REPORT

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

December, 2024
Chișinău

Organization for Security and Co-operation in Europe

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

List of figures

Acronyms

AML	anti-money laundering
ATM	automated teller machine
CASP	crypto-asset service provider
CBDCs	central bank digital currencies
CFT	counter financing of terrorism
CNPF	(Moldovan) National Commission for Financial Markets
DeFi	decentralized finance
DEX	decentralized exchange
DLT	distributed ledger technology
DNFBPs	designated non-financial businesses and professions
DNM	darknet marketplace
EDD	enhanced due diligence
EMCDDA	European Monitoring Centre for Drugs and Drug Addiction
FATF	Financial Action Task Force
FI	financial institution
FIU	financial intelligence unit
IaaS	infrastructure-as-a-service
ICO	initial coin offering
IEO	initial exchange offering
IT	information technology
KYC	know your customer
LEA	law enforcement agency
MDL	Moldovan leu
MiCA	(EU) Markets in Crypto-Assets Regulation
MiFID	Markets in Financial Instruments Directive
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
ODD	ongoing due diligence
OFAC	The Office of Foreign Assets Control (US Department of the Treasury)
OJEU	Official Journal of the European Union
OTC	over-the-counter
P2B	person-to-business
P2P	peer-to-peer
PoF	proof of funds
PoW	proof of work
PSP	(non-bank) payment service provider
R	FATF Recommendation
REs	reporting entities
SAR	suspicious activity report
SOF	source of funds
SOW	source of wealth
STO	security token offering
STR	suspicious transaction report
TF	terrorist financing
TFR	(EU) Transfer of Funds Regulation
TOEs	traditional obliged entities
VA/VAs	virtual assets
VASP	virtual assets service providers
VRE	virtual real estate
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, Financial Action Task Force (FATF) recommendations, and local data to assess these risks and proposes regulatory and operational measures to address the identified challenges.

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, and to 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 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, as well as its 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 has 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 the regulatory framework in alignment with EU directives and FATF standards, with a focus on licensing, registration, and VASP oversight; improving international collaboration; and enhancing the capacities of law enforcement agencies (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 best 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 such as 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, the FATF updated its Recommendations to encompass financial activities explicitly involving VAs. 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.[1] This gap in risk assessment could potentially expose the country's financial system to exploitation by illicit actors, which in turn could undermine 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 to the oversight of VAs and VASPs, thereby fostering a balanced regulatory environment that supports innovation while mitigating risks.

In the 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 https://rm.coe.int/moneyval-2024-4-md-5thround-2ndenhfur/1680b05e46

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 to strengthen 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.

To achieve these objectives, this NRA seeks to create a comprehensive and adaptive approach to managing ML/TF risks in the digital financial sector, an approach that will ultimately contribute 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 an early stage of 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 the existing AML/CFT legal framework (*Law No. 308/2017 on prevention and combating money laundering and terrorism financing*[2]), 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 is still available through foreign VASPs, leaving the financial sector vulnerable to ML/TF risks.

The lack of specific regulation in Moldova for VAs and VASPs has prompted policymakers to adopt a high-level strategy aimed at minimizing 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[3] 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[4] advising entities and natural persons to avoid involvement in virtual currency transactions,

2 State register of legal acts, website: https://www.legis.md/cautare/getResults?doc_id=136906&lang=ro# [last accessed: 29 October 2024].

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

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

highlighting potential exposure to ML/TF risks. In 2018, three additional follow-up notices and clarifications[5] were issued that reiterated the risks associated with VAs and advised citizens to proceed with caution in any VA-related activities.

In October 2021, amendments to Law No. 133 of 17 June 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 ten average monthly salaries in the economy.

Prior to the adoption of the 2023 amendments to the AML/CFT Law, the NBM issued another circular on 28 October 2022, instructing banks and payment service providers (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 1 July 2023. These amendments marked Moldova's first attempt to recognize virtual assets and to 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. And yet the enforcement and monitoring mechanisms for prohibition are not defined, which hinders the regulations' effectiveness and risk mitigation. However, reporting entities (REs) are allowed to facilitate transactions for resident clients with foreign-licensed VASPs. When facilitating such transactions, REs are under strict operational conditions and limitations related to clients, accounts, and other aspects.

In fact, according to Article 5 (4^{1-4}), of the AML/CFT Law No. 308/2017, 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;
- not to conduct occasional transactions for/at foreign VASPs;
- to limit activity of local residents with authorized foreign VASPs up to a monthly threshold of approximately €2,600 (50,000 MDL).

When providing such services, REs are required to apply enhanced due diligence, including opening special accounts and implementing information technology (IT) solutions to enable the traceability of transactions (Art. 8 (5^{1}) – AML/CFT Law No. 308/2017).

Furthermore, in addition to the prohibitions outlined in Article 5, paragraphs (4^{1}) – (4^{4}) of the AML/CFT Law 308/2017, 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.**

5 Bank of Moldova, website: https://www.bnm.md/ro/content/bnm-avertizeaza-ca-investitiile-criptovalute-implica-riscuri-inalte [last accessed: 1 November 2024]. https://www.bnm.md/ro/content/banca-nationala-atentioneaza-mod-repetat-asupra-riscurilor-de-investi-criptovalute [last accessed: 1 November 2024]. https://www.bnm.md/ro/content/clarificarea-pozitiei-de-reglementare-si-autorizare-monedei-virtuale [last accessed: 1 November 2024].

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, which was adapted 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 the judgement of experts. 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, private sector participants (banks and PSPs), and foreign FIUs, also requesting assistance in reaching 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: C**onsultation sessions were held with international experts and local institutions to analyse the evolving risks in the virtual asset space.

In evaluating risks, the assessment team relied on identifying threats and vulnerabilities for both VAs and VASPs based on an analysis of the information collected from the sources referred to above, in addition to calculations included in the assessment tool of the World Bank. The assessment also considered input variables in the set of characteristics and attributes through which threats and vulnerabilities in the activities of VAs and VASPs can be identified. This was done primarily from a local perspective, but also from an international perspective due to characteristics inherent in VAs that make them global, borderless, and without restrictions.

2.2. Risk assessment working group

To ensure a comprehensive and co-ordinated 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 in Moldova, including the:

- 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, which offered essential data, trends, and perspectives supporting the analysis and the formulation of recommendations for this risk assessment.

2.3. The World Bank's 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 types, outlines twelve distinct VASP services, and identifies twenty-seven specific activities or channels (*see Table 1, below*). Each of these categories is evaluated using tailored assessment criteria to allow for detailed risk profiling at the product, service, and activity levels.

2.3.1. Identifying relevant VASP channels

The WG's initial step was to identify relevant VASP channels through which Moldova's traditional obliged entities (TOE) and the informal sector potentially interact with VASPs. This structured framework helped 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	Type 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. **Product & services development**
	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 in VA-related commercial activities**
		22. **Non-security tokens & hybrid trading activities**
		23. **Stablecoins**
	Emerging products	24. **Crypto-escrow services**
		25. **Crypto-custodian services**
VALIDATORS / MINERS / ADMINISTRATORS	Proof of work	26. **Fees**
		27. **New assets**

Source: World Bank Methodology

Table 2: Definition of VASPs and types of services (according to the WB Toolkit)

NO	TERMS	DESCRIPTION
1	**VIRTUAL ASSET WALLET PROVIDERS**	**Provide storage for virtual assets or fiat currency on behalf of others and then facilitate exchanges or transfers between one or more virtual assets, or between virtual assets and fiat currency.**
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 the 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 the virtual asset to its owner; rather the funds are held by the custodian providing the virtual asset wallet service. Coinbase is a good example of an exchange and brokerage service that allows people to store virtual assets within a 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 has complete control over the wallet's virtual assets. Non-custodial wallets include the Bitcoin.com client, BRD, Blockchain, BTC.com, Electron Cash, Copay, Jaxx, Coinomi, Edge, and many more. These platforms give users the ability to store their own private keys.
2	**VIRTUAL ASSET EXCHANGES**	**VA exchanges provide 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. They also issue their own virtual assets in order to facilitate virtual asset transfers and exchanges.**
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 of virtual assets to government issued fiat currencies
2.4	VIRTUAL-TO-VIRTUAL	Conversion of one type of virtual asset to another
3	**VIRTUAL ASSET BROKING / PAYMENT PROCESSING**	**This arranges transactions involving virtual assets, or involving virtual assets and fiat currency.**
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 a cash or debit card. Some virtual currency ATMs offer bi-directional functionality enabling both the purchase of virtual assets and the sale of virtual assets for cash.
3.2	MERCHANTS	Acceptance of VA by merchants in exchange for fiat currencies for payment settlement
3.3	CARDS	Use of stored value virtual assets cards for purchases online

NO	TERMS	DESCRIPTION
4	**VIRTUAL ASSET MANAGEMENT PROVIDERS**	
4.1	FUND MANAGEMENT	Fund managers investing in virtual assets
4.2	FUND DISTRIBUTION	Firms that distribute funds which invest (wholly or partially) in virtual assets
4.3	COMPLIANCE, AUDIT & RISK MANAGEMENT	Support for guidance on risk management, management of liquid capital, segregation of assets, custodianship, funds structure, and other legal aspects.
5	**INITIAL COIN OFFERING (ICO) PROVIDERS**	**ICO providers issue and sell virtual assets to the public. They may be involved in participating in and providing financial services related to the ICO.**
5.1	FIAT-TO-VIRUAL	Fund raising for ICOs that attracts fiat currency investments converted into virtual assets
5.2	VIRTUAL	Fund raising for ICOs that attracts virtual asset investments
5.3	DEVELOPMENT OF PRODUCT & SERVICES	Raises funds used as an investment to develop product & services
5.4	INITIAL EXCHANGE OFFERING (IEOs)	An IEO is hosted by a project team alongside a cryptocurrency exchange.
5.5	SECURITY TOKEN OFFERINGS (STOs)	STOs offer equity in the form of tokens.
6	**VIRTUAL ASSET INVESTMENT PROVIDERS**	**Provide 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).**

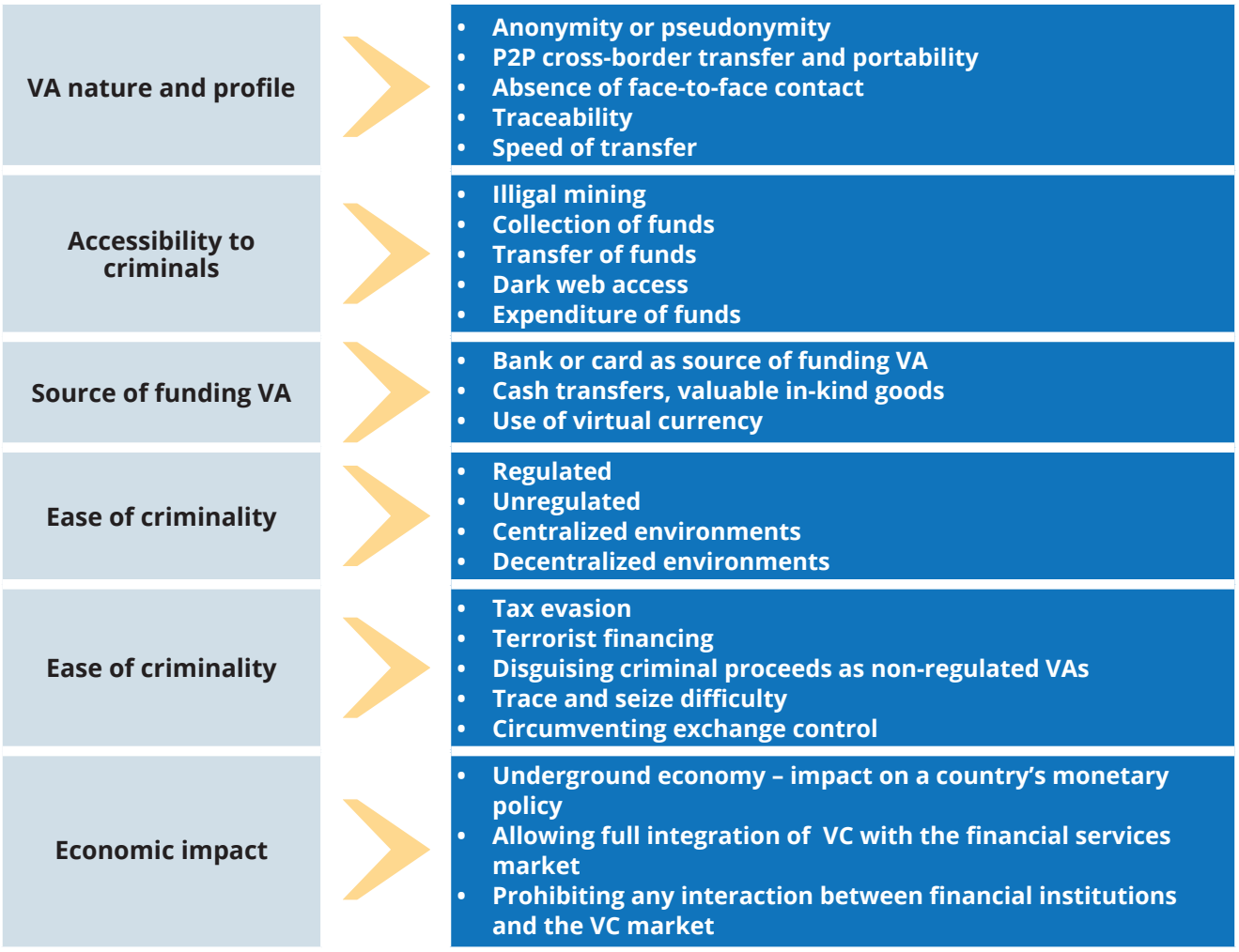
NO	TERMS	DESCRIPTION
6.1	PLATFORM OPERATORS	Online platforms that facilitate active trading (future contracts) in virtual assets inherently have a broad customer base, substantial local presence, and are considered to have a sound corporate governance structure. Unlike automated trading venues, or equities and futures exchanges where investors trade through licensed intermediaries, virtual asset trading platforms interface directly with the public. **1. Regulated environment:** Platforms are licensed, making the standards and controls they must comply by transparent for investors. Moreover, there is a clear basis for distinguishing between licensed and unlicensed platforms. Products included in a platform are licensed by a regulatory body and must comply with the specified requirements of that body's regulatory framework. **2. Unregulated environment:** 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.
6.2	CUSTODY OF ASSETS	Virtual asset trading platforms hold virtual assets on behalf of their clients and also act as marketplaces matching buyers and sellers. **1. Regulated environment:** A regulated entity is likely to find it easier to establish banking ties to facilitate conversion between cryptocurrency and fiat money. Such entities are expected to fulfil know-your-client requirements, to undertake anti-money-laundering and counter-financing of terrorism, and to know the source of funds and wealth of clients holding assets. A virtual asset trading platform operating in a regulatory environment is also expected to offer client protection in a manner equivalent to traditional financial institutions in the securities sector. **2. Unregulated environment:** an unregulated environment offers limited or no protection on investments, and practices anonymity without fulfilling know-your-client requirements, or anti-money-laundering and counter-financing of terrorism requirements
6.3	INVESTMENT INTO VARELATED COMMERCIAL ACTIVITIES	Virtual asset-related commodities (such as mining devices).
6.4	NON-SECURITY TOKENS & HYBRID TRADING ACTIVITIES	A tokenized security can provide its holder 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 accounting unit, like bitcoin.
6.5	STABLECOINS	Stablecoins typically claim to have a mechanism that seeks to stabilize 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 when they are planned to be adopted on a global scale.

NO	TERMS	DESCRIPTION
6.6	CRYPTO ESCROW SERVICE	In a crypto escrow service, virtual assets are held by a third party until the transaction is completed and all of the involved parties signal that they are satisfied. Escrow is usually done due to trust issues: the seller wants to be sure the buyer will send the money after they have received the goods or services; the buyer wants assurance that they receive the purchased item at the specified time and under the specified conditions. Crypto escrow services are especially important for online transactions in which the parties remain anonymous from one another, or if the parties are not in geographical contact and thus there may be factors preventing the transaction's completion. Parties may come to disagreements during or after the delivery of services, since there may be situations in which a transaction is not governed by law due to location-related issues, issues related to the legal jurisdiction, or other problems.
6.7	CRYPTO-CUSTODIAN SERVICES	Cryptocurrency custodian services provide independent storage and security systems used to hold large quantities of tokens or virtual assets. Custody solutions are one of the emerging services of the cryptocurrency ecosystem for supporting the entry of institutional capital into the virtual assets industry.
7	**VALIDATORS / MINERS**	**Mining hardware providers (e.g., Butterflylabs), or cloud-based mining companies (e.g., Genesis Mining)**
7.1	Fees	Institutional units that validate and confirm transactions are called miners. In a virtual currency transaction, miners are considered bookkeepers or distributed ledger updaters. A transaction can only be considered secure and complete once it is included in a block. Mining can be undertaken by miners individually (solo mining) or as part of a pool (pooled mining). Miners receive a fee for this service. They can also be a wallet holder.
7.2	New assets	In a proof of work (PoW) system, network participants must solve cryptographic puzzles in order to add new blocks to the blockchain. The first miner to successfully produce the PoW is rewarded with a newly mined virtual currency or assets.

2.3.2. Assessing threats, vulnerabilities, and mitigation measures

a. Input variables for a ML/TF threat[6] assessment
To determine the ML/TF threat level associated with VAs/VASPs, each VASP channel identified in *Table 1* was assessed based on the following six intermediate variables:

Figure 1: Input variables for ML/TF threat assessments



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

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[7] assessment
The inherent ML/TF vulnerability of each applicable VASP channel indicated in *Table 1* was analysed based on the **nature of products and services and the types of VAs**, which includes the following input variables:

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

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

Table 3: Input variables for ML/TF vulnerability assessments

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

The combined ML/TF threat and ML/TF inherent vulnerability rating for each channel was 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 was calculated based on the total combined ML/TF risk after taking mitigation measures into consideration.

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

Table 4: Mitigation measures input variables

	Intermediate Variable	Input Variables
MITIGATING MEASURES	**Government measures**	Comprehensiveness of the AML/CFT legal framework
		Availability and effectiveness of entry controls
		Adequate supervision and monitoring mechanisms
		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 VAs
		Effectiveness of international co-operation
		Quality of guidance issued to VASPs and engagement with VASPs
	VASP measures	Transparency of the VASP's shareholder structure
		Quality of the VASP's governance structure and level of accountability
		Effectiveness of compliance functions and internal control mechanisms
		AML/CFT knowledge of the VASP staff
	Financial institution (FI) measures and designated non-financial businesses and professions (DNFBPs)	Risk assessment and risk mitigation measures by FIs and DNFBPs, referred to in this guide as traditional obliged entities (TOEs)
		Effectiveness of compliance functions and internal control mechanisms

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 the 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 the 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, training, and key statistics. The WG received a total of 29 completed responses, as outlined below.

Table 5: VA/VASP questionnaire survey respondents

Category	Number of Respondents
PUBLIC SECTOR	
LEAs and intelligence services	9
Regulators	2
PRIVATE SECTOR (traditional obliged entities)	
Banks	11
PSPs	7
TOTAL	**29**

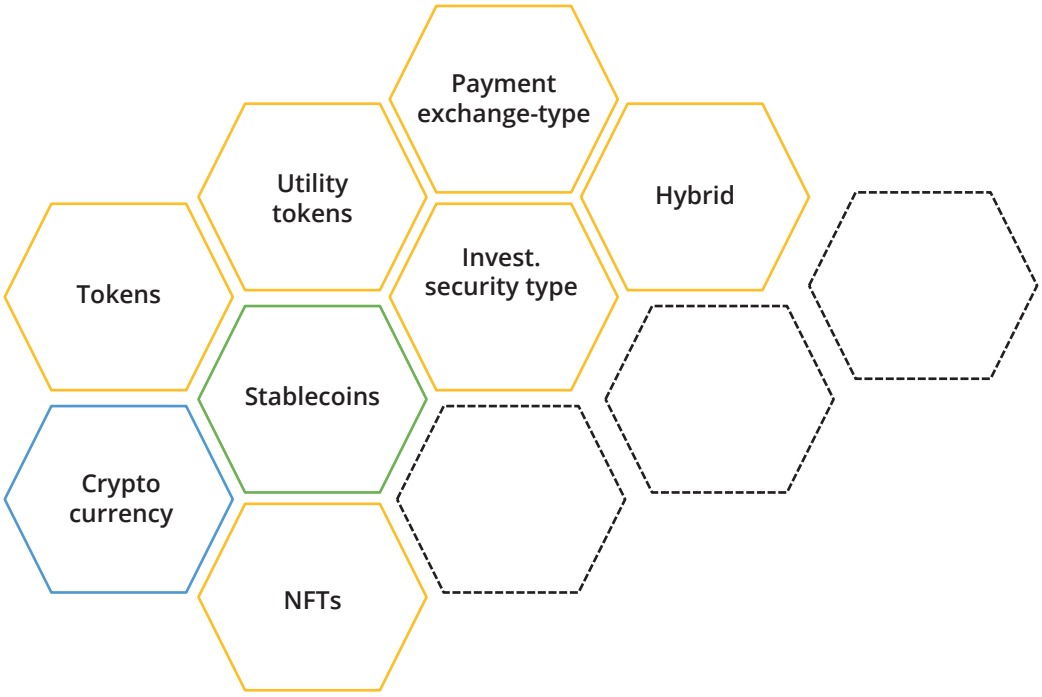
3. Overview of global VA and VASP ecosystems

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

3.1. Evolution of VA/VASP ecosystems and ML/TF risks

On 31 October 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.[8] Numerous prior attempts had been made to establish a peer-to-peer payment system guaranteeing its users anonymity (e.g., eCash, E-Gold, Bit Gold, B-Money, etc.), which illustrated the need for decentralized payments.

Figure 2: Growth of the VA ecosystem



Since then, many cryptocurrencies with new features have been developed and continue to emerge, with privacy-enhanced coins (e.g., Monero, Zcash, Dash, etc.) and stablecoins (Tether, USDC, DAI, etc.) the best-known examples. The VA ecosystem experienced growth due to 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. With unique, identifiable assets representing pieces of art, digital content, or videos being tokenized via blockchain, this served investment purposes.

According to publicly available statistical data, the global market capitalization of cryptocurrencies surpassed $3 trillion (as of November 2024),[9] a strong indication of the growing popularity and access to VAs. Globally, ever more individuals and entities are interested in purchasing cryptocurrencies, and thus the need for applying VAs

8 Bitcoin Whitepaper: https://bitcoin.org/files/bitcoin-paper/bitcoin_ro.pdf [last accessed: 11 November 2024]

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

to the range of transactions is visible.

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 in market size.[10] The NFTs market may also be vulnerable to ML threats and present opportunities for fraud and manipulation.[11] The same can be said about the stablecoins, which pose a 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 also represent the growing ML/TF threat, since the anonymous or pseudo-anonymous[12] characteristics and technological innovation of cryptocurrencies have naturally attracted and keep attracting the attention of illicit actors.

Indeed, being used in ML/TF schemes and associated with various predicate offences, such as fraud and drug trafficking, cryptocurrencies have 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 to €3.145 billion.[13] According to some estimates, Moldova, amongst the other countries, has exhibited an increase in DNM revenue engagement over time.

Facilitating payments while avoiding a central overseeing body and without adequate regulation leads to suspicious transactional activity remaining undetected and unreported to FIUs. Furthermore, cross-border transactions involving VAs have no restrictions on geographic location. Even though cryptocurrency exchanges are the most common channel for initially obtaining cryptocurrencies, they can also be obtained via other means, such as mining or the sale of goods and/or services.

It's important to note that most VA-related businesses are centralized to some degree or another. However, there are financial services on public blockchains, for example 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 have been early adopters of innovative technologies and have quickly exploited 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

10 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: 6 October 2024].

11 E.g., on 11 January 2022, scammers staged one of the biggest NFT rug-pull scams using the Solana blockchain. About $1.3 million in funds were lost with the promise to mint Big Daddy Ape Club NFT.

12 Enhanced anonymity VAs are designed to obscure the links between wallet addresses that could be traced through blockchain analytics.

13 European Monitoring Centre for Drugs and Drug Addiction, Cryptocurrencies, and Drugs: Analysis of cryptocurrency use on darknet markets in the EU and neighbouring countries, background paper commissioned by the 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 [last accessed: 3 October 2024].

service. In addition, cross-chain bridges are 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. = received; 3) values rounded to 2 decimal places.
Source: EuropeanMonitoring Centre for Drugs and Drug Addiction

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

Entities that are obliged to introduce know-your-customer (KYC) and AML rules can be of great help to LEAs in establishing perpetrators' identities and tracing transactions to real-world individuals. According to Europol,[15] in recent years, there has been 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 if they refuse 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 the awareness of the financial institution. Such customers may be acting as unlicensed peer-to-peer crypto brokers, or even holding accounts for companies that are trying to remain under the radar. For example, companies engaged in mining activities may declare their activities as related to technology, however, abnormally high utility bills, such as electricity, may be an 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 VAs/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 having prohibited VASPs have done so without assessing the risks relating to VAs/VASPs in their jurisdiction.**[16] 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 co-operation mechanisms**. Furthermore, it is essential to establish and enforce appropriate measures to sanction illegal VASP activities. When dealing with unregistered VASPs, the issue arises of how to detect them in practice. Detecting unregistered VASPs requires education at all levels: LEAs need grassroots training to identify the use of unregistered VASPs when investigating predicate offenses and parallel money laundering investigations. Traditional FIs need education and guidance to identify the flow of fiat currency into VASPs.[17] Globally, tendencies towards better regulation have been observed.

14 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 accessed: 8 October 2024].

15 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 accessed: 3 October 2024].

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

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

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. This regulation, which is mandatory for all EU Member States, creates a single market for VAs. MiCA is the first cross-jurisdictional regulatory and supervisory framework around the world that has not entered into power as a standalone document.

The EU, as a member of the FATF, is striving to fully implement the FATF's R.16, and thus the Transfer of Funds Regulation (TFR) sets EU-wide rules for enforcing the "Travel Rule". The TFR requires capturing transaction information for all amounts, with a threshold of €1000 for self-hosted wallets. However, it does not apply to hardware wallet providers, nor to software or self-custody wallet providers that do not have control over VAs.[18]

MiCA replaces individual regulations or the lack of regulation within individual Member States. It establishes a 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 between tokens that can be defined as financial instruments and other VAs. Financial instruments are regulated by already existing legislation (in particular, the Markets in Financial Instruments Directive [MiFID]). NFTs do not fall under MiCA regulation, and nor do decentralized digital assets. Also, MiCA excludes central bank digital currencies (CBDCs). Its implementation phase started in April 2023, and it came into power at the end of the year 2024. The regulation requires Member States to choose a national regulator to oversee authorization procedures for crypto-asset service providers (CASPs), i.e. licensing. **As this regulator, most jurisdictions have chosen either their financial market authority acting as an independent institution, or their national central bank** (*See Table 23, Section 9.3*).

The FATF Recommendations provide authorities with considerable flexibility in selecting the supervisory model that best suits their needs. The choice must 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, the MiCA regulation is not aimed at AML/CTF questions. However, the requirements presented by MiCA do add to the mitigation of risks related to ML/TF activities. The regulation has been implemented in stages: it became effective for stablecoins on 30 June 2024; it was fully implemented at the end of 2024.

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

- **White paper:** A mandatory document for crypto asset issuers that provides technical information about 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 non-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, or the offer is made only to qualified investors.
- **Reserve:** Asset reference tokens and e-money tokens are subject to additional requirements, such as 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 may not allow users** to trade assets with **full anonymization**.

Regulatory changes can significantly affect market concentration and the movement of VASPs between neighbouring countries. For example, in 2017, Estonia became one of the first EU nations to establish a licensing regime requiring VASPs to implement anti-money laundering programmes and other controls before being approved to operate. In 2020, the regulations for licensing VASPs were tightened still further, with capital requirements being raised and mandates that VASPs open physical offices and hire staff in Estonia, among other stipulations. As a result, hundreds of cryptocurrency platforms could no longer do business in Estonia, platforms that subsequently relocated to Lithuania, where regulations were laxer at the time.[19] By harmonizing such regulations, the EU ensures, amongst other benefits, that situations such as this will not occur in the future.

18 For more information, see the Annex.

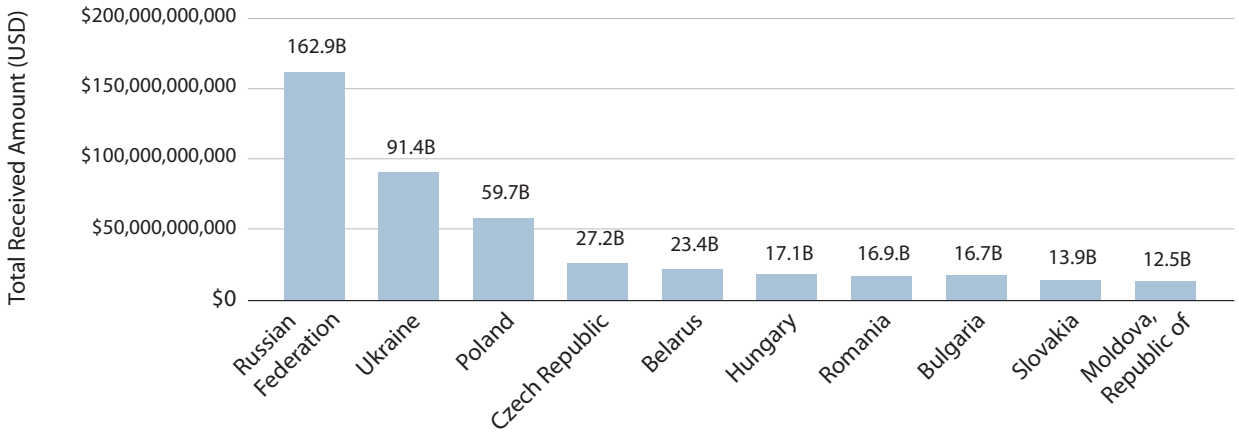
19 ACAMS, Baltic Officials Shed Light on Cryptocurrency Crackdown, Russia Sanctions Evasions, website:MoneyLaundering.com :: Changes in Bank Regulations, Financial Compliance Regulations, Regulation Banks, Money Laundering Cases, Anti Money Laundering, Money Laundering Training [last accessed: 1 November 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 neighbouring regions, as provided by Chainalysis.[20] 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 1 January 2021 to 30 June 2024. The most recen**t web traffic data included in this section is from 30 June 2024.

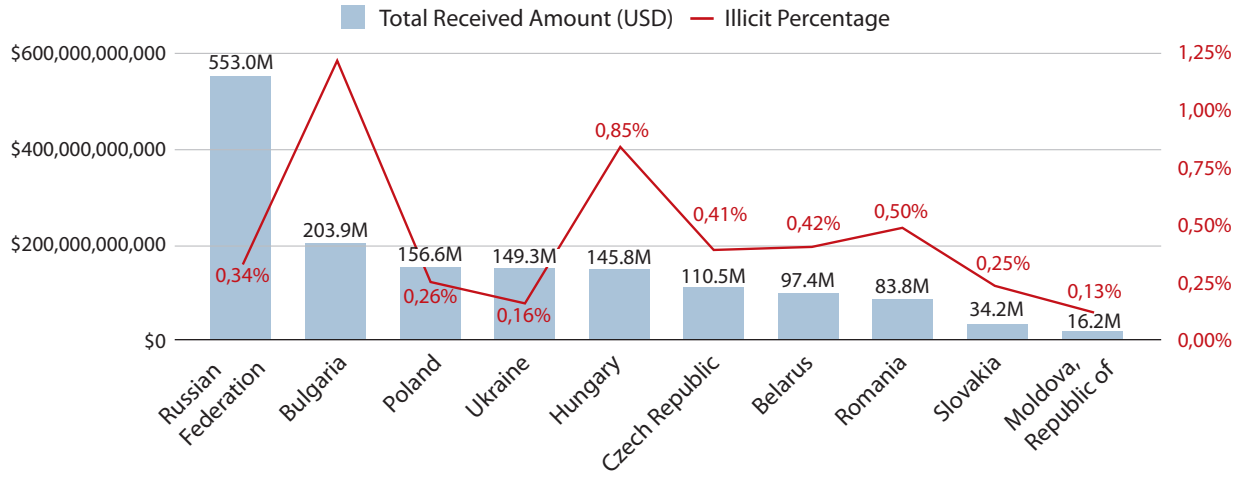
Figure 4: Total flows to a selection of Eastern European countries (June 2023 to June 2024)



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 one 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. Since the vast majority of cryptocurrency flows at some point in time through VASPs operating internationally, and in turn residents in the above countries also tend to utilize VASPs at some point in time, value received is a relatively good proxy for comparative levels of cryptocurrency activity in these countries.[21]

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

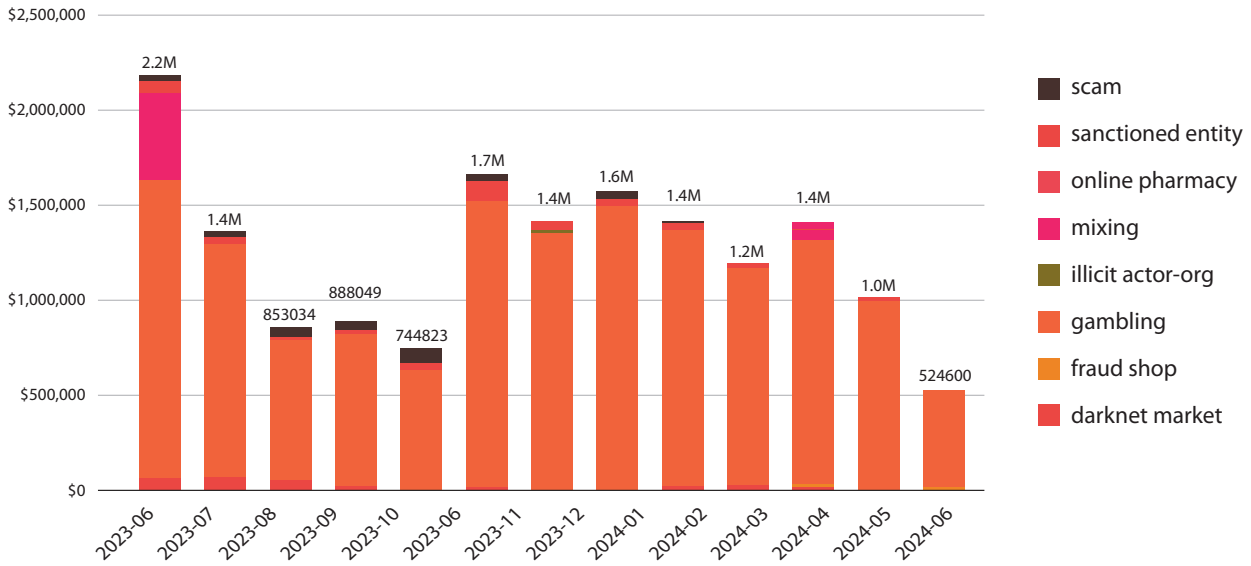


20 Chainalysis, 2024 Report: Election Interference & Cryptocurrency: Indicators of Russian Interference in Moldova.

21 Note though that as this is not value held, this figure represents activity or cryptocurrency movement, rather than aggregate value possessed by the residents of a country.

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 neighbouring 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 (June 2023 to June 2024)



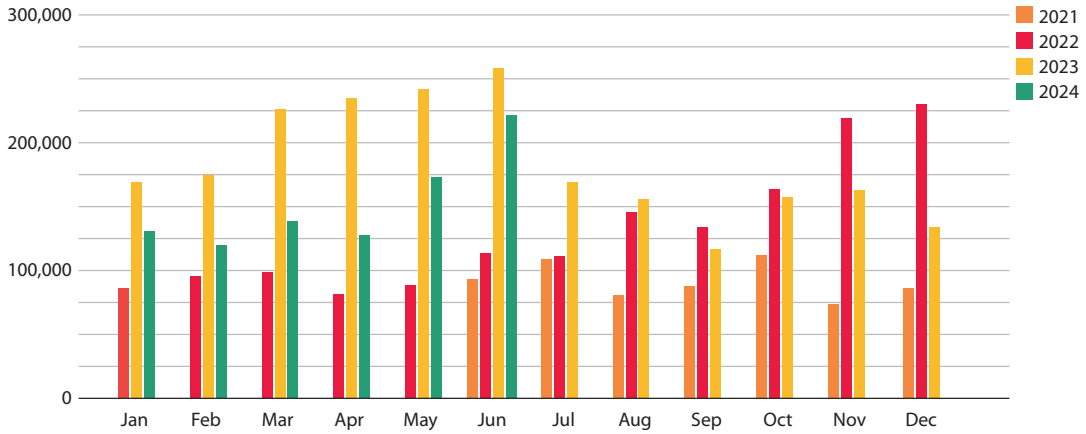
The "illicit" flows by category show a breakdown by month of the type of service at which "illicit" crypto originated before being received in Moldova from June 2023 to June 2024. The precise definition of "illicit" varies by country depending on the laws of specific countries. The categories above are 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 by month, June 2021 to June 2024**

The next three charts compare the frequency of deposit transactions in Moldova by month from June 2021 to June 2024. Examined is the number of deposit transactions, rather than the USD equivalent value of the amount of cryptocurrency sent or 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 (June 2021 to June 2024)



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

➢ **Most accessed services in Moldova by web visits, June 2024**

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 (June 2024)

Month/year	Name	Category	Visits	Share
June 2024	Reddit.com	other	1398254.29	0.00058747
June 2024	Telegram.org	wallet	860197.529	0.00254937
June 2024	Binance.com	exchange	685532.139	0.01081282
June 2024	FreeBitco.in	gambling	539785.367	0.01238618
June 2024	Whitebit.com	exchange	474728324	0.02003786
June 2024	Bitcoin.com	exchange	221472.251	0.04133182
June 2024	Bybit.com	exchange	146195.596	0.00438988
June 2024	NV.UA Donation (Ukrainian media)	other	118961.214	0.00501775
June 2024	Archive.org	other		0.0006959
June 2024	FaucetPay.io	exchange	81199.2218	0.01137306
June 2024	Rollercoin.com	gambling	79629.3225	0.0116982
June 2024	Okx.com	exchange	63597.6165	0.00219462
June 2024	Reported as etherscan.io	scam	55489.469	0.00524423
June 2024	Crypto.com	exchange	48445.5216	0.01193198
June 2024	Coinbase.com	exchange	44298.0737	0.00129343
June 2024	Bitfinex.com	exchange	42301.8787	0.04745851
June 2024	Reported as telegra.ph	scam	42198.7178	0.00175441
June 2024	AdBTC.top	scam	357341821	0.00591062
June 2024	proton.me	infrastructure as a service	33938.4751	0.00050028
June 2024	Pancake Swap V2: MAV USDT Ox1b0d5e- 0x55d398 [BNB Smart Chain]	dexchange	31778.5438	0.00907544

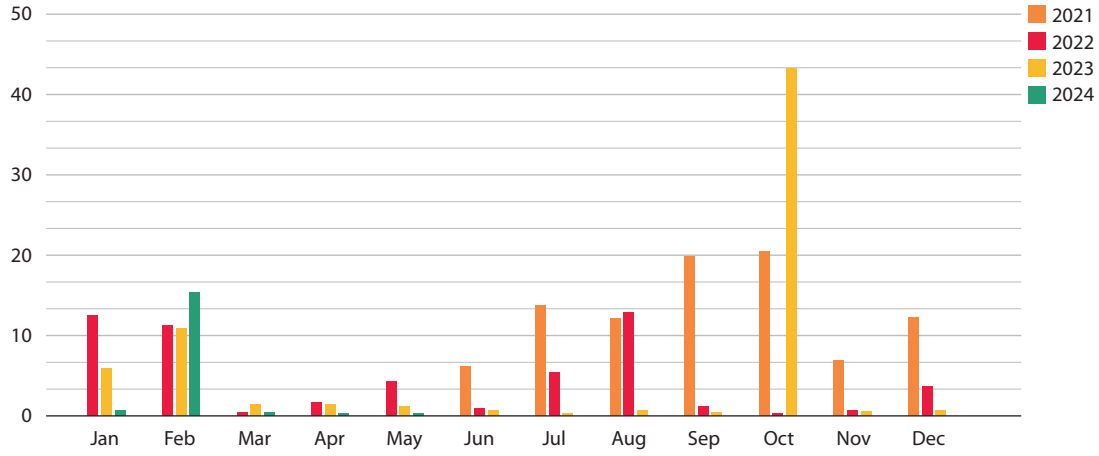
Listed above are the top twenty services by number of visits in Moldova in the most recent month for which Chainalysis has data. Notably one of these services is proton.me – an enhanced online privacy services provider that Chainalysis characterizes as an infrastructure-as-a-service (IaaS) provider.

➢ **Infrastructure-as-a-service deposits, June 2023 to June 2024**

IaaS may be used to host websites that seed misinformation while obscuring the true source of that misinformation. It can also 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 categories in Moldova over one 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. The graph shows the number of independent transactions per month (which are a 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 users to whom they are providing infrastructure. In most cases withdrawals represent funds controlled by the infrastructure providers, not their users.

Figure 8: Moldova deposit frequency to infrastructure-as-a-service providers (June 2021 to June 2024)



➢ **Chainalysis 2024 Crypto Adoption Index Report**

Recently, blockchain analytics company Chainalysis ranked Moldova as 59th out of 151 countries in the 2024 Global Crypto Adoption Index.[22] This is a significant increase compared to the ranking in 2020 when the index was introduced: At that time Moldova was ranked 88th.

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

a. **Centralized service value received**: Moldova ranks 37th, indicating a relatively high usage of centralized platforms for cryptocurrency transactions and services.

b. **Retail centralized service value received**: Moldova ranks 38th, showing that the country has a strong level of adoption among individual retail users in centralized crypto services, suggesting significant personal engagement with mainstream platforms.

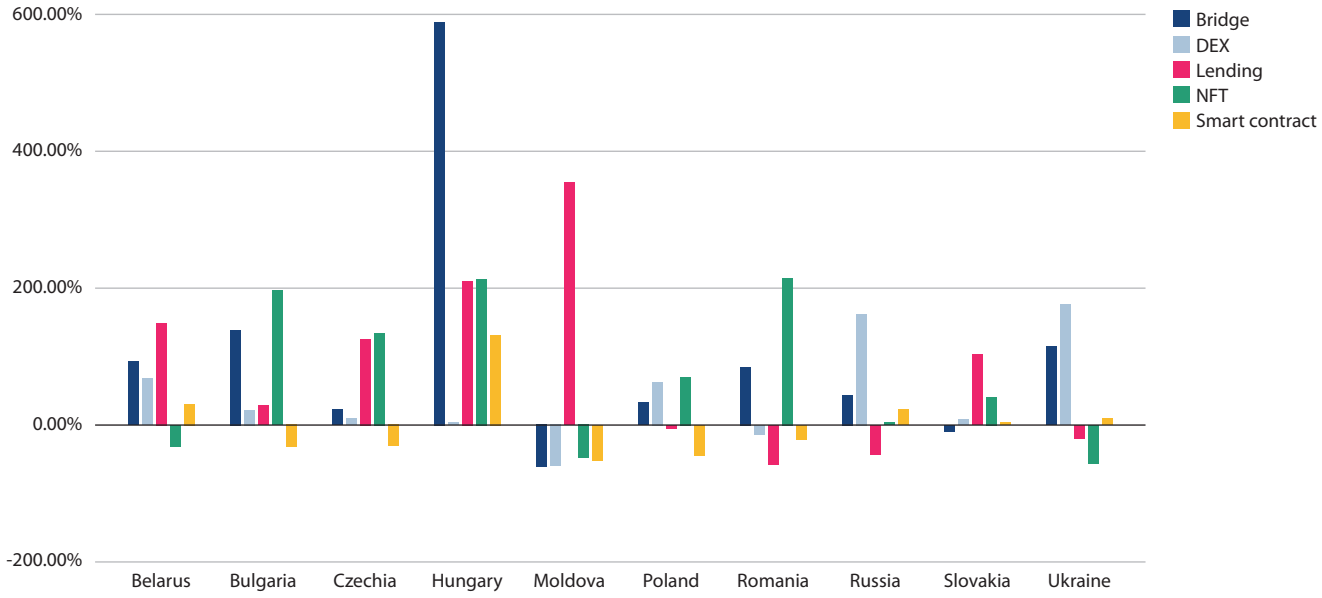
c. **DeFi value received**: Moldova ranks 94th in terms of value received through decentralized finance (DeFi) platforms. This lower position implies limited use and engagement with DeFi protocols.

d. **Retail DeFi value received**: Positioned at 88th, Moldova has modest participation in retail DeFi activities, which points to limited uptake of DeFi services among individual users.

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

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

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** in 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 in the region.

3.4. ML/TF risks associated with VAs and VASPs

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

Providing 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**.[23] 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 citizenship, 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. This adds a layer of difficulty to international co-operation and statistical data gathering. Although the activity of VASPs is prohibited in Moldova, ML/TF risks associated with 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

23 Art. 8 of AML/CFT Law No. 308/2017, website: https://www.legis.md/cautare/getResults?doc_id=136906&lang=ro

bridge the fiat and crypto worlds. Although AML/CFT requirements can vary by jurisdiction, and despite exchanges requiring customers to undergo know your customer (KYC), ongoing due diligence (ODD), and enhanced due diligence (EDD) procedures, if they have a lax approach to transaction monitoring and the reporting of suspicious activities, this poses 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 the 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): Such services obscure the on-chain connection between the source and current addresses. For example, the use of mixers (Tornado Cash,[24],Chip Mixer[25]) or privacy-enhanced wallets (e.g., Samourai wallet[26]) are known means used by criminals to obfuscate the origin of illicit funds or the illicit destination of transferred funds. According to Chainalysis, in 2023 mixers consistently accounted for a significant portion of ransomware-related transactions, which indicates that they are a preferred means for laundering ransomware payments.[27]

c. ML/TF risks associated with P2P exchanges, OTC desks, gambling services, and crypto ATMs: These type of services provide possibilities to convert fiat currency into VAs and VAs to fiat currency. P2P exchanges and online operators offering gambling services that allow deposits with cryptocurrencies offer a certain level of anonymity. Such services are attractive to illicit actors, who can use them to send funds from illicit activities 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 potential to threaten financial stability raise concerns.[28] **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 funds are being used for illegal activities**. However, a**ccording to Chainalysis,**[29] **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 proofs and ring signatures.[30] These features can facilitate layering for illicit activities. Criminals may convert their earnings from Bitcoin or other cryptocurrencies into privacy coins via unregulated exchanges. 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 allowing such transactions. Furthermore, sanctioned individuals may 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.[31] Criminals may deposit virtual assets obtained from illegal activities onto such cards, or use virtual assets of illicit origin to purchase fiat currency cards for laundering purposes. Additionally, bad actors may 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.[32]

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

24 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 accessed: 27 October 2024].

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

26 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].

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

28 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].

29 Chainalysis – The 2024 Crypto Crime Report, p. 7

30 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 accessed: 1 November 2024].

31 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.

32 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 [last accessed: 4 March 2025].

defined payout mechanisms and fee structures for their usage. Mining pools can be used as a means of self-funding[33] for illicit activities or money laundering.

i. **Other concerns (Metaverse)**: 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%.[34] New trends are emerging in the areas of Metaverse's economy, governance, and user experience, along with new types of crime specifically related to Metaverse. One notable development is blockchain-based virtual real estate (VRE) within Metaverse, as well as the use of Metaverse tokens to facilitate transactions within the ecosystem. While these tokens are primarily used within Metaverse, some are also available on exchanges.

33 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. Iran is also the eighth largest oil producer in the world, with 4% of global oil production. Given the extensive sanctions against Iran limiting 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.

34 Techreport, Metaverse Statistics 2024: Latest User & Market Trends, website: Metaverse Statistics 2024: Latest User & Market Trends [last accessed: 3 November 2024].

4. Survey responses

4.1. Responses of law enforcement agencies (LEAs) and intelligence services to the VA/VASP survey

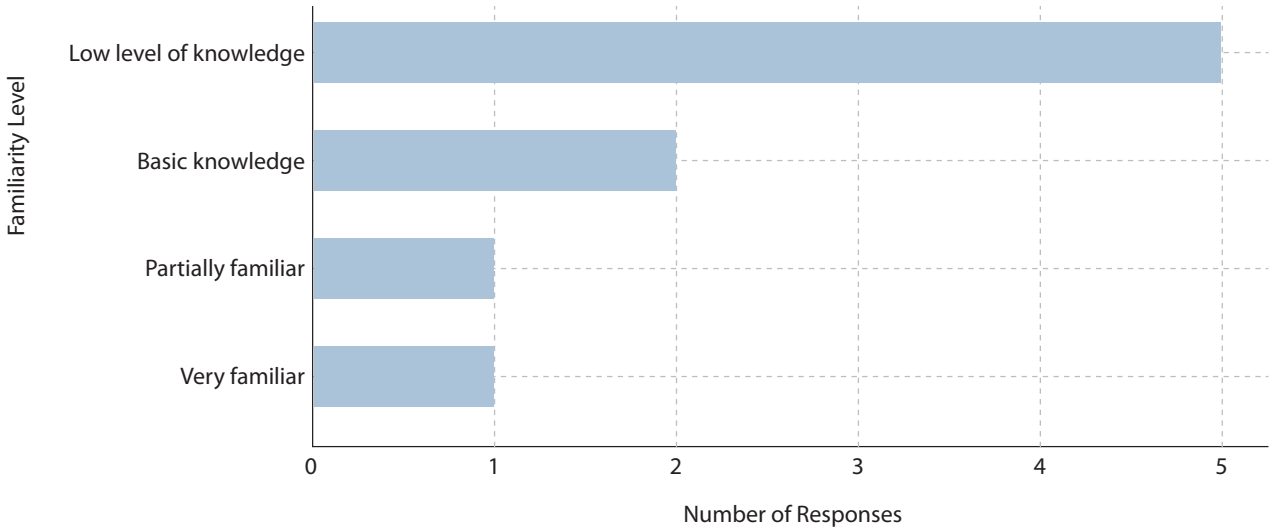
Respondents:

- 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 (five authorities) reported having a **low level of familiarity** with VAs/VASPs, suggesting a substantial knowledge gap in this sector. A smaller segment (two authorities) reported having **basic knowledge**, indicating some basic understanding but a lack of 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 such 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 co-operation through financial intelligence units (FIUs) may be prolonged. While tracing of borderless blockchain transactions can typically be accomplished within minutes, the above limitations hinder such 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. LEAs should also be able to seize and store assets in a designated wallet.

On a positive note, all the law enforcement agencies confirmed an increase over the last three years in training and workshops, which have been provided by various organizations and programmes. 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, 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 programmes 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 VAs/VASPs, including: lack of a supervision/regulatory authority in the sector; no reporting from this sector as a result of the prohibition of VASP services within the country; and no clear taxation regime for VAs.

Authorities also emphasized that rapid technological innovation and slow regulatory response has created 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 example, P2P trading (*as 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 co-operation 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 VA and VASP services as presenting a high risk of being 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,[35] 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 and have pointed to potential financial crimes such as money laundering, fraud, drug trafficking, and illicit use of virtual assets.

Statistical overview of filed STRs and SARs

The statistics on STRs and SARs related to VAs/VASPs indicate a notable increase in the frequency of reports, particularly from the 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:

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

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

Year	Banks	PSPs	Total
2021	6	10	**16**
2022	6	12	**18**
2023	11	1	**12**
2024	32	1	**33**

Key indicators and red flags leading to STR/SAR filings
Several key indicators have been identified as common triggers for filing STRs/SARs associated with VA-related activities. These indicators reflect complex layering tactics and financial behaviours 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. Such 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 and unemployed individuals, as well as retirees, who can be more susceptible to manipulation or less aware of compliance requirements.
- **Opening of multiple bank accounts:** Clients opening multiple accounts at the same bank or across different banks without a clear economic purpose have raised suspicions. Frequent transfers between these accounts, transfers that lack 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 transactions. This opacity can point to attempts to obfuscate illicit origins, especially in transactions involving cryptocurrency platforms.

Once received and analysed by the FIU, most of the STRs/SARs related to virtual assets 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 6 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 or fraudulent shops:** Instances in which individuals have engaged with known dark web marketplaces or fraudulent e-commerce platforms through cryptocurrency transactions.
- **Cryptocurrency investment scams:** Reports involving suspected fraudulent schemes in which 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 a 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 in which 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 the amount of 760,000 MDL. This dramatic decrease may be linked to the implementation of restrictive measures affecting VAs/VASPs, which has potentially discouraged voluntary disclosures.

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

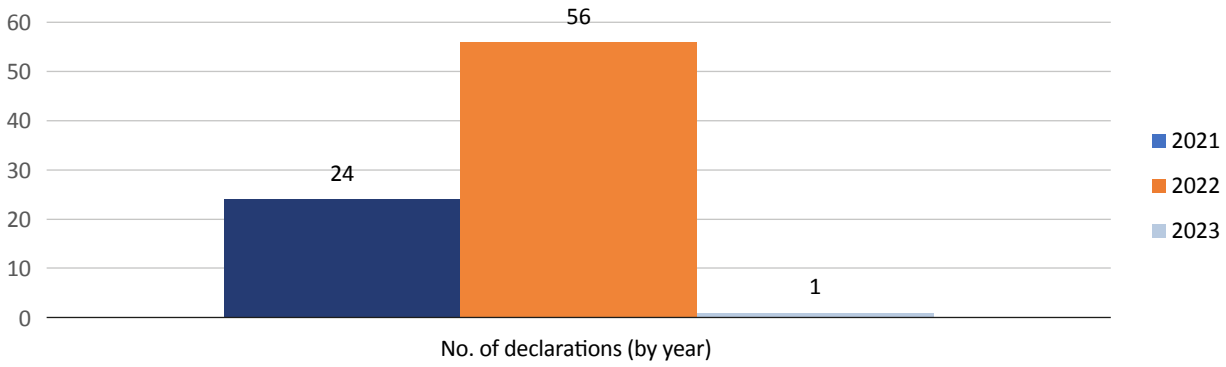
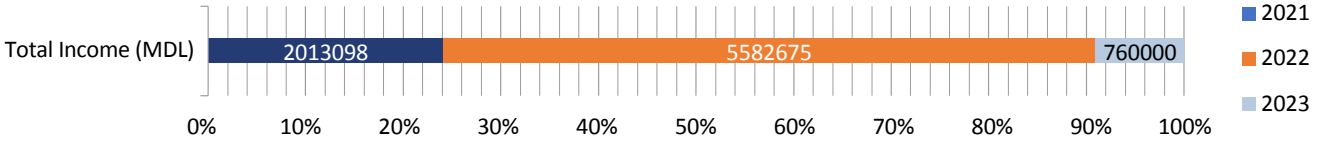


Figure 12: Total declared income from VAs (2021–2023)



Predicate offences associated with VAs/VASPs

According to the responses of LEAs, it was observed that between 2021 and 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 VAs and VASPs by predicate offence and by year (2021–2023)

Offence	No. of cases[36]		
	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 financing	0	1	2
TOTAL	**149**	**101**	**179**

36 Criminal cases and other type of investigations.

Figure 13: Total predicate offences associated with VAs and VASPs (2021–2023), as percentages

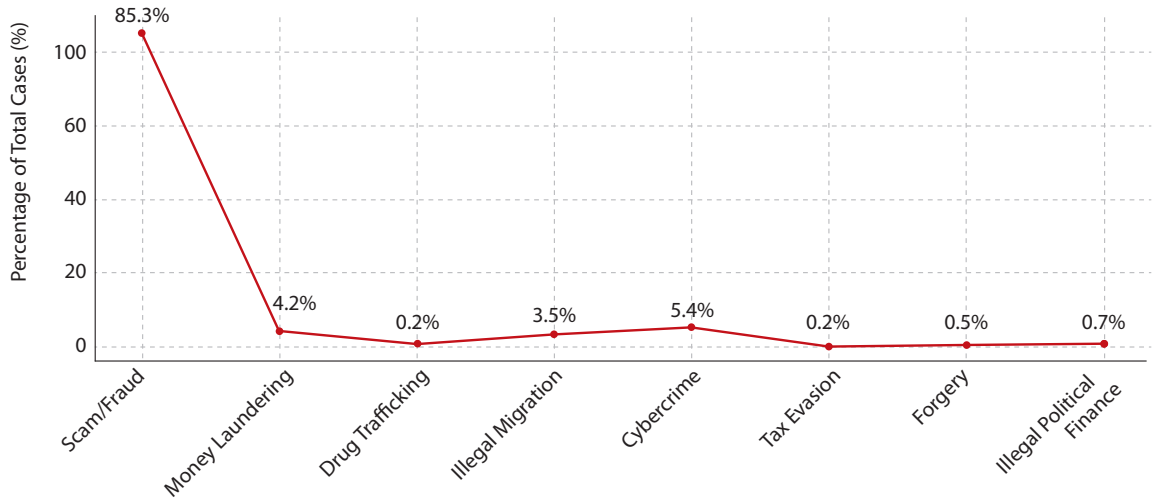
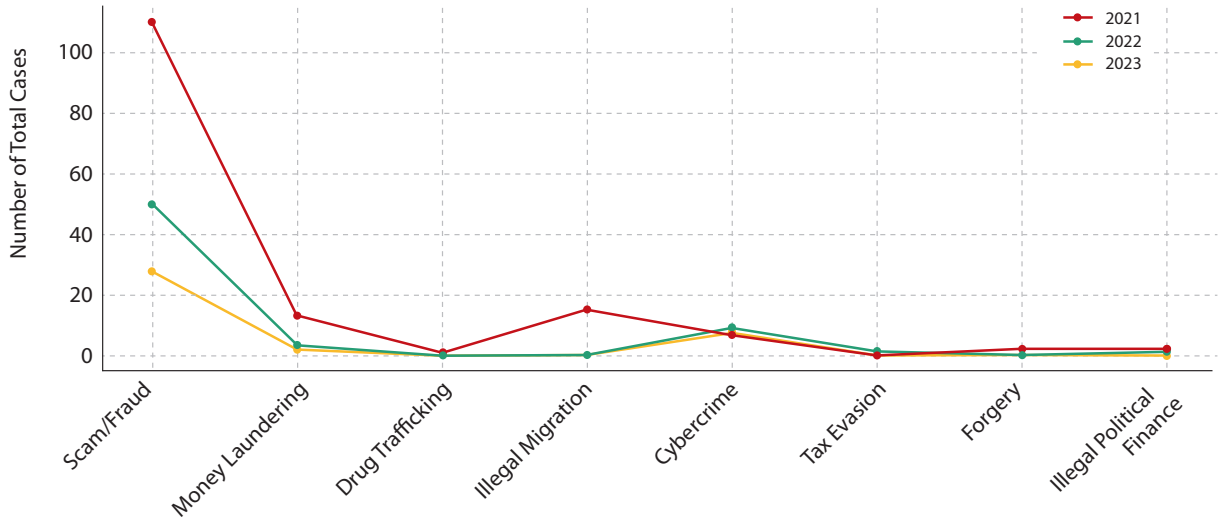


Figure 14: Number of predicate offences associated with VAs and VASPs (2021–2023), by year



Referring to *Table 9, and Figures 13 and 14,* we can see a notable rise in the number of scam cases linked to VAs/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 being increasingly targeted by scams**. To mitigate these risks effectively, proactive monitoring and preventive measures are needed by law enforcement, regulatory bodies, and private stakeholders.

The volume of seized cryptocurrency assets between 2021 and 2024
The statistical data provided by the LEAs highlights their 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 seized virtual assets 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)

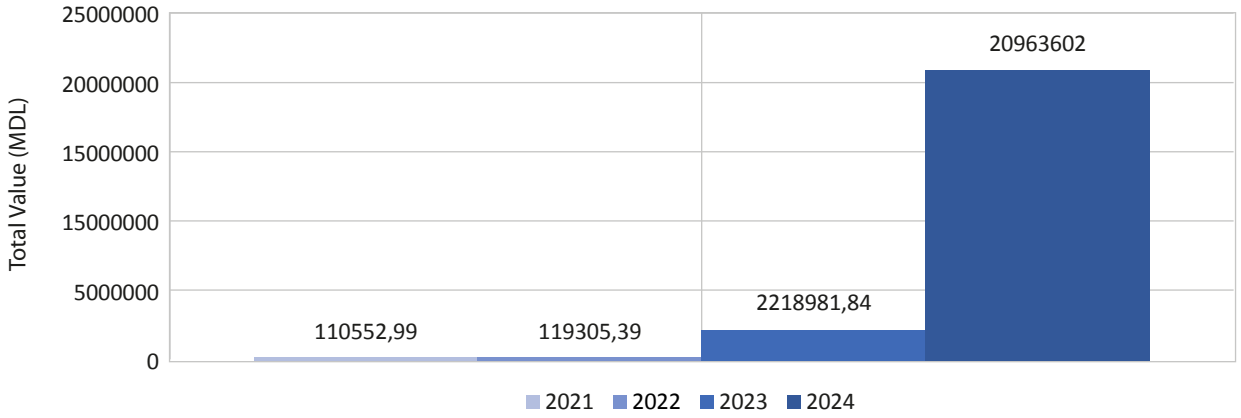


Table 10: Value of VAs seized by LEAs (2021–2024)

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 32,543.25 147.63 6,414.95
2024	1	BNB; SHIB; PEPE; FLOKI; MANTA; ALT; DYM; STRK; AEVO; ENA; BANANA; BTC; ETH; USDT; TRX; XRP; DOGE; SOL	1,167,784.64 USD	~20,963,602.00

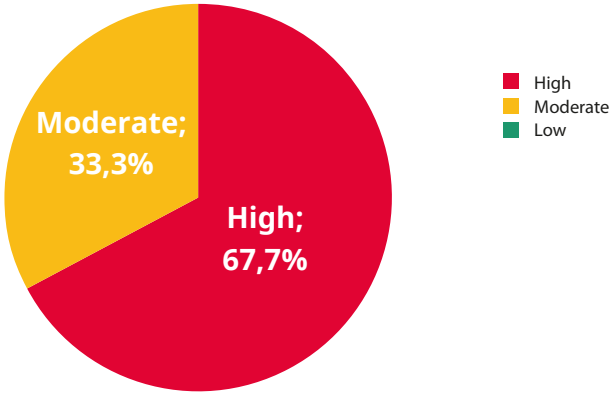
It is important to note that some of the seized cryptocurrencies carry inherent risks, particularly those with strong privacy features or limited recognition in the market. Cryptocurrencies like MANTA, for instance, are designed with a focus on anonymity, making them more susceptible to being used in 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, since 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 better-known cryptocurrencies such as 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 afterwards, leaving investors with significant losses. Furthermore, the lack of

regulatory oversight surrounding such 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. Of the responses, six LEAs view the risk as high, indicating a serious threat in this area. Meanwhile, three 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 emphasized the need for specialized training, technological investments, stronger national and international co-operation, 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 survey

Respondents:

- National Bank of Moldova
- National Commission for Financial Markets

The results of the survey conducted with Moldova's regulators concerning VAs/VASPs in the context of the 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 VAs/VASPs varies between **low** and **basic**, which highlights the need for an active process of developing advanced competencies in this field. Both regulators confirmed their participation in various training programmes related to VAs and VASPs in the last three years, with topics including regulatory and supervisory aspects of the virtual assets sector, blockchain technology, blockchain forensics, and virtual asset investigations.

Regulators also 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[37]):** 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

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

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[38] and AMLD6[39]). 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**[40] 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.

Public awareness activities

In terms of raising awareness 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[41] individuals and payment service providers about the potential risks tied to virtual currency transactions. This included warnings about the possibility of being involved 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 28 October 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 Moldovan National Commission for Financial Markets (CNPF) published two informational bulletins titled *Take Care of Your Money: The CNPF Warns About the Risks of Investing Through Unauthorized Trading Platforms*[42] 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 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.

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

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

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

41 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

42 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

4.3. Private sector responses to the VA/VASP survey

Respondents:

- Licensed banks (11)
- Non-bank payment service providers (PSPs) (7)

To gain deeper insights into the VA and VASP 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 per cent **(80%)** of respondents confirmed that they had **identified transactions related to VASP services during the last three years**. On a 1-to-3 scale (low, medium, or high), **73%** of respondents perceive the risk associated with VAs/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 were:

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: S**ome banks reported that they are unable to provide this service to their clients because the provisions of the AML/CFT Law No. 308/2017 require entities to adopt specialized IT solutions. These solutions are necessary to ensure enhanced monitoring of such transactions, to determine the source of funds, and to guarantee the traceability of transactions.

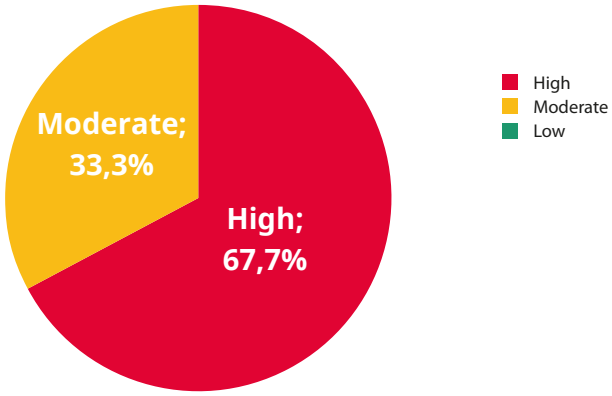
These factors, whether considered collectively or individually, have led banks to refrain from offering special accounts to clients wishing to conduct transactions with foreign VASPs. This decision reflects, on the one hand, the financial sector's cautious approach to the risks associated with VAs/VASPs, 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. Some form of risk assessment has been carried out by **36%**, and **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 for them 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. It is nonetheless also important to note that 13% perceive the risk associated with VAs as low, which in a given context is a concerning factor. It potentially indicates 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 VA/VASP-related transactions. This situation presents significant challenges in conducting a comprehensive internal investigation into the source 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

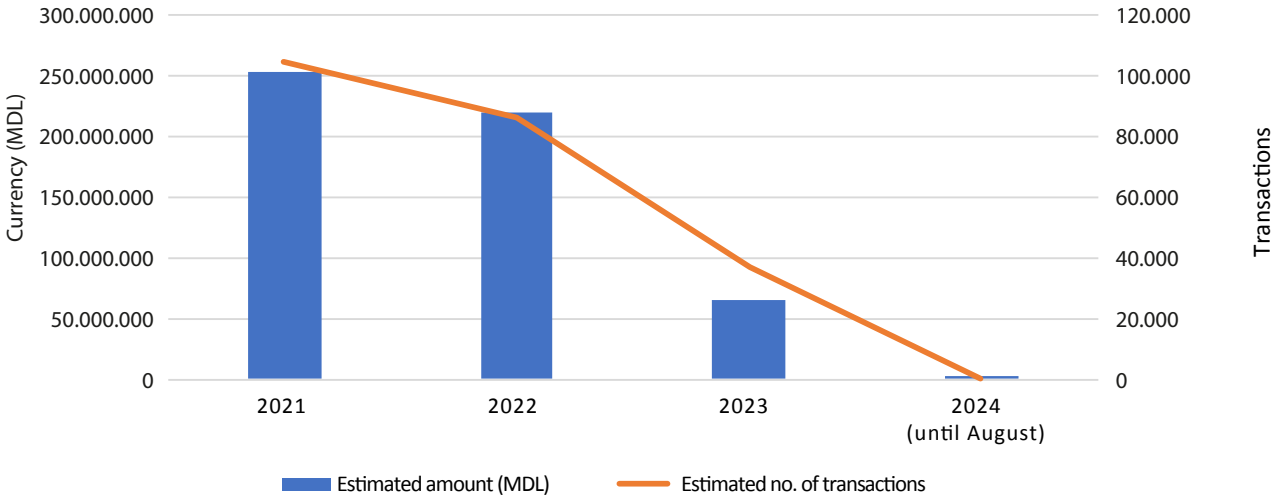


Table 11: Estimated number of transactions via bank accounts to/from foreign VASPs, for the period 2021–2024

Bank		Year							
		2021		2022		2023		2024	
		No. Txns	Amount (MDL)	No. Txns	Amount (MDL)	No. Txns	Amount (MDL)	No. Txns	Amount (MDL)
A		776	2,375,855.9	966	3,238,610.35	111	428,513.99	0	0
B		1	209,259.27	0	0	0	0	0	0
C		875	3,036,177	1530	3,920,626	373	565,135	14	23,080
D		425	3,069,103.26	551	4,151,333.57	74	384,109.67	1	210.4
E		38	190,548.74	967	2,534,826.21	126	346,455.7	0	0
F		3932	5,351,731	4055	10,710,597	488	447,419	33	35,096
G		0	0	0	0	0	0	0	0
H		47969	110,521,982.3	23216	52,964,806.92	32919	57,622,507.64	0	0
I		17144	39,033,962	11693	34,660,182	796	1,311,893	65	40,244
J		537	1,496,375.6	283	1,235,385.18	4	219.56	0	0
K		32681	88.225.374	43227	107,182,218	2211	3,574,672	0	0
TOTAL		**104378**	**253,510,369**	**86488**	**220,598,585.2**	**37102**	**64,680,925.56**	**113**	**98,630.4**
Inc/Dec (%)	vs 2021	-	-	**-17.13%**	**-13%**	**-64.45%**	**-74.48%**	**-99.89%**	**-99.96%**
	vs 2022	-	-	-	-	**-57%**	**-70.67%**	**-99.86%**	**-99.95%**
	vs 2023	-	-	-	-	-	-	**-99.69%**	**-99.84%**

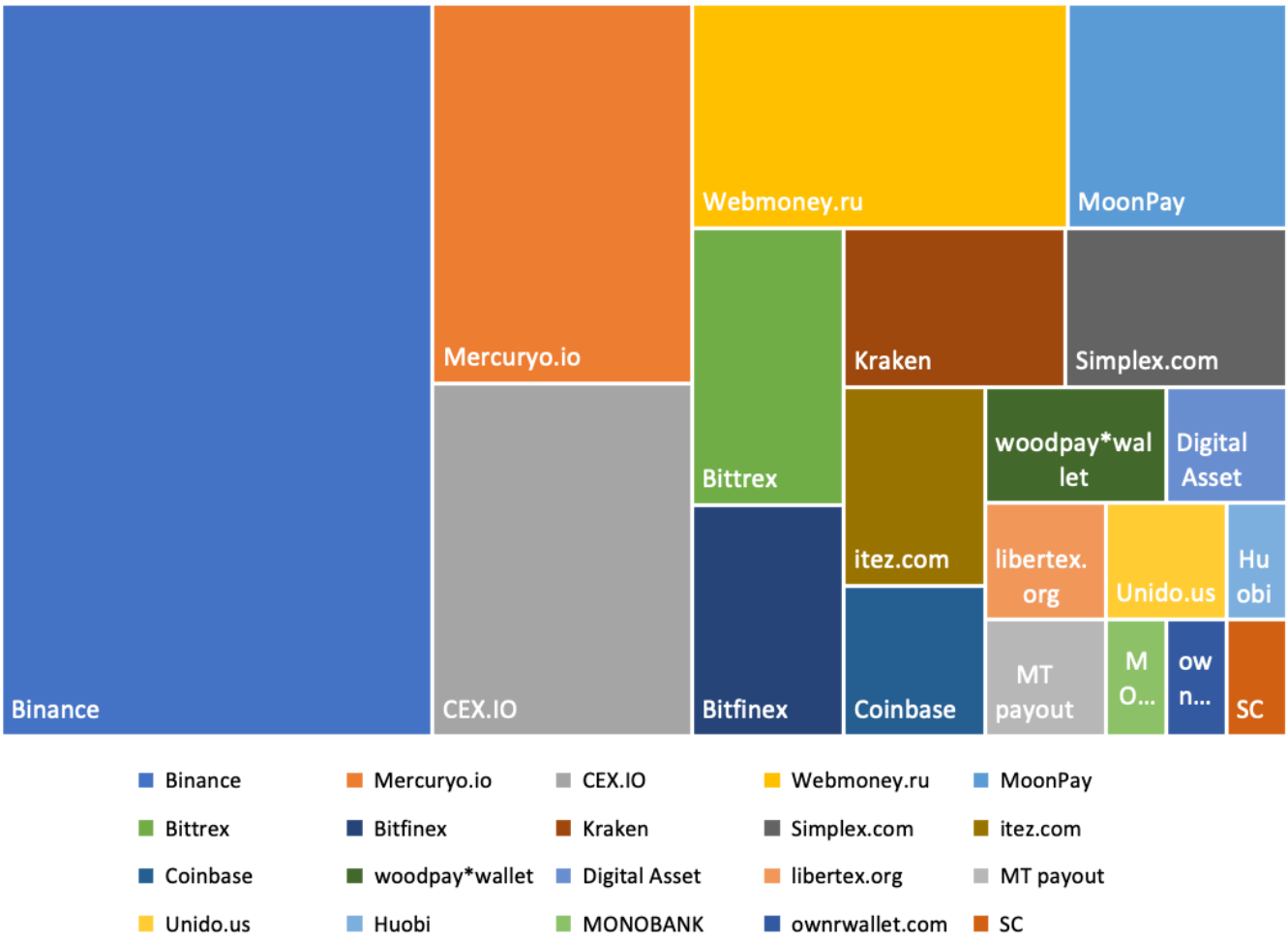
Figure 18 and *Table 11* presented above highlight a notable decline in transactions conducted by bank clients in Moldova with foreign VASPs. In 2023, transaction volume dropped significantly by 64.45% compared to 2021 and 57% compared to 2022. This decline can be primarily attributed to regulatory actions 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 the 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 have 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 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 decreased dramatically, 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 VA services.** Law enforcement data further reveal a 56.43% rise in VA-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. Payment service providers (PSPs)

The same survey conducted among non-bank PSPs shows a varied approach toward VA/VASP activity. Unlike commercial banks, one out of seven PSP respondents reported that as of April 2024, they had begun offering clients a "gateway" option to conduct transactions with foreign VASPs through dedicated ("special") accounts to ensure compliance with AML/CFT legal provisions. The remaining PSPs chose not to offer these services, citing reasons such as internal policies, the unclear regulatory framework, and the high risks associated with VAs.

The only PSP offering 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	15,500	40	11,510
May 2024	258	146,700	180	348,930
June 2024	818	447,480	314	174,390
August 2024	1444	816,947	537	672,930
Total	**2602**	**1,426,627**	**1071**	**1,207,760**

Internal risk assessment

Survey results reveal that **only one PSP** has taken specific actions to identify and evaluate the ML/TF risks associated with VAs/VASPs and two respondents have 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, unwittingly becoming involved in money laundering or terrorist financing schemes while remaining unaware of the threats and vulnerabilities associated with VAs.

In terms of risk perception, **57%** of respondents rated the risk associated with virtual assets as **"High"** on a 1-to-3 scale (low, medium, high), while another 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

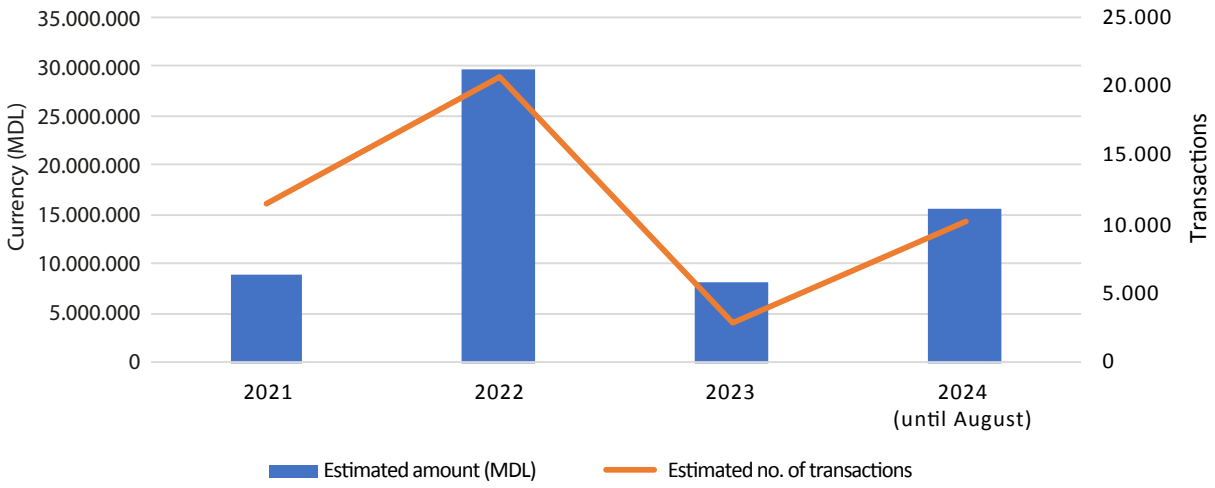
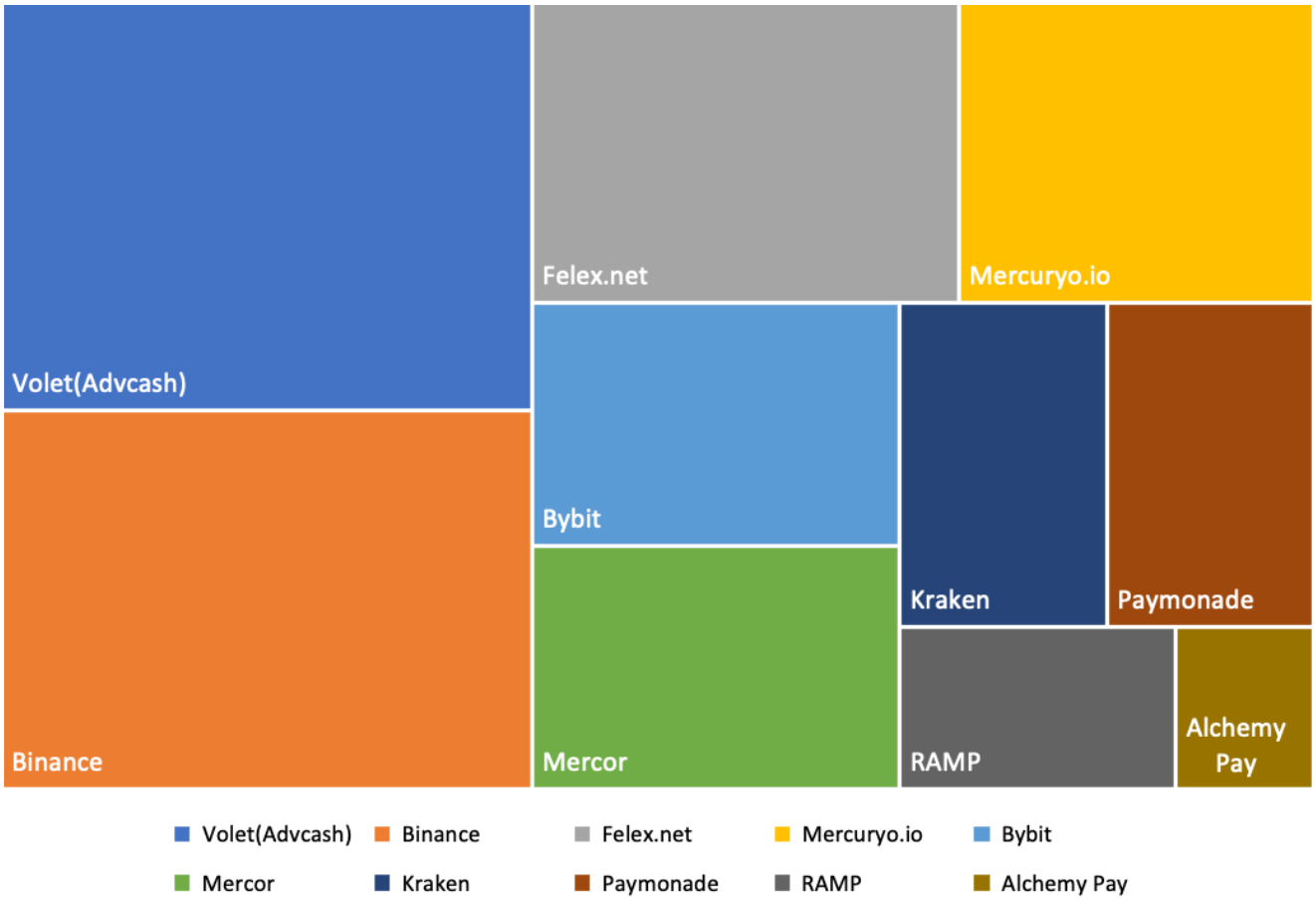


Table 13: Estimated number of transactions via PSP accounts to/from foreign VASPs, for the period 2021–2024

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	7,448,882	16338	26,044,616	0	0	0	0
B		665	973,110	1108	1,304,950	0	0	0	0
C		0	0	0	0	0	0	0	0
D		33	271,386	769	753,007.55	342	1,891,986.9	853	1,243,678,.2
E		16	282,612.7	347	1,630,021.66	598	6,195,450.14	7234	14,397,844
F		0	0	0	0	0	0	0	0
G		0	0	0	0	0	0	0	0
TOTAL		**9469**	**8,975,990.7**	**18562**	**29732595,2**	**940**	**8087437,04**	**8087**	**15,641,522**
Inc/Dec (%)	vs 2021	-	-	**96%**	**231%**	**-90%**	**-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 PSP accounts (2021–2024)



5. VA/VASP interaction with traditional obliged entities and the 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, which is 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 and/or indirectly with four 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
VIRTUAL ASSET WALLET PROVIDERS	**1**	Hot wallet	YES	YES	YES
	2	Cold wallet	N/A[43]	N/A	YES
VIRTUAL ASSET EXCHANGES	**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	Virtuall-to-virtual	N/A	N/A	N/A
VIRTUAL ASSET BROKING / PAYMENT PROCESSING	**8**	ATMs	N/A	N/A	N/A
	9	Merchants	N/A	N/A	N/A
	10	Cards	N/A	N/A	N/A
VIRTUAL ASSET MANAGEMENT PROVIDERS	**11**	Fund management	N/A	N/A	N/A
	12	Fund distribution	N/A	N/A	N/A
	13	Compliance, auditing & risk management	N/A	N/A	N/A
INITIAL COIN OFFERING (ICO) PROVIDERS	**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

43 N/A = information not available.

27 Channels			Interaction with Banking Sector	Interaction with PSPs	Interaction with Informal Sector
VIRTUAL ASSET INVESTMENT PROVIDERS	19	Platform operators	N/A	N/A	N/A
	20	Custody of assets	N/A	N/A	N/A
	21	Investment in 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 services	N/A	N/A	YES
	25	Crypto custodian services	N/A	N/A	N/A
VALIDATORS / MINERS/ ADMINISTRATORS	26	Fees	N/A	N/A	N/A
	27	New assets	N/A	N/A	N/A

5.1. Formal sectors (TOEs)

5.1.1. Banking sector

Overview
The banking system in Moldova operates under Law No. 202 din 06.10.2017[44] (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,[45] eleven banks are licensed and active in the Moldovan banking market; four 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 between the banking sector and VAs/VASPs
Of the six channels identified as having interaction in informal sectors, four 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[46] 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.

44 https://www.legis.md/cautare/getResults?doc_id=128663&lang=ro
45 https://www.bnm.md/en/content/financial-situation-banking-sector-first-semester-2024
46 The questionnaire survey results for the banking sector are detailed above in Chapter 4, Section 4.3.1.

According to statistical data provided by the surveyed 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 have not been distinctly flagged as VASPs. These emerging providers often expand their offerings to include both electronic payment and virtual asset services, complicating classification and monitoring efforts.

While VASP transactions through Moldova's banking sector have declined significantly, 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 increased notably. 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 are presented below 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 banks may lack a comprehensive understanding of VA/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 VA/VASP 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 VA 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)**[47]**:** In one of the earliest and most notorious exchange hacks, Mt. Gox lost 850,000 BTC, worth hundreds of millions of USD at the time, due to severe security vulnerabilities. This incident brought global attention to the risks related to VASPs.
- **Coincheck (2018)**[48]: 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)**[49]: In September 2020, hackers targeted KuCoin, stealing an estimated $280 million in various cryptocurrencies.
- **Ronin Network (2022)**[50]**:** In March 2022, the Ronin Network, used by the blockchain game Axie Infinity, was hacked, resulting in a loss of over $620 million. This hack exposed security weaknesses in DeFi, particularly within gaming ecosystems.
- **FTX Hack (2022)**[51]**:** 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[52]

The highly volatile nature of VAs can lead to substantial financial losses, often far 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.

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

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

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

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

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

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

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,[53] 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[54]), 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 31 October 2024, there are nine active PSPs in the Republic of Moldova. These include two payment institutions, one postal service provider, and six electronic money institutions.

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

- **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 between the PSP sector and VAs/VASPs
Four out of six 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 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 their diverse approaches to VA/VASP activities. Unlike the banking sector, some PSPs tend to be more open to new technologies due to a higher risk appetite, responsiveness to market demand, and technological adaptability. According to the results, one of the seven PSP respondents indicated that since April 2024, they had begun 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

53 https://www.bnm.md/files/Raport_anual.pdf
54 https://www.legis.md/cautare/getResults?doc_id=125243&lang=ro

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 are presented above in Section 4.3.2, "PSPs"*). The average growth rate across these periods was approximately 169%, suggesting exponential monthly growth.

Internal risk assessment
Survey results for PSPs (*Section 4.3.2*) show that currently, only one 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. This 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. The 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 VA/VASP 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 by bypassing regulatory scrutiny.

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

The informal sector captures players, actors, entities, platforms, and tokens that fall outside the traditional AML/CFT sector. It falls within a much less developed or non-existent AML/CFT compliance framework, with little to no corporate accountability to regulators. This can 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 such assets either directly (peer-to-peer), or through platforms using accounts they hold in foreign financial institutions.

Interaction between the informal sector and the VA/VASP ecosystem
Following the prohibition of VASP services within the country in 2023, underground activities involving the VA sector have expanded rapidly. Various unregulated platforms based on encrypted messaging now facilitate VA transactions that bypass regulatory oversight. These informal channels, particularly those hosted on encrypted platforms, have become major facilitators for VA 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 VA 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. This 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.

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.

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 that 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.

The following screenshots present several announcements of goods that can be bought on the Telegram group called "*Crypto Magazin*."

Figure 22: CryptoMD Escrow service on Telegram

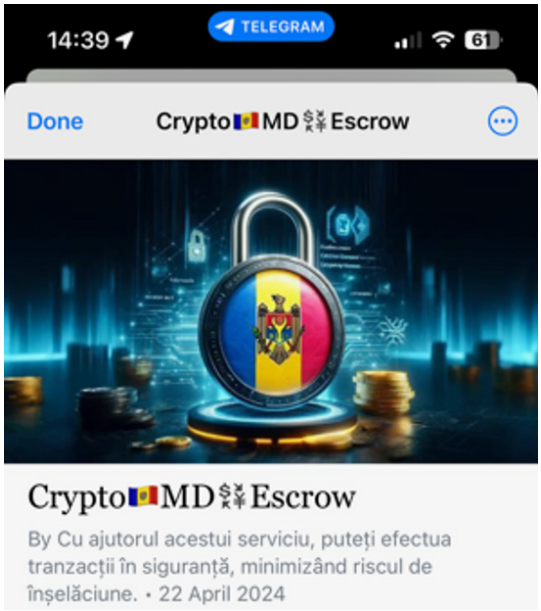


Figure 23: Crypto Exchange Chat on Telegram

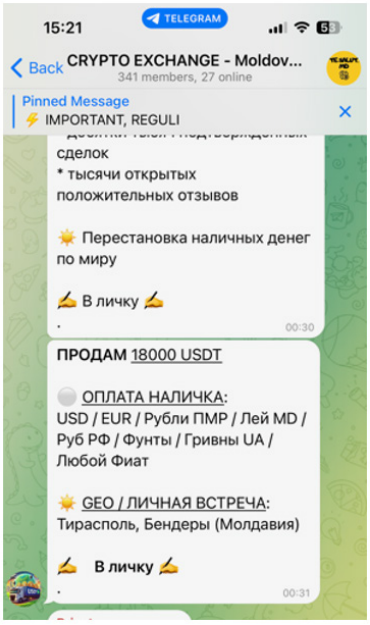
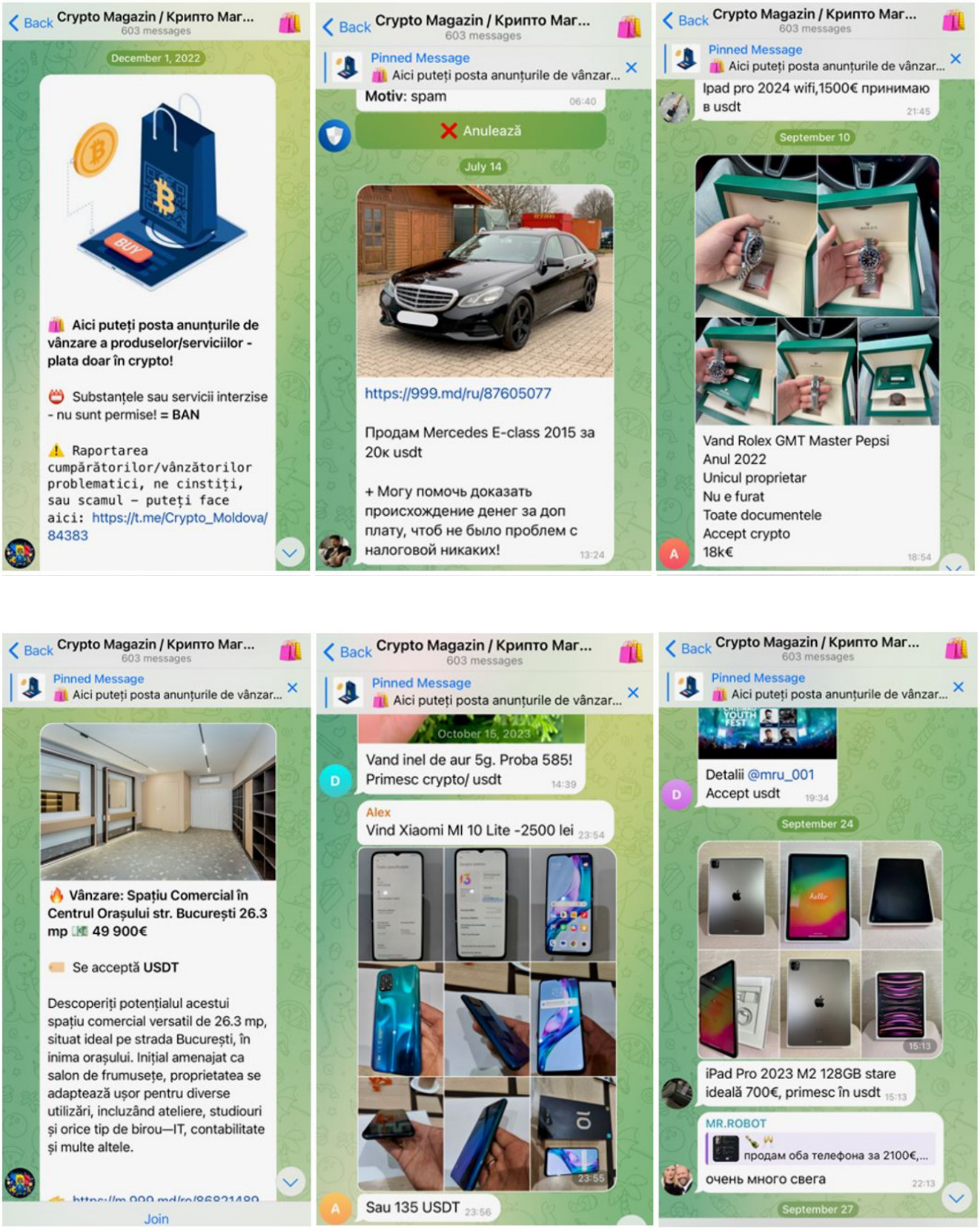
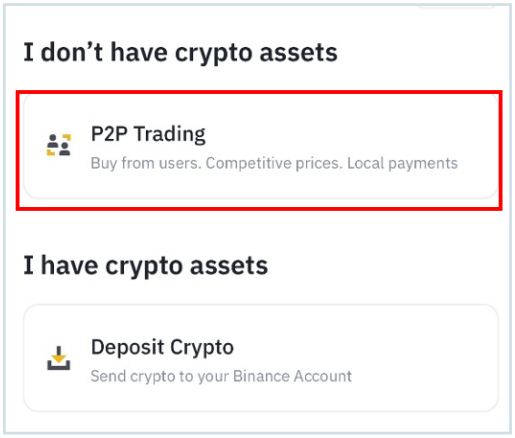


Figure 24: "Crypto Magazin" goods for sale



5.2.2. P2P crypto trading platforms

Figure 25: Binance App screenshot – P2P trading

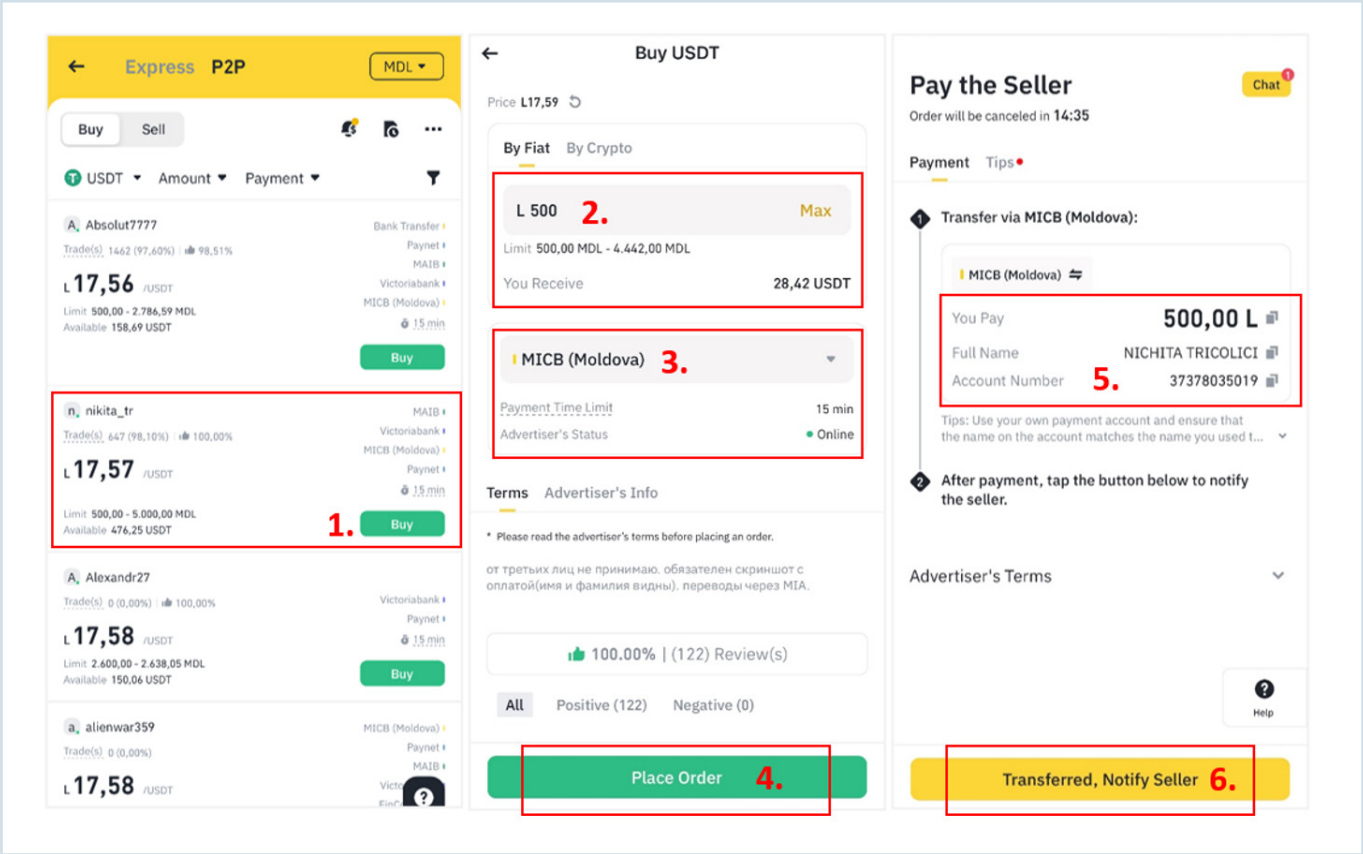


An alternative method of buying and selling cryptocurrency in Moldova while circumventing legal restrictions is through P2P crypto trading services provided by foreign VASPs.
For instance, Binance's P2P trading platform allows users in regions with restrictive regulations on VAs/VASPs, like Moldova, 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 or card payments. They do not interact directly with Binance, making it difficult for Moldovan banks to detect any link to cryptocurrency or the Binance platform.

In this kind of transaction, individuals typically utilize locally opened bank accounts. 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 unaware 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. Such payments resembling standard domestic P2P transactions can hide illicit financial flows and make it challenging for authorities to detect the true nature of the transactions and implement appropriate safeguards.

Figure 26: Binance P2P trading operations



In the presented screenshots, 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.

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, as it can facilitate the laundering and concealment of illicit proceeds obtained by criminal groups or the illegal financing of certain 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 Dniester River. 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, and emerging trends

6.1. Case studies and typologies

Case 1 – "OneCoin" Ponzi scheme (2016)

The OneCoin scam involved local promoters who attracted numerous Moldovan citizens into a 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, since many investors lost money in this international pyramid scheme. One of these cases is currently under review at the Chișinău Court of Appeal.[55]

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

Case 2 – Laundering drug trafficking proceeds (2018)

This case[56] 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 and 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.

55 https://instante.justice.md/ro/pigd_integration/pdf/4B2DB86D-9027-4C44-AA0B-9787DD33F4B5
https://www.rise.md/articol/decriptarea-operatiunii-onecoin/

56 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 – The "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 MDL, and investigations are ongoing to identify all victims.[57]

Officers from the National Anticorruption Centre, Asset Recovery Office, and National Investigations Inspectorate conducting a search at a computer gaming and virtual reality venue owned by a member of an organized criminal group (Source: politia.md)

Case 5 – Fake stock brokers (2023)

Between 3 and 14 November 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 is currently under investigation.

Case 6 – False promises of investment (2023)

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

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

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 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. 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.[58]

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.

Modus operandi:

1. ***Identifying migrants:*** *Through the Telegram and TikTok platforms using the account @g...l...tiktok, the group recruited Ukrainian citizens affected by the armed conflict;*

58 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

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 Chișinău, 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 EU 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 and cryptocurrency

Election interference, particularly through disinformation, has becomew 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.[59]

Disinformation campaigns involve the deliberate spread of false information to influence public opinion or obscure the truth. Such 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.[60]

Symbolic photo. Source: The Cyber Express[61]

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

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

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

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[62] 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 roubles into cryptocurrencies**, which facilitated 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 these illicit financial flows.[63]

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

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

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

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

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

7. The risk assessment

7.1. ML/TF threat assessment

According to the FATF guidance on National ML and TF risk assessment,[65] 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 table below portray general tendencies across all six 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)
VA nature and profile	Anonymity or pseudonymity	Very High
	P2P cross-border transfer and portability	High
	Absence of face-to-face contact	High
	Traceability	High
	Speed of transfer	High
Accessibility to criminals	Illegal mining	Very High
	Collection of funds	High
	Transfer of funds	High
	Dark web access	Very High
	Expenditure of funds	Medium
Source of funding VAs	Bank or card as source of funding VAs	Medium
	Cash transfers, valuable in-kind goods	High
	Use of virtual currency stablecoins	High
Operational features of VAs	Regulated	N/A
	Unregulated	Medium
	Centralized environment	Low
	Decentralized environments	High
Ease of criminality	Tax evasion	High
	Terrorist financing	Medium
	Disguising criminal proceeds in non-regulated VAs	High
	Tracing and seizure difficulties	High
	Circumvention of exchange controls	High

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

Intermediary variables	Input variables (risk elements)	Threat (overview across 6 channels)
Economic impact	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)
VIRTUAL ASSET WALLET PROVIDERS	**Custodial services**	Hot wallet
	Non-custodial services	Cold wallet
VIRTUAL ASSET EXCHANGES	**Transfer services**	P2P
	Conversion services	Fiat-to-virtual
		Virtual-to-fiat
VIRTUAL ASSET INVESTMENT PROVIDERS	**Emerging products**	Crypto escrow services

7.1.1. VA Nature and Profile

Figure 27: VA nature and profile – Summary of different risk elements

Very High	• Anonymity or pseudonymity
High	• P2P cross-border transfer and portability
High	• Absence of face-to-face contact
High	• Lack of traceability
High	• Speed of Transfer

a. Anonymity or pseudonymity (Very High) – The inherent risk of anonymity or pseudonymity in VA 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 (P2P) 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 P2P exchange trade volumes,[66] indicating that P2P activity 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, since 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 VAs/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 P2P exchanges, which operate with minimal regulatory oversight, making it difficult to trace or verify the identities of the 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 threats.

d. Lack of traceability (High) – Moldova's prohibition on domestic VASP operations and the lack of a corresponding "Travel Rule" regulation (see above, p. XX) 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 related to such conflicts such as illicit financing and organized crime. VAs amplify these risks through cross-border pseudonymous transactions, which are difficult to trace without international co-operation. The lack of traceability tools compounds this challenge, since 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 above in Section 4.1*), which constrains their ability to analyse transaction flows effectively. This limitation reduces the capacity to trace the origin and 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 can hinder authorities' ability to detect and trace suspicious criminal activities.

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

7.1.2. Accessibility to criminals

Figure 28: Accessibility to criminals – 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,[67] 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 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.

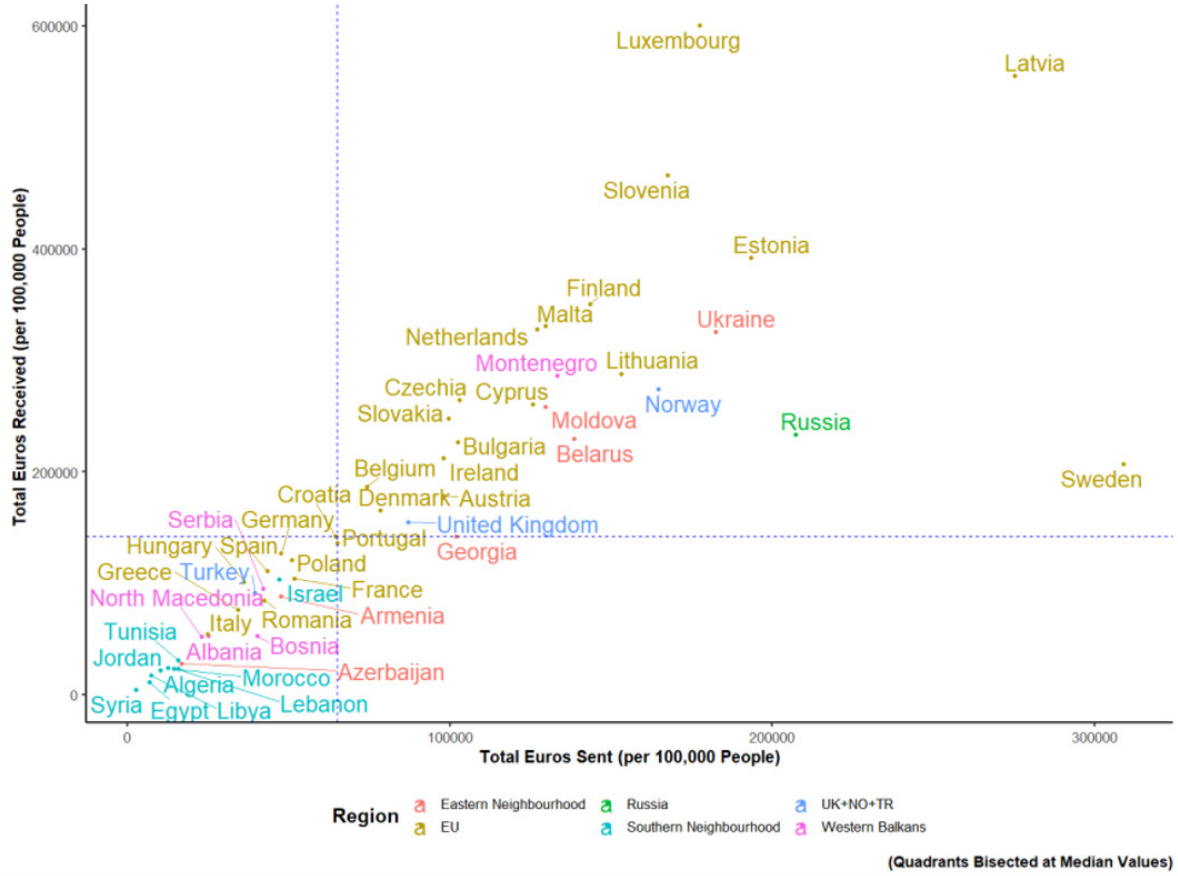
Although no stablecoins are issued locally, internationally accessible dollar-backed stablecoins are frequently used for fund transfers within Moldova. This raises concerns, since stablecoins, often backed by fiat reserves, may create a loophole in which "dirty money" could support transactions without 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.

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

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[68] illustrated 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 Neighbourhood countries, with a total darknet market engagement (sent, received) estimated at approximately €387,770 per 100,000 persons, between April 2019 and June 2021.[69] This statistic underscores Moldova's heightened exposure to dark web-enabled financial crimes. Moldova is particular susceptible due to limited regulation and significant proximity to high-risk areas, factors that increase both accessibility and attraction to dark web markets.

Figure 29: Total per capita sent/received on 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 VA ecosystem, criminals can leverage these assets for expenditure in both legitimate and illicit transactions, obscuring the origin of the 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 favourable environment for laundering and misuse, elevating the risk level.

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

69 https://www.euda.europa.eu/drugs-library/cryptocurrencies-and-drugs-analysis-cryptocurrency-use-darknet-markets-eu-and-neighbouring-countries_en

7.1.3. Source of funding VAs

Figure 30: Source of funding – Summary of risk elements

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

a. Bank or card as source of funding VAs (Medium) – In the Republic of Moldova, the risk level associated with funding VAs through bank or card sources is medium to 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 the lower overall risk, Moldova still carries residual risks, especially from potential misrepresentation of transaction purposes by bank account holders (*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 VA market 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 risks, 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 10) 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 VAs

Figure 31: Operational features of VAs – 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 37th 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 (High) – 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 an 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.

Highlighted above (*Section 5.2.1*) are 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, since they can 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

High	• Tax evasion
Medium	• Terrorist financing
High	• Disguising criminal proceeds in non-regulated VAs
High	• Tracing and seizure difficulties
High	• Circumvention of exchange controls

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.[70]

The State Tax Service has provided clarification[71] 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, and declarations plummeted 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 may have deterred voluntary disclosures.

Given the regulatory ambiguities, sporadic voluntary reporting, and notable declines in declarations, the risk level for ease of criminality in the form of tax evasion related to VAs/VASPs can be assessed as high. The framework's limitations and the observed behavioural 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 a medium risk, reflecting a balance between the limited number of 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 counter TF through this channel.

c. Disguising criminal proceeds in non-regulated VAs (High) – Although Moldova has stringent regulations that limit domestic VASP operations and heavily control interaction with foreign authorized VASPs, the risk of criminal proceeds being disguised in non-regulated VAs remains due to alternative channels outside the formal financial sector. Criminals looking to launder proceeds of crime can bypass formal restrictions by leveraging the informal sector to acquire VAs through cash-based transactions. Once obtained, these assets can be easily moved to unregulated VASPs services for a laundering process (such as 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 this risk, which is evaluated as high. Criminals can exploit informal channels to engage in laundering activities by moving assets across jurisdictions and employing sophisticated methods to disguise fund origins.

d. Tracing and seizure difficulties (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

70 https://www.legis.md/cautare/getResults?doc_id=134161&lang=ro

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

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

e. Circumvention of exchange controls (High) – The potential threat posed by unidentified underground VASPs in Moldova is significant, since 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 can 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
Very 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 Sections 4.3.1"Banking sector" and 4.3.2 "PSPs"*).

c. Prohibit any interaction between 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 VAs/VASPs, and evaluated the level of ML/TF threats resulting from these interactions.

The analysis was built upon by assessing each input variable, which contributed to understanding the intermediate variables across six relevant VASP channels, with an evaluation of 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 services	High
Overall VAs/VASPs ML/TF threat			**High**

The table above indicates that all six 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 stems primarily from their substantial exposure to ML/TF threats, lack of regulatory oversight, as well as their increasing use in 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 VA 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 have shifted to the informal economy.

These interactions demonstrate that despite regulatory constraints, VA activities persist through alternative channels. The banking and PSP sectors, although reluctant and limited in their direct involvement, maintain indirect links with foreign VASPs, while the informal sector has 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 inherent vulnerabilities before implementing any regulatory controls or mitigating measures.

Table 19: Overall vulnerability exposure summary

Intermediary Variables	Input Variables	Vulnerability Rating
Products & services provided, and types of VA	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
	Institutions dealing with VASPs	High
	VA anonymity or pseudonymity	High
	Rapid transaction settlement	High
	Dealing with unregistered VASPs from overseas	High
Overall Vulnerability Rating		High

Table 20: Description of vulnerability input variables according to the WB Methodology

Licensed in the country or abroad	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, and 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 an economic area (e.g., the EU), must also register with the relevant authority, regardless of their registration status in their home country.
Nature, size, and complexity of business	According to the 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.
Products and services	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.
Methods of delivery of products/services	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.
Customer types	The VASP sector tends to be at a very high risk of exposure to criminals and organized crime, and the sector is considered attractive to this type of customer due to its reduced transparency.
Country risk	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.

Institutions dealing with VASPs	VASPs have exposure to other VASPs such as exchanges and wallet providers that may have insufficient AML/CFT controls in place. Tumblers, P2P exchanges, and other methods of enhancing anonymity or obfuscating the flow of funds should be considered higher risk factors.
VA anonymity or pseudonymity	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.
Rapid transaction settlement	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.
Dealing with unregistered VASPs from overseas	Specific challenges emerge when VA 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.

Results of the ML/TF inherent vulnerability assessment

Due to the prohibition of VA services within Moldova 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 the country. 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, formal 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 the 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 co-operation efforts. Furthermore, **decentralized exchanges (DEXs)** facilitate direct user-to-user transactions without intermediaries, reducing regulatory oversight and making enforcement more difficult.

- **International co-operation 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 co-operative or transparent. This fragmentation complicates the process of tracing transactions and identifying beneficiaries, creating substantial challenges for Moldovan intelligence agencies to pursue comprehensive investigations and ensure 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, since VAs 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. 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 services	High

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

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 services	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 co-operation. 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, categorizing it 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 has shifted to peer-to-peer markets, with consumers investing in anonymity-enhancement solutions. **The measures intended to enforce the ban and reduce exposure to VAs are ineffective**, lacking the means to identify illegally operating VASPs and to impose dissuasive sanctions on such entities.
- **Underground economy**: The data collected during the NRA indicates a rapid expansion of the underground VA-related activities. Various unregulated platforms based on encrypted messaging now facilitate VA transactions that bypass regulatory oversight. These informal channels, particularly those hosted on encrypted platforms, have become major facilitators for VA transactions, enabling an array of services from P2P crypto exchanges to large-scale purchases using cryptocurrencies. This has created 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 received a series of training courses and developed basic expertise in the VA field, the number of specialists involved in these training programmes is very limited, **leaving significant knowledge gaps.** Furthermore, there are **insufficient technological resources** necessary for effectively tracing and prosecuting crimes related to VAs.
- **International co-operation 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 co-operative 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 STR/SAR reporting:** Reports from financial institutions have indicated a **rise in suspicious transactions involving VAs**, often related to illegal VA 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, 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 per cent 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. This raises concerns about the sector's capability to apply a risk-based approach.

8.2. Recommendations

- **Strengthen the 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 the 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 the capabilities of LEAs:** 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 that authority given necessary resources to effectively identify threats arising from unregulated activities related to VAs posing ML/TF threats.
- **Comprehensive training programmes:** Provide substantial capacity-building initiatives to relevant public authorities and a broader group of specialists 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 evolving risks in the VA/VASP sector.

- **Enhance collaboration at the national level:** Establish 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 programmes 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 current national legislation to ensure a uniform basis with international practices for tax on income from cryptocurrency transactions, to ensure clear and fair fiscal treatment, and to simplify the way to declare and pay taxes for such incomes.
- **Statistical data related to VA/VASP activities:** Authorities should begin collecting, maintaining, and sharing data and metrics specific to VAs/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 this NRA, the WG encountered significant challenges in gathering essential data related to VAs/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 have allowed the WG to accurately evaluate the extent of interest and engagement of Moldovan citizens in the VA space. Such data would be critical for a comprehensive evaluation of the risks associated with VAs within the country.

To address this issue, the WG 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 co-operative jurisdictions. As a result, the FIU Moldova did not receive any responses from these outreach efforts, which highlights the challenges in accessing cross-border data for effective risk assessment.

9. Annex

9.1. Glossary

Table 22: Glossary

Blockchain	A technology solution that enables digital assets. It is a method of securely recording information on a peer-to-peer network.[72]
Blockchain analytics	A technology solution to analyse 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)	Digital money issued by a central bank. A CBDC differs from cryptocurrency in that it is issued by a central bank.
Cryptocurrency	A 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	A service that blends the cryptocurrencies of many users together to obfuscate the origins and owners of the funds.[73]
Metaverse	A term referring to virtual worlds in which users represented by avatars interact.
Privacy coin	Or anonymity enhanced coin. A privacy coin is designed to prioritize anonymity by enhancing features that reduce traceability.
Smart contract	A self-executing contract that is typically used to automate execution of an arrangement without an 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.

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

73 Chainalysis, Crypto Mixers and AML Compliance, website: https://www.chainalysis.com/blog/crypto-mixers/ [last accessed: 6 October 2024].

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

Table 23: Timeline of key events and developments in the VA/VASP ecosystem and Moldova's specific actions

31 October 2008	Satoshi Nakamoto releases the Bitcoin White Paper.[74]
15 January 2010	First cryptocurrency exchange BitcoinMarket was launched.[75]
21 October 2011	Bitcoin Fog mixing service is launched.[76]
June 2012	P2P exchange Localbitcoins was launched.[77]
23 January 2014	Ethereum network introduced by Vitalik Buterin.[78]
18 April 2014	Privacy coin Monero is launched.[79]
19 November 2015	The ERC-20 standard is proposed, paving the new way for the issuance of new tokens, including stablecoins, on the Ethereum network.[80]
12 May 2017	WannaCry ransomware attack is launched by the cybercrime group Lazarus.[81]
10 July 2017	The National Bank of Moldova publishes a press release on virtual currency and its associated risks.[82]
24 January 2018	The ERC-721standard is proposed, providing the basis for non-fungible tokens (NFTs) on the Ethereum network.[83]
15 February 2018	The National Bank of Moldova warns about high risks of investing in cryptocurrencies.[84]
8 March 2018	The EU Commission adopts the Fintech action plan.
15 May 2018	The National Bank of Moldova again warns about the risks associated with investing in cryptocurrencies.[85]
14 September 2018	The National Bank of Moldova releases 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.[86]
28 November 2018	OFAC identifies Iran-based financial facilitators of malicious cyber activity and reveals associated digital currency addresses for the first time.[87]
21 June 2019	The FATF publishes *Guidance for Risk-based Approach to Virtual Assets and Virtual Asset Service Providers*.[88]
24 September 2020	Legislative proposal of Crypto assets (MiCA) and digital operational resilience act (DORA).
October 2021	Amendments to Law No. 133 of 17 June 2016 on the declaration of assets and personal interests come into effect, requiring declaration subjects to include virtual assets in their declaration of assets and personal interests if their value exceeds ten average monthly salaries in the economy.
May 2022	MONEYVAL's 1st Enhanced Follow-up Report is released. Moldova's technical compliance with the R.15 is downgraded to NC (non-compliant).

74 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 accessed: 22 September 2024].

75 Guiness World Records, First cryptocurrency exchange, website: https://www.guinnessworldrecords.com/world-records/696258-first-cryptocurrency-exchange [last accessed: 22 September 2024].

76 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 accessed: 22 September 2024].

77 Localbitcoins, About LocalBitcoins, website: https://localbitcoins.com/about [last accessed: 22 September 2024].

78 Etherium community (ethereum.org), Ethereum Whitepaper, website: https://ethereum.org/en/whitepaper/ [last accessed: 22 September 2024].

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

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

81 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 accessed: 22 September 2024].

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

83 Ethereum Community (ethereum.org), ERC-&21 Non-Fungible Token Standard, website: https://ethereum.org/lt/developers/docs/standards/tokens/erc-721/ [last accessed: 22 September 2024].

84 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: 6 October 2024].

85 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: 6 October 2024].

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

87 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 accessed: 22 September 2024].

88 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 accessed: 22 September, 2024].

20 October 2022	INTERPOL announces the launch of the first global police Metaverse.[89]
28 October 2022	The National Bank of Moldova sends letter to banks and PSPs requesting that they terminate all activities related to virtual assets.
16 January 2023	The EU Digital Operational Resilience Act (DORA) enters into force.
29 May 2023	The National Commission for Financial Markets warns about the risks of investing through unauthorized trading platforms.[90]
June 2023	Publication of MiCA in the OJEU.[91]
1 July 2023	A series of amendments to the AML/CFT Law No. 308/2017 are adopted. These amendments mark the first step for the Republic of Moldova in recognizing virtual assets (VAs) by introducing new concepts such as "virtual asset" and "virtual asset service provider" into national legislation. In addition, 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 is released. The assessment team identifies 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 completes its first National Risk Assessment of ML/TF risks associated with VAs/VASPs.

9.3. List of CASP regulatory authorities in the EU

Table 24: List of CASP licensing authorities in the EU

No.	EU Member State	Regulator
1	Austria	Financial Market Authority (FMA)[92]
2	Belgium	Financial Services and Markets Authority (FSMA)[93]
3	Bulgaria	Financial Supervision Commission (FSC)[94]
4	Croatia	Croatian Financial Services Supervisory Agency (HANFA)[95]
5	Cyprus	Cyprus Securities and Exchange Commission (CySEC)[96]
6	Czech Republic	Czech National Bank (ČNB)[97]
7	Denmark	Danish Financial Supervisory Authority (DFSA)[98]
8	Estonia	Estonian Financial Supervision Authority (EFSA)[99]
9	Finland	Financial Supervisory Authority (FIN-FSA)[100]
10	France	Autorité des Marchés Financiers (AMF)[101]
11	Germany	Federal Financial Supervisory Authority (BaFin)[102]
12	Greece	Hellenic Capital Market Commission (HCMC) and National Bank of Greece (NGB)[103]
13	Hungary	Hungarian National Bank (MNB)
14	Ireland	Central Bank of Ireland
15	Italy	Bank of Italy[104]
16	Latvia	Bank of Latvia[105]

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

90 https://www.cnpf.md/ro/ai-grija-de-banii-tai-cnpf-atentioneaza-despre-riscurile-investitiilor-prin-inte-6307_93595.html

91 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 accessed: 22 September 2024].

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

93 https://cryptoforinnovation.org/belgium-champions-eu-crypto-policy-with-mica-blockchain-pilots-and-esg-standards/

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

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

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

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

98 https://www.dfsa.dk/news/2024/jun/crypto-assets_250624

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

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

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

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

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

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

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

17	Lithuania	Bank of Lithuania[106]
18	Luxembourg	Commission de Surveillance du Secteur Financier (CSSF)[107]
19	Malta	Malta Financial Services Authority (MFSA)[108]
20	Netherlands	Bank of Netherlands[109]
21	Poland	Polish Financial Supervision Authority[110]
22	Portugal	Bank of Portugal[111]
23	Romania	The Foreign Exchange Licensing Commission of the Ministry of Finance[112]
24	Slovakia	National Bank of Slovakia[113]
25	Slovenia	The Securities Markets Agency and the Bank of Slovenia[114]
26	Spain	Bank of Spain[115]
27	Sweden	Swedish Financial Supervisory Authority[116]

106 https://www.lb.lt/en/authorisation-of-crypto-asset-service-providers
107 https://www.cssf.lu/en/virtual-asset-service-provider/
108 https://www.mfsa.mt/our-work/virtual-financial-assets/
109 https://www.dnb.nl/en/login/my-dnb-supervision-services/supervisory-applications-service-new-forms/
110 https://www.financemagnates.com/cryptocurrency/poland-to-regulate-crypto-in-2024-knf-empowered-to-impose-fines/
111 https://manimama.eu/mica-implementation-in-portugal/
112 https://manimama.eu/mica-implementation-in-romania/
113 https://manimama.eu/mica-implementation-in-slovakia/
114 https://practiceguides.chambers.com/practice-guides/comparison/990/13590/21421-21422-21423-21424-21425-21426-21427-21428
115 https://gofaizen-sherle.com/crypto-license/spain
116 https://manimama.eu/mica-implementation-in-sweden/

Organization for Security and
Co-operation in Europe