & Services
	Other Offerings	17. Security Token Offerings (STOs) 18. Initial Exchange Offerings (IEOs)
VIRTUAL ASSET INVESTMENT PROVIDERS	Trading Platforms	19. Platform Operators
		20. Custody of Assets
		21. Investment into VA related commercial activities
		22. Non-Security Tokens & Hybrid Trading Activities
	Emerging Products	23. Stablecoins 24. Crypto Escrow service 25. Crypto-custodian Services
VALIDATORS / MINERS/ ADMINISTRATORS	Proof of work	26. Fees
		27. New Assets

Source: World Bank Methodology

Table 2: Definition of the VASPs and Types of Services (according to WB Toolkit)

NO	TERMS	DESCRIPTION
1	VIRTUAL ASSET WALLET PROVIDERS	<b>Providing storage for virtual assets or fiat currency on behalf of others and then facilitating exchanges or transfers between one or more virtual assets, or between virtual assets and fiat currency.</b>
1.1	CUSTODIAL WALLET	A custodial business offers to protect virtual assets within their system. The platform providing custodial cryptocurrency services can also include most exchanges and brokerage services allowing buying, selling, and storage of virtual assets in the product called 'Wallet'.  A custodial wallet is a wallet in which the private keys, of the subject holding the virtual asset, are stored by a third party. This arrangement does not provide full control of virtual asset to its owner rather the funds are held by the custodian providing the Virtual Asset Wallet Service. Coinbase is a great example of an exchange and brokerage service that also allows people to store virtual assets within their wallet system.

1.2	NON-CUSTODIAL WALLET	A non-custodial wallet is a wallet in which the private keys are held by the virtual asset owner, who have complete control over the its virtual assets. Non-custodial wallets include the Bitcoin.com client, BRD, Blockchain, BTC.com, Electron Cash, Copay, Jaxx, Coinomi, Edge, and many more because these platforms give users the ability to store their own private keys.
2	VIRTUAL ASSET EXCHANGES	<b>Providing a digital online platform facilitating virtual asset transfers and exchanges. Exchanges may occur between one or more forms of virtual assets, or between virtual assets and fiat currency. Issuing own virtual assets in order to facilitate virtual asset transfers and exchanges.</b>
2.1	PEER-TO-PEER	Transfer of virtual assets by one user to another.
2.2	FIAT-TO-VIRTUAL	Conversion of Government issued fiat currency to Virtual Assets
2.3	VIRTUAL-TO-FIAT	Conversion Virtual Assets to Government issued fiat currencies
2.4	VIRTUAL-TO-VIRTUAL	Conversion of one type of Virtual Assets to another
3	VIRTUAL ASSET BROKING / PAYMENT PROCESSING	<b>Arranging transactions involving virtual assets, or involving virtual assets and fiat currency.</b>
3.1	ATMS	An ATM (Automated Teller Machine) dealing with virtual currencies is a kiosk that allows a person to purchase virtual currencies by using cash or debit card. Some virtual currency ATMs offer bi-directional functionality enabling both the purchase of virtual assets as well as the sale of virtual assets for cash.
3.2	MERCHANTS	Acceptance of Virtual Assets by Merchants in exchange of Fiat Currencies for settlement
3.3	CARDS	Use of Stored Value Virtual Assets cards for Purchases online
4	VIRTUAL ASSET MANAGEMENT PROVIDERS	
4.1	FUND MANAGEMENT	Fund managers investing in virtual assets
4.2	FUND DISTRIBUTION	Firms which distribute funds that invest (wholly or partially) in virtual assets
4.3	COMPLIANCE, AUDIT & RISK MANAGEMENT	Support over guidance on risk management, management of liquid capital, segregation of assets, custodianship, funds structure, and other legal aspects.
5	INITIAL COIN OFFERING (ICO) PROVIDERS	<b>Issuing and selling virtual assets to the public. May involve participating in and providing financial services relating to the ICO.</b>
5.1	FIAT-TO-VIRTUAL	Fund raising for ICOs that attracts fiat currencies investments converted into Virtual assets
5.2	VIRTUAL	Fund raising for ICOs that attracts virtual assets investments
5.3	DEVELOPMENT OF PRODUCT & SERVICES	Raised funds used as an investment to develop product & services
5.4	INITIAL EXCHANGE OFFERING (IEOs)	Initial Exchange Offerings (IEOs): IEO is hosted by the project team alongside a cryptocurrency exchange.
5.5	SECURITY TOKEN OFFERINGS (STOs)	Security Token Offerings (STOs): STO offer equity in the form of tokens
6	VIRTUAL ASSET INVESTMENT PROVIDERS	<b>Providing an investment vehicle enabling investment in/ purchase of virtual assets (i.e. via a managed investment scheme or a derivatives issuer providing virtual asset options, or via a private equity vehicle that invests in virtual assets).</b>
6.1	PLATFORM OPERATORS	Online Platforms that facilitate active trading (future contracts) in virtual assets, inherently have a broad customer base, substantial local presence and considered to be have a sound corporate governance structure. Unlike automated trading venues or equities and futures exchanges where investors trade through licensed intermediaries, virtual asset trading platforms interface directly with the public. <b>1. Regulated Environment:</b> Investors have clarity over the standards and controls that must be complied with by Platforms that are licensed and have a clear basis for distinguishing between licensed and unlicensed Platforms. Products that are to be included in a Platform are licensed by regulatory body and need to comply with the specified requirements of the Regulatory Framework.

		<p><b>2. Unregulated Environment:</b> Unregulated trading platforms have inherent regulatory concerns related to the safe custody of assets, know-your-client requirements, anti-money laundering and counter-financing of terrorism, market manipulation, accounting and auditing, risk management, conflicts of interest and the acceptance of virtual assets for trading.</p>
6.2	CUSTODY OF ASSETS	<p>Virtual asset trading platforms can hold virtual assets on behalf of their clients and also act as marketplaces matching buyers and sellers.</p> <p><b>1. Regulated Environment:</b> A regulated entity is likely to find it easier to establish banking ties to facilitate a conversion between cryptocurrency and fiat money. In addition, the entity is expected to fulfil know-your-client requirements, anti-money-laundering, counter-financing of terrorism and also support source of funds and wealth of clients holding the assets. Virtual Asset Trading Platform operating in a regulatory environment also expected to offer client protection which is equivalent to traditional financial institutions in the securities sector.</p> <p><b>2. Unregulated Environment:</b> Unregulated environment offers limited or no protection on investments, and practice anonymity without fulfilment of know-your-client requirements, anti-money-laundering and counter-financing of terrorism requirements</p>
6.3	INVESTMENT INTO VA-RELATED COMMERCIAL ACTIVITIES	Virtual asset-related commodities (such as mining devices)
6.4	NON-SECURITY TOKENS & HYBRID TRADING ACTIVITIES	A tokenized security can also provide its holder with rights to a non-security token—either a so-called “utility token,” which allows a holder to consume or redeem the token for a good or service in a functioning system, or a cryptocurrency token, which exists solely as a medium of exchange, store of value, or unit of account, like bitcoin
6.5	STABLECOINS	Stablecoins typically claim to have a mechanism which seeks to stabilise their value by backing them with fiat currencies, commodities or a basket of cryptocurrencies. These virtual assets have given rise to significant regulatory concerns among global central bankers and financial regulators, particularly where they are intended to be adopted on a global scale.
6.6	CRYPTO ESCROW SERVICE	In a Crypto escrow service, virtual assets are held by a third party until all of the parties involved in a transaction can complete the transaction and signal that they are satisfied with the transaction. Escrow is usually done because of trust issues where the seller may want to be sure that the money will be sent by the buyer after the buyer has received the goods and services. Escrow ensures that the buyer will receive the item they purchased in the order, time and conditions specified. Crypto Escrow services are important especially for online transactions where parties need to remain anonymous to each other; parties may not be in geographical contact and there may be reasonable factors preventing transactions from being completed. Parties may come to disagreements during or after the delivery of services; there may be situations where transacting is itself not governed by law due to location-related issues or issues related to legal jurisdictions and other similar problems.
6.7	CRYPTO-CUSTODIAN SERVICES	Cryptocurrency custodian services provide independent storage and security systems used to hold large quantities of tokens/Virtual assets. Custody solutions are one of the emerging services of the cryptocurrency ecosystem supporting the entry of institutional capital into the Virtual assets industry.
7	VALIDATORS / MINERS	<b>Mining hardware providers (e.g., Butterflylabs) Cloud-based mining companies (e.g., Genesis Mining)</b>

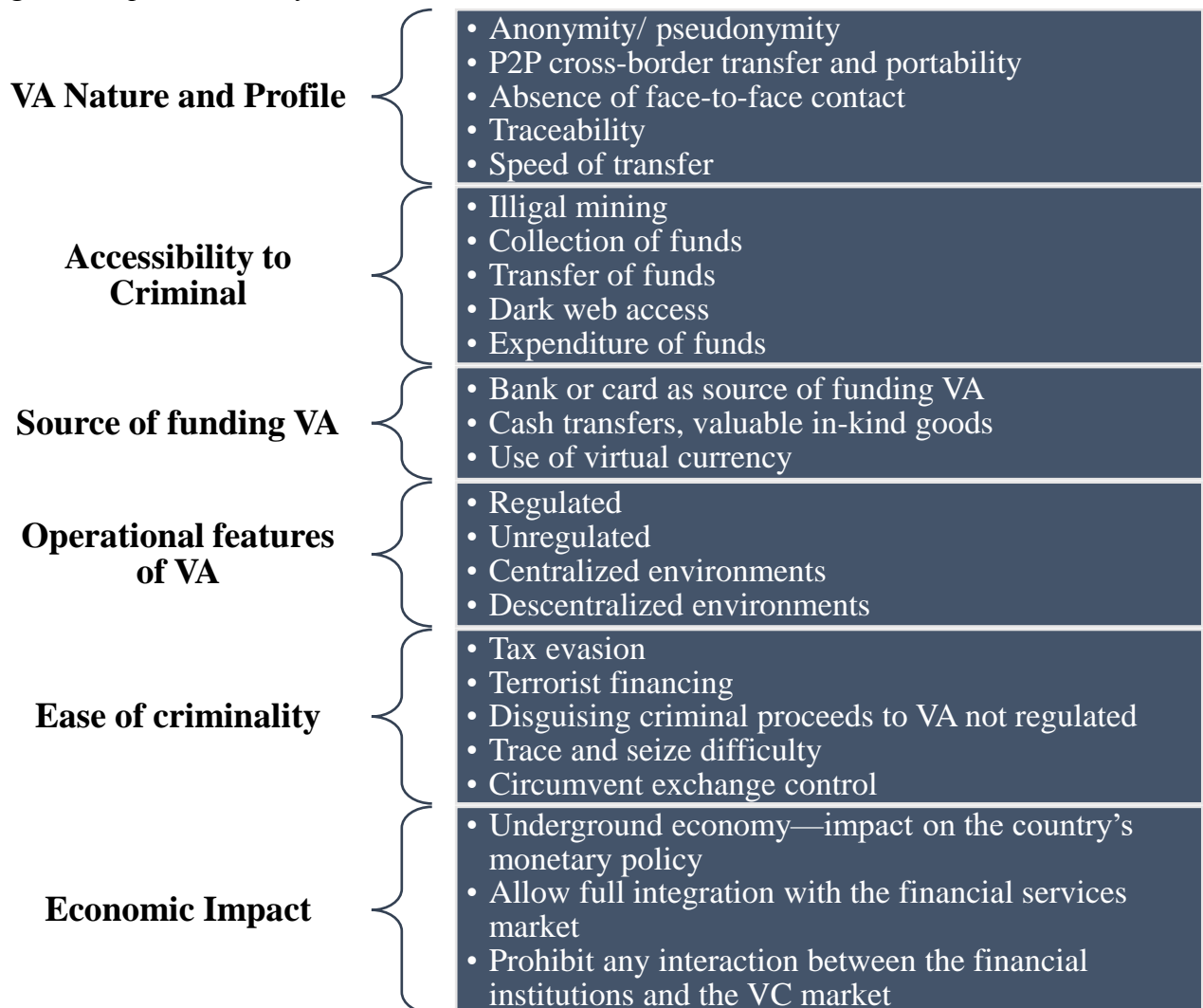
7.1	Fees	Institutional units that validate and confirm the transactions are called Miners. Miners as considered as book keepers / distributed ledger updaters in a Virtual currency transaction. A transaction can only be considered secure and complete once it is included in a block. Mining could be undertaken by miners individually (solo mining) or as part of a pool (pooled mining). Miners can receive a fee against the service and can also be a wallet holder.
7.2	New Assets	In a Proof of Work system, network participants have to solve cryptographic puzzles in order to add new blocks to the blockchain. The first miner to successfully produce the PoW is rewarded with newly mined Virtual currency / Assets.

### 2.3.2. Assessing Threats, Vulnerabilities, and Mitigation Measures

#### a. Input Variables for ML/TF Threat<sup>6</sup> Assessment

In determining the ML/TF threat level associated with VAs/VASPs, each VASP channel identified in *Table 1*. was assessed based on the following 6 intermediate variables:

*Figure 1: Input Variables for ML/TF Threat Assessment*



The risk ratings for assessing threats have been categorized as follows: **Very High, High, Medium, Low and Very Low.**

<sup>6</sup> Threats are defined by FATF as a person, object or activity with the potential to cause harm to, for example, the state, society, economy, etc.

The overall ML/TF threat level was calculated by consolidating the ML/TF threat ratings of each applicable channel.

### b. Input Variables for ML/TF Vulnerability<sup>7</sup> Assessment

The ML/TF inherent vulnerability of each applicable VASP channels indicated in *Table 1* were analyzed based on the **Nature of Products and Services and the Types of VAs** which includes the following input variables:

*Table 3: Input Variables for ML/TF Vulnerability Assessment*

VULNERABILITY – ENTITY DIMENSION	Intermediate Variable	Input Variables	
	<b>Products and services provided and types of VAs</b>		Licensed in the country or abroad
			Nature, size and complexity of business
			Products and Services
			Methods of delivery of products/ services
			Customer types
			Country risk
			Institutions dealing with VASP
			VA (anonymity/pseudonymity)
			Rapid transaction settlement
		Dealing with unregistered VASP from overseas	

The combined ML/TF threat and ML/TF inherent vulnerability rating for each channel were used to produce a total risk level rating before considering mitigating measures for each applicable channel.

### c. Calculating Overall VA/VASP ML/TF Country Risk

A residual combined ML/TF risk rating for each applicable channel has been calculated based on the total combined ML/TF risk after taking into consideration the mitigation measures.

The mitigation measures were assessed based on the following input variables:

*Table 4: Mitigation Measures Input Variables*

MITIGATING MEASURES	Intermediate Variable	Input Variables	
	<b>Government measures</b>		Comprehensiveness of AML/CFT legal framework
			Availability and effectiveness of entry controls
			Adequate supervision and monitoring mechanism
			Regulation for customer due diligence and source of funds and availability of reliable identification infrastructure
			Financial and human resource capacity of law enforcement authorities to investigate, trace, seize, and secure virtual assets
			Effectiveness of international cooperation
			Quality of guidance issued to VASPs and engagement with VASPs
	<b>VASP measures</b>		Transparency of shareholder structure of VASP
			Quality of governance structure and level of accountability of VASP
		Effectiveness of compliance function and internal control mechanism	
<b>Financial institution (FI) measures and Designated</b>		AML/CFT knowledge of VASP staff	
		Risk assessment and risk mitigation measures by FIs and DNFBPs, referred to in this guidance as Traditional Obligated Entities	

<sup>7</sup> Vulnerabilities are defined by the FATF as things that can be exploited by the threat or that may support or facilitate its activities.

<b>Non-Financial Businesses and Professions (DNFBPs)</b>	Effectiveness of compliance function and internal control mechanism
--	---

The ratings for assessing mitigating measures have been categorized as follows: **Very High Mitigation, High Mitigation, Medium Mitigation, Low Mitigation, Very Low Mitigation and Does Not Exist.**

## 2.4. Data Collection and Analysis

The following data and information sources were used for completing the assessment:

- Information collected through survey questionnaires from public authorities and private sector (banks and PSPs);
- Blockchain and web traffic analysis reports to understand cryptocurrency flows in Moldova and surrounding countries;
- Statistics (national and international);
- Intelligence;
- Reports produced by LEAs;
- Meetings and workshops with relevant authorities;
- Informal discussions with selected TOEs;
- Articles and reports based on academic research;
- Reports from international standard-setting bodies;
- National and international case studies;
- Relevant Government reports; and
- Media, social media, internet and other sources of public information.

The WG concentrated on collecting both quantitative and qualitative data from diverse sources to establish a consistent risk assessment of ML/TF threats and vulnerabilities related to VA/VASPs sector that Moldova is facing. To facilitate data collection, the WG developed survey questionnaires, which were distributed to respondents, including LEAs, regulators, and TOEs. These questionnaires addressed various topics, such as risk perception, internal controls, available tools, staff knowledge, trainings and key statistics. The Working Group received a total of 29 completed responses, as outlined below.

*Table 5: VA/VASP Questionnaire Survey Respondents*

Category	Number of Respondents
<b>PUBLIC SECTOR</b>	
LEAs and Intelligence Services	9
Regulators	2
<b>PRIVATE SECTOR (Traditional Obligated Entities)</b>	
Banks	11
PSPs	7
<b>TOTAL</b>	<b>29</b>

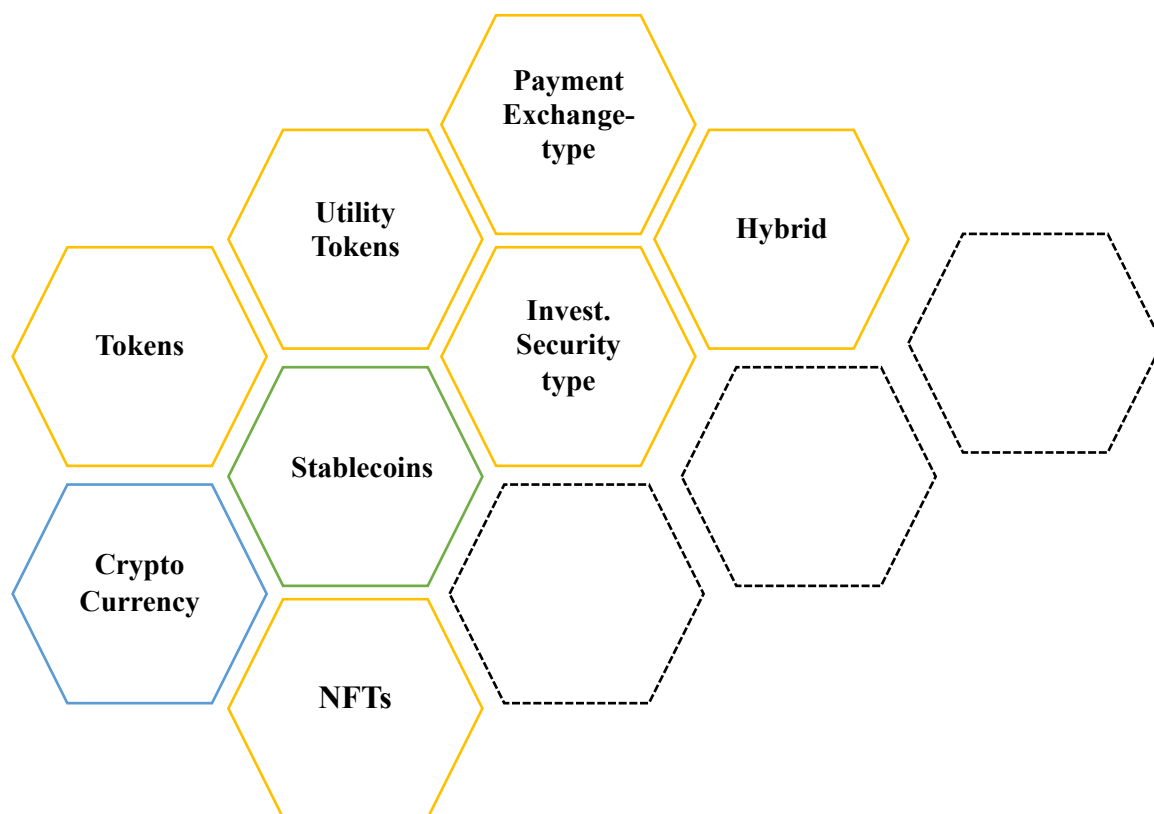
## 3. Overview of Global VA and VASP Ecosystems

This chapter briefly describes the ecosystems of VAs and VASPs, upcoming trends, emerging ML/TF risks, and global regulatory framework. Additionally, it provides an overview of international standards.

### 3.1. Evolution of VAs/VASPs Ecosystems and ML/TF Risks

On October 31, 2008, an individual or a group of individuals operating under the pseudonym "Satoshi Nakamoto" published the Bitcoin Whitepaper that introduced a truly decentralized, peer-to-peer payment mechanism.<sup>8</sup> Numerous prior attempts had been made to establish a peer-to-peer payment system that guaranteed its users anonymity (e.g., eCash, E-Gold, Bit Gold, B-Money, etc.), illustrating the need for decentralized payments.

Figure 2: Growth of VAs ecosystem



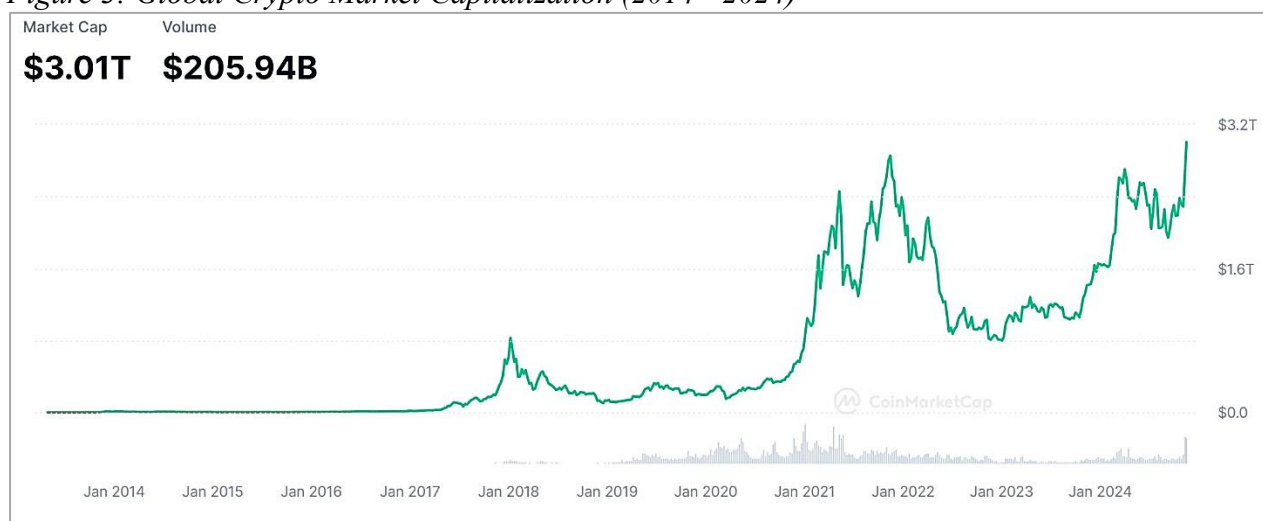
Since then, many cryptocurrencies with new features have been developed and continue to emerge, including privacy-enhanced coins (e.g., Monero, Zcash, Dash, etc.) and stablecoins (Tether, USDC, DAI, etc.) as the most well-known examples. VAs ecosystem experienced growth from cryptocurrencies acting as means of payment and presenting possibilities to conduct faster, cheaper, and more efficient cross-border payments by limiting the number of intermediaries to serving investment purposes and unique, identifiable assets representing pieces of art, digital content, or video that have been tokenized via blockchain.

According to the publicly available statistical data, the global market capitalization of cryptocurrencies surpassed 3 trillion USD (as of November, 2024)<sup>9</sup>, indicating the trends of growing popularity and access to VAs. Globally, more individuals and entities are interested in purchasing cryptocurrencies, and the need for the application of VAs to the range of transactions is visible.

<sup>8</sup> Bitcoin Whitepaper: [https://bitcoin.org/files/bitcoin-paper/bitcoin\\_ro.pdf](https://bitcoin.org/files/bitcoin-paper/bitcoin_ro.pdf) [last accessed: 11.11.2024]

<sup>9</sup> Coinmarketcap, Global Live Cryptocurrency Charts & Market Data, website: <https://coinmarketcap.com/charts/> [last accessed: 15 November 2024].

Figure 3: Global Crypto Market Capitalization (2014 - 2024)



Source: *CoinMarketCap*

Blockchain is being deployed to new ends, as shown by the popularity of non-fungible tokens (NFTs), which peaked in 2021, reaching around 41 billion USD in market size.<sup>10</sup> The NFTs market may also be vulnerable to ML threats and present opportunities for fraud and manipulation<sup>11</sup>. The same can be said about the stablecoins posing significant risk due to perceived stability and their potential use in ML/TF schemes to avoid market value fluctuation. Finally, it is important to acknowledge the most recent popularity of blockchain-based virtual real estate (VRE) on the metaverse and the use of metaverse tokens to facilitate transactions within the metaverse ecosystem. Though spent within the metaverse world, some metaverse tokens are available on exchanges.

The numbers above represent also the growing ML/TF threat as the anonymous and pseudo-anonymous<sup>12</sup> characteristics and technological innovation of cryptocurrencies naturally attracted and kept attracting the illicit actors' attention.

Indeed, being used in ML/TF schemes and associated with various predicate offences, such as fraud and drug trafficking, cryptocurrencies facilitated the expansion of darknet marketplaces (DNMs) that conduct transactions in cryptocurrencies for illicit goods and services. From 2011 to 2020, the total value of transactions in virtual assets on DNMs increased from approximately 6.7 million EUR to 3.145 billion EUR<sup>13</sup>. According to some estimates, Moldova, amongst the other countries, exhibits an increase in DNM revenue engagement over time.

Facilitating payments while avoiding the central overseeing body and without adequate regulation leads to suspicious transactional activity remaining undetected and unreported to the FIU. Furthermore, cross-border transactions involving VAs have no restrictions on

<sup>10</sup> Business Insider, NFTs ballooned to a \$41 billion market in 2021 and are catching up to the total size of the global fine art market, website: <https://markets.businessinsider.com/news/currencies/nft-market-41-billion-nearing-fine-art-market-size-2022-1> [last accessed: 06 October, 2024].

<sup>11</sup> E.g., on January 11, 2022, scammers staged one of the biggest NFT rug-pull scams using the Solana blockchain. About 1.3 mln USD in funds was lost with the promise to mint Big Daddy Ape Club NFT.

<sup>12</sup> Enhanced anonymity VAs are designed to obscure the links between wallet addresses which could be traced through blockchain analytics.

<sup>13</sup> European Monitoring Centre for Drugs and Drug Addiction, Cryptocurrencies, and Rugs: Analysis of cryptocurrency use on Darknet markets in the EU and Neighboring countries, Background paper commissioned by EMCDDA, 2022, p. 8, website: [https://www.euda.europa.eu/drugs-library/cryptocurrencies-and-drugs-analysis-cryptocurrency-use-darknet-markets-eu-and-neighbouring-countries\\_en](https://www.euda.europa.eu/drugs-library/cryptocurrencies-and-drugs-analysis-cryptocurrency-use-darknet-markets-eu-and-neighbouring-countries_en) [last accessed: 03 October, 2024].

geographic location. Even though cryptocurrency exchanges are the most common channel of initially obtaining cryptocurrencies, they can also be obtained via other means such as mining or sale of goods and/or services.

It's important to note that most virtual assets-related businesses are centralized to some degree or another. However, there are financial services on public blockchains, primarily Ethereum – the first blockchain to incorporate decentralized smart contracts. While traditional exchanges focus on converting fiat currencies into VAs, decentralized exchanges concentrate on converting VAs into other coins and tokens.

Illicit actors are early adopters of innovative technologies and quickly exploit weaknesses, decentralized finance (DeFi) is no exception. Services like decentralized exchanges (DEXs), mixers/tumblers, and liquidity pools can be leveraged for ML purposes to layer illicit proceeds. For example, illicit actors can place criminals' proceeds in a DeFi service's liquidity pool, where the assets provide liquidity to support trades on the service. In addition, cross-chain bridges may be used to convert one virtual asset to another to obfuscate the illicit origin and add layers making it more difficult to trace the funds.

*Table 6: Eastern Neighbourhood countries' per capita received, sent and total darknet market revenue engagement (in euros), period: April 2019 - June 2021*

Country	Rank	Mean rec.	Mean sent	Mean total	Total rec.	Total sent	Total	Population
Ukraine	1	6.76	12.06	18.82	182.46	325.66	508.12	44 260.45
Moldova	2	4.80	9.56	14.36	129.71	258.06	387.77	2 640.54
Belarus	3	5.13	8.52	13.65	138.60	230.01	368.61	9 408.36
Georgia	4	3.78	5.26	9.04	102.06	141.94	244.00	3 717.08
Armenia	5	1.77	3.27	5.03	47.69	88.16	135.86	2 960.48
Azerbaijan	6	0.62	1.04	1.66	16.66	28.03	44.69	10 067.20

Notes: 1) All revenue and population data in thousands. 2) rec is an abbreviation for received. 3) values rounded to 2 decimal places. Source: European Monitoring Centre for Drugs and Drug Addiction

Indeed, decentralized services were observed to be used to layer funds before moving the assets to the regulated exchanges to convert them to FIAT currencies<sup>14</sup>. These exit points need robust AML controls and blockchain analytics to manage the ML-associated risks.

The entities that are obliged to introduce know-your-customer (KYC) and AML rules can be of great help to the LEAs in establishing the perpetrator's identities and tracing the transactions to real-world individuals. According to Europol<sup>15</sup>, in recent years, there has been an increasing use of cryptocurrency in criminal activities, including money laundering. Criminals have also become more sophisticated in their use of cryptocurrencies.

It is important to emphasize that even though refusing to engage in activities related to VAs, banks, and other traditional financial institutions face VAs-related risks via customers that may be wiring fiat to exchanges or receiving wires from exchanges, without any awareness of the financial institution. Such customers may be acting as unlicensed peer-to-peer crypto

<sup>14</sup> ACAMS, More Illicit Cryptocurrency Moving Through 'DeFi' Systems, Research Shows, website: <https://www.moneylaundering.com/news/more-illicit-cryptocurrency-moving-through-defi-systems-research-shows/> [last access: October 8, 2024].

<sup>15</sup> Europol, Cryptocurrencies: tracing the evolution of criminal finances, website: <https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20Spotlight%20-%20Cryptocurrencies%20-%20Tracing%20the%20evolution%20of%20criminal%20finances.pdf> [last access: 3 October, 2024].

brokers or even holding accounts for companies that are trying to remain under the radar. E.g., companies that are engaged in mining activities may declare their activities as related to technologies, however, the abnormally high utility bills, such as electricity, may be the indicator of mining activities taking place.

### **3.2. VA/VASP Global Regulatory Developments**

In October 2018, the FATF revised its Recommendation 15 (also known as R.15) to include new requirements for VA/VASPs. Furthermore, in June 2019, the FATF adopted the Interpretative Note to R.15, which explains that VA activities and VASPs are within the scope of FATF Recommendations. According to FATF, **38% of jurisdictions that report prohibiting VASPs have done so without assessing the risks relating to VAs/VASPs in their jurisdiction**<sup>16</sup>. However, **effectively prohibiting VASPs poses a considerable challenge**. To successfully implement a prohibition approach, it is imperative to conduct a comprehensive risk assessment. **Actively identifying unauthorized VASP activities necessitates robust international cooperation mechanisms**. Furthermore, it is essential to establish and enforce appropriate measures to sanction any illegal VASP activities. For e.g., when dealing with unregistered VASPs the issue of how to detect them in practice arises, practically detecting unregistered VASPs requires education on all levels, and LEAs need grassroots training to identify the use of unregistered VASPs through investigation of predicate offenses and parallel money laundering investigations. Traditional FIs need education and guidance to identify the flow of fiat currency into such VASPs<sup>17</sup>. Globally the tendencies towards better regulation have been observed.

#### **The European Union**

The European Union (EU) is one of the largest markets with advanced digital asset regulation. To prevent market abuse and manipulation, the Markets in Crypto-Assets Regulation (MiCA) was introduced. The Regulation, which is mandatory for all the member states, is creating a single market for VAs. MiCA is the first cross-jurisdictional regulatory and supervisory framework around the World, that does not enter power as a standalone document.

Furthermore, the EU, as a member of the FATF, is striving to fully implement R.16, and thus the Transfer of Funds Regulation (TRF) sets the EU-wide rules for enforcement of the “Travel Rule”. It is required to capture transaction information for all amounts, with a threshold of 1000 EUR for self-hosted wallets, however, it does not apply to hardware wallet providers, as well as software and self-custody wallet providers that do not have control over the VAs<sup>18</sup>.

MiCA replaces individual regulations or the lack of regulation within the individual member states. It establishes the regulatory framework for facilitating and adopting distributed ledger technology (DLT) and crypto assets into the financial sector by adopting an already existing regulatory framework. It is important to distinguish tokens that can be defined as financial instruments and other VAs. Financial instruments are to be regulated by already existing legislation (Markets in Financial Instruments Directive or MiFID in particular), also NFTs do not fall under MiCA regulation as well as decentralized digital assets. Also, MiCA

---

<sup>16</sup> FATF, Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers, June 2023, p. 12.

<sup>17</sup> MONEYVAL, Money Laundering and Terrorist Financing Risks in the World of Virtual Assets, 2023, p. 26

<sup>18</sup> See the Annex.

excludes central bank digital currencies (CBDCs). Starting its implementation phase on April 2023 it will fully come into power by the end of the year 2024. The Regulation requires the member states to choose their national regulator to oversee the Crypto-Asset Service Providers (CASPs) authorization procedures, i.e. licensing. **Most jurisdictions chose either the Financial Market Authority acting as an independent institution or the national central bank as the regulator** (See Table 23, Section 9.3).

The FATF Recommendations provide authorities with considerable flexibility in selecting the supervisory model that best suits their needs. This choice should consider the risks and significance of the sector, as well as the specific structure of public institutions. It is also important to emphasize that the licensing or registration authority is not supposed to be the same authority that conducts the AML/CFT supervision of CASPs.

Primarily introduced to ensure consumer protection and market integrity, MiCA regulation is not aimed at AML/TF questions, however, the requirements presented by MiCA are adding to the mitigation of risks related to ML/TF activities. The Regulation is being implemented in stages, e.g., it became effective for stablecoins from 30 June 2024, and by the end of 2024 it will be fully implemented.

**The requirements.** MiCA is establishing new requirements and mandatory compliance with existing legislation. To name a few:

- **White paper.** It is a mandatory document for crypto asset issuers and must describe the technical information of the crypto asset. The requirement to publish a white paper does not apply if the assets are offered for free, are created through mining, or are unique and not fungible. Furthermore, a white paper is not necessary if the offer is made to fewer than 150 natural or legal persons per Member State, the total consideration does not exceed 1 million EUR, or the offer is made to qualified investors.
- **Reserve.** Asset reference tokens and e-money tokens are subject to additional requirements, including the disclosure of reserve funds and internal control systems.
- **CASPS must comply with KYC and AML rules** and perform enhanced due diligence for customers from high-risk jurisdictions
- **Trading platforms must not allow users** to trade assets with **full anonymization**.

Regulatory changes can significantly affect market concentration and the movement of VASPs between neighboring countries. For example, in 2017, Estonia became one of the first EU nations to establish a licensing regime that required VASPs to implement anti-money laundering programs and other controls before being approved to operate. In 2020, the regulations for licensed VASPs were further tightened, raising capital requirements and mandating that they open a physical office and hire staff in Estonia, among other stipulations. As a result, hundreds of cryptocurrency platforms were rejected in Estonia and subsequently relocated to Lithuania where regulation was considered lax at that time<sup>19</sup>. By harmonizing the regulation, the EU amongst other benefits ensures that these situations will not occur in the future.

---

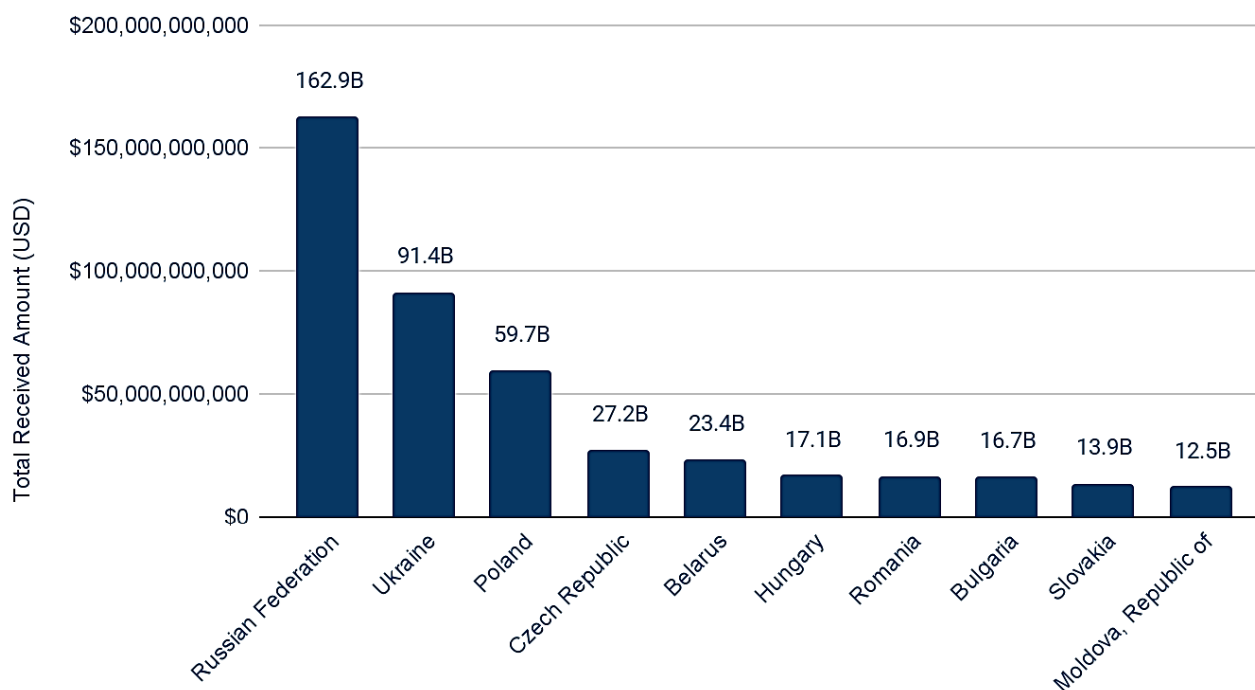
<sup>19</sup> ACAMS, Baltic Officials Shed Light on Cryptocurrency Crackdown, Russia Sanctions Evasions, website: [MoneyLaundering.com :: Changes in Bank Regulations, Financial Compliance Regulations, Regulation Banks, Money Laundering Cases, Anti Money Laundering, Money Laundering Training](https://www.moneylaundering.com/changes-in-bank-regulations-financial-compliance-regulations-regulation-banks-money-laundering-cases-anti-money-laundering-money-laundering-training). [last access: 1 November, 2024].

### 3.3. Cryptocurrency Activity in Moldova: An Overview from Chainalysis

#### ➤ Overview of Cryptocurrency Flows in Moldova

This section provides an overview of estimated cryptocurrency activity in Moldova and neighboring regions, as provided by Chainalysis.<sup>20</sup> The aim is to establish a baseline for cryptocurrency engagement in Moldova and comparable countries, while also illustrating changes in the cryptocurrency landscape over time. The data presented is based on web traffic statistics covering the period from January 1, 2021, to June 30, 2024. The most recent web traffic data included in this section is as of June 30, 2024.

Figure 4: Total flows to a selection of Eastern European countries (2023-06 to 2024-06)



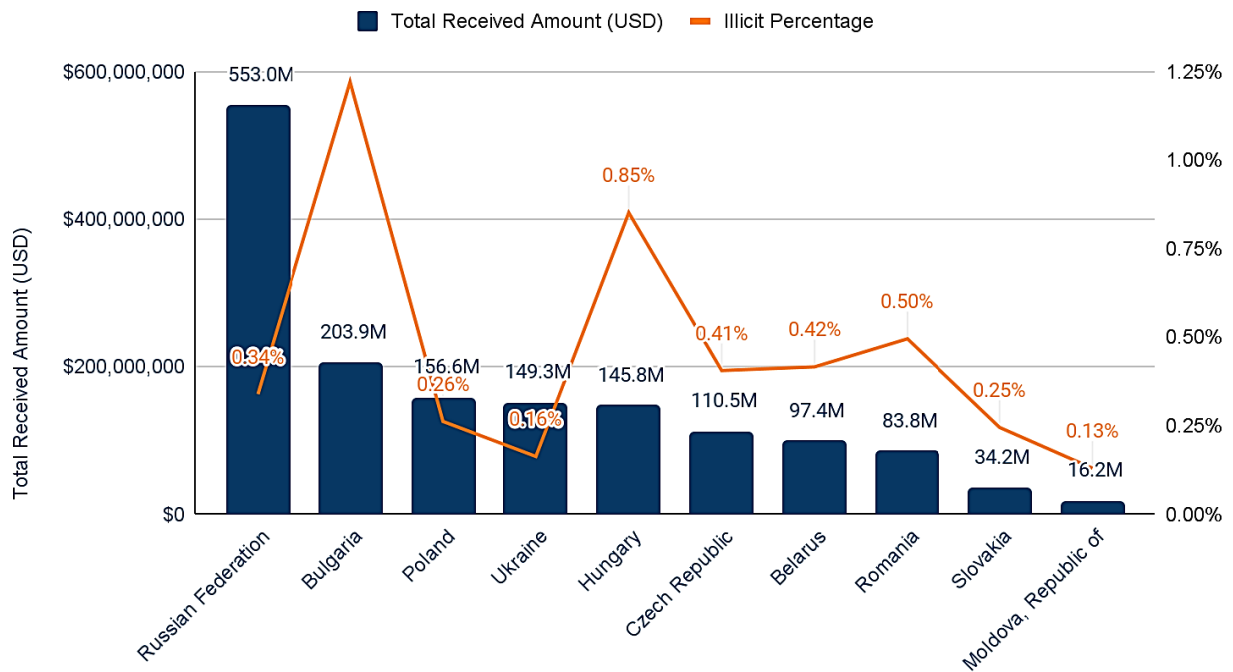
Source: Chainalysis 2024 Report on Election Interference & Cryptocurrency, p.12.

This graph provided by Chainalysis illustrates comparative volume estimates of cryptocurrency activity across selected Eastern European countries over the past year. The estimates are derived by combining third-party web traffic data from specific services with the cryptocurrency volume processed through those services. It is important to note that the graph represents the value received in each country, not the value held. As the vast majority of cryptocurrency at some point in time flows through VASPs that operate internationally, and residents in those countries in turn tend to utilize VASPs at some point in time, value received is a relatively good proxy for comparative levels of cryptocurrency activity in those countries.<sup>21</sup>

<sup>20</sup> Chainalysis 2024 Report: Election Interference & Cryptocurrency: Indicators of Russian Interference in Moldova

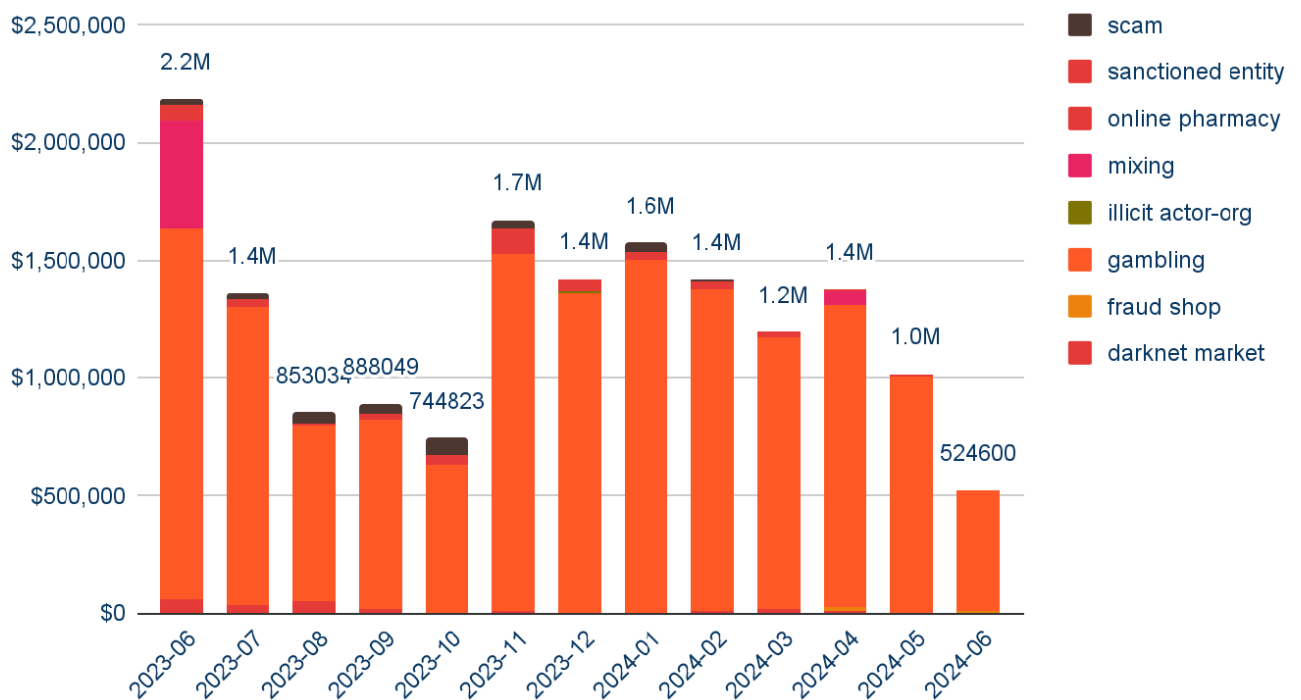
<sup>21</sup> Note though that as this is not value held, this is meant to represent activity or cryptocurrency movement, rather than aggregate value possessed by the residents of a country.

Figure 5: Total illicit value received in selected Eastern European countries (2023-06 to 2024-06)



The above two charts are closely related. The first shows the total value received in a selection of Eastern European countries that are in close geographic proximity to Moldova. The percentage of illicit activity line is relative to the first graph, which shows total value received. Moldova has a similar volume of activity to its neighboring countries, but comparatively low amounts of illicit activity. In both charts, the amounts received are expressed as the USD equivalent value of the aggregate amount of cryptocurrency received in each country. It is worth noting that the "illicit activity" numbers are based on entities Chainalysis has explicitly detected and categorized, but does not encompass uncategorized cryptocurrency transactions used for things like money laundering, or in the facilitation of crime more strongly grounded in the real world, such as human trafficking.

Figure 6: Moldova Illicit Flows by Category (2023-06 to 2024-06)



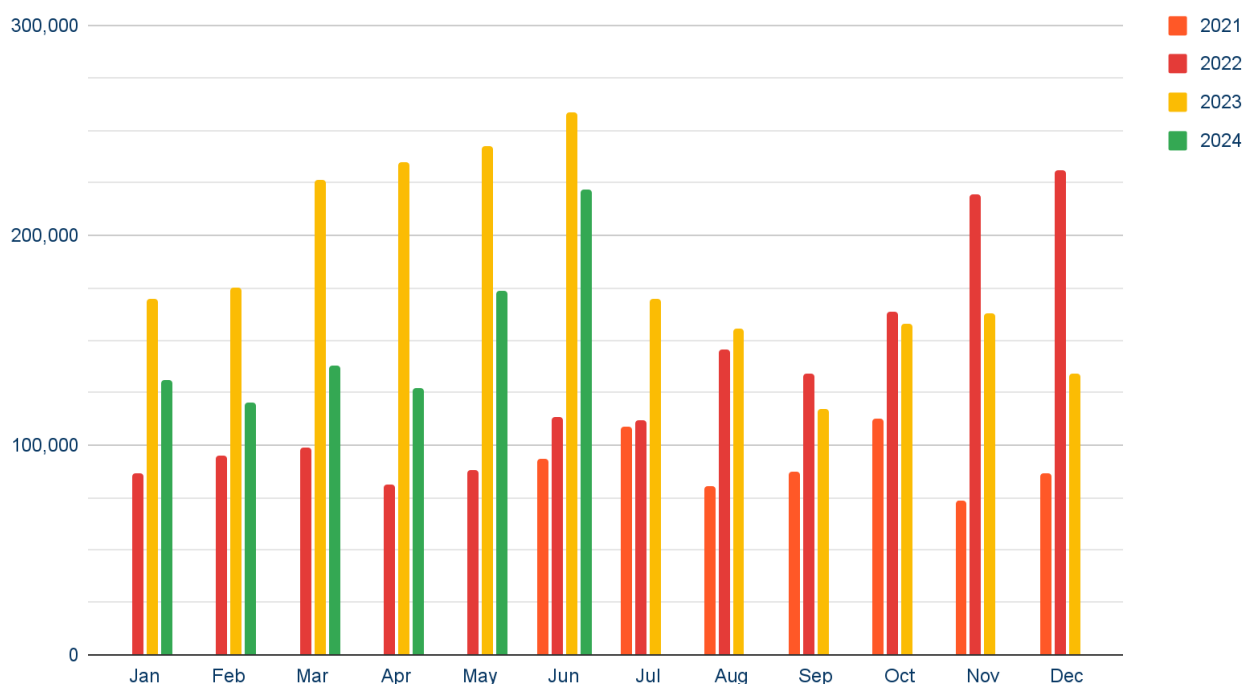
The "illicit" flows by category show a breakdown of the type of service at which "illicit" crypto originated before being received in Moldova by month from June, 2023 to June, 2024. The precise definition of "illicit" varies by country depending on the laws of specific countries. The categories above are some commonly restricted or explicitly outlawed activities in which cryptocurrency plays a role. It is worth noting that **the majority of "illicit" cryptocurrency activity in Moldova has been traced to gambling services.**

While gambling itself is legal in Moldova, it operates as a state monopoly, with only the state-owned enterprise, the “National Lottery of Moldova,” authorized to administer and organize lottery and gambling activities. All other gambling companies, including online gambling platforms, are prohibited, and access to unauthorized gambling sites is blocked within the country. Additionally, facilitating payments to unauthorized gambling sites is considered illegal. Unregulated gambling service providers can also serve as money laundering vehicles for more illicit types of cryptocurrency activity when used as a pass-through method of layering in the money laundering process. When used this way, this can prevent or problematize the ability to trace the origin of the cryptocurrency to the original illicit activity. However, there is no presumption that this is what is going on with this gambling activity, which is only .12% of the overall cryptocurrency activity in the last year.

➤ **Cryptocurrency deposit frequency in Moldova, 2021-06 to 2024-06 by month**

The next three charts compare the frequency of deposit transactions from 2021-06 to 2024-06 by month in Moldova. Examining the number of deposit transactions rather than the USD equivalent value of the amount of cryptocurrency sent and received accounts for the fluctuating values of various cryptocurrencies. Increased adoption of cryptocurrency and regulatory acceptance could explain the general upward trend in the amount of activity in each country.

Figure 7: Moldova Deposit Frequency Between 2021-06 and 2024-06



The graph above shows an **increase in general cryptocurrency activity in Moldova in the year 2024**, not reaching 2023 levels but with a steady upward trend.

➤ **Most accessed services in Moldova by web visits 2024-06**

The below charts depict the top services with a cryptocurrency nexus accessed from Moldova IP addresses, sorted by number of visits. Note that not all of these are considered VASPs, but merely allow cryptocurrency to be used in various ways other than for the purpose of money transmission.

Table 7: Top Services Related to Cryptocurrency Accessed from Moldova (2024-06)

Year_month	Name	Category	Visits	Share
2024-06	<a href="https://www.reddit.com">Reddit.com</a>	other	1398254.29	0.00058747
2024-06	<a href="https://www.telegram.org">Telegram.org</a>	wallet	860197.529	0.00254937
2024-06	<a href="https://www.binance.com">Binance.com</a>	exchange	685532.139	0.01081282
2024-06	<a href="https://www.freebitco.in">FreeBitco.in</a>	gambling	539785.367	0.01238618
2024-06	<a href="https://www.whitebit.com">Whitebit.com</a>	exchange	474728324	0.02003786
2024-06	<a href="https://www.bitcoin.com">Bitcoin.com</a>	exchange	221472.251	0.04133182
2024-06	<a href="https://www.bybit.com">Bybit.com</a>	exchange	146195.596	0.00438988
2024-06	NV.UA Donation (Ukrainian media)	other	118961.214	0.00501775
2024-06	<a href="https://www.archive.org">Archive.org</a>	other		0.0006959
2024-06	<a href="https://www.faucetpay.io">FaucetPay.io</a>	exchange	81199.2218	0.01137306
2024-06	<a href="https://www.rollercoin.com">Rollercoin.com</a>	gambling	79629.3225	0.0116982
2024-06	<a href="https://www.okx.com">Okx.com</a>	exchange	63597.6165	0.00219462
2024-06	Reported as <a href="https://www.etherscan.io">etherscan.io</a>	scam	55489.469	0.00524423
2024-06	<a href="https://www.crypto.com">Crypto.com</a>	exchange	48445.5216	0.01193198
2024-06	<a href="https://www.coinbase.com">Coinbase.com</a>	exchange	44298.0737	0.00129343
2024-06	<a href="https://www.bitfinex.com">Bitfinex.com</a>	exchange	42301.8787	0.04745851
2024-06	Reported as <a href="https://www.telegra.ph">telegra.ph</a>	scam	42198.7178	0.00175441
2024-06	<a href="https://www.adbtc.top">AdBTC.top</a>	scam	357341821	0.00591062
2024-06	<a href="https://www.proton.me">proton.me</a>	infrastructure as a service	33938.4751	0.00050028
2024-06	Pancake Swap V2: MAV USDT 0x1b0d5e- 0x55d398 [BNB Smart Chain]	dexchange	31778.5438	0.00907544

Above are the top 20 services by number of visits in Moldova in the most recent month for which Chainalysis has data. Notably one of these services is proton.me – enhanced online privacy services provider, which is characterized as an infrastructure as a service (IaaS) provider by Chainalysis.

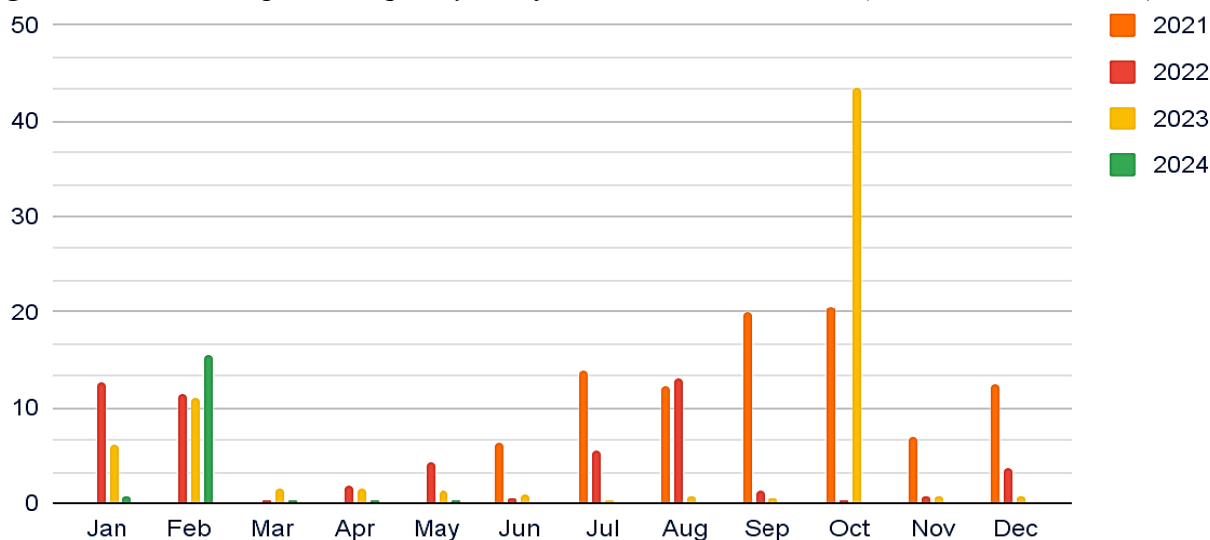
➤ **Infrastructure as a service deposit: 2023-06 to 2024-06**

IaaS may be used to host websites that seed misinformation while obscuring the true source of misinformation, could be used to create bulk email addresses used in disinformation campaigns, or allow for the purpose of social media accounts or virtual phone numbers at scale. The graphs below depict the transactional value sent to IaaS category in Moldova over the last year.

The following graph focuses on sending exposure (from country to IaaS) as an indicator of potential hosting services being purchased by individuals from Moldova based on web traffic data. These graphs show the number of independent transactions per month (which are likely equivalent to the number of infrastructure purchases in a given month). Note that unlike cryptocurrency exchanges, which often have a roughly equal number of deposits and

withdrawals, infrastructure providers are far more likely to have more deposits coming to them from those that they are providing infrastructure to. In most cases withdrawals will represent funds controlled by the infrastructure providers, rather than their users.

Figure 8: Moldova Deposit Frequency to Infrastructure as a Service (2021-06 and 2024-06)



### ➤ Chainalysis 2024 Crypto Adoption Index Report

Recently, blockchain analytics company Chainalysis ranked Moldova as 59<sup>th</sup> out of 151 countries in the 2024 Global Crypto Adoption Index<sup>22</sup>. This is a significant increase compared to the ranking of 2020 when the index was introduced, and Moldova was ranked 88<sup>th</sup>.

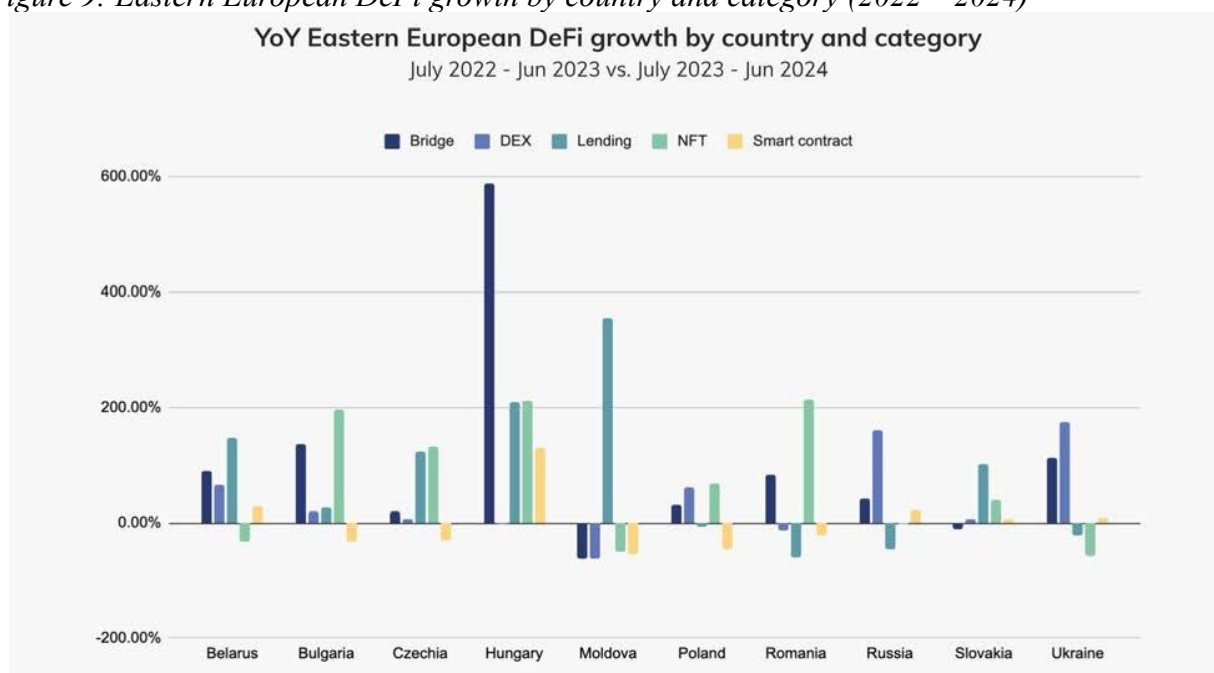
The country’s position reflects varied levels of engagement across different aspects of the digital asset ecosystem:

- a. **Centralized Service Value Received:** Moldova ranks 37<sup>th</sup>, indicating a relatively high usage of centralized platforms for cryptocurrency transactions and services.
- b. **Retail Centralized Service Value Received:** Ranked 38<sup>th</sup>, Moldova shows a strong level of adoption among individual retail users in centralized crypto services, suggesting significant personal engagement with mainstream platforms.
- c. **DeFi Value Received:** Moldova ranks 94<sup>th</sup> in terms of value received through decentralized finance (DeFi) platforms. This lower position implies limited use and engagement with DeFi protocols.
- d. **Retail DeFi Value Received:** Positioned at 88<sup>th</sup>, Moldova has modest participation in retail DeFi activities, which points to limited uptake of DeFi services among individual users.

Overall, Moldova’s rankings highlight a stronger reliance on centralized crypto services compared to decentralized ones, with retail engagement particularly prominent within centralized platforms.

<sup>22</sup> Chainalysis, The 2024 Geography of Crypto Report, 2024 October, p. 63, 128.  
<https://www.chainalysis.com/blog/2024-global-crypto-adoption-index/>

Figure 9: Eastern European DeFi growth by country and category (2022 – 2024)



Source: Chainalysis, *The 2024 Geography of Crypto Report*, p.63.

Based on the above chart, Chainalysis noted that **Moldova experienced an explosive growth in DeFi lending transactions** between the period July 2023 – June 2024 compared to the previous year (July 2022 – June 2023). Despite this rapid expansion, Moldova's relatively small market size means that crypto inflows to DeFi lending still represent only a minor share of the total DeFi volume within the region.

### 3.4. ML/TF Risks Associated with the VAs and VASPs

Under AML/TF Law No. 307/2017 - VASP is defined as individual or legal entity that performs any of the following activities on behalf of others: 1. Exchange between VA and fiat currencies 2. Exchange between different types of VA; 3. Transfer of VA; 4. Custody and/or administration of VA or instruments enabling control over VA; 5. Provide financial services related to an issuer's offer and/or sale of VA.

The provision of services related to virtual assets is prohibited in Moldova, even if these activities are auxiliary or supplementary to the main business. Additionally, reporting entities cannot open accounts for VASPs. **However, they may open “special” accounts for customers who conduct transactions to or from virtual asset service providers authorized in other jurisdictions, under certain conditions and limits.**<sup>23</sup> This allows Moldovan citizens to access virtual assets through traditional financial channels involving other jurisdictions. It is important to note that **citizens of the Republic of Moldova are eligible to hold multiple citizenships. The most common are Romanian citizenship, acquired based on Romanian descent, as well as Russian and Ukrainian citizenships, particularly among residents of the Transnistrian region.** This status allows them to access services related to VAs without the need to disclose their Moldovan citizenship, which adds a layer of difficulty to international cooperation and statistical data gathering. Although the activity of VASPs is prohibited in Moldova, ML/TF risks associated with

<sup>23</sup> Art. 8 of AML/CFT Law no. 308/2017, website: [https://www.legis.md/cautare/getResults?doc\\_id=136906&lang=ro](https://www.legis.md/cautare/getResults?doc_id=136906&lang=ro)

VASPs, and VAs persist through both direct (via unofficial channels) and indirect means (through specialized accounts).

### **Global ML/TF Risks Associated with VAs/VASPs:**

#### **a. ML/TF risks associated with virtual assets exchanges:**

- **Use of non-compliant exchanges.** Criminals may target exchanges with weak AML/CFT controls to bridge the fiat and crypto worlds. Although AML/CFT requirements can vary by jurisdiction, exchanges that require customers to undergo Know Your Customer (KYC), ongoing due diligence (ODD), and enhanced due diligence (EDD) procedures, while also having a lax approach to transaction monitoring and reporting suspicious activities, pose significant ML/TF risks.
- **Use of exchanges in high-risk jurisdictions.** Funds of illicit origin may be transferred to/from exchanges in jurisdictions that pose substantial financial crime risks (e. g., jurisdictions under Increased monitoring or FATF’s “grey list”).

**b. ML/TF risks associated with intermediary services and wallets** (mixers, instant exchangers, various types of DeFi protocols, and other services of both legitimate and illicit nature). These services obscure the on-chain connection between the source and current addresses. E.g., the use of mixers (Tornado Cash<sup>24</sup>, Chip Mixer<sup>25</sup>) or privacy-enhanced wallets (e.g., Samurai wallet<sup>26</sup>) are known means used by criminals to obfuscate the origin of the illicit funds or the illicit destination of the transferred funds. In 2023, mixers consistently accounted for a significant portion of ransomware-related transactions, indicating they are the preferred method for laundering ransomware payments, according to Chainalysis<sup>27</sup>.

**c. ML/TF risks associated with P2P exchanges, OTC desks, gambling services, and crypto ATMs.** This type of services provide possibilities to convert FIAT currency to VAs and VAs to FIAT currency. P2P exchanges and online gambling operators offering gambling services allowing deposits with cryptocurrencies offer a certain level of anonymity attractive to illicit actors that can send the funds from illicit activities to P2P exchanges to obtain new “clean” coins.

**d. ML/TF risks related to the use of stablecoins.** While stablecoins might bring a range of benefits, they also introduce significant risks. Their role in illicit activities and the potential to threaten financial stability raise concerns<sup>28</sup>. Criminals may be attracted to the perceived stability of stablecoins because their value is tied to other assets. Stablecoin issuers may have the ability to freeze funds (USDT, USDC) if they become aware that those funds are being used for illegal activities, however, according to Chainalysis<sup>29</sup>, stablecoins now account for the majority of all illicit transaction volume.

**e. ML/TF risks associated to privacy coins.** Privacy coins, such as Monero, Dash, and Zcash, offer enhanced anonymity features through technologies like zero-knowledge

---

<sup>24</sup> U.S. Department of the Treasury, U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash, website: <https://home.treasury.gov/news/press-releases/jy0916>, [last access: 27 October, 2024].

<sup>25</sup> DOJ, Justice Department Investigation Leads to Takedown of Darknet Cryptocurrency Mixer that Processed Over \$3 Billion of Unlawful Transactions [last accessed: 27 October, 2024].

<sup>26</sup> DOJ, Founders and CEO of Cryptocurrency Mixing service Arrested and Charged with Money Laundering and Unlicensed Money Transmitting Offenses, website: <https://www.justice.gov/usao-sdny/pr/founders-and-ceo-cryptocurrency-mixing-service-arrested-and-charged-money-laundering> [last accessed: 27 October, 2024].

<sup>27</sup> Chainalysis, The 2024 Crypto Crime Report. The latest trends in ransomware, scams, hacking, and more. February 2024, p.20

<sup>28</sup> BIS, FSI Insights on policy implementation No 57, Stablecoins: regulatory responses to their promised stability, April 2024, website: <https://www.bis.org/fsi/publ/insights57.pdf>, [last accessed: 27 October, 2024].

<sup>29</sup> Chainalysis - The 2024 Crypto Crime Report, p. 7

proofs and ring signatures<sup>30</sup>. These features can facilitate layering for illicit activities. Criminals may convert their earnings from Bitcoin or other cryptocurrencies into privacy coins via unregulated exchanges. Additionally, individuals engaged in illegal activities can generate proceeds in privacy coins and then swap them for more transparent cryptocurrencies such as Bitcoin, Ether, Solana, or Ripple through platforms that allow such transactions. Furthermore, sanctioned individuals might use privacy coins to evade sanctions. Due to the advanced privacy features of these coins, tracking the flow of value can be extremely challenging, and in some cases, nearly impossible.

- f. ML/TF risks associated with card and voucher use.** Prepaid cards and vouchers can be used for money laundering<sup>31</sup>. Criminals may deposit virtual assets obtained from illegal activities onto these cards or use virtual assets of illicit origin to purchase fiat currency cards for laundering purposes. Additionally, bad actors might use stolen card details to buy cryptocurrency, which can then be employed in further criminal activities, such as purchasing malware or financing terrorism.
- g. ML/TF risks related to NFTs.** Customers of an NFT marketplace may purchase NFTs using funds linked to illicit activities. NFT platforms facilitate the exchange of non-fungible tokens, which are unique and not interchangeable. Additionally, NFTs can represent tokenized versions of physical goods, such as real estate or precious metals. The ease of transferring NFTs and the lack of transparency in transactions attract money launderers. Moreover, criminals may manipulate NFT values, potentially scamming unsuspecting buyers. It is important to stress that NFTs continue to pose risks for ML/TF, although some jurisdictions have seen a decrease in risk level in this area following the market boom in 2021<sup>32</sup>.
- h. ML/TF risks associated with mining pools.** A mining pool is a platform that provides services for miners to enhance their chances of receiving rewards by combining their mining power. Mining pools typically have defined payout mechanisms and fee structures for their usage. Mining pools can be used as a means of self-funding<sup>33</sup> for illicit activities or money laundering.
- i. Other concerns (Metaverse).** The metaverse is evolving into a new, three-dimensional digital world that transcends geographical limitations and currently lacks clear rules and regulations. The worldwide number of Metaverse users is predicted to exceed 1.4 billion by 2030, with the user penetration growing three-fold and hitting 18%<sup>34</sup>. New trends are

---

<sup>30</sup> Monero also employs Ring Confidential Transactions (RingCT) to hide transaction amounts. Introduced in 2017, this cryptographic method ensures that the sent amounts are completely hidden from view. Even though all transactions are recorded on the blockchain, there is no way for observers to know exactly how much Monero is being sent. Source: TRM LABS, website: <https://www.trmlabs.com/post/the-rise-of-monero-traceability-challenges-and-research-review> [last access: 1 November, 2024].

<sup>31</sup> Between 2019 and 2023, investigations by France's FIU (Traitement du renseignement et action contre les circuits financiers clandestins, or Tracfin) demonstrated how crypto assets can be used as an effective terrorism financing tool, in which anonymously purchased vouchers are converted into crypto assets. As a result of Tracfin's analysis, a complex new terrorism financing scheme (mixing various financial tools) was identified. Source: Egmont group, BEST EGMONT CASES, Financial Analysis Cases 2021-2023, p. 25.

<sup>32</sup> FATF, Targeted Update on Implementation of the FATF Standards on VAs/VASPs, June, 2023, website: [Virtual Assets: Targeted Update on Implementation of the FATF Standards](#)

<sup>33</sup> The third largest counterpart to Iranian crypto services is mining pools, with 3.16% of the total volume across all assets and 29.1% of Bitcoin flows. Iran legalized cryptocurrency mining in 2019 and it's also the eighth largest oil producer in the world, with 4% of global oil production. Given the extensive sanctions against Iran and its access to affordable energy, experts have warned that Iran could use crypto mining as a revenue generation tool to mitigate the impact of global sanctions. Source: Chainalysis, The 2024 Crypto Crime Report, The latest trends in ransomware, scams, hacking, and more, February, 2024, p. 78.

<sup>34</sup> Techreport, Metaverse Statistics 2024: Latest User & Market Trends, website: [Metaverse Statistics 2024: Latest User & Market Trends](#) [last access: 3 November, 2024].

emerging in the areas of the Metaverse’s economy, governance, and user experience, along with new types of crime specifically related to the metaverse. One notable development is blockchain-based virtual real estate (VRE) within the metaverse, as well as the use of metaverse tokens to facilitate transactions within this ecosystem. While these tokens are primarily used within the metaverse, some are also available on exchanges.

## 4. Survey Responses

### 4.1. Law Enforcement Agencies (LEAs) and Intelligence Services’ Responses to the VAs/VASPs Survey

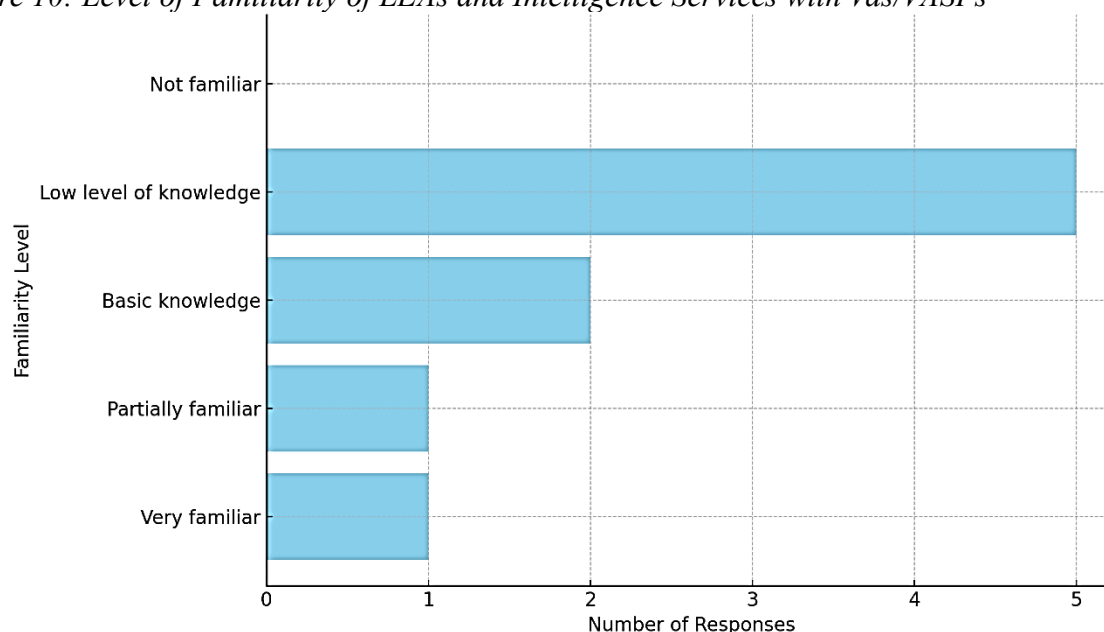
#### Respondents:

- Prosecutor General’s Office
- National Investigation Inspectorate
- Border Police
- National Anticorruption Office (Asset Recovery Office)
- Customs Service
- State Tax Service
- Security and Intelligence Service
- Financial Intelligence Unit
- National Integrity Authority

#### Summary of Findings

The majority of the respondents (5 authorities) reported having a **low level of familiarity** with VAs/VASPs, suggesting a substantial knowledge gap in this sector. A smaller segment (2 authorities) reported having **basic knowledge**, indicating some foundational understanding but lacking in-depth expertise. Notably, only one authority in each category identified themselves as either **very familiar** or **partially familiar**, while none claimed to be completely unfamiliar with VAs and VASPs.

Figure 10: Level of Familiarity of LEAs and Intelligence Services with VAs/VASPs



When it comes to investigative capacity, most of the agencies (55%) acknowledged having limited expertise in areas related to the investigation, tracing, prosecution, and seizure of VAs. Furthermore, a substantial 77% of respondents highlighted deficiencies in resources and technological tools necessary for effectively handling these cases. Only three authorities reported using commercial blockchain analysis tools, each with a limited license allowing access to just one user per authority. Limited access to blockchain analytics tools hampers the ability of LEA staff to work on multiple cases at the same time. This not only slows down the overall investigation process but also makes it challenging to conduct joint investigations across various divisions. As a result, the effectiveness of monitoring targeted wallets is diminished, and the response time for mutual legal assistance requests and international cooperation through Financial Intelligence Units (FIUs) may be prolonged. Timely tracing of borderless blockchain transactions can typically be accomplished within minutes, but these limitations hinder that efficiency. Additionally, only one agency has established a VA wallet specifically for storing and securing seized virtual assets, raising concerns about the effectiveness of timely asset seizure efforts. Moreover, LEAs should be able to seize and store assets in a designated wallet.

On a positive note, all the law enforcement agencies confirmed an increase in training and workshops over the last three years, provided by various organizations and programs. These educational initiatives have covered a wide range of topics, including investigations involving crypto-assets, blockchain forensics, non-fungible tokens (NFTs), digital evidence and cryptocurrency, the management of seized and confiscated virtual assets, as well as the supervision and regulation of VAs and VASPs. This growing focus on training reflects a broader recognition of the challenges posed by virtual assets and the urgent need to address knowledge and skill gaps in this evolving field.

Overall, the results underscore a critical need for enhanced training programs and better resource development to equip Moldovan agencies with the tools and expertise required to handle the complexities of virtual assets. Strengthening both national and regional security frameworks in this emerging area will be essential to meeting these challenges head-on.

Further, the LEAs indicated that there are gaps in the current legal provisions related to VA/VASPs, among which are: no supervision/regulatory authority in the sector; as a result of the prohibition of VASP services within the country, there is no reporting from this sector; no clear taxation regime for VAs.

Authorities also emphasized that rapid technological innovation and slow regulatory response create vulnerabilities. For instance, emerging crypto technologies, such as decentralized finance (DeFi) platforms, decentralized exchanges (DEXs), and new types of digital assets, are advancing at a faster pace than regulatory frameworks. Criminals can exploit these innovations, using them for money laundering and terrorist financing through innovative methods that evade existing controls (prohibitions), for e.g. P2P trading (*presented in Chapter 5*). These regulatory gaps provide opportunities for bad actors to obscure the origins of funds or facilitate illicit transactions.

To mitigate these risks, LEAs stressed the importance of greater international cooperation and the development of coherent regulations aligned with EU standards. Such measures would significantly reduce the risk of money laundering and terrorist financing in the VAs/VASPs sector.

LEAs highlighted the following types of VAs and VASPs services that present a higher risk to be exploited by criminals for ML/TF:

- Anonymous cryptocurrencies (e.g., Monero, Zcash)
- Non-fungible tokens (NFTs)
- Decentralized exchanges (DEXs), such as Uniswap and PancakeSwap
- Mixers and tumblers (e.g., Tornado Cash, Wasabi Wallet)
- Peer-to-peer trading platforms (e.g., LocalBitcoins<sup>35</sup>, Paxful), which facilitate direct exchanges between users without intermediaries.

### STRs/SARs

Between 2021 and 2024, Moldova’s Financial Intelligence Unit (FIU) received a growing number of Suspicious Transaction Reports (STRs) and Suspicious Activity Reports (SARs) associated with VAs/VASPs, reported primarily by banks and PSPs. These reports have been triggered by a variety of red flags, pointing to potential financial crimes such as money laundering, fraud, drug trafficking and illicit use of virtual assets.

### Statistical Overview of STRs and SARs Reported

The statistics on STRs and SARs related to VA/VASPs indicate a notable increase in the frequency of reports, particularly from banking sector. This increase suggests a heightened vigilance and responsiveness among financial institutions as they adapt to the evolving landscape of VA-related activities. Below is a summary of the reported STRs and SARs from banks and PSPs:

*Table 8: Number of STRs/SARs associated with VA/VASPs reported (2021 – 2024)*

Year	Banks	PSPs	Total
2021	6	10	<b>16</b>
2022	6	12	<b>18</b>
2023	11	1	<b>12</b>
2024	32	1	<b>33</b>

### Key Indicators and Red Flags Leading to STR/SAR Filings

Several key indicators have been identified as common triggers for filing of STRs/SARs associated with VA-related activities. These indicators reflect complex layering tactics and financial behaviors often associated with illicit activities. Below are the primary reasons and red flags observed:

- **Use of “Money Mules” or “Drop Accounts”:**  
A complex network of “drop accounts,” commonly held by individuals known as “mules,” was identified. These individuals either knowingly or unknowingly facilitate the movement of funds through various accounts, often for compensation. This scheme involves multiple transfers to obscure the origin and destination of funds.
- **Profile of Suspected Account Holders:**  
Individuals involved in suspicious transactions, potentially related to the layering of funds derived from fraud, carding schemes, or laundering funds from Darknet operations, often fall into specific demographic groups. These groups include students,

---

<sup>35</sup> According to an announcement on its website, the peer-to-peer Bitcoin platform LocalBitcoins has decided to stop its services on February, 2023, website: <https://localbitcoins.com/>

unemployed individuals, and retirees, who might be more susceptible to manipulation or less aware of compliance requirements.

➤ **Opening of Multiple Bank Accounts:**

Clients opening multiple accounts within the same bank or across different banks without a clear economic purpose have raised suspicions. Frequent transfers between these accounts, lacking logical or economic rationale, are a red flag indicating potential structuring or layering efforts.

➤ **Challenges in Determining the Source of Funds:**

In many cases, reporting entities face difficulties in establishing the source of funds involved in the transactions. This opacity can point to attempts to obfuscate illicit origins, especially in transactions involving cryptocurrency platforms.

Most STRs/SARs related to virtual assets, once received and analyzed by the FIU, were passed on to the National Inspectorate of Investigations for additional investigative action.

### **Spontaneous Intelligence Reports and Requests from Foreign FIUs**

Over the past three years, the FIU Moldova has observed a significant **increase in the number of spontaneous intelligence reports and requests received from foreign FIUs** regarding Moldovan citizens involved in suspicious cryptocurrency activities.

Between 2021 and 2024, FIU Moldova recorded a total of 12 spontaneous dissemination reports and intelligence requests, with six reports received in 2024 alone. These reports/requests originated from 10 different jurisdictions and involved a total of 83 individuals.

The majority of the intelligence received has been related to various types of suspicious activities, which include:

- **Direct or Indirect Transactions with Dark Markets and Fraudulent Shops:** Instances where individuals have engaged with known dark web marketplaces or fraudulent e-commerce platforms through cryptocurrency transactions.
- **Cryptocurrency Investment Scams:** Reports involving suspected fraudulent schemes where individuals were lured into fake or deceptive cryptocurrency investment opportunities.
- **Abnormal Activity (layering):** Patterns of unusual financial layering, often used to obscure the origin of funds and evade detection in the laundering process.
- **Transactions with Non-KYC Exchangers:** Transactions conducted through VASPs that do not adhere to KYC (Know Your Customer) standards, increasing the risk of illicit financial activity.
- **Refusal to Provide KYC Information:** Situations where individuals or entities actively avoid providing KYC information, a red flag for potential illicit intentions.
- Other Suspicious Activities.

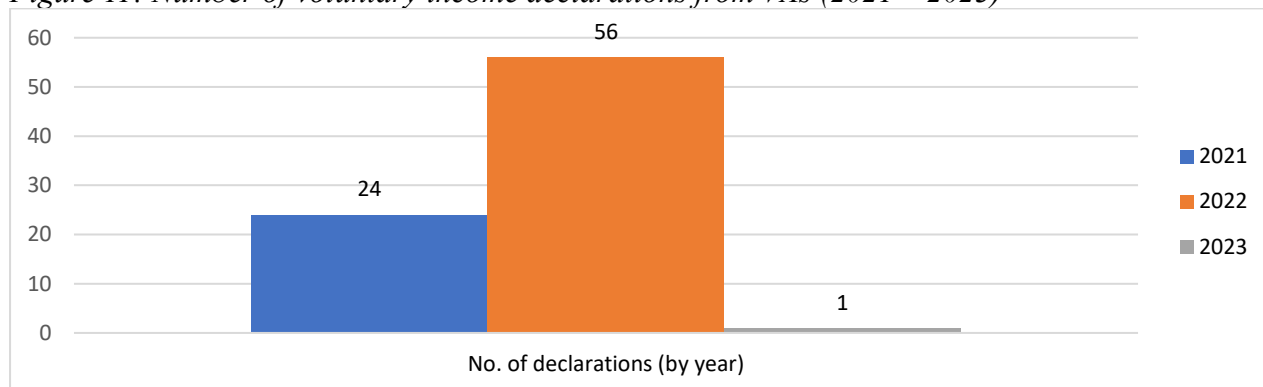
This increase in intelligence reports underscores the growing complexity and transnational nature of cryptocurrency-related financial crime, as well as the importance of international collaboration in identifying and mitigating risks associated with digital asset transactions.

### **Indicators of Tax Compliance and Potential Evasion**

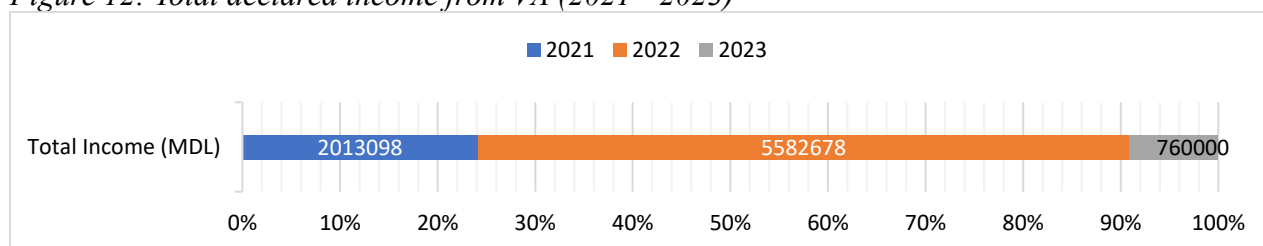
According to the survey results, it was reported that between 2021 and 2023, a total of 81 resident individuals voluntarily declared income derived from virtual assets (VAs),

amounting to a combined total of 8,355,776 MDL. Notably, as shown in *Figure 11*, there was a significant decline in the number of income declarations in 2023 compared to 2022, with the number dropping sharply from 56 declarations in 2022 in the total amount of 5,582,678 MDL to just 1 in 2023 in amount of 760,000. This dramatic decrease may be linked to the implementation of restrictive measures affecting VAs/VASPs, potentially discouraging voluntary disclosures.

*Figure 11: Number of voluntary income declarations from VAs (2021 – 2023)*



*Figure 12: Total declared income from VA (2021 - 2023)*



### **Predicate Offences associated with the VA/VASP**

According to LEAs responses, it was observed that between 2021 – 2023, scam, cybercrime, money laundering and illegal migration were among the top predicate offences associated with VAs and VASPs as shown below.

*Table 9: No. of cases associated with VA and VASPs by predicate offence, by year (2021 – 2023)*

Offence	No. of cases <sup>36</sup>		
	2021	2022	2023
Scam / Fraud	140	87	139
Money Laundering	2	3	13
Drug Trafficking	0	0	1
Illegal Migration	0	0	15
Cybercrime	7	9	7
Tax Evasion	0	1	0
Forgery	0	0	2
Illegal Political Finance	0	1	2
<b>TOTAL</b>	<b>149</b>	<b>101</b>	<b>179</b>

<sup>36</sup> Criminal cases and other type of investigations

Figure 13: Total Predicate Offences Associated with VA and VASP (2021-2023), in Percentage

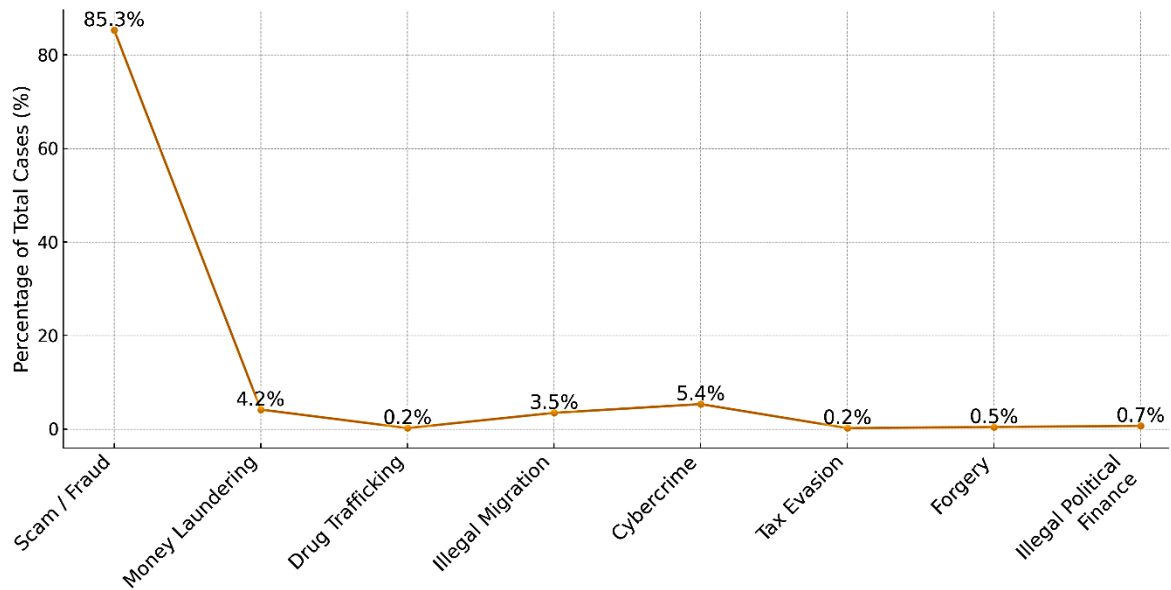
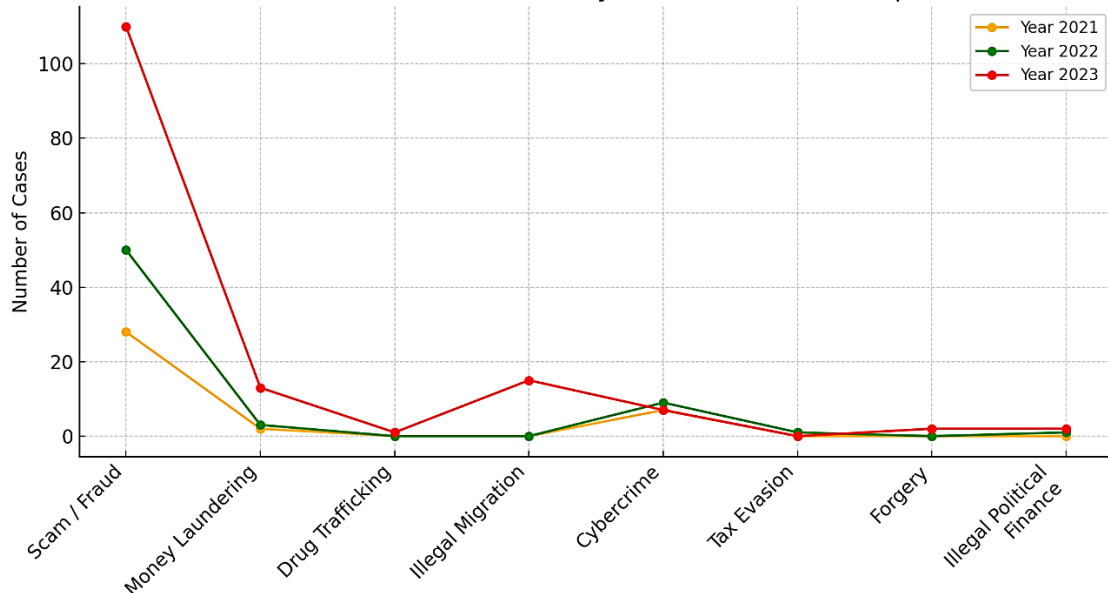


Figure 14: No. of Predicate Offences Associated with VA and VASPs (2021-2023), by Year



Referring to Table 9, Figure 13 and 14, we can see a notable rise in the number of scam cases linked to VA/VASPs between 2022 and 2023. **The data shows an increase in the number of cases from 87 in 2022 to 139 in 2023, representing a 59,8% rise.**

This accelerating trend signals that the **sector is increasingly targeted by scams**, emphasizing the importance of proactive monitoring and preventive measures by law enforcement, regulatory bodies and private stakeholders to mitigate these risks effectively.

#### The volume of seized cryptocurrency assets between 2021 and 2024

The statistical data provided by the LEAs highlights the escalating involvement in the seizure of cryptocurrencies between 2021 and 2024:

- In **2021**, a single seizure order was issued, resulting in the confiscation of **0.08 BTC** and **3715.07 USDT**, with an estimated total value of **667,053.56 MDL**.

- In **2022**, the number of orders increased to two, leading to the seizure of **0.27 BTC**, with a total estimated value of **119,305.39 MDL**.
- In **2023**, the range of virtual assets seized expanded significantly. A variety of cryptocurrencies, including **4.57 BTC**, **0.05 BUSD**, **100 ETC**, and **398 million LUNC**, were sized, with a total estimated value of **2,218,981.84 MDL**.
- In **2024**, a substantial order was issued that led to the seizure of numerous cryptocurrencies, including BNB, SHIB, PEPE, FLOKI, MANTA, AEVO, ENA, DYM, STRK and others, valued at approximately **20,963,602 MDL**.

This data demonstrates an increasing trend in the volume and variety of seized virtual assets, reflecting the growing use of cryptocurrencies in illicit activities.

Figure 15: Total Value of Seized Cryptocurrency Assets by LEAs (2021-2024)

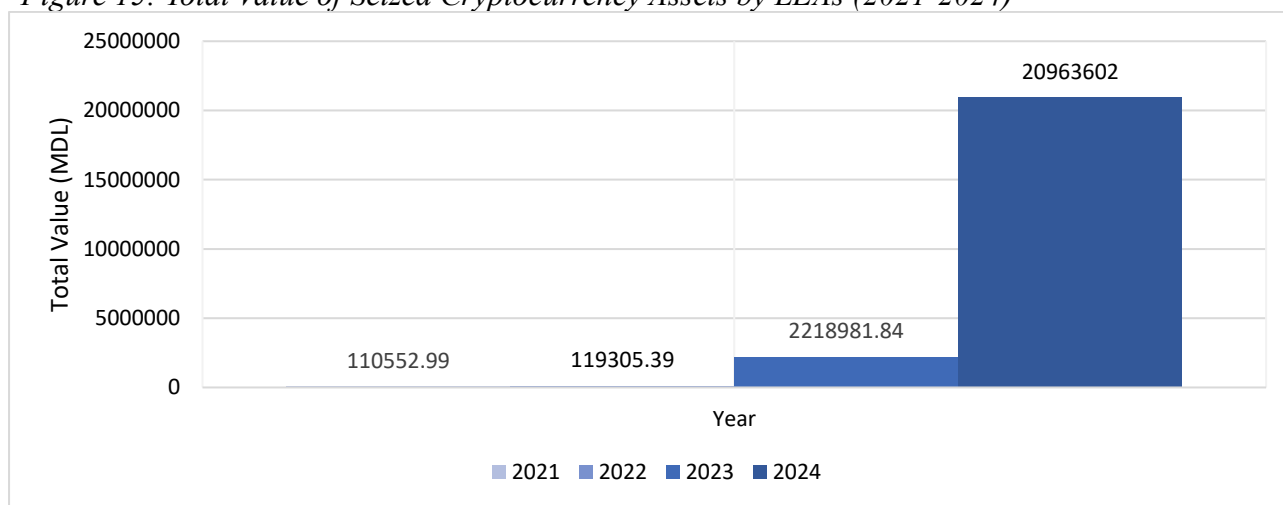


Table 10: Value of sized VAs by LEAs (2021-2024)

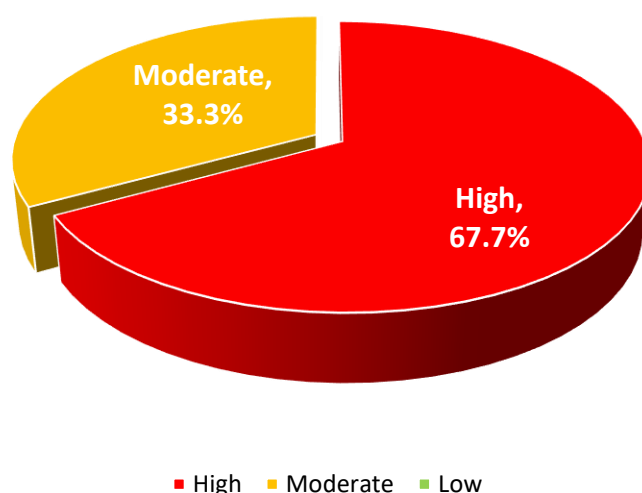
Year	No. of orders	VA type	Amount	Estimated value in local currency (MDL)
2021	1	BTC USDT	0,08 BTC 3715,07 USDT	43 847,43 66 705,56
2022	2	BTC BTC	0,19 BTC 0,08 BTC	83 827,32 35 478,07
2023	1	BTC BUSD ETC LUNA LUNC	4,57161799 BTC 0,05274375 BUSD 100,1776495 ETC 8,88810025 LUNA 3981399,529 LUNC	2 179 875,07 0,94 32543,25 147,63 6414,95
2024	1	BNB; SHIB; PEPE; FLOKI; MANTA; ALT; DYM; STRK; AEVO; ENA; BANANA; BTC; ETH; USDT; TRX; XRP; DOGE; SOL	1167784,64 USD	~20 963 602,00

It is important to note that some of the seized cryptocurrencies carry inherent risks, particularly those with strong privacy features or limited recognition in the market. Cryptocurrencies like MANTA, for instance, are designed with a focus on anonymity, making them more susceptible to being used in illicit activities such as money laundering or other financial crimes. Privacy coins, in general, often face intense scrutiny from regulators due to their potential misuse, as their ability to obfuscate transactions complicates efforts to track illegal activities.

In addition to privacy-focused coins, lesser-known cryptocurrencies such as AEVO, ENA, DYM, and STRK also pose significant risks. These tokens tend to be highly speculative, often lacking the liquidity and market trust associated with more well-known cryptocurrencies, e.g. Bitcoin Cash (BCH), Ripple (XRP), Litecoin (LTC) and others. Their relative obscurity makes them prime targets for pump-and-dump schemes, where prices are artificially inflated by speculators only to crash shortly after, leaving investors with significant losses. Furthermore, the lack of regulatory oversight surrounding these assets increases the chances of them being linked to fraudulent projects, amplifying the potential dangers for investors and authorities alike.

The following graph illustrates the perceived risk of ML/TF associated with VAs as seen by LEAs. Thus, out of the responses, 6 LEAs view the risk as high, indicating a serious threat in this area. Meanwhile, 3 LEAs consider the risk to be moderate, reflecting a more cautious but still notable concern. Notably, none of the agencies assessed the risk as low, suggesting that virtual assets are widely recognized as a source of potential vulnerability in financial crime and illicit activities.

Figure 16: LEAs Perceived Risk for ML/TF associated with VAs/VASPs (%)



The LEAs' responses indicate a growing awareness of the risks posed by virtual assets in Moldova, with an emphasis on **high-risk** perceptions. The **proposed mitigation measures emphasize the need for specialized training, technological investments, stronger national and international cooperation, and improvements to the legal framework.** Addressing these areas will help Moldova strengthen both national and regional security, equipping its law enforcement agencies with the tools and expertise necessary to counter the evolving threat landscape associated with virtual assets.

## 4.2. Regulators Responses to the VA&VASP Questionnaire Survey

### Respondents:

- National Bank of Moldova
- National Commission for Financial Markets

The results of the survey conducted with Moldova's regulators concerning VA/VASPs in the context of ML/TF NRA revealed important findings and regulatory gaps that need to be addressed.

### Summary of Findings

According to respondents, the level of knowledge regarding VA/VASPs varies between **low** and **basic**, highlighting an active process of developing advanced competencies in this field. Both regulators confirmed their participation in various training programs related to VAs and VASPs in the last 3 years, including topics such as regulatory and supervisory aspects of the virtual assets sector, blockchain technology, blockchain forensics, and virtual asset investigations.

Further, regulators agreed that there are gaps in the current legal provisions related to VAs/VASPs and provided the following comments/recommendations:

- a. **Implementation of the Markets in Crypto-Assets Regulation (MiCA<sup>37</sup>):** The MiCA Regulation is an EU legislative act that plays a crucial role in establishing a comprehensive framework for the regulation of crypto-assets. MiCA introduces clear rules for the issuance, offering, and marketing of crypto-assets and aims to protect investors while ensuring financial stability and market integrity. It covers areas such as the classification of different types of crypto-assets, the obligations of issuers, and the oversight of crypto-asset service providers. MiCA also imposes operational and governance requirements on VASPs to safeguard against financial misconduct and bolster investor confidence.
- b. **Alignment of the Republic of Moldova's AML/CFT legal framework with EU standards:** following the implementation of MiCA requirements Moldova needs to harmonize its legislation with key EU directives, including the 5th and 6th Anti-Money Laundering Directives (AMLD5<sup>38</sup> and AMLD6<sup>39</sup>). These directives mandate the registration, monitoring, and reporting obligations of VASPs, as well as the implementation of robust customer due diligence procedures to prevent misuse of virtual assets.
- c. **Define clear supervisory roles:** The regulatory framework for the VA/VASP sector must clearly define and allocate the supervisory roles of different authorities following their areas of expertise.
- d. **Addressing the deficiencies highlighted in the 2nd MONEYVAL Enhanced Follow-up Report:** Authorities must prioritize addressing all shortcomings and implementing the recommendations from the **2nd Enhanced Follow-up Report**<sup>40</sup> and Technical Compliance Re-Rating on the Republic of Moldova, adopted by the MONEYVAL Committee at its 67th Plenary Meeting in Strasbourg on 24 May 2024. Particular attention should be given to **Recommendation 15 (R.15)**, which focuses on mitigating risks associated with new technologies, including virtual assets and service providers. Ensuring compliance with R.15 is crucial for enhancing Moldova's capacity to combat ML/TF, as well as for aligning with international standards in financial regulation.

---

<sup>37</sup> <https://eur-lex.europa.eu/eli/reg/2023/1114/oj>

<sup>38</sup> <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32018L0843>

<sup>39</sup> <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024L1640>

<sup>40</sup> <https://rm.coe.int/moneyval-2024-4-md-5thround-2ndenhfur/1680b05e46>

## Public Awareness Activities

In terms of raising awareness and informing about the emerging risks associated with virtual asset activities, both regulators have taken proactive measures to inform and caution banking and non-banking financial institutions, as well as the general public. These initiatives include:

- e. **Issuing press releases on official websites:** The NBM alerted<sup>41</sup> individuals and payment service providers about the potential risks tied to virtual currency transactions. This included warnings about the possibility of engaging in illegal activities, such as ML/TF, through the use of virtual assets;
- f. **High-risk alerts to financial institutions:** In response to the heightened risks of ML/TF linked to virtual currencies, the NBM issued a formal communication on October 28, 2022. This notice informed banks and non-banking payment service providers (PSPs) about the significant risks associated with VASP transactions. It mandated the suspension of any facilitation or intermediation of payments to/from payment and electronic money accounts used by virtual currency exchange platforms, and required the termination of services for companies engaged in virtual-to-fiat currency exchange activities;
- g. **Public awareness campaigns:** Throughout 2023, the National Commission for Financial Markets (CNPF) published two informational bulletins titled “*Take Care of Your Money: CNPF Warns About the Risks of Investing Through Unauthorized Trading Platforms*”<sup>42</sup> on its official website (www.cnpf.md). These bulletins warned about the risks of investing in non-bank financial products through unauthorized institutions and highlighted the risks associated with using unauthorized financial instruments, which can lead to significant financial losses, especially for those with limited experience in the financial markets.

Regulators highlighted that certain types of VAs/VASPs present a higher risk of being exploited for money laundering and terrorism financing (ML/TF). These include:

- Anonymous cryptocurrencies (e.g., Monero, Zcash);
- Non-fungible tokens (NFTs);
- Decentralized exchanges (DEXs), such as Uniswap and PancakeSwap;
- Mixers and tumblers (e.g., Tornado Cash, Wasabi Wallet);
- Peer-to-peer trading platforms (e.g., LocalBitcoins, Paxful), which facilitate direct exchanges between users without intermediaries.

**Assessment of Risks:** Both regulators agreed that VAs/VASPs pose the **highest** risk for Moldova in terms of ML/TF.

---

<sup>41</sup> <https://www.bnm.md/ro/content/clarificarea-pozitiei-de-reglementare-si-autorizare-monedei-virtuale>  
<https://www.bnm.md/ro/content/moneda-virtuala-si-riscuri-asociate>  
<https://www.bnm.md/ro/content/banca-nationala-atentioneaza-mod-repetat-asupra-riscurilor-de-investi-criptovalute>  
<https://www.bnm.md/ro/content/bnm-avertizeaza-ca-investitiile-criptovalute-implica-riscuri-inalte>

<sup>42</sup> [https://www.cnpf.md/ro/ai-grija-de-banii-tai-cnpf-atentioneaza-despre-riscurile-investitiilor-prin-inte-6307\\_93595.html](https://www.cnpf.md/ro/ai-grija-de-banii-tai-cnpf-atentioneaza-despre-riscurile-investitiilor-prin-inte-6307_93595.html)  
[https://www.cnpf.md/ro/ai-grija-de-banii-tai-cnpf-atentioneaza-despre-riscurile-investitiilor-financiar-6307\\_93590.html](https://www.cnpf.md/ro/ai-grija-de-banii-tai-cnpf-atentioneaza-despre-riscurile-investitiilor-financiar-6307_93590.html)

### 4.3. Private Sector Responses to the VA&VASPs Surveys

#### Respondents:

- Licensed Banks (11)
- Non-bank Payment Service Providers (PSPs) (7)

To gain deeper insights into the VAs and VASPs ecosystem in Moldova and examine the potential facilitation of ML/TF, the WG expanded its questionnaire distribution to include Commercial Banks and PSPs. These questionnaires were disseminated to a total number of 18 entities, comprising 11 banks and 7 PSPs.

#### Summary

Eighty percent (**80%**) of respondents confirmed that they had **identified transactions related to VASP services during the last 3 years**. On a 1-to-3 scale (low, medium, or high), **73%** of respondents perceive the risk associated with VA/VASPs as **High**.

#### 4.3.1. Banking Sector

Following the 2023 amendments to the AML/CFT Law No. 308/2017 in Moldova, which introduced restrictions and stricter controls over virtual asset services in the country, **100% of the surveyed banks** reported that they have **opted not to establish business relationships with clients wishing to transact with foreign VASPs**.

It is important to note that under current AML/CFT provisions, transactions with authorized foreign VASPs can be conducted by resident natural persons only through special accounts opened at commercial banks or PSPs in Moldova.

According to their responses, the main reasons for this decision are:

- a. **Internal Bank Policies:** The internal policies of the banks do not allow them to offer such services.
- b. **Lack of Client Demand:** There has been no significant demand from clients for these services.
- c. **Regulatory Ambiguity:** The absence of a clear regulatory framework on virtual assets in Moldova poses challenges.
- d. **Perceived Risks:** Banks remain cautious due to the perceived risks associated with virtual asset transactions.
- e. **Requirement to implement specialized IT solutions:** Some banks reported that they are unable to provide this service to their clients because the provisions of the AML/CFT Law No. 308/2017 requires entities to adopt specialized IT solutions. These solutions are necessary to ensure enhanced monitoring of such transactions, determine the source of funds, and guarantee the traceability of transactions.

These factors, whether considered collectively or individually, have led banks to refrain from offering special accounts to clients wishing to conduct transactions with foreign VASPs. This decision reflects, on the one hand, the financial sector's cautious approach to the risks associated with VAs/VASPs, and on the other hand, the excessively strict and costly requirements linked to engaging in such transactions.

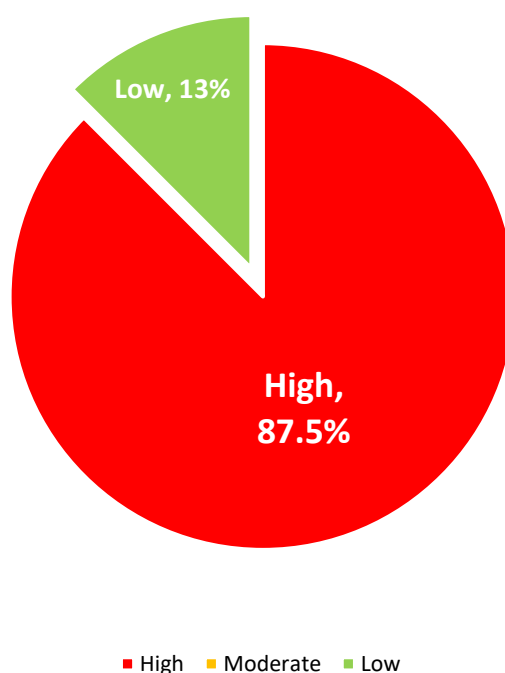
#### Internal Risk Assessment

Survey results reveal that - **45% of commercial banks** in Moldova have not yet taken specific actions to identify and evaluate the ML/TF risks associated with VAs/VASPs. In

contrast, **36%** have carried out some form of risk assessment, while **18%** reported that they are currently in the process of conducting evaluations. It is important to note that, while banks may choose not to work with virtual assets (VAs) due to their high-risk nature, it is still of utmost importance to evaluate and understand the risks associated with indirect exposure to these assets. Failing to address these risks could leave banks vulnerable to being unintentionally involved in potential ML/TF schemes that involve VAs.

In terms of risk perception, an overwhelming **87.5%** of respondents rated the risk associated with virtual assets as **"High"** on a 1-to-3 scale (low, medium, high). This significant majority reflects a cautious outlook within the banking sector, with virtual assets widely viewed as a high-risk area, particularly in light of potential vulnerabilities to ML/TF activities and the evolving regulatory framework. Also, it is important to note that 13% perceive the risk associated with VAs as low, which in a given context is a concerning factor potentially indicating that the lack of internal risk assessment left a segment of the banking sector “blind” towards their indirect exposure to VAs/VASPs and threats of abuse of their services in ML/TF schemes.

*Figure 17: Banks perception of ML/TF risks associated to VAs/VASPs (%)*



### **Technological capabilities**

The survey results show that, currently, none of the responding banks possess specialized IT solutions for blockchain analysis or AML/KYC screening for VAs/VASPs-related transactions. This situation presents significant challenges in conducting a comprehensive internal investigation into the origin of funds (SOF). It also hinders the ability to trace on-chain operations and verify the accuracy of the claims regarding customers' sources of wealth (SOW).

## Key Statistics

Figure 18: Estimated number of transactions/amounts via bank accounts to/from foreign VASPs, for the period 2021 – 2024

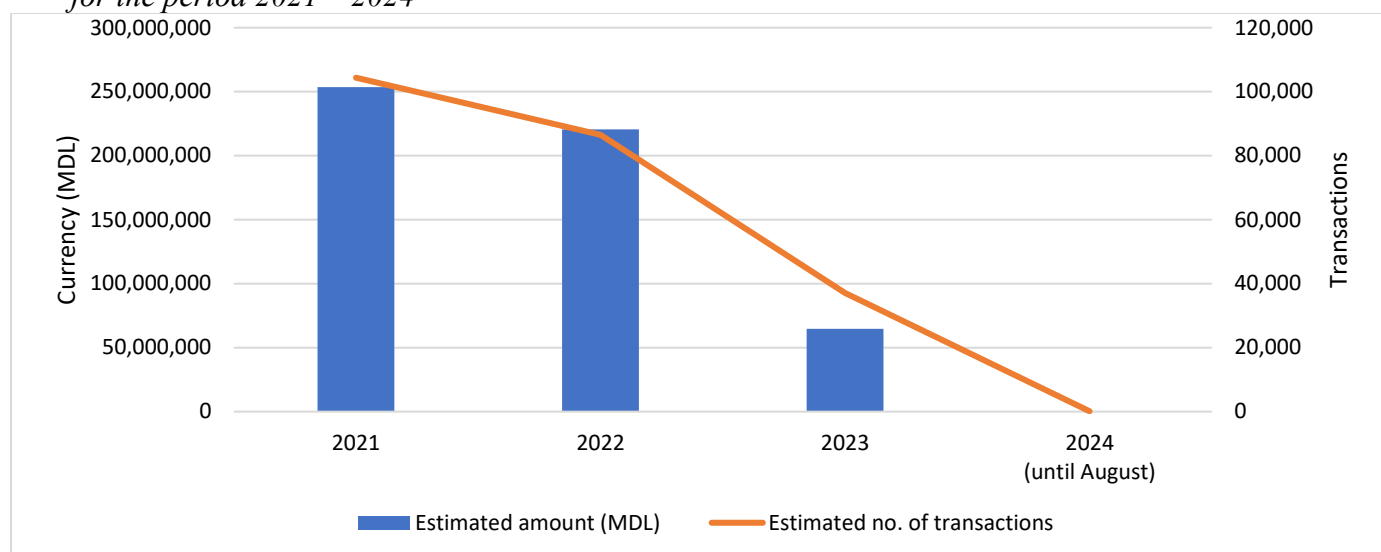


Table 11: Estimated number of transactions via bank accounts to/from foreign VASPs, for the period 2021 – 2024

Bank	Year								
	2021		2022		2023		2024		
	No. Txns	Amount (MDL)	No. Txns	Amount (MDL)	No. Txns	Amount (MDL)	No. Txns	Amount (MDL)	
<b>A</b>	776	2375855,9	966	3238610,35	111	428513,99	0	0	
<b>B</b>	1	209259,27	0	0	0	0	0	0	
<b>C</b>	875	3036177	1530	3920626	373	565135	14	23080	
<b>D</b>	425	3069103,26	551	4151333,57	74	384109,67	1	210,4	
<b>E</b>	38	190548,74	967	2534826,21	126	346455,7	0	0	
<b>F</b>	3932	5351731	4055	10710597	488	447419	33	35096	
<b>G</b>	0	0	0	0	0	0	0	0	
<b>H</b>	47969	110521982,3	23216	52964806,92	32919	57622507,64	0	0	
<b>I</b>	17144	39033962	11693	34660182	796	1311893	65	40244	
<b>J</b>	537	1496375,6	283	1235385,18	4	219,56	0	0	
<b>K</b>	32681	88225374	43227	107182218	2211	3574672	0	0	
<b>TOTAL</b>	<b>104378</b>	<b>253510369</b>	<b>86488</b>	<b>220598585,2</b>	<b>37102</b>	<b>64680925,56</b>	<b>113</b>	<b>98630,4</b>	
Inc/Dec (%)	vs 2021	-	-	-17,13%	-13%	-64,45%	-74,48%	-99,89%	-99,96%
	vs 2022	-	-	-	-	-57,00%	-70,67%	-99,86%	-99,95%
	vs 2023	-	-	-	-	-	-	-99,69%	-99,84%

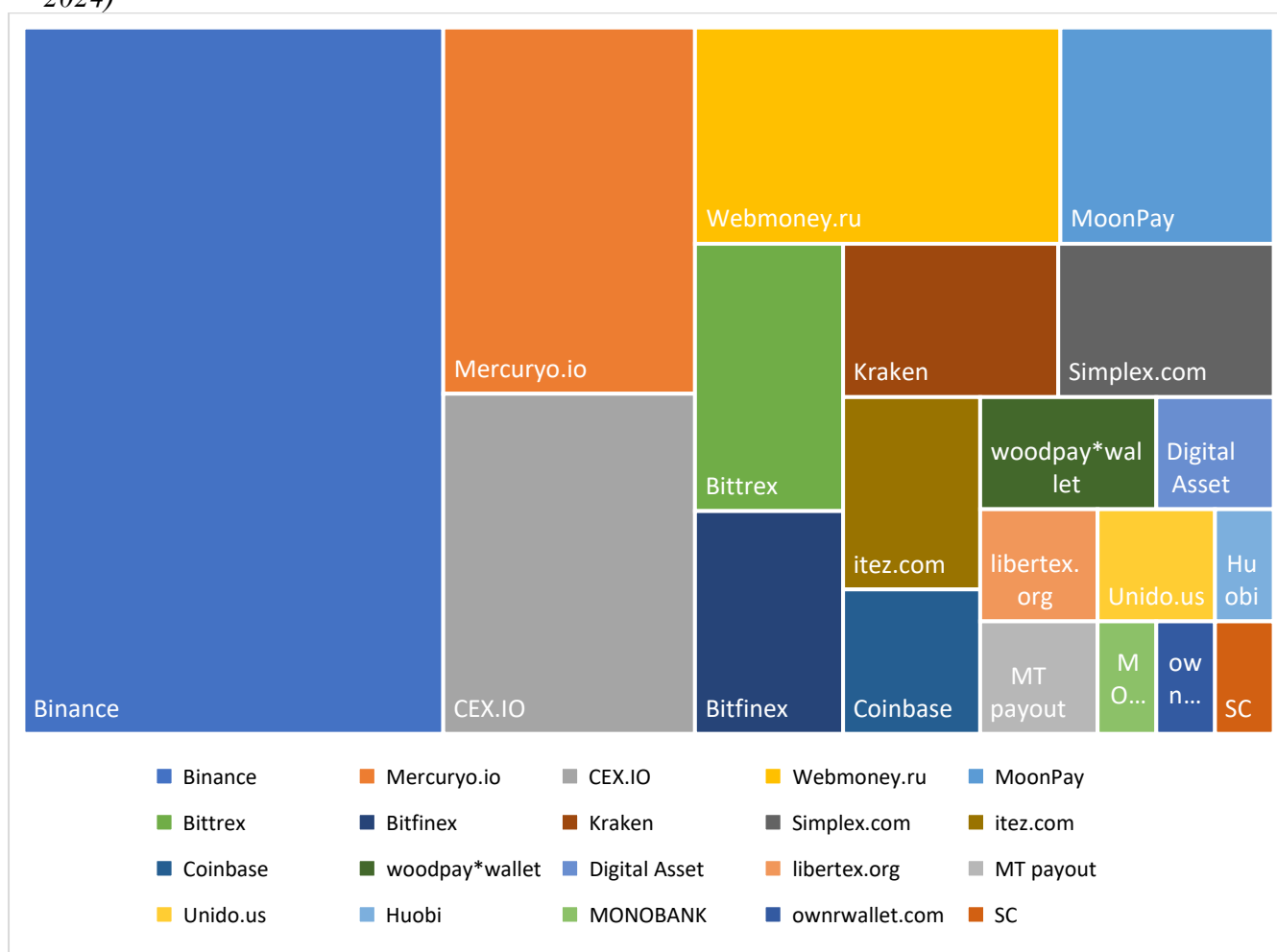
Figure 18 and Table 11 presented above highlight a notable decline in transactions conducted by bank clients in Moldova with foreign VASPs. In 2023, transaction volume dropped significantly by approximately 64.45% compared to 2021 and by 57% compared to 2022. This decline is primarily attributed to regulatory actions aimed at safeguarding the banking sector and society. Early measures included awareness campaigns and warnings issued to financial institutions, which were further reinforced by amendments to AML/CFT Law in March 2023, prohibiting VASP services within Moldova. Limited exceptions were allowed, however, for transactions conducted by resident clients, under stringent conditions, and specific limitations, and only with authorized foreign VASPs that are licensed or registered in other jurisdictions and supervised by foreign regulators.

As of September 2024, transaction volumes have decreased even further—by a striking **99.89%** in comparison to 2021. **Some banks still occasionally detect transactions involving VASPs**, largely due to the presence of newly established VASPs that either **managed to bypass early regulatory screening or were not explicitly flagged as VASPs**. These emerging providers frequently diversify their services, providing electronic payment services in addition to virtual asset services, which complicates the classification and monitoring processes. This dual functionality makes it more challenging for banks to distinguish and restrict transactions specifically linked to virtual assets, underscoring the need for refined monitoring mechanisms to better address these emerging complexities.

Although VASPs transactions through the banking sector have dramatically decreased, this shift does not necessarily indicate a positive outcome. Over the past two years, **Moldova has experienced a notable increase in informal and black-market activity related to virtual assets and VAs services**. Law enforcement data further reveal a 56.43% rise in virtual asset-related crimes in 2023 compared to the previous year. These developments suggest that while regulatory efforts have succeeded in reducing bank-facilitated VASP transactions, a comprehensive strategy is essential to address the unintended growth of unregulated markets and to strengthen both national and regional security.

Respondents indicated that, among the transactions listed in *Table 11*, the following VASPs appeared most frequently:

*Figure 19: Top Frequently Observed VASPs in Transactions Conducted via Bank Accounts (2021 - 2024)*



### 4.3.2. Non-bank Payment Service Providers (PSPs)

The same survey conducted among PSPs showed a varied approach toward VAs/VASPs activity. Unlike commercial banks, 1 out of 7 PSP respondents reported that, as of April 2024, they begun offering clients a “gateway” option to conduct transactions with foreign VASPs through dedicated (“special”) accounts, ensuring compliance with AML/CFT legal provisions. The remaining PSPs chose not to offer these services, citing reasons such as internal policies; unclear regulatory framework, and high risks associated with VAs.

The only PSP providing the possibility to open dedicated accounts reported that, in 2024, their company opened 1,595 dedicated accounts for clients interested in transferring funds to/or withdrawing from foreign VASPs. From April to August 2024, these accounts recorded a total of 3,673 transactions, with a cumulative transaction value of 2,634,387 MDL. Most transactions involved foreign VASP platforms like PAYWRX or Binance.

Table 12: Total number of transactions conducted through special accounts in relation to foreign VASPs (April – August 2024)

Month/Year	No. of transfers sent to VASPs	Amount (MDL)	No. of transfers received from VASPs	Amount (MDL)
April/2024	82	15500	40	11510
May/2024	258	146700	180	348930
June/2024	818	447480	314	174390
August/2024	1444	816947	537	672930
<b>Total</b>	<b>2602</b>	<b>1426627</b>	<b>1071</b>	<b>1207760</b>

#### Internal Risk Assessment

Survey results reveal that – **only 1 PSP** has taken specific actions to identify and evaluate the ML/TF risks associated with VAs/VASPs and 2 respondents adopted tailored policies and procedures for mitigating risks related to VAs. Similar to the banking sector, this raises concerns as PSPs may also be indirectly exposed to VAs/VASPs and may unwittingly become involved in money laundering or terrorist financing schemes while remaining unaware of the threats and vulnerabilities associated with VAs.

In terms of risk perception, an **57%** of respondents rated the risk associated with virtual assets as **"High"** on a 1-to-3 scale (low, medium, high) while other 43% indicated a “Medium” risk level.

Figure 20: Estimated number of transactions/amounts via PSPs accounts to/from foreign VASPs, for the period 2021 – 2024

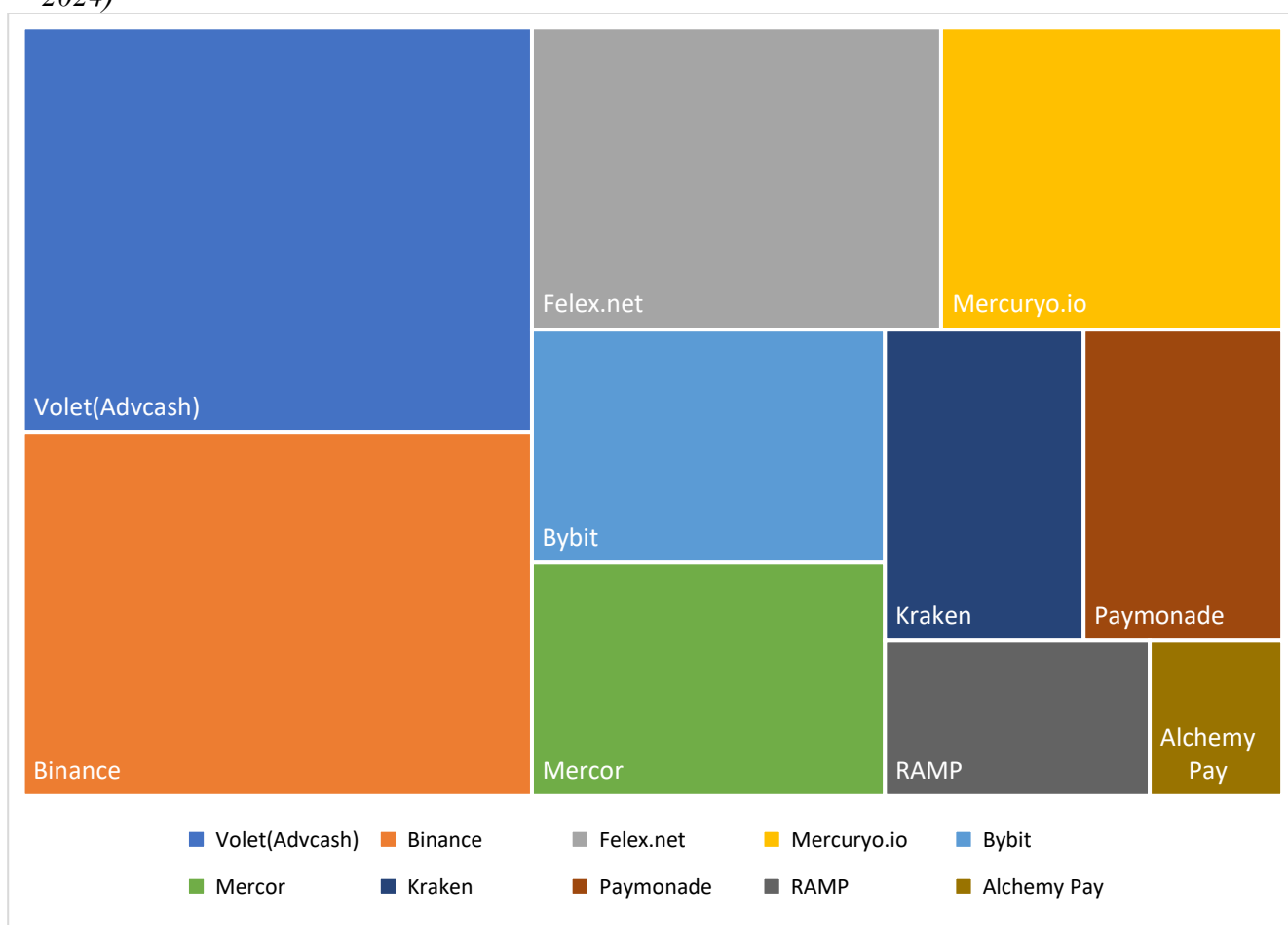


Table 13: Estimated number of transactions via PSP accounts to/from foreign VASPs,

PSP	Year								
	2021		2022		2023		2024 (until August)		
	No. Txns	Amount (MDL)	No. Txns	Amount (MDL)	No. Txns	Amount (MDL)	No. Txns	Amount (MDL)	
A	8755	7448882	16338	26044616	0	0	0	0	
B	665	973110	1108	1304950	0	0	0	0	
C	0	0	0	0	0	0	0	0	
D	33	271386	769	753007,55	342	1891986,9	853	1243678,2	
E	16	282612,7	347	1630021,66	598	6195450,14	7234	14397844	
F	0	0	0	0	0	0	0	0	
G	0	0	0	0	0	0	0	0	
<b>TOTAL</b>	<b>9469</b>	<b>8975990,7</b>	<b>18562</b>	<b>29732595,2</b>	<b>940</b>	<b>8087437,04</b>	<b>8087</b>	<b>15641522</b>	
Inc/Dec (%)	vs 2021	-	-	96,00%	231%	-90,00%	-9,89%	-14,59%	74,25%
	vs 2022	-	-	-	-	-94,93%	-72,79	-56,43	-47,39
	vs 2023	-	-	-	-	-	-	760%	93,40%

Respondents from PSPs indicated that, among the transactions listed in Table 13, the following VASPs appeared most frequently:

Figure 21: Top Frequently Observed VASPs in Transactions Conducted via PSPs Accounts (2021 -2024)



## 5. VA/VASP Interaction with Traditional Obligated Entities and Informal Economy in Moldova

The risk assessment WG analysed the interaction of VASP channels within two distinct ecosystems:

- The first is the formal, traditional obliged entity (TOE) sector, regulated and aligned with AML/CFT requirements, where compliance frameworks are established.
- The second is the informal sector, which lies outside conventional AML/CFT oversight, often lacking a developed compliance framework and corporate accountability, potentially facilitating illicit financing.

After analysing various formal TOEs against all 27 VASP channels, only two formal sectors - Banks and PSPs were found to interact directly or/and indirectly with four (4) VASP channels, as detailed in *Table 14* below.

*Table 14: Sector interaction with the VASP Channels*

27 Channels			Interaction with Banking Sector	Interaction with PSPs	Interaction with Informal Sector
<b>VIRTUAL ASSET WALLET PROVIDERS</b>	1	Hot Wallet	YES	YES	YES
	2	Cold Wallet	N/A <sup>43</sup>	N/A	YES
<b>VIRTUAL ASSET EXCHANGES</b>	3	P2P	YES	YES	YES
	4	P2B	N/A	N/A	N/A
	5	Fiat-to-Virtual	YES	YES	YES
	6	Virtual-to-Fiat	YES	YES	YES
	7	Virtual-to-Virtual	N/A	N/A	N/A
<b>VIRTUAL ASSET BROKING / PAYMENT PROCESSING</b>	8	ATMs	N/A	N/A	N/A
	9	Merchants	N/A	N/A	N/A
	10	Cards	N/A	N/A	N/A
<b>VIRTUAL ASSET MANAGEMENT PROVIDERS</b>	11	Fund Management	N/A	N/A	N/A
	12	Fund Distribution	N/A	N/A	N/A
	13	Compliance, Audit & Risk Management	N/A	N/A	N/A
<b>INITIAL COIN OFFERING (ICO) PROVIDERS</b>	14	Fiat-to-Virtual	N/A	N/A	N/A
	15	Virtual-to-Virtual	N/A	N/A	N/A
	16	Development of Product & Services	N/A	N/A	N/A
	17	Security Token Offerings (STOs)	N/A	N/A	N/A
	18	Initial Exchange Offerings (IEOs)	N/A	N/A	N/A
<b>VIRTUAL ASSET INVESTMENT PROVIDERS</b>	19	Platform Operators	N/A	N/A	N/A
	20	Custody of Assets	N/A	N/A	N/A
	21	Investment into VA related commercial activities	N/A	N/A	N/A
	22	Non-Security Tokens & Hybrid Trading Activities	N/A	N/A	N/A
	23	Stablecoins	N/A	N/A	N/A
	24	Crypto Escrow service	N/A	N/A	YES
	25	Crypto-custodian Services	N/A	N/A	N/A
<b>VALIDATORS / MINERS/ ADMINISTRATORS</b>	26	Fees	N/A	N/A	N/A
	27	New Assets	N/A	N/A	N/A

<sup>43</sup>N/A – Information Not Available

## 5.1. Formal Sector (TOE)

### 5.1.1. Banking Sector

#### Overview

The banking system in Moldova operates under Law No. 202 din 06.10.2017<sup>44</sup> (Law on banking activity) and is licensed, regulated and supervised by the NBM, which oversees and ensures that all banks adhere to Moldova's financial regulations, prudential requirements, and AML/CFT legislation.

As of September 2024,<sup>45</sup> 11 banks are licensed and active in the Moldovan banking market, 4 of them are part of international financial groups and have major foreign investors with branches in Europe. Commercial banks hold a dominant position in Moldova's financial sector, serving as the primary providers of financial services and credit across the country.

#### Interaction of the Banking Sector and the VAs/VASPs

Among the eight (6) channels identified across formal and informal sectors, four (4) channels - namely: Hot Wallet (1), P2P (3), Fiat to Virtual (5), and Virtual to Fiat (6) - have been found to either interact with or have the potential to interact with the banking sector. These channels relate to conversion and storing services typically offered by Virtual Asset Exchanges and Virtual Asset Wallet Providers.

The NRA surveys<sup>46</sup> indicate that banks in Moldova are generally hesitant to engage in activities related to VAs/VASPs. This reluctance is driven by several factors, including restrictive internal policies, an absence of a well-defined regulatory framework for VAs/VASPs, and operational limitations that impose constraints on clients, accounts, and transaction amounts per month. Additionally, the high costs of technical requirements and the perceived risks, associated with VAs transactions further contribute to this cautious approach among banks.

Nevertheless, it was noted that, in previous years, an increasing number of banking transactions (*see Table 11*) have been carried out using traditional payment instruments, such as debit and credit cards, to buy or sell virtual assets online from foreign VASPs.

As a result of the 2023 amendments to Moldova's AML/CFT Law No. 308/2017, which introduced restrictions and limitations over virtual asset services, all surveyed banks (100%) reported that they have chosen not to establish business relationships with clients seeking to transact with foreign VASPs. It is important to note that, under current AML/CFT requirements towards the resident customers who engage with VAs/VASPs, banks are required to open special bank accounts for these kinds of transactions and limit them to 50 000 MDL/per month/per client.

According to statistical data provided by banks, transaction volumes with VASPs had decreased by 99.69% as of September 2024, compared to 2023. However, some banks continue to identify occasional transactions between their clients and foreign VASPs, primarily due to newly established VASPs that either bypassed initial regulatory checks or were not distinctly flagged as VASPs. These emerging providers often expand their offerings

---

<sup>44</sup> [https://www.legis.md/cautare/getResults?doc\\_id=128663&lang=ro](https://www.legis.md/cautare/getResults?doc_id=128663&lang=ro)

<sup>45</sup> <https://www.bnm.md/en/content/financial-situation-banking-sector-first-semester-2024>

<sup>46</sup> The questionnaire survey results for Banking sector are detailed in Chapter 4, section 4.3.1.

to include both electronic payment and virtual asset services, complicating classification and monitoring efforts.

While VASP transactions through Moldova’s banking sector have significantly declined, this shift does not necessarily indicate positive progress. In fact, over the past two years, informal and black-market activities related to VA services have notably increased. Many of these VA-related transactions are disguised as routine peer-to-peer (P2P) payments within the banking sector, making it difficult for banks to identify any connection to cryptocurrency activity and exposing them to potential risks (*more details presented in Section 5.2 “Informal Sector”*).

### **Internal Risk Assessment**

As described in *Chapter 4*, survey results show that 64% of commercial banks in Moldova have not yet assessed the ML/TF risks associated with VAs/VASPs. This suggests that the majority of the banks may lack a comprehensive understanding of VAs/VASP-related risks and may not have implemented specialized monitoring practices for transactions involving virtual assets.

### **Customer Protection Issues for Banking Clients Engaging in VA/VASP Transactions**

The interaction between the banking sector and the VAs/VASPs sector presents significant customer protection challenges. While traditional banking investments are generally perceived as relatively safe, VAs present a higher risk for customers due to their distinct characteristics and lack of comprehensive regulatory oversight. This difference exposes clients to potential fraud, misrepresentation, and a lack of transparency from VASPs, which may not adhere to the same consumer protection standards as established financial institutions.

Many consumers are unfamiliar with the VAs ecosystem, leaving them susceptible to fraud, theft, and hacking. Unlike conventional banking institutions, VASPs may not provide the same level of security and financial protection, such as deposit insurance. In some cases, if funds are lost due to fraud, hacking, or platform insolvency, customers may have limited legal recourse or recovery options. The following are some of the most notable examples of major cryptocurrency exchange and DeFi platform breaches:

- **Mt. Gox (2014)**<sup>47</sup>: In one of the earliest and most notorious exchange hacks, Mt. Gox lost 850,000 BTC, worth hundreds of millions at the time, due to severe security vulnerabilities. This incident brought global attention to risks related to VASPs.
- **Coincheck (2018)**<sup>48</sup>: In January 2018, Coincheck, a Japanese exchange, suffered a massive hack with around \$530 million worth of NEM tokens stolen. This hack led Japan to tighten cryptocurrency exchange regulations.
- **KuCoin (2020)**<sup>49</sup>: In September 2020, hackers targeted KuCoin, stealing an estimated \$280 million in various cryptocurrencies.
- **Ronin Network (2022)**<sup>50</sup>: In March 2022, the Ronin Network, used by the blockchain game Axie Infinity, was hacked, resulting in a loss of over \$620 million.

---

<sup>47</sup> <https://cryptobriefing.com/what-happened-to-mt-gox-history-bitcoin-exchange/>

<sup>48</sup> <https://www.dw.com/en/cryptocurrencies-japan-sanctions-coincheck-exchange-after-massive-nem-coin-heist/a-42346789>

<sup>49</sup> <https://decrypt.co/56425/the-kucoin-hackers-successfully-took-45-million-in-crypto-says-ceo>

<sup>50</sup> <https://markets.businessinsider.com/news/currencies/crypto-heist-axie-infinity-hackers-north-korea-stole-620-million-fbi-2022-4>

This hack exposed security weaknesses in DeFi, particularly within gaming ecosystems.

- **FTX Hack (2022):**<sup>51</sup> Shortly after FTX's collapse in November 2022, the exchange was hacked for around \$400 million in various cryptocurrencies. This incident remains under investigation and compounded the issues surrounding FTX's bankruptcy.

**Price Volatility and Liquidity Risks:**<sup>52</sup> The highly volatile nature of VAs can lead to substantial financial losses, often beyond what consumers expect in traditional banking. Price fluctuations can be rapid and unpredictable, with some assets experiencing extreme devaluation within short periods. This volatility can also impact liquidity, making it difficult for customers to sell their holdings promptly without incurring significant losses, potentially leaving them with little or no recourse if they cannot recover their investments.

**AML/KYC Compliance Gaps:** VASPs, depending on the jurisdiction, may lack the rigorous AML and KYC standards that are standard in traditional banking. This gap in compliance poses a risk that customers could unintentionally engage in transactions with sanctioned or illicit entities, which may have repercussions for both consumers and financial institutions in terms of reputation and regulatory scrutiny.

### 5.1.2. PSPs

#### Overview of the PSP Sector in Moldova

The non-banking payment service providers (PSP) sector in Moldova has seen growth in recent years<sup>53</sup>, driven by increased demand for alternative financial services and digital payment solutions. This sector includes various entities offering financial services outside traditional banking, playing a significant role in promoting financial inclusion and supporting the digital economy.

The PSP sector is governed by the Law on Payment Services and Electronic Money (Law No. 114/2012<sup>54</sup>), which establishes the regulatory framework for payment services and the issuance of electronic money in Moldova. This law aligns with EU directives, providing a legal basis for licensing, operations, and oversight of non-banking payment service providers to ensure the sector's integrity and stability.

As with the case of the banking sector, the NBM acts as the main supervisory authority for PSPs. It holds responsibility for issuing licenses, ensuring compliance with regulatory standards, and conducting regular monitoring and inspections to maintain the sector's stability and prevent misuse of the sector for the ML/TF purposes.

As of October 31, 2024, there are nine (9) active PSPs in the Republic of Moldova. These include two (2) payment institutions, one (1) postal service provider, and six (6) electronic money institutions.

The non-banking payment service providers in Moldova offer a range of services that include, but are not limited to:

---

<sup>51</sup> <https://www.ibtimes.com/us-charges-3-400-million-sim-swapping-hack-linked-ftx-3723621>

<sup>52</sup> <https://academic.oup.com/rfs/article/34/6/2689/5912024>

<sup>53</sup> [https://www.bnm.md/files/Raport\\_anual.pdf](https://www.bnm.md/files/Raport_anual.pdf)

<sup>54</sup> [https://www.legis.md/cautare/getResults?doc\\_id=125243&lang=ro](https://www.legis.md/cautare/getResults?doc_id=125243&lang=ro)

- **Payment Processing:** Enabling electronic fund transfers, bill payments, and merchant transactions.
- **Electronic Money Issuance:** Providing digital wallets and prepaid cards, facilitating secure and convenient digital transactions.
- **Money Remittance Services:** Facilitating domestic and international money transfers, supporting both individuals and businesses.
- **Mobile Payments and Digital Solutions:** Offering mobile-based financial services, enhancing financial inclusion, and enabling convenient access to digital payments.

### Interaction of the PSPs Sector and the VAs/VASPs

Four (4) out of eight (6) identified channels - namely: Hot Wallet (1), P2P (3), Fiat to Virtual (5), and Virtual to Fiat (6) - have been found to either interact with or have the potential to interact with the PSP sector. These channels relate to conversion and storing services typically offered by Virtual Asset Exchanges and Virtual Asset Wallet Providers.

Table 15: Interaction of the PSP Sector and the VAs/VASPs

VASP	Channel
VIRTUAL ASSET WALLET PROVIDERS	Hot Wallet
VIRTUAL ASSET EXCHANGES	P2P
	Fiat-to-Virtual
	Virtual-to-Fiat

The survey among PSPs highlighted diverse approaches to VAs/VASP activities. Unlike the banking sector, some PSPs tend to be more open to new technologies due to higher risk appetite, responsiveness to market demand, and technological adaptability. According to the results, one of seven PSP respondents indicated that, since April 2024, they began providing clients with a “gateway” option to transact with foreign VASPs through dedicated (“special”) accounts with a monthly limit of 50,000 MDL per client to ensure AML/CFT compliance. This PSP reported opening - 1,595 special accounts (as of August 2024) and processing 3,673 transactions totalling 2,634,387 MDL, mainly with platforms such as PAYWRX and Binance. The number of transactions grew rapidly each month, surging from 124 in April to 3,673 by August, with monthly growth rates of 215% from April to May, 217% from May to June, and 76.5% from June to August. (*more details presented in Section 4.3.2 “PSPs” Survey Results*). The average growth rate across these periods is approximately 169%, suggesting exponential monthly growth.

### Internal Risk Assessment

Survey results for PSPs (*Section 4.3.2*) have shown that currently, only 1 PSP has taken specific actions to identify and evaluate the ML/TF risks associated with Vas/VASPs. This finding suggests a lack of awareness among PSPs regarding their potential direct or indirect exposure to VA/VASP-related transactions. The limited action may stem from insufficient understanding of how virtual asset activities intersect with traditional payment systems.

Given the growing integration of virtual assets into the financial ecosystem and the increasing sophistication of ML/TF schemes, this gap represents a critical vulnerability.

## 5.2. Informal Sector: The Underground Economy in Moldova

### Overview

This Section of the report describes the interaction of the informal economy (otherwise known as the shadow economy or underground economy) with the VAs/VASPs ecosystem.

In this report, we refer to the “informal sector” as economic activities that are not regulated and/or supervised by government institutions and typically fall outside formal financial and legal systems. This sector includes unregistered businesses, cash-based transactions, and employment without formal contracts. Although not all informal sector activities are illegal, this sector presents substantial risk due to its potential for misuse in ML/TF schemes

Because informal sector activities often lack transparency and oversight, they can facilitate ML/TF by allowing illicit actors to disguise or integrate illicit funds into the economy, bypassing regulatory scrutiny.

The assessment showed that the informal sector may interact **with 6 of the 27 VASP channels** as detailed in *Table 14*.

Informal sector - captures players, actors, entities, platforms and tokens that fall outside the traditional AML/CFT sector within a much less developed or non-existent AML/CFT compliance framework and with little to no corporate accountability to regulators that could open the doors to illicit financing.

Despite the limitations and reluctance from banks and PSPs to facilitate their clients’ access to VASP platforms, citizens are still able to exchange these assets either directly (peer to peer), or through the platforms using accounts they hold in foreign financial institutions.

### Interaction of the Informal Sector and the VA/VASP Ecosystem

Following the prohibition of VASP services within the country in 2023, the underground activities involving the VAs sector have rapidly expanded. Various unregulated platforms, based on the encrypted messaging, now facilitate VAs transactions that bypass regulatory oversight. These informal channels, particularly those hosted on encrypted platforms, have become major facilitators for virtual assets transactions, enabling an array of services from peer-to-peer crypto exchanges to large-scale purchases using cryptocurrencies, creating a fertile ground for money laundering and terrorist financing. With no official oversight, these channels allow for the movement of illicit funds with minimal detection or reporting requirements.

#### 5.2.1. Telegram as a Key Hub for Informal VAs Transactions and Activities

The growth of VA activities in the informal sector is particularly evident through platforms like Telegram, where numerous crypto-related chat groups/channels have emerged. These groups are relatively easy to find with simple keyword searches like "Crypto Moldova," which yields a variety of results offering a wide range of services, including cryptocurrency escrow services, buy-sell markets, and even crypto stores. These informal channels, operating outside the legal framework, serve as a hub for individuals looking to engage in cryptocurrency transactions without government oversight or the need for formal identification.

## Examples of active services found on Telegram:

**a. Crypto Escrow Services:** Platforms, such as “CryptoMD Escrow” (<https://telegra.ph/CryptoMDEscrow-04-22>), offer services for facilitating secure cryptocurrency transactions between buyers and sellers, acting as a trusted intermediary. It ensures that funds are held in a so-called “escrow” account until both parties fulfil their obligations, reducing the risk of fraud in crypto deals. While these services reduce fraud risk for users, they operate outside any official financial oversight. The anonymity provided by such informal platforms allows for the movement of significant amounts of fiat currency and cryptocurrencies with minimal traceability.



Figure 22: Crypto Escrow Service on Telegram

**b. Crypto Exchange:** Another prevalent form of VA activity in the informal sector is peer-to-peer (P2P) buy-sell crypto markets. These platforms, such as @CryptoExchangeMD\_bot on Telegram, allow individuals to exchange fiat currency for cryptocurrency (and vice versa) without involving a third-party financial institution or complying with formal regulatory checks. Individuals can post offers, negotiate terms privately, and meet at a specific location to conduct the transaction. This peer-to-peer model increases anonymity and complicates traceability, making these transactions particularly vulnerable to illicit use.

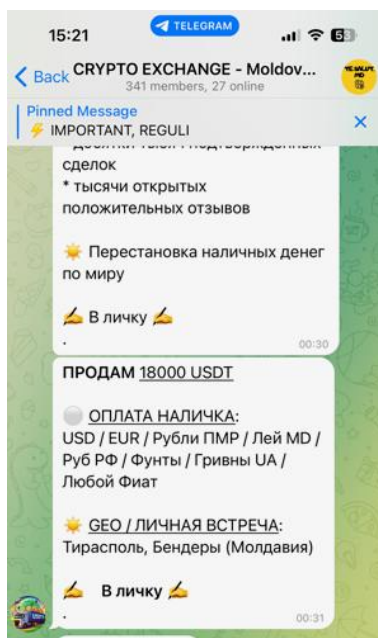
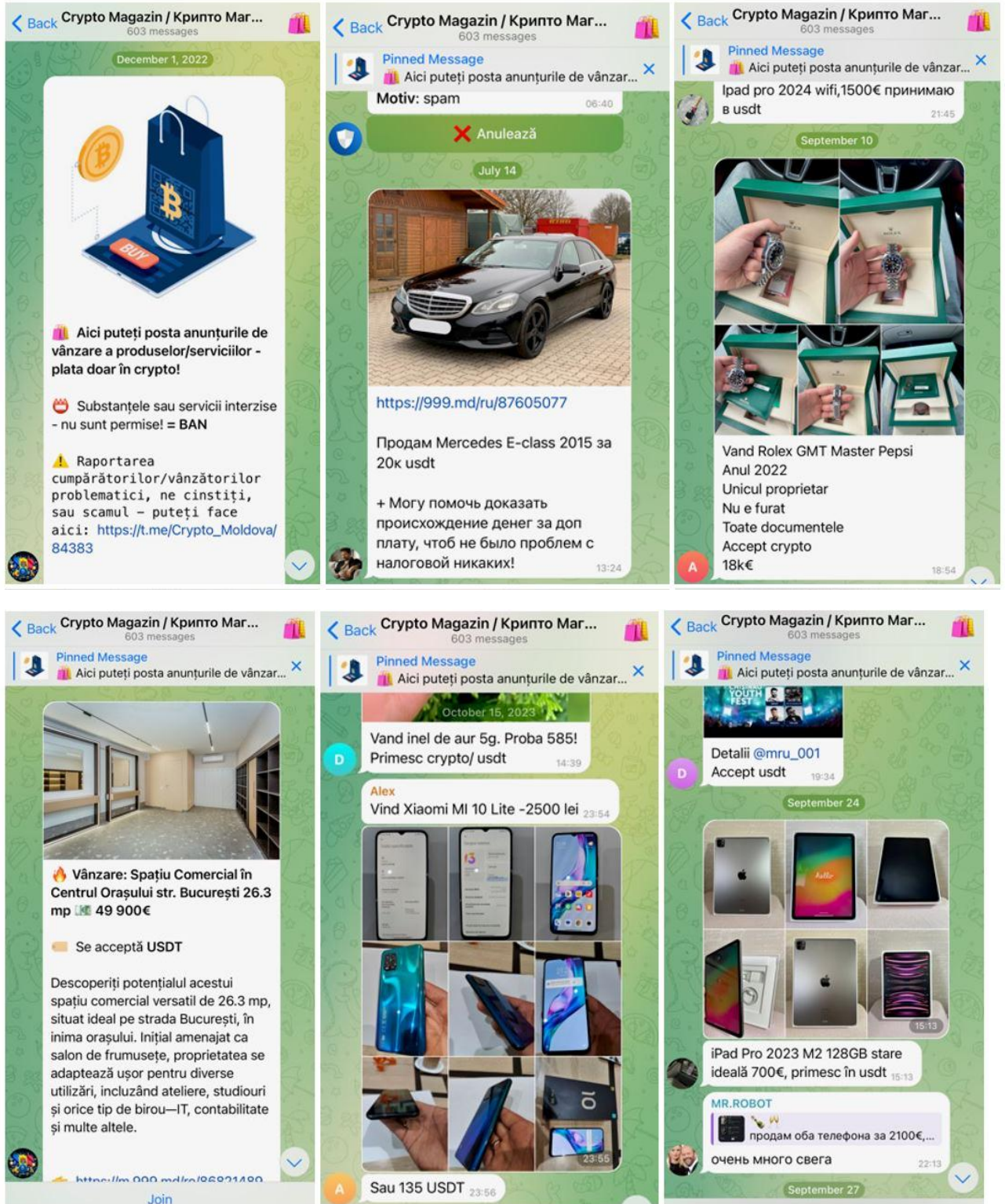


Figure 23: Crypto Exchange Chat on Telegram

**c. Crypto Stores:** An emerging trend in Moldova’s informal VA economy is the use of cryptocurrencies in online marketplaces or “crypto stores.” These stores allow users to purchase luxury goods, electronics, and even real estate using cryptocurrencies like USDT. These transactions enable the movement of large sums of money outside formal banking channels, a red flag for potential ML/TF activity. Crypto stores pose a significant challenge for authorities attempting to prevent money laundering and terrorist financing. Transactions conducted in cryptocurrencies, especially stablecoins like USDT, which are widely accepted, bypass the traditional financial system. This allows criminal actors to launder their funds by purchasing high-value assets in an unregulated environment, further complicating law enforcement’s ability to trace illicit funds.

In the following screenshots are presented several announcements with goods that can be bought on the Telegram group called - “Crypto Magazin”.

Figure 24: Crypto “Magazin” – Goods for Sale



### 5.2.2. P2P Crypto Trading Platforms

An alternative method of buying and selling cryptocurrency in Moldova, while circumventing legal restrictions, is through P2P crypto trading services provided by foreign VASPs.

For instance, Binance's P2P Trading platform allows users in regions with restrictive regulations on VAs/VASPs, like Moldova, a way to buy or sell crypto directly with other users. Binance acts as a guarantor by securing transactions through its escrow system. The fiat payments for buying or selling cryptocurrency between users are conducted locally, typically through P2P bank transfers, and card payments, making it difficult for Moldovan banks to detect any link to cryptocurrency or the Binance platform, as they do not directly interact with Binance.

In this kind of transaction, individuals typically utilize locally opened bank accounts, and the transfers between the buyers and sellers appear on their account statements as ordinary P2P payments, without any reference to cryptocurrency. The absence of clear indicators linking these transactions to crypto trading creates a significant gap in regulatory oversight. For example, a transaction might involve as little as MDL 200, with the upper limit reaching approximately MDL 100,000 per trade. These amounts can easily slip through the banking system as regular payments, bypassing any suspicion or scrutiny from financial institutions.

This lack of transparency presents a challenge for the Moldovan regulatory framework. Since financial institutions are not aware that the transactions are linked to crypto exchanges, they cannot effectively implement AML/CFT measures in these cases. As a result, individuals can exploit this loophole to facilitate ML/TF activities. The payments, which resemble standard domestic P2P transactions, can hide illicit financial flows, making it challenging for authorities to detect the true nature of the transactions and implement appropriate safeguards.

In the screenshots presented, all the steps for purchasing USDT in Moldova from a real P2P trader on Binance are outlined:

1. Selecting preferred trader (based on the type of virtual asset you want to buy, price, available volumes, and limits);
2. Entering the amount you wish to purchase;
3. Choosing the payment method and bank;
4. Placing one's order;
5. Use of the provided phone number to complete a P2P transfer via the MIA payment system to the seller's bank card;
6. Notifying the seller and providing payment confirmation.

Figure 25: Binance App Screenshot - P2P Trading

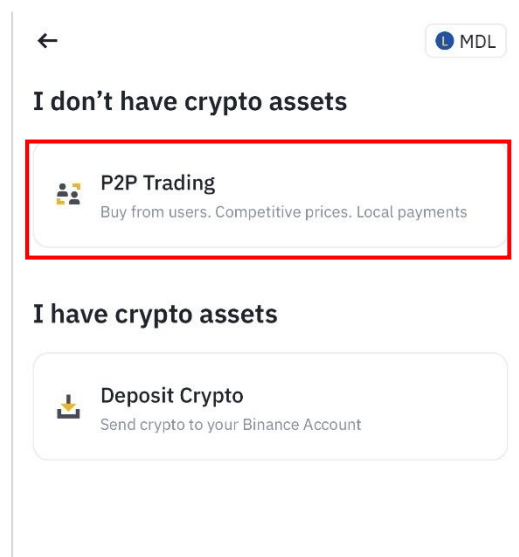
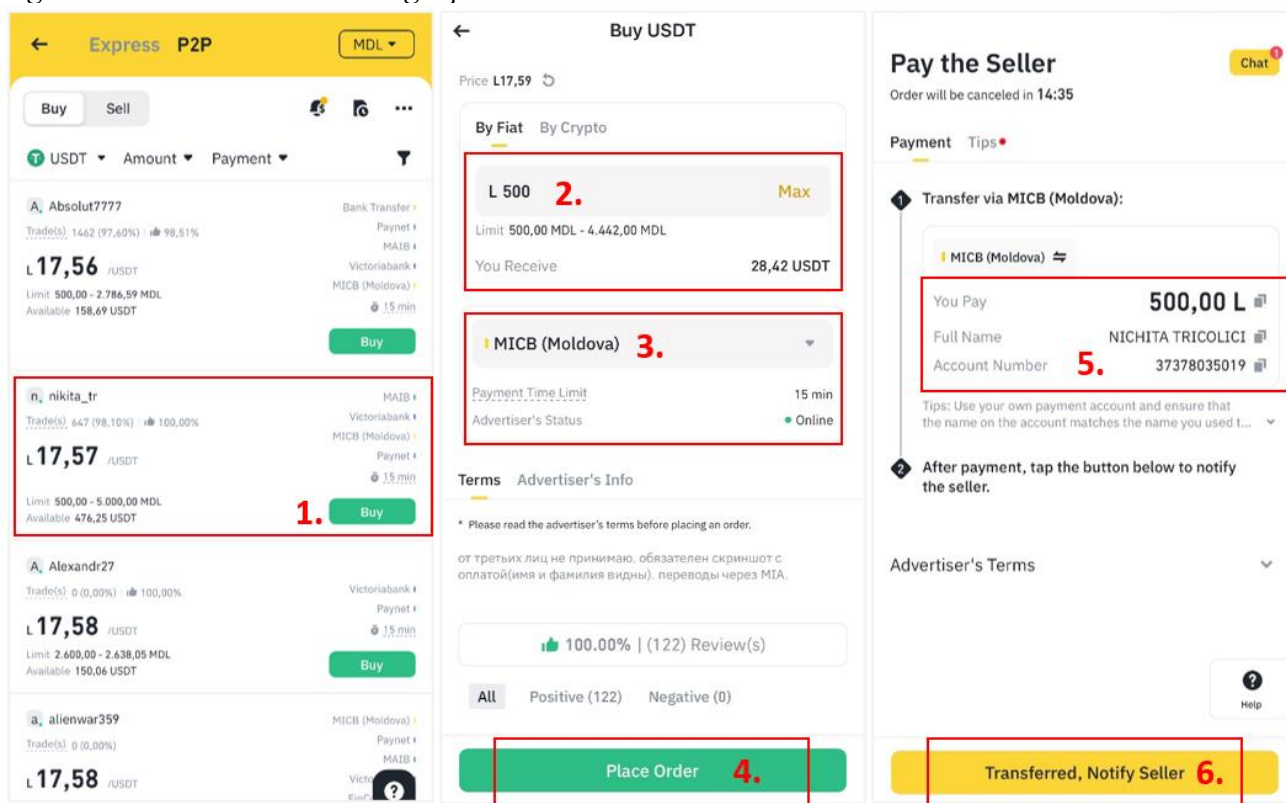


Figure 26: Binance P2P Trading Operations



### 5.2.3. Exchange Couriers (USDT-FIAT)

According to information provided by authorities, there has been a recent increase in illegal activities involving individuals offering virtual asset exchange services (primarily stablecoins such as USDT) for fiat currency, with their operational capabilities reaching significant levels. These transactions are conducted in cash with the involvement of couriers and operate outside the oversight of supervisory authorities. This phenomenon poses risks in the areas of AML/CFT as well as national security, facilitating the laundering and concealment of illicit proceeds obtained by certain criminal groups and the illegal financing of some political parties.

### 5.2.4. Transnistria Region (Mining Activity)

Another challenge facing Moldova is the mining of cryptocurrency that has been ongoing in the breakaway region of Transnistria, which has the potential to become a significant funding source for the separatist regime. Since 2018, the Transnistrian region has been increasingly active in cryptocurrency mining, following the adoption of the so-called Law for the Development of Information Technologies by the region's unconstitutional authorities. Virtual assets generated through mining activities in this unregulated environment pose risks for integration into the legal economy on the right bank of the Dniester River. These assets could potentially flow into the black market or even, in the future, be channeled through authorized VASPs and integrated into the formal economy.

The lack of regulation and oversight in Transnistria provides fertile ground for large-scale mining operations, which can operate with minimal transparency and accountability. This situation enables the separatist authorities to financially support their regime by capitalizing on energy subsidies and limited regulatory barriers to establish extensive cryptocurrency mining farms. Given the potential for these assets to cross into the formal economy, there are growing concerns about the role of such operations in financing illicit activities and

undermining economic security on both sides of the river Dniester, as Transnistria's mining operations have the potential of becoming a hub for illicit financial activity, including money laundering or sanction evasion.

## 6. Case Studies, Typologies & Emerging Trends

### 6.1. Case Studies & Typologies

#### **Case 1 - "OneCoin" Ponzi Scheme (2016)**

*The OneCoin scam involved local promoters who attracted numerous Moldovan citizens into the global Ponzi scheme by organizing public events and encouraging investments in the OneCoin cryptocurrency. Victims were persuaded to invest large sums, sometimes secured by real estate. The scheme led to criminal charges for fraud as many investors lost money in this international pyramid scheme. One of these cases is currently under review at the Chişinău Court of Appeal.<sup>55</sup>*



*OneCoin logo on the door of their office in Sofia, Bulgaria (Source: Wikimedia)*

#### **Case 2 - Laundering Drug Trafficking Proceeds (2018)**

*The case<sup>56</sup> revolves around A.R., who led a criminal group involved in drug trafficking from 2016 to July 2018. Using encrypted communication platforms, A.R. purchased and transported drugs into Moldova, distributing them through hidden locations. A.R. also facilitated the sale of drugs using electronic payment methods and laundered the proceeds through multiple bank accounts, disguising them as legitimate income.*

*In 2017-2018, A.R. purchased cryptocurrency, specifically Bitcoin, with criminal proceeds, amassing nearly 29 BTC, equivalent to over \$300,000. Despite efforts to confiscate the illicit gains, the authorities encountered challenges in seizing all of the cryptocurrency involved. The Moldovan courts sentenced A.R. to prison and confiscated his criminal assets, although several legal oversights and procedural errors, such as failure to trace all cryptocurrency and properly apply confiscation laws, were highlighted in the final judgment.*

---

<sup>55</sup> [https://instante.justice.md/ro/pigd\\_integration/pdf/4B2DB86D-9027-4C44-AA0B-9787DD33F4B5](https://instante.justice.md/ro/pigd_integration/pdf/4B2DB86D-9027-4C44-AA0B-9787DD33F4B5)  
<https://www.rise.md/articol/decriptarea-operatiunii-onecoin/>

<sup>56</sup> [https://jurisprudenta.csj.md/search\\_col\\_penal.php?id=16935](https://jurisprudenta.csj.md/search_col_penal.php?id=16935)

*This case demonstrates the increasing use of cryptocurrencies in money laundering and the need for clear legal frameworks and thorough financial investigations to combat these crimes.*

### **Case 3 - “Maxi Capital” Scam (2023)**

*According to criminal case no. 2023XXXXXX, a group of unidentified individuals, claiming to represent the company "Freedom Finance," contacted C.I., a resident of Straseni district, via "Whatsapp." Under the false pretext of providing investment services and trading assistance on the "Maxi Capital" platform using foreign currencies and cryptocurrencies, they defrauded C.I. of 547,800 MDL. After the transactions were completed, the individuals disappeared and stopped responding to C.I.'s messages.*

### **Case 4 - Fake Crypto Trading Platform (2023)**

*A group in Moldova is accused of creating a fraudulent cryptocurrency trading platform that imitated a well-known VASP. They allegedly scammed clients of nearly 4 million MDL and used the funds to purchase luxury assets. Authorities have seized assets worth 1.5 million lei, and investigations are ongoing to identify all victims.<sup>57</sup>*



*NAC, ARO, and NII officers conducting searches at a computer gaming and virtual reality venue owned by a member of the organized criminal group (Source: politia.md)*

### **Case 5 - Fake Stock Brokers (2023)**

*Between November 3 and November 14, 2023, unidentified individuals, pretending to be brokers from the company "Cripto Algoritm," deceived a person (citizen XXXXXX) by claiming they were collecting funds for stock market investments. Through this manipulation, they fraudulently obtained 166,720 MDL from the victim in multiple installments, resulting in considerable financial harm. A criminal case has been opened under Article 190 (Scam) of the Criminal Code, and it is currently under investigation.*

### **Case 6 - False Promises of Investment: Scammers Target and Defraud a 68-Year-Old Woman (2023)**

*Between April 20, 2023, and July 7, 2023, a criminal group defrauded a 68-year-old woman of 500,000 lei by posing as brokers offering investment opportunities. Using remote access software AnyDesk and TeamViewer, the suspects created a Binance account for the victim*

<sup>57</sup><https://politia.md/ro/content/prejudiciati-cu-aproape-4000000-lei-la-bursa-de-criptomonede-schema-fost-deconspirata/>

and convinced her to transfer funds from her bank cards to them. They also persuaded her to take out loans from microcredit institutions. Seven suspects were identified, and five were arrested. Investigators seized phones, bank cards, and other assets. A criminal case was opened under Article 190, paragraph (5) of the Criminal Code (Scam), and it is currently under investigation.



In the photo, police are seen carrying out arrest operations at the suspect's location (Source: politia.md)

### **Case 7 - “Deep Fake” Investment Scam (2024)**

A transnational criminal network based in Moldova and Ukraine scammed dozens of Romanians and Moldovans into investing in virtual currencies, using fake online ads featuring deepfakes of prominent public figures. Victims were promised quick, substantial returns after an initial investment of just 250 EUR. The group stole over 15 million RON in Romania and over 1 million euros in Moldova. Authorities arrested 12 individuals for scam and money laundering following large-scale raids in Moldova and Ukraine. The suspects, working from call centers, used remote access software to steal sensitive financial data from victims<sup>58</sup>.



Source: AI generated image

### **Case 8 - Illegal Migration Scheme Paid in Cryptocurrencies (2024)**

Between August 2023 and July 2024, an organized criminal group led by an individual known as "G.I." developed an illegal migration scheme, using the Republic of Moldova as a transit zone for Ukrainian citizens seeking to reach the European Union.

---

<sup>58</sup> <https://tv8.md/2024/08/08/video-investitii-de-milioane-in-platforme-false-12-persoane-retinute-in-cadrul-operatiunii-deep-fake-cum-functiona-schema/263205>

### **Modus Operandi:**

- 1. Identifying Migrants:** Through Telegram and TikTok platforms, using the account @g...I...tiktok, the group recruited Ukrainian citizens affected by the armed conflict;
- 2. Fees Charged:** The group charged fees ranging from \$2,000 to \$2,500 per person, transferred in cryptocurrency to a Binance account;
- 3. Route Organization:** Upon receiving payments, migrants were instructed to travel to Odessa, where they were provided with details about alternative routes and methods for illegally crossing the Moldovan border outside official checkpoints. Migrants were transported to the border and guided to cross illegally into Moldova. Once in Moldova, they were picked up by other group members and taken to Chişinău, where they stayed briefly;
- 4. Transit to the EU:** After their temporary stay in Moldova, the migrants were assisted in leaving the country, continuing their illegal journey to European Union states.

**During the documented period (2023-2024), the organized criminal group received cryptocurrency payments totalling 1,167,784.64479600 USDT, equivalent to \$1,167,784.64, deposited into their Binance account.**

### **Distinctive Features:**

- **High Level of Conspiracy:** The group used encrypted communications and strict role separation to avoid detection by authorities.
- **Use of Cryptocurrencies:** Payments were exclusively processed in digital currency, complicating financial transaction tracing.

## **6.2. Emerging Trends**

### **Election Interference & Cryptocurrency**

Election interference, particularly through disinformation, has become a significant global concern in the digital age. While foreign interference in elections dates back to the 19th century, advancements in technology and the proliferation of social media have dramatically increased both the frequency and ease of such activities. The democratization of information and the rise of social media platforms have opened new avenues for misinformation and disinformation campaigns, as highlighted by Russia's interference in the 2016 U.S. presidential election<sup>59</sup>.

Disinformation campaigns involve the deliberate spread of false information to influence public opinion or obscure the truth. These campaigns often utilize social media manipulation tactics, including the creation of fake accounts, theft of account credentials, and targeted analytics to amplify disinformation and sow division, especially during election periods<sup>60</sup>.

---

<sup>59</sup> <https://il.boell.org/en/2022/01/25/global-story-election-interference>

<sup>60</sup> <https://freedomhouse.org/report/freedom-on-the-net/2019/the-crisis-of-social-media/digital-election-interference>



*Photo symbol. Source: The Cyber Express<sup>61</sup>*

### **Indicators of Russian Interference in Moldova**

Recent reports indicate that Russia has employed various tactics to interfere in Moldova's recent electoral processes, including the use of cryptocurrencies to fund pro-Russian activities.

In October 2024, Moldovan LEAs uncovered a significant illegal financing scheme<sup>62</sup> aimed at influencing the country's presidential election and referendum on European Union membership. The investigation revealed that over 130,000 Moldovan citizens received funds exceeding \$15 million originating from Russian sources, channeled specifically through Promsvyazbank, a Russian bank subject to international sanctions. These funds were then routed through various obfuscation methods, including cryptocurrency platforms, before reaching beneficiaries in Moldova via peer-to-peer (P2P) transfers.

The group members **used the Bybit platform to convert Russian rubles into cryptocurrencies**, facilitating the swift and discreet transfer of funds across borders. The cryptocurrencies were later exchanged for cash in Moldova, financing various illegal activities such as voter bribery and the organization of protests. This approach circumvented traditional banking systems and financial monitoring mechanisms, complicating the detection and tracking of illicit financial flows.<sup>63</sup>

The scheme was orchestrated by individuals linked to fugitive politician Ilan Shor, who fled to Russia following a prison sentence in Moldova. The operation involved a hierarchical network comprising 130 territorial leaders, nearly 2,000 sector leaders, over 50,000

---

<sup>61</sup> <https://thecyberexpress.com/russia-election-interference-plot-moldova/>

<sup>62</sup> <https://radiochisinau.md/rusia-a-transferat-in-luna-septembrie-15-mln-de-dolari-pentru-coruperea-electoral-a-130-de-mii-de-cetateni-din-republica-moldova---201879.html>

<sup>63</sup> <https://nordnews.md/alegeri-old/alegeri-locale/exclusiv-lichefiatorul-gruparii-sor-din-floresti-dezvaluie-cum-introducea-banii-din-rusia/>

activists, and more than 70,000 sympathizers. These individuals were allegedly bribed to vote for specific candidates and to oppose the EU membership referendum<sup>64</sup>.

Authorities conducted extensive investigations, including over 100 searches, leading to the detention of several individuals. The funds were reportedly distributed through a sophisticated system involving Telegram bots and other covert methods.

## 7. The Risk Assessment

### 7.1. ML/TF Threat Assessment

According to the FATF guidance on National ML and TF risk assessment<sup>65</sup>, threat is a person or group of people, object or activity with the potential to cause harm to, for example, the state, society, or the economy. In the ML/TF context this includes criminals, terrorist groups and their facilitators, their funds, as well as past, present and future ML or TF activities. Therefore, the threat is described as one of the factors related to risk.

This section provides an analysis of threats facing both VAs and VASPs, examining relevant intermediate and input variables from domestic and international perspectives across various VAs and VASPs.

The threat ratings in the below table portray general tendencies across all 6 VASP channels related to VA Wallet Providers, VA Exchanges and VA Investment Providers.

Table 16: ML/TF Threat Ratings by Input Variables

Intermediary variables	Input variables (Risk Elements)	Threat (Overview across 6 Channels)
<b>VA Nature and Profile</b>	Anonymity/pseudonymity	Very High
	P2P Cross-Border Transfer and Portability	High
	Absence of face-to-face contact	High
	Traceability	High
	Speed of Transfer	High
<b>Accessibility to Criminal</b>	Illegal mining	Very High
	Collection of funds	High
	Transfer of funds	High
	Dark Web Access	Very High
	Expenditure of funds	Medium
<b>Source of funding VA</b>	Bank or card as source of funding VA	Medium
	Cash transfers, valuable in-kind goods	High
	Use of virtual currency “stablecoins”	High
<b>Operational features of VA</b>	Regulated	N/A
	Unregulated	Medium
	Centralized Environment	Low
	Decentralized Environments	High
<b>Ease of criminality</b>	Tax evasion	High
	Terrorist financing	Medium
	Disguising criminal proceeds to VA not regulated	High
	Trace and Seize Difficulty	High

<sup>64</sup> <https://politia.md/ro/content/noi-metode-de-finantare-ilegala-unor-partide-politice-documentate-de-pa-si-ini>  
<https://politia.md/ro/content/igp-pesto-20-de-perchezitii-efectuate-si-2-persoane-retinute-temeiul-mai-multor-cauze-penale>

<sup>65</sup> <https://www.fatf-gafi.org/en/publications/Methodsandtrends/Nationalmoneylaunderingandterroristfinancingriskassessment.html>

	Circumvent Exchange Control	High
<b>Economic Impact</b>	Underground economy – Impact on the country's monetary policy	High
	Allow full integration with the financial services market	Medium
	Prohibit any interaction between the financial institutions and the VC market	High

Table 17: Assessed VASP Channels

VASPs	Types of Services	Sub-type (Channel)
<b>VIRTUAL ASSET WALLET PROVIDERS</b>	<b>Custodial Services</b>	Hot Wallet
	<b>Non-Custodial Services</b>	Cold Wallet
<b>VIRTUAL ASSET EXCHANGES</b>	<b>Transfer Services</b>	P2P
	<b>Conversion Services</b>	Fiat-to-Virtual Virtual-to-Fiat
<b>VIRTUAL ASSET INVESTMENT PROVIDERS</b>	<b>Emerging Products</b>	Crypto Escrow Service

### 7.1.1. VA Nature and Profile

Figure 27: VA Nature and Profile – Summary of different risk elements

Very High	• Anonymity/pseudonymity
High	• P2P Cross-Border Transfer and Portability
High	• Absence of face-to-face contact
High	• Traceability
High	• Speed of Transfer

**a. Anonymity and pseudonymity (Very High)** – The inherent risk of anonymity and pseudonymity in VAs operations is a significant concern, especially within the context of the Republic of Moldova. Moldova lacks specific legislation and supervision over VASPs, which creates substantial threats of ML/TF. Despite recent amendments to the AML/CFT Law No. 308/2017, the regulatory scope remains limited, primarily focusing on prohibiting domestic VASP activities and limiting interactions with authorized foreign VASPs under stringent conditions, such as only allowing the transactions related to VAs via “special” accounts. Moldovan banks’ reluctance to facilitate transactions involving foreign VASPs shifts the activity to less-regulated spaces, where anonymity and pseudonymity risks are exacerbated.

**b. Peer-to-Peer cross-border transfer and portability (High)** – VAs inherently possess cross-border capabilities, enabling swift, anonymous, and largely unregulated transactions across international boundaries. This characteristic, when paired with Moldova's limited regulatory infrastructure and lack of comprehensive oversight, significantly elevates the risk of ML/TF. The decentralized and global nature of VAs allows criminal actors, including those from high-risk jurisdictions, to bypass traditional financial channels and evade scrutiny. Moldova’s financial system is particularly exposed to these risks due to the absence of active, domestically regulated VASPs and direct regulatory supervision over foreign VASP activities within its borders.

The 2023 Geography of Cryptocurrency Report by Chainalysis ranks Moldova 77th out of 155 countries in peer-to-peer exchange trade volumes<sup>66</sup>, indicating a P2P activity that should not be neglected. **This volume of cross-border P2P transactions increases ML/TF risks and creates opportunities for illegal activities, such as ransomware, to proliferate within these decentralized transfers.** The potential for P2P transfers to go undetected remains particularly high, as these transactions often occur on decentralized platforms beyond Moldova’s jurisdictional reach. Moreover, the informal access Moldovan users have to VAs through foreign VASPs complicates regulatory enforcement, making it difficult to track, monitor, and regulate P2P VA transactions effectively.

**c. Absence of face-to-face control (High)** - The risk level associated with the absence of face-to-face control in VA/VASPs is assessed as high in Moldova. This assessment is based on several key factors, including the inherent anonymity or pseudonymity of VA transactions. This risk is especially pronounced in peer-to-peer (P2P) exchanges, which operate with minimal regulatory oversight, making it difficult to trace or verify the identities of parties involved. Such an environment creates a substantial threat of facilitating transactions with high-risk individuals or entities, as well as enabling anonymous transfers and third-party funding through virtual exchanges.

In Moldova, this risk is further exacerbated by the large volume of VA transactions conducted within the “underground” economy, which bypasses formal financial systems and often evades regulatory scrutiny. This unregulated activity makes it challenging for authorities to monitor transactions or enforce KYC standards, leaving significant gaps in oversight. Consequently, VA-related activities in Moldova represent a growing concern for ML/TF threat.

**d. Traceability (High)** – Moldova's prohibition on domestic VASP operations and the lack of a corresponding ‘travel rule’ regulation means that VAs remain accessible primarily through foreign VASPs or unregulated exchanges, where compliance with Moldova’s ML/TF standards cannot be enforced. Although blockchain technology allows for some transaction transparency, the prohibition of VASP services within the country and the absence of the ‘travel rule’ implementation prevents identifying the true identity of transaction parties effectively. **This absence of the ‘travel rule’, along with the limited regulatory oversight and technological resources, complicates Moldova's ability to track and monitor virtual asset transactions adequately.**

Moldova’s proximity to conflict zones adds further risk, exposing it to regional threats such as illicit financing and organized crime. VAs amplify these risks through cross-border, pseudonymous transactions, which are difficult to trace without international cooperation. The lack of traceability tools compounds this challenge, as cross-jurisdictional activities require sophisticated systems for tracking flows across multiple regions.

Furthermore, Moldova’s LEAs lack consistent access to advanced blockchain forensics and expertise (*as highlighted in the Section 4.1.*), which constrains their ability to analyze transaction flows effectively. This limitation reduces the capacity to trace the origin and

---

<sup>66</sup> <https://www.chainalysis.com/wp-content/uploads/2024/06/the-2023-geography-of-cryptocurrency-report-release.pdf>

movement of funds, especially as obfuscation methods like privacy-enhanced wallets and DeFi protocols become increasingly common.

**e. Speed of transfer (High)** – The rapid transaction speeds enabled by blockchain technology allow for near-instantaneous movement of funds across borders, circumventing traditional financial oversight mechanisms. This ease of transferring large volumes of value without significant delays makes it attractive for criminals seeking to quickly relocate illicit funds. For Moldova, where the regulatory framework and technological tools for monitoring VAs remain limited, the high speed of VA transactions could hinder authorities' ability to detect and trace suspicious criminal activities.

### 7.1.2. Accessibility to Criminal

Figure 28: Accessibility to Criminal – Summary of risk elements

Very High	• Illegal mining
High	• Collection of funds
High	• Transfer of funds
Very High	• Dark Web Access
Medium	• Expenditure of funds

**a. Illegal mining (Very High)** - The mining of cryptocurrencies in the breakaway region of Transnistria presents a very high risk to the Republic of Moldova's national security. Since 2018, Transnistria has become increasingly active in cryptocurrency mining due to energy subsidies and minimal regulatory barriers established by its unconstitutional authorities. This environment allows large-scale mining operations to function with little transparency or accountability.

The virtual assets generated in this separatist region pose significant risks when they potentially flow into the black market or are channeled through authorized VASPs into the formal economy. Such integration can facilitate ML/TF activities by disguising the illicit origins of these assets. The lack of oversight makes it challenging to monitor these funds, increasing the likelihood of them being used to finance illicit activities and undermining economic security on both sides of the Dniester River.

Taking into account the combined impact of unregulated mining activities, the capacity of these operations to fund illicit operations, and the relative ease with which illegally obtained assets can flow into the formal economy, the risk level associated with *illicit mining* is deemed to be very high.

**b. Collection of funds (High)** - VAs pose an inherent risk due to their potential use in terrorist financing. Despite representing a small share of illicit transactions in the cryptocurrency ecosystem, as noted in the 2024 Chainalysis report<sup>67</sup>, their potential use by terrorist organizations is a growing area of concern. The ability of these assets to facilitate anonymous transfers makes them attractive for illicit financing, particularly among groups seeking to evade traditional financial surveillance mechanisms. The unregulated nature of

<sup>67</sup> <https://www.chainalysis.com/wp-content/uploads/2024/06/the-2024-crypto-crime-report-release.pdf>

VAs increases their appeal for funding terrorism discreetly, allowing supporters to contribute funds without exposing their identities.

Certain types of virtual assets, particularly those prioritizing privacy and anonymity, can be exploited by terrorist groups due to their decentralized nature and lack of regulation. Privacy-focused virtual assets, like Monero, and unregulated exchanges, are particularly attractive. Such assets allow terrorist groups to collect and transfer funds without revealing participants' identities, enhancing their capability to raise funds without drawing attention. Moldova's geographic proximity to conflict zones, combined with internal vulnerabilities, particularly those related to the Transnistrian region, heightens the risk of ML/TF activities facilitated through virtual assets.

**c. Transfer of Funds (High)** - Given the borderless nature of most VAs and the absence of a regulatory framework in Moldova, the risk of fund transfers to and from unregulated jurisdictions is high. The anonymity of some identified VAs, combined with ease of transferability, makes them accessible and attractive for exploitation by criminals.

Although no stablecoins are issued locally, internationally accessible dollar-backed stablecoins are frequently used for fund transfers within Moldova. This raises concerns, as stablecoins, often backed by fiat reserves, may create a loophole where "dirty money" could support transactions without sufficient oversight. This risk is heightened by unlicensed stablecoin operators in other jurisdictions, which often operate under minimal regulatory scrutiny, furthering their potential misuse.

**d. Dark Web Access (Very High)** – The dark web provides a semi-anonymous trading environment, where transactions are difficult to trace and link to real identities. With VAs as the preferred payment medium, users benefit from the combined anonymity of cryptocurrency and encrypted networks, amplifying the challenge for law enforcement to monitor illegal financial flows.

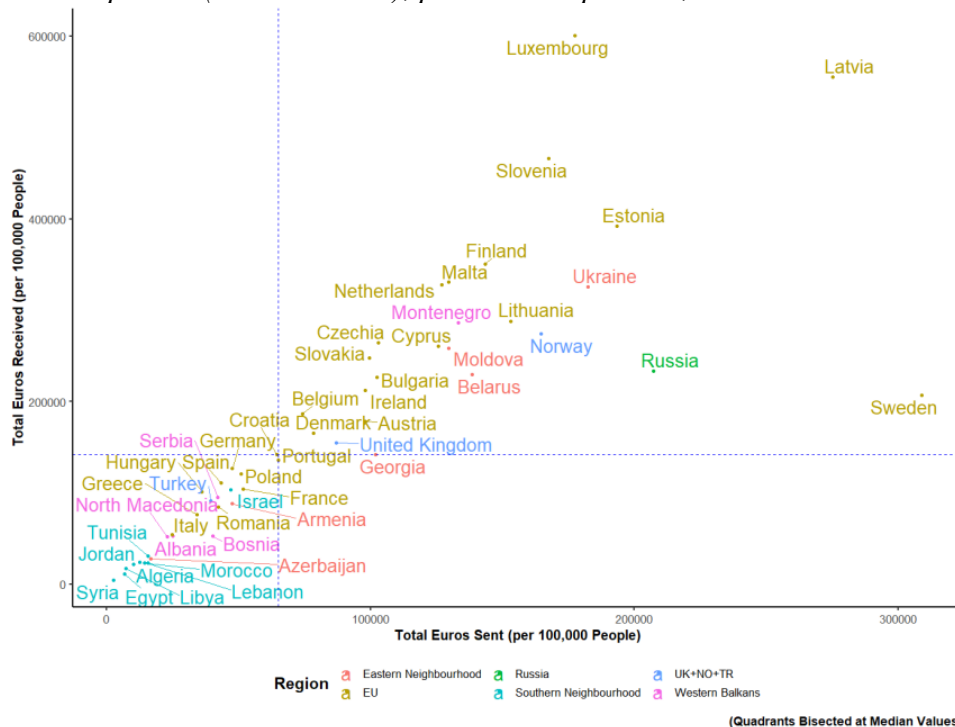
Several examples highlight the accessibility and attractiveness of dark web channels for illegal activities. For example, the seizure of \$3.36 billion in Bitcoin by the U.S. Department of Justice in 2022 from the Silk Road darknet market<sup>68</sup> illustrates the dark web's reliance on virtual assets for illicit transactions. Furthermore, the 2023 European Monitoring Centre for Drugs and Drug Addiction (EMCDDA) Report ranked Moldova as the second-highest in darknet revenue among Eastern Neighborhood countries, with a total darknet market engagement (sent, received) estimated at approximately 387,770 EUR (per 100 000 persons) between April 2019 and June 2021<sup>69</sup>. This statistic underscores Moldova's heightened exposure to dark web-enabled financial crimes, particularly susceptible due to limited regulation and significant proximity to high-risk areas, which increases both accessibility and attraction to dark web markets.

---

<sup>68</sup> <https://www.occrp.org/en/news/us-doj-announces-historic-336b-crypto-seizure>

<sup>69</sup> [https://www.euda.europa.eu/drugs-library/cryptocurrencies-and-drugs-analysis-cryptocurrency-use-darknet-markets-eu-and-neighbouring-countries\\_en](https://www.euda.europa.eu/drugs-library/cryptocurrencies-and-drugs-analysis-cryptocurrency-use-darknet-markets-eu-and-neighbouring-countries_en)

Figure 29: Total Exposure (Sent/Received), per 100 000 persons, in Dark Web Market



**e. Expenditure of funds (Medium)** - The expenditure of funds within the VA ecosystems is evaluated as medium due to the sector's accessibility to illicit actors. This highlights the potential for criminals to incorporate illicit proceeds into VA ecosystems, facilitated by the absence of a comprehensive regulatory framework and the innovation-focused nature of VA markets. This variable is significant because once illicit funds enter the virtual asset ecosystem, criminals can leverage these assets for expenditure in both legitimate and illicit transactions, obscuring the origin of funds. The ease of converting virtual assets into fiat currency or other goods and services further complicates tracking. Although Moldova's formal sector imposes some limitations on transactions with foreign VASPs, many global VASP entities issue crypto-linked cards, such as those backed by VISA or Mastercard. These cards enable seamless spending across the globe, including within Moldova, bypassing existing limitations for VA-related transactions. This high level of accessibility and flexibility in expenditure creates a favorable environment for laundering and misuse, elevating the risk level.

### 7.1.3. Source of Funding VA

Figure 30: Source of Funding – Summary of risk elements

Medium	• Bank or card as source of funding VA
High	• Cash transfers, valuable in-kind goods
High	• Use of virtual currency - "stablecoins"

**a. Bank or card as source of funding VA (Medium)** – In the Republic of Moldova, the risk level associated with funding VAs through bank or card sources is relatively medium-low, largely due to legislative restrictions that currently prohibit local VASPs and place strict conditions on the activities of foreign VASPs within the country. Moldovan banks and PSPs are subject to regulatory requirements that significantly limit clients' ability to deposit or withdraw funds to or from foreign VASP wallets, thereby decreasing the attractiveness of

these channels for illicit funding activities. Despite lower overall risk, Moldova still carries residual risks, especially from potential misrepresentation of transaction purposes by bank accountholders (*as explained in Section 5.2.2. P2p Crypto Trading*). Without local VA regulatory frameworks, foreign VASP activity poses some residual risks of undetected criminal activities, including through decentralized wallets. However, Moldova’s limited VAMarket and the absence of local VASPs contribute to a restricted risk exposure.

**b. Cash transfers, valuable in-kind goods (High)** – The prohibition on VASP services within Moldova, implemented in 2023, has inadvertently fueled a rapid expansion of underground activities related to VAs. Unregulated platforms, especially those operating on encrypted communication channels, have become increasingly prevalent, facilitating transactions that are largely invisible to regulatory authorities. This informal market allows for a range of activities, including the purchase of goods and services through cryptocurrencies, creating a conducive environment for illicit financial activities such as ML/TF (*more details in Section 5.2*).

The reliance on cash and in-kind valuables as sources of funding for VA transactions further exacerbates the risk, given these methods' lack of traceability. The increase in illegal activities involving VA exchanges—predominantly Tether (USDT) for fiat currency—is significant, with transactions reaching substantial amounts. Such exchanges often operate through trusted intermediaries or couriers who transport funds, bypassing supervisory controls. This operational model provides anonymity to the parties involved, making it difficult for authorities to monitor or intervene effectively (*mentioned in Section 5.3*).

**c. Use of virtual currency (“stablecoins”) (High)** – Despite the absence of stablecoin issuance, launch, or formal use in Moldova due to restrictive legislation and a lack of domestic VASPs, there is an observable threat from the underground channels where stablecoins and privacy-focused VAs may be acquired for illicit purposes.

The 2024 data on seized cryptocurrencies (referenced in Table xx.) reveals the presence of stablecoins and other VAs with strong privacy characteristics. These findings underscore a dual risk: stablecoins, due to their price stability and global usage, can facilitate low-profile transfers, while privacy-enhanced VAs that employ “zero-proof” technology can offer high degree of anonymity. This combination increases the risk of criminal exploitation of VAs/VASPs in Moldova, particularly given the limited regulatory reach and monitoring capacity over these types of virtual assets. Therefore, the use of VAs should be assessed as carrying a high risk for ML/TF activities in the absence of stringent regulatory and monitoring mechanisms.

#### 7.1.4. Operational Features of VA

Figure 31: Operational Features of VA – Summary of risk elements

N/A	• Regulated
Medium	• Unregulated
Low	• Centralized Environment
High	• Decentralized Environments

**a. Regulated (Not Applicable)** – Currently, Moldova does not have a regulatory framework for VAs, making this section of the criteria inapplicable.

**b. Unregulated (Medium)** – Moldova's regulatory landscape is largely restrictive, primarily focusing on prohibiting domestic VASP activities and limiting interactions with authorized foreign VASPs under stringent conditions. The current legislative environment relies primarily on the general provisions of existing AML/CFT legal framework (Law No. 308/2017), which have been updated to address the growing relevance of virtual assets. However, there is no specific regulation, licensing regime or dedicated supervision for VASPs.

**c. Centralized Environment (Low)** – The centralized environment implies that transactions occur within a contained ecosystem, such as a crypto exchange or a financial node linked to the traditional financial system, where activities are typically tracked and managed within a regulatory framework. According to survey data completed by the private sector (*Sections 4.3.1 and 4.3.2*), between 2021 and 2024, most of the transactions involving virtual assets and facilitated through Moldovan banks and PSPs were directed to foreign centralized crypto exchanges. In addition, according to the Chainalysis 2024 Crypto Adoption Index Report (*detailed in Chapter 3*), Moldova ranks 37<sup>th</sup> out of 151 countries in terms of Centralized Service Value Received, indicating a relatively high usage of centralized platforms for cryptocurrency transactions and services. This reliance on centralized exchanges, which typically implement some degree of compliance mechanisms, contributes to a relatively lower risk level. These mechanisms, even if varied, support transactional traceability and adherence to certain AML standards.

**d. Decentralized Environments** – Decentralized Finance (DeFi) is a financial ecosystem designed to minimize or eliminate the need for intermediaries in transactions by leveraging decentralized computer networks. The system functions independently of traditional institutions and is powered by smart contracts for seamless operation.

The rapid growth in DeFi lending transactions within Moldova, as reported by the 2024 Crypto Adoption Index from Chainalysis, highlights a significant shift towards decentralized financial activities. Between July 2023 and June 2024, the country saw explosive expansion in DeFi lending transactions compared to the previous period (July 2022 – June 2023). However, despite this increase, the overall market share of DeFi-related crypto inflows remains limited due to Moldova's smaller market size in the regional context. Nevertheless, this trend may signal an evolving and potentially risky environment that needs careful examination.

Previously (*section 5.2.1*), we highlighted examples of underground services actively operating on encrypted messaging platforms like Telegram. These services offer a variety of options, including cryptocurrency escrow services that function autonomously through chatbots. These Crypto Escrow Services can be categorized as part of the DeFi ecosystem, as they could act as intermediaries to secure transactions between parties. This is typically done by holding cryptocurrency within a smart contract until all specified transaction conditions are fulfilled.

### 7.1.5. Ease of Criminality

Figure 32: Ease of Criminality – Tax Evasion

High	• Tax evasion
Medium	• Terrorist financing
High	• Disguising criminal proceeds to VA not regulated
High	• Trace and Seize Difficulty
High	• Circumvent Exchange Control

**a. Tax evasion (High)** – The FATF has pointed out that virtual assets pose an emerging risk for ML/TF, with tax evasion being a commonly associated issue. The structure of VAs, which typically operate beyond the reach of traditional financial and regulatory systems, makes them attractive to those looking to avoid taxation. This concern is particularly relevant for the Republic of Moldova, where the capacity for monitoring and enforcement may be hindered by a large informal economy and the lack of specific regulations and supervision over VAs/VASPs.

The tax legislation in the Republic of Moldova does not explicitly specify whether income generated from cryptocurrency is taxable or non-taxable. Nevertheless, when viewed as a property with inherent value, cryptocurrency qualifies as an asset held by an individual who owns a right to it. Consequently, any income an individual receives from financial investments in cryptocurrency is treated under tax legislation as income from capital investments and financial assets. Under Article 14 para. (1) lit. b) and letter. c) from the Fiscal Code, the said income is subject to tax on income.<sup>70</sup>

The State Tax Service has provided clarification<sup>71</sup> indicating that income earned by a resident individual in Moldova from the sale of cryptocurrency is considered taxable income, with cryptocurrency classified under the capital asset category. According to Article 40, paragraph (7) of the Fiscal Code, the taxable growth during the tax period is equal to 50% of the excess amount of recognized capital growth over the level of any capital losses incurred during the tax period. The size of the increase or loss of capital resulting from the sale, exchange, or other forms of alienation of capital assets is equal to the difference between the amount received (income obtained) and the value base of these assets.

**Indicators of Tax Compliance and Potential Evasion:** Based on the survey findings detailed in Section 4.1, between 2021 and 2023, 81 resident individuals voluntarily declared income generated from VAs, totaling 8,355,776 MDL. As depicted in *Figure 11*, a significant decline in the number of income declarations was observed in 2023 compared to 2022, with declarations plummeting from 56 in 2022 to only 1 in 2023. This notable decrease may be attributed to the introduction of restrictive measures impacting VAs/VASPs, which could have deterred voluntary disclosures.

Given the regulatory ambiguities, sporadic voluntary reporting, and a notable decline in declarations, the risk level for ease of criminality in the form of tax evasion related to

<sup>70</sup> [https://www.legis.md/cautare/getResults?doc\\_id=134161&lang=ro](https://www.legis.md/cautare/getResults?doc_id=134161&lang=ro)

<sup>71</sup> <https://sfs.md/ro/ordinele-de-baze-de-date-de-generalizare/1063>

VAs/VASPs can be assessed as high. The framework's limitations and the observed behavioral trends among taxpayers reinforce the need for more stringent oversight and comprehensive regulations to mitigate these risks effectively.

**b. Terrorist financing (Medium)** – Although specific cases of terrorist financing involving VAs or other means have not been detected within Moldova, the country's unique geopolitical position contributes to an elevated risk profile. The breakaway region of Transnistria and Moldova's proximity to conflict zones, notably the ongoing war in Ukraine, raise concerns about potential VA misuse for TF activities. The 2022 National Risk Assessment identified Moldova as a potential transit zone for foreign terrorist fighters, which, combined with limited border control in certain areas, increases the risk of such financing schemes exploiting the region.

Overall, the ease of criminality related to TF in VAs/VASPs in Moldova is assessed as medium risk, reflecting the balance between limited detected cases and the potential exposure due to geopolitical and regulatory factors. While measures have been implemented to mitigate these risks, the inherent characteristics of VAs—such as anonymity, speed, and scalability—combined with the region's specific vulnerabilities, continue to present challenges to effectively countering TF through this channel.

**c. Disguising criminal proceeds to VA not regulated (High)** – Although Moldova has stringent regulations that limit domestic VASP operations and heavily control interaction with foreign authorized VASPs, the risk remains due to alternative channels outside the formal financial sector. Criminals looking to launder proceeds of crime can bypass these formal restrictions by leveraging the informal sector to acquire VAs through cash-based transactions. Once obtained, these assets can be easily moved to unregulated VASP services for laundering process (mixing and layering). Techniques such as using mixers, tumblers, and engaging in chain hopping across various blockchains create opportunities for criminals to obscure the origin of illicit funds.

While the regulatory measures in place act as a deterrent within the formal financial system, the existence of an informal cash-based VA market combined with the ease of accessing unregulated international VA services raises the risk of being evaluated as high. Criminals can exploit these channels to engage in laundering activities by moving assets across jurisdictions and employing sophisticated methods to disguise fund origins.

**d. Trace and Seize Difficulty (High)** – This risk element aligns with the input variable of 'Traceability' (*Section 7.1.1*), highlighting both the potential and challenges within the current landscape. While blockchain technology provides a measure of transaction transparency, significant challenges persist due to the prohibition of VASP services domestically and the lack of implementation of the 'travel rule,' which complicates the identification of true transaction parties. The process becomes increasingly difficult without advanced blockchain forensics tools and specialized knowledge, both of which are currently insufficient within Moldovan LEAs.

Although LEAs possess the legal authority to trace, freeze, and seize virtual assets, they face notable limitations in terms of expertise, technological capabilities, and a comprehensive understanding of VAs and VASPs. This deficiency in technical knowledge and resources hampers their operational effectiveness. Nonetheless, statistical data (*Table 10*) from LEAs

reveals a marked increase in the volume and variety of cryptocurrencies seized between 2021 and 2024. This data shows an upward trend in both the volume and variety of seized virtual assets, indicating not only the increased use of cryptocurrencies in illicit activities but also an improving capacity of LEAs to investigate, seize, store, and manage these assets.

Overall, the current environment suggests a complex situation where the ease of criminal activity involving VAs remains significant due to existing barriers in effective tracing and seizing, but there are early signs of progress in capacity building among LEAs. This mixed picture places the risk level at a moderate to high range, requiring targeted efforts in skill development, access to forensic tools, and legislative advancements for enhanced mitigation.

**e. Circumvent Exchange Control (High)** – The potential threat posed by unidentified underground VASPs in Moldova is significant, as these entities may facilitate the circumvention of capital flow restrictions. By enabling cross-border transfers that bypass traditional financial and payment systems, these underground VASPs could undermine regulatory frameworks, compromise financial integrity, and potentially be exploited for illicit activities, including ML/TF.

### 7.1.6. Economic Impact

Figure 33: Economic Impact – Summary of risk elements

High	• Underground economy - Impact on the country's monetary policy
Medium	• Allow full integration with the financial services market
High	• Prohibit any interaction between the FIs and the VC market

**a. Underground economy - Impact on the country's monetary policy (High)** – The absence of robust regulatory frameworks and oversight mechanisms can facilitate the increased adoption of VAs on a peer-to-peer (P2P) basis, which, in turn, supports domestic tax evasion. This unregulated environment may lead to a portion of the economy functioning outside the traditional monetary system, thereby undermining state control over financial operations.

VASPs pose additional concerns, especially in regions where the informal economy is substantial. As described in Section 5.2, following the prohibition of VASP services within the country in 2023, underground activities in the VA sector have expanded rapidly. Various unregulated platforms, often utilizing encrypted messaging, now enable VA transactions that circumvent regulatory oversight. Moldova risks becoming an appealing jurisdiction for criminal activity if VA services continue to operate without adequate licensing and supervision. Unregulated and unsupervised VASPs can act as conduits for money laundering and other financial crimes, thereby increasing the size and influence of the underground economy.

**b. Allow full integration with the financial services market (Medium)** – The economic impact of allowing full integration of VAs/VASPs into the financial services market is assessed as Medium. While risks are present due to the potential for misuse, these risks are somewhat balanced by the current limited integration of VAs into the financial sector and restrictive regulatory measures. The absence of comprehensive risk assessments

by financial institutions indicates areas that need enhancement, emphasizing the importance of building stronger risk management frameworks and monitoring systems (*more details presented in Section 4.3.1 “Banking Sector” and 4.3.2 “PSPs” Survey Results*).

**c. Prohibit any interaction between the Financial Institutions and the VC market (High)** – Currently, Moldova's regulatory landscape remains restricted, primarily focusing on prohibiting domestic VASP activities and limiting interactions with authorized foreign VASPs through stringent conditions.

### The Overall Threat Rating

The threat analysis drew on data from surveys conducted with LEAs, regulators, and traditional obliged entities, while also reviewing national legislation, international reports, and emerging typologies. It also examined how Moldova's formal and informal sectors may engage directly or indirectly with VA/VASP and evaluates the level of ML/TF threats resulting from these interactions.

The analysis was built upon assessing each input variable, which contributed to understanding the intermediate variables across 6 relevant VASP channels, evaluating the risk exposure for each. This assessment took into account the specific characteristics of VAs and how various types of VASPs within the VA value chain might be exploited for committing predicate offences and laundering proceeds.

Below is the ML/TF threat rating assigned to each of the identified channels:

*Table 18: ML/TF Threat Ratings by VASP Channels*

VASPs	Types of Services	Sub-type (Channel)	Threat Rating
VIRTUAL ASSET WALLET PROVIDERS	Custodial Services	Hot Wallet	High
	Non-Custodial Services	Cold Wallet	High
VIRTUAL ASSET EXCHANGES	Transfer Services	P2P	High
	Conversion Services	Fiat-to-Virtual	High
		Virtual-to-Fiat	High
VIRTUAL ASSET INVESTMENT PROVIDERS	Emerging Products	Crypto Escrow Service	High
<b>Overall VA &amp; VASPs ML/TF Threat</b>			<b>High</b>

The table above indicates that all 6 VASP channels — Hot Wallet, Cold Wallet, P2P, Fiat-to-Virtual, Virtual-to-Fiat and Crypto Escrow Services — present a *High* level of risk. This elevated risk primarily stems from their substantial exposure to ML/TF threats, and lack of regulatory oversight, coupled with their increasing use in the underground activities.

## 7.2. ML/TF Inherent Vulnerability Assessment

This section highlights the vulnerability assessment of both VAs and VASPs in Moldova with regard to ML/TF.

Despite the absence of officially licensed or registered VASPs in the Republic of Moldova due to restrictions set by the legislative framework, the NRA has identified active transactions and interactions involving the formal financial system (banks and PSPs), the informal sector, and foreign VASP channels. The analysis in *Chapter 5* indicates that a significant share of these activities has shifted to the informal economy.

These interactions demonstrate that, despite regulatory constraints, VA activities persisted through alternative channels. The banking and PSP sectors, although reluctant and limited in their direct involvement, maintained indirect links with foreign VASPs, while the informal sector emerged as a significant facilitator of VA transactions. This situation highlights the complexities of monitoring and regulating VAs in Moldova, emphasizing the challenges authorities face in addressing these evolving financial interactions.

The table below provides a summary of overall vulnerability exposure, based on the input variables from the World Bank Methodology, to assess the inherent vulnerabilities before implementing any regulatory controls or mitigating measures.

*Table 19: Overall Vulnerability Exposure Summary*

<b>Intermediary Variables</b>	<b>Input Variables</b>	<b>Vulnerability Rating</b>
<b>Products &amp; services provided, and the types of VA</b>	Licensed in the country or abroad	High
	Nature, size and complexity of business	High
	Products and services	High
	Methods of delivery of products/services	High
	Customer types	High
	Country risk	High
	Institution dealing with VASPs	High
	VA (Anonymity/pseudonymity)	High
	Rapid transaction settlement	High
	Dealing with unregistered VASP from overseas	High
<b>Overall Vulnerability Rating</b>		<b>High</b>

#### **Description of the Vulnerability Input Variables according to WB Methodology:**

<b>Licensed in the country or abroad</b>	VASPs must meet licensing and registration criteria established by relevant authorities to ensure adequate supervision and oversight. This includes conditions such as appointing a resident executive director, maintaining a substantial management presence, or meeting financial requirements based on the scale and nature of their activities. Given the cross-border nature of VAs and the uneven implementation of international standards, VASPs offering services domestically or abroad must register with the appropriate authority. Additionally, entities based overseas but operating in the domestic market, including those from countries in the Economic Area (e.g., the EU), must also register with the relevant authority, regardless of their registration status in their home country.
<b>Nature, size and complexity of business</b>	According to WB Methodology, the inherent nature of most VASPs allows for the swift transfer of value, frequently with limited oversight or controls. The complexity of a VASP's operations can differ significantly; for instance, certain exchanges may provide only a limited range of virtual assets and may not support fiat currency transactions. These elements are crucial to consider when evaluating the risks associated with a specific VASP.
<b>Products and services</b>	Anonymity-enhanced cryptocurrencies, mixers, tumblers, decentralized platforms, and other products or services that enable or allow for reduced transparency and increased obfuscation of financial flows should be considered when assessing risk.
<b>Methods of delivery of products/services</b>	The risk factors linked to the delivery of VA products, services, transactions, or channels, particularly if the activity includes

	pseudonymous or anonymous transactions, non-face-to-face business relationships or transactions, and/or payments from unknown or unrelated third parties. Given that most VAs exhibit one or more of these features, a country may conclude that activities involving VAs are inherently higher risk due to the fundamental nature of their products, services, transactions, or delivery methods.
<b>Customer types</b>	The VASP sector tends to be at a very high risk of exposure to criminals and organised crime, and the sector is considered attractive to this type of customer due to its reduced transparency.
<b>Country risk</b>	The VASP sector is significantly exposed to higher-risk jurisdictions through internet channels due to its inherently borderless nature. Exchanges, intermediaries, and related service providers may operate in jurisdictions with minimal or no AML/CFT requirements, creating opportunities for countries or individuals to potentially bypass international sanctions.
<b>Institution dealing with VASPs</b>	VASPs have exposure to other VASPs such as exchanges and wallet providers, which may have insufficient AML/CFT controls in place. Tumblers, peer-to-peer exchanges, and other methods of enhancing anonymity or obfuscating the flow of funds should be considered higher risk factors.
<b>VA (Anonymity/pseudonymity)</b>	VASPs that deal in VAs but provide varying degrees of anonymity in name and transaction-level detail directly confront KYC/CDD principles and transaction reporting, both core components of the AML/CFT regimes. Mixing services and other location/identity hiding services adds additional anonymity in serving non-residents.
<b>Rapid transaction settlement</b>	Virtual assets enable near real-time cross-border transaction settlements at a lower cost compared to traditional methods. This feature can be particularly appealing to global criminal and terrorist groups seeking borderless financial channels.
<b>Dealing with unregistered VASP from overseas</b>	Specific challenges emerge when virtual asset services are offered by unlicensed overseas VASPs, which may be operated by criminals or noncompliant entities. Such operators can exploit initial coin offerings and capitalize on the limited awareness of securities token issuers regarding their AML/CFT obligations, especially in jurisdictions that lack registration requirements or have insufficient regulatory frameworks in place.

Table 20: Description of the Vulnerability Input Variables according to WB Methodology:

### Results of the ML/TF Inherent Vulnerability Assessment

Due to the prohibition of VA services within the country and the shift of VA/VASP activities to the informal economy, **assessing vulnerabilities using the input variables outlined by the World Bank Methodology needed adjustments.** Consequently, all input variables were uniformly classified as representing **high vulnerability**. This classification also aligns with the findings related to existing threats and highlights significant challenges, including limited access to comprehensive data, regulatory gaps, a lack of adequate tools and technical expertise among national authorities, and the inherent characteristics of VAs that promote anonymity and enable rapid cross-border transactions. These factors collectively underscore the difficulties in accurately assessing the risks posed by unregulated and informal VA operations in Moldova. Below is a detailed breakdown of these contributing elements:

- **Lack of comprehensive legal framework:** A major factor contributing to the high vulnerability rating is the absence of a comprehensive regulatory framework governing VAs

and VASPs in Moldova. Current legislation bans the provision of VA services within Moldova. However, REs are allowed to facilitate transactions for resident clients with foreign-licensed VASPs, subject to strict operational conditions and limitations related to clients, accounts and other enhanced measures when conducting such transactions.

As explained in *Section 5.2*, these regulatory measures, combined with the reluctance of banks and PSPs to facilitate client access to VASP platforms **have pushed VA-related transactions out of the formal financial system**. Survey data indicates that by September 2024, transaction volumes have **fallen dramatically—by a striking 99.86%** compared to 2023.

Despite the limitations and the formal sector's hesitance to act as a “gateway” to VASP platforms, the assessment has revealed data illustrating how individuals are still able to bypass these limitations. This is achieved through the use of P2P trading platforms (Section 5.2.2), accounts held in foreign financial institutions, and interactions with underground VASPs. These findings suggest that while regulatory efforts have succeeded in reducing VA-related transactions through the formal sector, these actions provoked an unintended growth of unregulated markets.

In addition, Moldova has **not fully aligned its regulatory framework with the FATF Recommendations** pertaining to virtual assets, particularly Recommendation 15, which addresses new technologies, as noted in the 2nd MONEYVAL Enhanced Follow-up Report.

- **Limited tools and expertise among LEAs and regulators:** LEAs and regulators lack the necessary tools and technical expertise to trace and monitor VA transactions effectively. Insufficient funding and resources hinder the development of specialized units or the acquisition of advanced analytical tools.

- **Unique characteristics of VAs:** VAs possess unique characteristics that present significant challenges for authorities. **Enhanced anonymity features**, such as those found in privacy-focused cryptocurrencies like Monero and Zcash, and the use of mixing services, obscure transaction trails and complicate investigations, hindering the ability to trace financial flows crucial for ML/TF cases. Additionally, VAs enable **instantaneous cross-border transfers**, outpacing authorities' ability to monitor and intercept illicit transactions, and complicating jurisdictional authority and international cooperation efforts. Furthermore, **decentralized exchanges (DEXs)** facilitate direct user-to-user transactions without intermediaries, reducing regulatory oversight and making enforcement more difficult.

- **International cooperation challenges:** Due to the inherent features of VAs, such as anonymity, pseudonymity, and the capability for instantaneous cross-border transactions, international collaboration is crucial for effective intelligence analysis and the investigation of suspicious ML/TF activities. However, Moldova's current non-member status in the EU, combined with the absence of a specific regulatory framework for VAs/VASPs, presents additional challenges. The complex structure of VASPs and their global operations framework, results in **essential transaction data and KYC information being dispersed across various jurisdictions**, each with different regulatory requirements. Consequently, operations and data control related to clients who are citizens of the Republic of Moldova is often stored outside the EU, in jurisdictions that are less cooperative or transparent. This fragmentation complicates the process of tracing transactions and identifying beneficiaries,

creating substantial challenges for Moldovan intelligence agencies in pursuing comprehensive investigations and ensuring compliance with international standards.

- **Economic factors and the rise of informal economy:** Moldova's economy has a high reliance on cash transactions, which are inherently difficult to trace and tax. This reliance creates vulnerabilities, as VA have the potential to serve as a bridge for integrating cash obtained through illegal activities into the formal economy. The widespread use of informal financial practices further facilitates ML/TF through VAs. The 2023 ban on VASP services within Moldova has inadvertently fueled a rapid expansion of underground VA-related activities. Unregulated platforms, often operating through encrypted communication channels, have become more common, enabling transactions that evade regulatory oversight. This informal market allows for a range of activities, including the purchase of goods and services through cryptocurrencies, creating a conducive environment for illicit financial activities such as ML/TF.

Additionally, Moldovan **migrant workers**, particularly those employed unofficially, may be attracted to using VAs for remittances through unregulated VASPs due to their minimal requirements for KYC procedures and proof of funds (POF). This practice poses significant risks, as the lack of stringent KYC protocols and regulatory oversight makes it difficult to monitor the source and flow of funds, creating vulnerabilities that can be exploited for ML/TF.

**The table below presents the assessment of vulnerabilities of each VASP channel interacting with formal and informal sectors:**

*Table 21: ML/TF Inherent Vulnerability Ratings by VASP Channels*

VASPs	Types of Services	Sub-type (Channel)	Vulnerability Rating
VIRTUAL ASSET WALLET PROVIDERS	Custodial Services	Hot Wallet	High
	Non-Custodial Services	Cold Wallet	High
VIRTUAL ASSET EXCHANGES	Transfer Services	P2P	High
	Conversion Services	Fiat-to-Virtual	High
		Virtual-to-Fiat	High
VIRTUAL ASSET INVESTMENT PROVIDERS	Emerging Products	Crypto Escrow Service	High

The overall vulnerability of the VASP channels were assessed as **High Vulnerability**.

### 7.3. Mitigation Measures (Low)

The Republic of Moldova faces substantial challenges in mitigating the risks associated with VAs/VASPs, primarily due to legislative and regulatory deficiencies. Current measures to assess and mitigate these risks reveal significant inefficiencies, stemming from the country's limited legislative framework and absence of essential tools to manage identified vulnerabilities effectively. Although there is a general prohibition on VA-related services, this measure is not sufficiently comprehensive and fails to cover the full spectrum of VA-related risks. Authorities also face challenges due to a lack of appropriate tools and expertise, preventing them from effectively identify and sanction individuals or entities engaged in illegal VA activities. This gap allows illicit actors to exploit the system with minimal fear of detection or prosecution.

## 7.4. Overall ML/TF Risk

Based on the risk ratings across all the channels, the overall ML/TF residual risk associated with VA/VASP is considered to be “**High**” after considering mitigating measures at the time of assessment.

Table 22: VA/VASP ML/TF threat, inherent vulnerability and residual risk ratings across all VASP channels

VASPs	Types of Services	Sub-type (Channel)	Threat Rating	Vulnerability Rating	Total Risk Level	Residual Risk
VIRTUAL ASSET WALLET PROVIDERS	Custodial Services	Hot Wallet	High	High	High	High
	Non-Custodial Services	Cold Wallet	High	High	High	High
VIRTUAL ASSET EXCHANGES	Transfer Services	P2P	High	High	High	High
	Conversion Services	Fiat-to-Virtual	High	High	High	High
		Virtual-to-Fiat	High	High	High	High
VIRTUAL ASSET INVESTMENT PROVIDERS	Emerging Products	Crypto Escrow Service	High	High	High	High

## 8. Conclusions

### 8.1. Key Findings

The 2024 ML/TF National Risk Assessment of VAs and VASPs in the Republic of Moldova provided valuable insights into the evolving landscape of digital finance and its implications for national security. While the assessment revealed a notable increase in VA and VASP activities in the informal economy, the country’s regulatory framework remains underdeveloped, heightening exposure to ML/TF risks.

The assessment highlighted significant shortcomings, including the lack of a comprehensive regulatory framework, ineffective ban measures, limited expertise among law enforcement, and difficulties with international cooperation. Although existing legislation prohibits VA, effectively reducing certain risks within the formal financial sector, this approach has inadvertently driven VA activities into the informal economy, complicating regulatory oversight.

#### Some of the main findings are outlined below:

- This NRA represents the **first in-depth analysis** of ML/TF risks associated with VAs and VASPs within the Republic of Moldova. The evaluation concluded that Moldova's exposure to ML/TF risks related to VAs and VASPs is significant, categorized as **high risk**.
- **Regulatory gaps:** Moldova currently lacks a comprehensive regulatory framework dedicated to overseeing VASPs. This regulatory void limits effective oversight and creates opportunities for criminal exploitation due to existing loopholes. Due to the ban on VA-related activities within the country, VA and VASP operations have become concentrated in the informal sector, where transactions are conducted directly between individuals. This shift makes controlling and monitoring VA activities highly challenging.
- Banning VASP activities did not achieve the desired outcome. Cryptocurrency-related activity in Moldova persists. Instead, it is observed that it shifted to peer-to-peer markets, with consumers investing in anonymity-enhancement solutions. **The measures**

**intended to enforce the ban and reduce exposure to virtual assets are ineffective**, lacking the means to identify illegally operating VASPs and to impose dissuasive sanctions on such entities.

- **Underground economy:** The data collected during NRA indicates a rapid expansion of the underground VA-related activities. Various unregulated platforms, based on the encrypted messaging, now facilitate VAs transactions that bypass regulatory oversight. These informal channels, particularly those hosted on encrypted platforms, have become major facilitators for virtual assets transactions, enabling an array of services from peer-to-peer crypto exchanges to large-scale purchases using cryptocurrencies., creating a fertile ground for money laundering and terrorist financing.
- The high rate of VA and VASP activities occurring in the informal economy contributes to the **inability to conduct a comprehensive and qualitative ML/FT risk assessment**.
- Although LEAs and regulatory bodies have undergone a series of trainings and developed basic expertise in the VA field, the number of specialists involved in these training programs is very limited, **leaving significant knowledge gaps**. Furthermore, there are **insufficient technological resources** necessary for effectively tracing and prosecuting crimes related to VAs.
- **International cooperation and data accessibility:** The global operations of VASPs lead to essential transaction data and KYC information being spread across various jurisdictions, often placing data for Moldovan clients in less cooperative regions outside the EU. This fragmentation complicates the ability of Moldovan intelligence agencies to trace transactions and identify beneficiaries, creating significant challenges for thorough investigations.
- **Increased STRs/SARs Reporting:** Reports from financial institutions indicated a **rise in suspicious transactions involving VAs**, often related to illegal VAs services, fraud and drug trafficking.
- **Transnistrian crypto-mining activity:** The breakaway region of Transnistria poses a significant threat due to its high levels of cryptocurrency mining. This activity has grown since 2018, fueled by energy subsidies and minimal regulatory restrictions imposed by the region's unconstitutional authorities.
- **Taxation ambiguities:** Current tax legislation in the Republic of Moldova does not explicitly specify whether income generated from cryptocurrency is taxable or non-taxable. Presently, any income an individual receives from financial investments in cryptocurrency is treated under tax legislation as income from capital investments and financial assets.
- **Geopolitical risks:** Moldova's proximity to conflict zones increases the risk of ML/TF facilitated through VA channels. This adds an additional layer of complexity to national and regional security considerations.
- **The private sector lacks experience:** Often refraining from opening specialized accounts, approximately 45 percent of banks do not perform internal risk assessments to identify ML/TF risks associated with VASPs and VAs. While there is a high perception of risk related to ML/TF threats from VASPs, the sector is not equipped with the necessary tools and knowledge to effectively identify indirect exposure. The prevailing view is that the reluctance to open specialized accounts and engage in crypto activities undermines the recognition of these threats posed by VASPs. Raising concerns about the sectors capability of applying risk-based approach (RBA).

## 8.2. Recommendations

- **Strengthen regulatory framework:** Implement a comprehensive legal and regulatory framework that aligns with EU Directives and FATF standards, shifting towards licensing or, registration, and the enhanced oversight of VASPs, introducing necessary measures to effectively supervise the sector and impose repercussions if discrepancies are observed. Authorities should monitor developments in the VA sector and evaluate whether adjustments to national legal and regulatory AML/CFT frameworks are necessary.
- **Risk Assessment Measures for TOEs:** TOEs should begin conducting internal risk assessments to identify and evaluate the ML/TF risks associated with Vas/VASPs. This process will help to identify, assess, and mitigate the risks linked to indirect exposure to VAs and VASPs.
- **Enhance LEAs Capabilities:** Increase investment in training and technological solutions for LEAs to improve their ability to monitor, trace, and prosecute ML/TF activities involving VAs. In addition, it is recommended to assign express responsibility to a designated authority, to detect and identify underground VASP activities with necessary resources to effectively identify threats arising from unregulated activities related to VAs posing ML/TF threats.
- **Comprehensive training programs:** Substantial capacity-building initiatives to a broader group of specialists should be provided to relevant public authorities to enhance their understanding and management of ML/TF risks associated with VAs/VASPs. These initiatives should include specialized courses in blockchain analytics and risk assessment techniques. Additionally, ongoing workshops and certifications tailored to regulatory and supervisory bodies will ensure that authorities remain equipped with up-to-date knowledge and skills to effectively identify, monitor, and mitigate the evolving risks in the VA/VASP sector.
- **Enhance collaboration at the national level:** Establishing a public-private partnership channel for information sharing. It is essential to facilitate the efficient communication between obligated reporting entities and the FIU, as well as other public institutions to maintain collaboration in the sharing of emerging ML/TF typologies related to Vas/VASPs. It would enhance and level the knowledge landscape among the various entities in both sectors.
- **Improve international collaboration:** Establish partnerships with international bodies and neighbouring countries to facilitate information sharing and joint investigations related to VAs/VASPs. Participate in best practices sharing events and training or exchange programs for LEAs and other public institutions.
- **Clarify Tax Policies:** Define clear tax obligations for VA-related income to encourage voluntary compliance and minimize evasion risks. Review the provisions of the national legislation to ensure a uniform basis with the international practices for tax on income from cryptocurrency transactions, ensuring a clear and fair fiscal treatment, simplifying the way to declare and pay the tax for such incomes.
- **Statistical data related to VA/VASPs activities:** Authorities should begin collecting, maintaining, and sharing data and metrics specific to VA/VASPs. While current activity levels are considered minimal in the formal sector, establishing an evidence-based baseline will support the early detection of emerging risks or shifts in risk levels as activity increases.

These steps will help Moldova address its existing vulnerabilities, align with international standards, and create a safer environment for the legitimate use of digital financial technologies. To ensure the effective implementation of these measures, it is recommended to develop a medium-term (3-year) Action Plan that includes clear objectives and concrete actions, specifying deadlines and the responsible institutions for each action. This plan should be incorporated in the existing Action Plan for implementing AML/CFT National Strategy.

### **8.3. Challenges and Limitations**

As part of the NRA, the WG has encountered a significant challenge in gathering essential data related to VA/VASPs: given that existing AML/CFT law in Moldova contains limitations for VA-related activities, the country currently lacks domestic VASPs. This situation has created a gap in the ability to gather essential statistical data, that would allow WG to accurately evaluate the extent of interest and engagement of Moldovan citizens in the virtual assets space. Such data is critical for a comprehensive evaluation of the risks associated with VAs within the country.

To address this issue, the WG has developed a targeted questionnaire designed to gather key, sanitized statistical information from several foreign licensed VASPs. This questionnaire was forwarded to foreign FIUs with a request to facilitate communication with VASPs registered in their jurisdictions. However, due to the global operational structure of these VASPs, data pertaining to Moldovan clients is predominantly stored and managed by subsidiary companies registered in less cooperative jurisdictions. As a result, FIU Moldova did not receive any responses from these outreach efforts, highlighting the challenges in accessing cross-border data for effective risk assessment.

## 9. Annex

### 9.1. Glossary

Blockchain	A technology solution that enables digital assets. It is a method of securely recording information on a peer-to-peer network <sup>72</sup> .
Blockchain analytics	A technology solution to analyze transaction data on blockchain networks to trace the movement of virtual assets, identify patterns and assess the risks for compliance, security and investigative purposes.
Bridge	A blockchain bridge serves as a gateway linking multiple separate blockchains, allowing for the transfer of data and assets between them.
Central bank digital currencies (CBDCs)	It is digital money issued by a central bank. A CBDC differs from cryptocurrency as it would be issued by a central bank.
Cryptocurrency	Digital currency class that does not possess the legal status of currency or money but can be accepted by natural and legal persons as a means of exchange and can be transferred, stored, and traded electronically.
ERC-20	ERC-20 is the technical standard for fungible tokens created using the Ethereum blockchain.
ERC-721	ERC-721 is a non-fungible token standard on the Ethereum blockchain. It provides a set of guidelines for creating unique tokens that represent digital assets.
FIAT	The type of currency that is not backed by precious metals or any other tangible asset or commodity. It is a government issued currency.
Mixer/Tumbler	It is a service that blends the cryptocurrencies of many users together to obfuscate the origins and owners of the funds <sup>73</sup> .
Metaverse	The term refers to virtual worlds in which users, represented by avatars interact.
Privacy coin	Or anonymity enhanced coin is designed to prioritize anonymity with enhancing features that reduce traceability.
Smart contract	A self-executing contract that is typically used to automate execution of an arrangement without intermediary's involvement.
Token	A representation of an asset or interest that has been tokenized on an existing cryptocurrency's blockchain.
VA	Virtual asset (crypto asset) refers to any digital representation of value that can be digitally traded, transferred or used for payment. It does not include digital representation of FIAT currencies.
VASP	Virtual assets service provider (or crypto assets service provider).
White paper	A white paper is a report or guide that informs readers concisely about a complex issue and presents the issuing body's philosophy on the matter.

---

<sup>72</sup> PwC, Demystifying cryptocurrency and digital assets, website: <https://www.pwc.com/us/en/tech-effect/emerging-tech/understanding-cryptocurrency-digital-assets.html> [last accessed September 22, 2024].

<sup>73</sup> Chainalysis, Crypto Mixers and AML Compliance, website: <https://www.chainalysis.com/blog/crypto-mixers/> [last accessed October 06, 2024].

## 9.2. Timeline of key events and developments in the VA/VASP Ecosystem and Moldova's specific actions

October 31, 2008	Satoshi Nakamoto releases the Bitcoin White Paper. <sup>74</sup>
January 15, 2010	First cryptocurrency exchange BitcoinMarket was launched <sup>75</sup> .
October 21, 2011	Bitcoin Fog mixing service is launched <sup>76</sup> .
June, 2012	P2P exchange Localbitcoins was launched <sup>77</sup> .
January 23, 2014	Ethereum network introduced by Vitalik Buterin <sup>78</sup> .
April 18, 2014	Privacy coin Monero is launched <sup>79</sup> .
November 19, 2015	The ERC-20 standard is proposed, paving the new way for the issuance of new tokens, including stablecoins, on the Ethereum network <sup>80</sup> .
May 12, 2017	WannaCry ransomware attack is launched by cybercrime group Lazarus <sup>81</sup> .
July 10, 2017	National Bank of Moldova published press release on virtual currency and its associated risks <sup>82</sup> .
January 24, 2018	The ERC-721 standard proposed. It provided the base for non-fungible tokens (NFTs) on Ethereum network <sup>83</sup> .
February 15, 2018	The National Bank of Moldova warned about high risks of investing in cryptocurrencies <sup>84</sup> .
March 8, 2018	EU Commission adopted the Fintech action plan.
May 15, 2018	The National Bank of Moldova repeatedly warned about the risks associated with investing in cryptocurrencies <sup>85</sup> .
September 14, 2018	The National Bank of Moldova has released a new statement reaffirming its earlier stance on so-called "virtual currencies," emphasizing that they do not qualify as currencies in the traditional sense and are neither guaranteed nor recognized as a means of payment by the monetary authority. <sup>86</sup>
November 28, 2018	OFAC designated Iran-based financial facilitators of malicious cyber activity and for the first time identified associated digital currency addresses <sup>87</sup> .

<sup>74</sup> Forbes, The Bitcoin White Paper is Now Officially 15 Years Old, website: <https://www.forbes.com/sites/peterizzo/2023/10/31/15-facts-about-the-satoshi-white-paper-on-bitcoins-15th-birthday/> [last access: September 22, 2024].

<sup>75</sup> Guinness World Records, First cryptocurrency exchange, website: <https://www.guinnessworldrecords.com/world-records/696258-first-cryptocurrency-exchange> [last access: September 22, 2024].

<sup>76</sup> U.S. Department of Justice, Bitcoin Fog Operator Convicted of Money Laundering Conspiracy, website: <https://www.justice.gov/opa/pr/bitcoin-fog-operator-convicted-money-laundering-conspiracy> [last access: 22 September, 2024].

<sup>77</sup> Localbitcoins, About LocalBitcoins, website: <https://localbitcoins.com/about> [last access: 22 September, 2024].

<sup>78</sup> Ethereum community (ethereum.org), Ethereum Whitepaper, website: <https://ethereum.org/en/whitepaper/> [22 September, 2024].

<sup>79</sup> Monero (getmore.org), About Monero, A Brief History website: <https://www.getmonero.org/resources/about/> [last access: 22 September, 2024].

<sup>80</sup> Ethereum Community (ethereum.org), ERC-20 Token Standard, website: <https://ethereum.org/en/developers/docs/standards/tokens/erc-20/> [last access 22 September, 2024].

<sup>81</sup> U.S. Department of Justice, North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions, website: <https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and> [last access: 22 September, 2024].

<sup>82</sup> National Bank of Moldova, Virtual currency and its associated risks, website: <https://www.bnm.md/en/content/virtual-currency-and-its-associated-risks> [last access: 22 September, 2024].

<sup>83</sup> Ethereum Community (ethereum.org), ERC-721 Non-Fungible Token Standard, website: <https://ethereum.org/lt/developers/docs/standards/tokens/erc-721/> [last access: 22 September, 2024].

<sup>84</sup> National Bank of Moldova, The National Bank of Moldova warns about high risks of investing in cryptocurrencies, website: <https://www.bnm.md/en/content/national-bank-moldova-warns-about-high-risks-investing-cryptocurrencies> [last accessed: October 06, 2024].

<sup>85</sup> National Bank of Moldova, The National Bank of Moldova repeatedly warns about the risks associated with investing in so-called cryptocurrencies, also known as "virtual currencies" (VCs), website: <https://www.bnm.md/en/content/national-bank-moldova-repeatedly-warns-about-risks-associated-investing-so-called> [last accessed: October 06, 2024].

<sup>86</sup> <https://www.bnm.md/ro/content/clarificarea-pozitiei-de-reglementare-si-autorizare-monedei-virtuale>

<sup>87</sup> U.S. Department of the Treasury, Treasury Designates Iran-Based Financial Facilitators of Malicious Cyber Activity and for the First Time Identifies Associated Digital Currency Addresses, website: <https://home.treasury.gov/news/press-releases/sm556> [last access: September 22, 2024].

June 21, 2019	FATF published Guidance for Risk-based Approach to Virtual Assets and Virtual Asset Service Providers <sup>88</sup> .
September 24, 2020	Legislative proposal of Crypto assets (MiCA) and digital operational resilience (DORA).
October, 2021	Amendments to Law No. 133 of June 17, 2016, on the declaration of assets and personal interests have come into effect, requiring declaration subjects to include virtual assets in their declaration of assets and personal interests if their value exceeds 10 average monthly salaries in the economy.
May, 2022	MONEYVAL's 1 <sup>st</sup> Enhanced Follow-up Report released. Moldova's technical compliance with the R.15 was downgraded to NC (non-compliant).
October 20, 2022	INTERPOL announces the launch of the first global police metaverse <sup>89</sup> .
October 28, 2022	National Bank of Moldova sends out letter to Banks and PSPs requesting to terminate all activities related to virtual assets.
January 16, 2023	The EU Digital Operational Resilience Act (DORA) entered into force.
May 29, 2023	The National Commission for Financial Markets warns about the risks of investing through unauthorized trading platforms. <sup>90</sup>
June, 2023	MiCA Publication in the OJEU <sup>91</sup>
July 1, 2023	A series of amendments to the AML/CFT Law No. 308/2017 have been adopted. These amendments mark a first step for the Republic of Moldova in recognizing virtual assets (VA) by introducing new concepts, such as "virtual asset" and "virtual asset service provider," into national legislation. Furthermore, the law prohibits the provision of VA services within the territory of the Republic of Moldova.
May, 2024	MONEYVAL's 2nd Enhanced Follow-up Report released. The assessment team has identified shortcomings in Moldova's compliance with FATF's Recommendation 15, including the absence of a comprehensive assessment of the ML/TF risks emerging from VA and VASP activities.
November 2024	The Republic of Moldova has completed its first National Risk Assessment of ML/TF risks associated with VAs/VASPs.

Table 23: Timeline of key events and developments in the VA/VASP Ecosystem and Moldova's Specific Actions

### 9.3. List of CASPs regulatory authorities in the EU

No.	EU Member State	Regulator
1	Austria	Financial Market Authority (FMA) <sup>92</sup>
2	Belgium	Financial Services and Markets Authority (FSMA) <sup>93</sup>
3	Bulgaria	Financial Supervision Commission (FSC) <sup>94</sup>
4	Croatia	Croatian Financial Services Supervisory Agency (HANFA) <sup>95</sup>
5	Cyprus	Cyprus Securities and Exchange Commission (CySEC) <sup>96</sup>
6	Czech Republic	Czech National Bank (ČNB) <sup>97</sup>

<sup>88</sup> FATF, Guidance for Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, website: <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets.html> [last access 22 September, 2024].

<sup>89</sup> Interpol, Interpol launches first global police Metaverse, website: <https://www.interpol.int/News-and-Events/News/2022/INTERPOL-launches-first-global-police-Metaverse> [last access: September 22, 2024].

<sup>90</sup> [https://www.cnpf.md/ro/ai-grija-de-banii-tai-cnpf-atentioneaza-despre-riscurile-investitiilor-prin-inte-6307\\_93595.html](https://www.cnpf.md/ro/ai-grija-de-banii-tai-cnpf-atentioneaza-despre-riscurile-investitiilor-prin-inte-6307_93595.html)

<sup>91</sup> ESMA, Markets in Crypto-Assets Regulation (MiCA), website: <https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/markets-crypto-assets-regulation-mica#:~:text=The%20Markets%20in%20Crypto%20Assets,into%20force%20in%20June%202023.> [last access: 22 September, 2024].

<sup>92</sup> <https://cms.law/en/int/expert-guides/cms-expert-guide-to-crypto-regulation/austria>

<sup>93</sup> <https://crypto4innovation.org/belgium-champions-eu-crypto-policy-with-mica-blockchain-pilots-and-esg-standards/>

<sup>94</sup> <https://prifinance.com/en/bulgaria-cryptocurrency-license/>

<sup>95</sup> <https://manimama.eu/cryptocurrency-regulation-in-croatia/>

<sup>96</sup> <https://cyprus-mail.com/2024/10/18/a-guide-to-cryptocurrency-in-cyprus/>

<sup>97</sup> <https://cms.law/en/int/expert-guides/cms-expert-guide-to-crypto-regulation/czech-republic>

7	Denmark	Danish Financial Supervisory Authority (DFSA) <sup>98</sup>
8	Estonia	Estonian Financial Supervision Authority (EFSA) <sup>99</sup>
9	Finland	Financial Supervisory Authority (FIN-FSA) <sup>100</sup>
10	France	Autorité des Marchés Financiers (AMF) <sup>101</sup>
11	Germany	Federal Financial Supervisory Authority (BaFin) <sup>102</sup>
12	Greece	Hellenic Capital Market Commission (HCMC) and National Bank of Greece (NGB) <sup>103</sup>
13	Hungary	Hungarian National Bank (MNB)
14	Ireland	Central Bank of Ireland
15	Italy	Bank of Italy <sup>104</sup>
16	Latvia	Bank of Latvia <sup>105</sup>
17	Lithuania	Bank of Lithuania <sup>106</sup>
18	Luxembourg	Commission de Surveillance du Secteur Financier (CSSF) <sup>107</sup>
19	Malta	Malta Financial Services Authority (MFSA) <sup>108</sup>
20	Netherlands	Bank of Netherlands <sup>109</sup>
21	Poland	Polish Financial Supervision Authority <sup>110</sup>
22	Portugal	Bank of Portugal <sup>111</sup>
23	Romania	The Foreign Exchange Licensing Commission of the Ministry of Finance <sup>112</sup>
24	Slovakia	National Bank of Slovakia <sup>113</sup>
25	Slovenia	The Securities Markets Agency and the Bank of Slovenia <sup>114</sup>
26	Spain	Bank of Spain <sup>115</sup>
27	Sweden	Swedish Financial Supervisory Authority <sup>116</sup>
28	Iceland	Bank of Iceland <sup>117</sup>

Table 24: List of CASPs licensing authorities in the EU

<sup>98</sup> [https://www.dfsa.dk/news/2024/jun/crypto-assets\\_250624](https://www.dfsa.dk/news/2024/jun/crypto-assets_250624)

<sup>99</sup> <https://news.err.ee/1609289883/estonia-introduces-legislation-to-regulate-cryptocurrency-providers>

<sup>100</sup> <https://prifinance.com/en/cryptocurrency-license/finland/>

<sup>101</sup> <https://www.amf-france.org/en/news-publications/news/mica-regulation-amf-now-accepting-applications-authorisation-casp>

<sup>102</sup> <https://www.bundesbank.de/en/tasks/topics/bitcoin-and-co-how-crypto-assets-are-regulated-920632>

<sup>103</sup> <https://manimama.eu/how-to-obtain-a-cryptocurrency-license-in-greece/>

<sup>104</sup> <https://www.bancaditalia.it/media/approfondimenti/2024/micar/index.html?com.dotmarketing.htmlpage.language=1&dotcache=refresh&dotcache=refresh>

<sup>105</sup> <https://www.bank.lv/en/operational-areas/licensing/crypto-asset/crypto-asset-service-providers>

<sup>106</sup> <https://www.lb.lt/en/authorisation-of-crypto-asset-service-providers>

<sup>107</sup> <https://www.cssf.lu/en/virtual-asset-service-provider/>

<sup>108</sup> <https://www.mfsa.mt/our-work/virtual-financial-assets/>

<sup>109</sup> <https://www.dnb.nl/en/login/my-dnb-supervision-services/supervisory-applications-service-new-forms/>

<sup>110</sup> <https://www.financemagnates.com/cryptocurrency/poland-to-regulate-crypto-in-2024-knf-empowered-to-impose-fines/>

<sup>111</sup> <https://manimama.eu/mica-implementation-in-portugal/>

<sup>112</sup> <https://manimama.eu/mica-implementation-in-romania/>

<sup>113</sup> <https://manimama.eu/mica-implementation-in-slovakia/>

<sup>114</sup> <https://practiceguides.chambers.com/practice-guides/comparison/990/13590/21421-21422-21423-21424-21425-21426-21427-21428>

<sup>115</sup> <https://gofaizen-sherle.com/crypto-license/spain>

<sup>116</sup> <https://manimama.eu/mica-implementation-in-sweden/>

<sup>117</sup> <https://en.fme.is/supervision/operating-licence-and-registration/>

© FINANCIAL INTELLIGENCE UNIT  
REPUBLIC OF MOLDOVA  
2024

[www.spcsb.gov.md](http://www.spcsb.gov.md)