

<https://doi.org/10.26565/2786-4995-2026-1-10>

UDC 336.7:004.9

**Utenkova Karina**

*Doctor of Economic Sciences, Professor,  
Professor of Department of Banking Business and Financial Technologies  
Educational and Scientific Institute «Karazin Banking Institute»  
V.N. Karazin Kharkiv National University, Kharkiv, Ukraine  
4, Svobody Sq., Kharkiv, 61022, Ukraine  
e-mail: [utenkova@karazin.ua](mailto:utenkova@karazin.ua)  
ORCID ID: [0000-0001-9097-5431](https://orcid.org/0000-0001-9097-5431)*

## **Financial monitoring of virtual assets: international standards and challenges of implementation in Ukraine**

**Annotation.** The article examines financial monitoring in the field of virtual asset circulation, including cryptocurrencies, tokenized assets, and decentralized financial platforms. The rapid expansion of the virtual asset market creates new economic opportunities while simultaneously generating heightened risks related to money laundering, terrorist financing, and sanctions evasion, which necessitates effective regulatory and supervisory responses.

**Problem statement.** The core problem lies in the insufficient alignment of national financial monitoring mechanisms for virtual assets with international FATF standards and European regulatory approaches, as well as the fragmented enforcement practices in Ukraine amid the rapid evolution of the crypto market.

**Unresolved aspects.** Despite ongoing regulatory efforts, significant gaps remain in the effective implementation of FATF Recommendation 15, the operationalization of the Travel Rule, coordination among national supervisory authorities, and oversight of decentralized finance services and cross-border virtual asset transactions.

**Purpose of the article.** The purpose of the study is to conduct a comprehensive analysis of international financial monitoring standards applicable to virtual assets, assess current money laundering and terrorist financing risks, and substantiate directions for improving Ukraine's regulatory framework in line with FATF requirements and EU practices.

**Main content.** The article analyzes the legal nature of virtual assets, FATF requirements for Virtual Asset Service Providers (VASPs), the application of the Travel Rule, and empirical data on illicit crypto transactions based on Chainalysis reports. Particular attention is paid to the European regulatory model established by the Markets in Crypto-Assets Regulation (MiCA), as well as to the comparative analysis of the concepts of VASP and Crypto-Asset Service Provider (CASP). The current state of legal regulation and financial monitoring of virtual assets in Ukraine is also assessed.

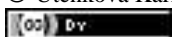
**Conclusions.** The study demonstrates that effective financial monitoring of virtual assets can be achieved only through a comprehensive approach combining FATF international standards, harmonization with EU law, advanced analytical technologies, and strengthened institutional capacity of national regulators. The practical value of the research lies in developing recommendations aimed at enhancing Ukraine's financial security and reducing money laundering and terrorist financing risks in the virtual asset market.

**Keywords:** *virtual assets; financial monitoring; anti-money laundering (AML); counter-terrorist financing (CFT); FATF; Travel Rule; VASP; CASP; Markets in Crypto-Assets Regulation (MiCA); cryptocurrency market; financial security.*

**Formulas: 0; fig.: 2, tabl.: 3, bibl.: 15.**

**JEL Classification: G 18, G28, F 38, K 22**

**For citation:** Utenkova Karina. Financial monitoring of virtual assets: international standards and challenges of implementation in Ukraine. *Financial and Credit Systems: Prospects for Development*. №1(20) 2026. P. 133-145. <https://doi.org/10.26565/2786-4995-2026-1-10>



**Introduction.** The rapid development of the virtual asset market—including cryptocurrencies, tokenized financial instruments, and decentralized platforms—creates new opportunities for the global economy while simultaneously generating unprecedented risks for the system of anti-money laundering and counter-terrorist financing (AML/CFT). According to international analytical platforms, the volume of illicit transactions in the cryptocurrency sector has been increasing annually, with criminals employing innovative methods to disguise financial flows, such as mixers, decentralized exchanges, over-the-counter (OTC) brokers, and cross-chain bridges.

Research into financial monitoring of virtual assets has become particularly relevant due to the following factors:

- the growth in illicit cryptocurrency transactions, including theft, fraud, cybercrime financing, and sanctions evasion;
- the active use of virtual assets in money laundering and terrorist financing (ML/TF) schemes, including by terrorist organizations;
- the rapid evolution of technologies that often outpaces the development of regulatory approaches;
- the global nature of the crypto market, which necessitates the harmonization of cross-border control mechanisms and information exchange;
- the need to implement a risk-based approach to transaction monitoring in an environment where anonymity and decentralization complicate the identification of ultimate beneficial owners.

For Ukraine, this issue is particularly significant under wartime conditions, as the risks of using crypto-assets to evade sanctions and finance illegal activities increase substantially, while the digitalization of the financial sector requires modern regulatory solutions. Therefore, studying the specifics of financial monitoring in the virtual asset sphere is critically important for ensuring financial security, harmonizing national regulations with FATF standards, and enhancing the effectiveness of regulators and reporting entities.

**Literature Review.** The relevance of the outlined issues is confirmed by numerous academic studies in this field.

Kulyk (2025) emphasizes the need to clearly define the range of participants in the virtual asset market, as these participants constitute a key element of legal relations within the market, while their precise classification remains insufficiently developed. The emergence of new actors alongside market growth underscores the urgency of this task.

Ustymenko, Dzhabrailov, and Hudima (2023) highlight that shifts in the socio-economic sphere must be accompanied by timely state responses in the form of adequate legislative frameworks capable of effectively regulating newly formed social relations. Due to the spread of digitalization, innovative sectors—such as IT technologies, the virtual asset market, and artificial intelligence—remain underregulated and insufficiently aligned with contemporary challenges.

Cappai (2023) notes that through the Digital Finance Package (MiCA, the DLT Pilot Regime, and DORA, later complemented by the DAC8 proposal), the European Union aims to establish an appropriate legal framework for crypto-assets of a financial nature. This package represents an initial attempt to regulate a complex and emerging phenomenon characterized by significant trade-offs. At this early stage, several aspects of the crypto ecosystem—such as pure DeFi models, DAOs, and NFTs—remain unaddressed, largely due to the difficulty of regulating technologically complex systems through traditional top-down legislative approaches.

Popova, Liu, and Yi (2025) analyze the cryptocurrency market in the context of the Russia–Ukraine war, finding that as the conflict intensifies, demand for cryptocurrencies—particularly those previously viewed as safe-haven assets during the COVID-19 pandemic—significantly increases.

Dote-Pardo and Espinosa-Jaramillo (2025) review studies from 2016 to 2024 on the role of digital assets in illicit financial flows and evaluate the effectiveness of existing prevention

strategies. They identify two key policy imperatives for Latin America: (i) promoting regional cooperation among central banks to harmonize AML standards and address regulatory arbitrage, and (ii) integrating supervisory technologies (SupTech and RegTech) into compliance systems to improve detection efficiency.

At the global level, regulators and financial institutions are developing strategies to enhance the detection and prevention of illicit cryptocurrency transactions, including blockchain analytics, artificial intelligence-based monitoring systems, and international regulatory standards such as the FATF Travel Rule (Gupta et al., 2023).

Horobets et al. (2025) focus on the challenges of balancing regulatory compliance with the technological capabilities of AI-based AML tools used by banks, emphasizing current regulatory initiatives and the experience of leading countries in implementing such systems.

At the same time, the legal regulation of virtual asset circulation in Ukraine and the corresponding AML/CFT/CPF regulatory framework remain insufficiently studied.

#### **Purpose, Objectives, and Research Methods.**

The purpose of this study is to conduct a comprehensive analysis of financial monitoring in the virtual asset sector, assess current money laundering and terrorist financing risks, and substantiate directions for improving national and international regulation in line with FATF standards, EU practices, and the specific characteristics of the Ukrainian crypto market.

The object of the research is the system of anti-money laundering, counter-terrorist financing, and counter-proliferation financing (AML/CFT/CPF) in the sphere of virtual asset circulation.

The study employs a combination of general scientific and special research methods, including:

- analysis and synthesis - to examine the nature of virtual assets, mechanisms of their use, and AML/CFT risk identification;
- comparative analysis - to compare FATF, European Union (MiCA), and Ukrainian regulatory approaches, as well as to distinguish between VASP and CASP concepts;
- systemic approach - to consider financial monitoring of virtual assets as an integrated system of interconnected institutions, instruments, and regulatory requirements;
- statistical and empirical analysis - to summarize data from international reports (FATF, Chainalysis) on the scale and dynamics of illicit cryptocurrency transactions;
- legal and regulatory analysis - to assess existing and draft Ukrainian legislation and international standards governing virtual assets;
- generalization and scientific interpretation - to formulate conclusions and practical recommendations for improving financial monitoring in the virtual asset sector.

**Results.** Under current Ukrainian legislation, the interpretation of the essence of virtual assets is directly linked to the concept of a “*digital thing*.” According to Article 179-1 of the Civil Code of Ukraine, a digital thing is an asset that is created and exists exclusively in a digital environment and has economic value. The concept of a digital thing includes virtual assets, digital content, and other intangible assets [1].

According to the FATF methodology, *virtual assets* are defined as a digital representation of value that can be digitally traded or transferred and may be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities, or other financial assets already covered by other sections of the FATF Recommendations [2].

According to the Chainalysis report “*Money Laundering and Cryptocurrency*,” nearly USD 100 billion was transferred from known illicit wallets to conversion services between 2019 and 2024. The highest volume was recorded in 2022, when USD 30 billion in illicit transactions was detected, largely linked to dealings involving sanctioned services such as the Russian exchange Garantex [3].

The same report indicates a steady increase in illicit flows through cryptocurrency bridges between 2020 and 2024. In January 2024, a record USD 234 million in illegal flows was recorded, primarily originating from Tornado Cash and routed through cross-chain bridges [3].

Most criminals seek to convert cryptocurrency into fiat currency through centralized exchanges, which provide high liquidity and integration with traditional financial services. Despite this, the volume of illicit funds flowing into centralized exchanges declined from nearly USD 2 billion per month to approximately USD 780 million per month, largely due to the implementation of more effective AML programs on these platforms.

Another method of money laundering involves the use of OTC brokers, which facilitate large transactions between two parties outside public exchanges. Some OTC brokers do not apply adequate customer due diligence (KYC) procedures, making them particularly attractive to criminal actors.

One of the most well-known examples of cryptocurrency use for money laundering is the Russian darknet marketplace Hydra, which was widely used for drug trafficking, money laundering, and other illicit activities.

According to the report, more than 50% of illicit funds ultimately reach centralized exchanges, owing to their high liquidity and ease of converting crypto-assets into fiat currency. This continues to make centralized exchanges attractive to money launderers, despite strengthened AML controls on these platforms.

In response to these challenges, FATF, the European Union, and leading jurisdictions are tightening regulatory requirements for virtual assets, licensing standards for crypto-asset service providers, risk-based monitoring criteria, and transparency requirements for blockchain transactions. At the same time, national regulators, including those in Ukraine, remain in the active phase of adapting domestic legislation to align with international standards.

Subsequently, the regulatory requirements imposed by FATF on virtual asset service providers are examined. In 2019, FATF updated its standards by introducing the category of Virtual Asset Service Providers (VASPs).

Key FATF requirements are set out in Recommendation 10 on Customer Due Diligence, which mandates customer identification (KYC), verification of beneficial ownership, and establishes that non-face-to-face threshold transactions of USD/EUR 1,000 or more require the application of customer due diligence measures.

The core AML/CFT requirements applicable to virtual assets and VASPs are contained in FATF Recommendation 15 on *New Technologies*, which:

- defines virtual assets and VASPs as objects of financial monitoring;
- introduces mandatory licensing or registration of crypto-asset service providers;
- extends all fundamental AML/CFT obligations to VASPs;
- requires implementation of the Travel Rule;
- strengthens international cooperation;
- promotes the application of a risk-based approach.

VASPs are equated with financial institutions and are required to implement a full set of AML/CFT measures, including:

1. Customer due diligence (CDD), encompassing:
  - identification and verification of customers and ultimate beneficial owners (UBOs);
  - customer risk assessment;
  - enhanced monitoring of high-risk transactions.
2. Record-keeping of transaction data and customer information for at least five years;
3. Ongoing transaction monitoring, detection of suspicious activities, and submission of suspicious transaction reports to competent authorities;

4. Identification and monitoring of politically exposed persons (PEPs), including the application of enhanced due diligence (EDD) to PEPs, their family members, and close associates.

The status of FATF Recommendation implementation is reflected in recent assessments. As of April 2025, a total of 138 jurisdictions had been evaluated for compliance with FATF standards on virtual assets and VASPs under Recommendation 15 and its Interpretive Note (INR.15). Global implementation has shown moderate improvement compared to 2024. Specifically, 29% of jurisdictions (40 out of 138) were assessed as largely compliant, up from 25% in 2024, while the proportion of non-compliant jurisdictions declined from 25% to 21%. Nearly half of jurisdictions (49%) remain only partially compliant, and, as in the previous year, only one jurisdiction achieved full compliance.

Positive developments were observed in international cooperation and cross-border information exchange. However, substantial challenges persist, particularly in conducting comprehensive ML/TF risk assessments, identifying and supervising VASP entities, and effectively implementing the FATF Travel Rule.

According to the FATF survey conducted in March 2025, 76% of jurisdictions (124 out of 163) reported having conducted ML/TF risk assessments related to virtual assets and VASPs, compared to 71% in 2024. Nevertheless, only 40 out of 138 jurisdictions met or largely met the requirements for applying a risk-based approach in this area, indicating a persistent gap between formal compliance and effective implementation [6].

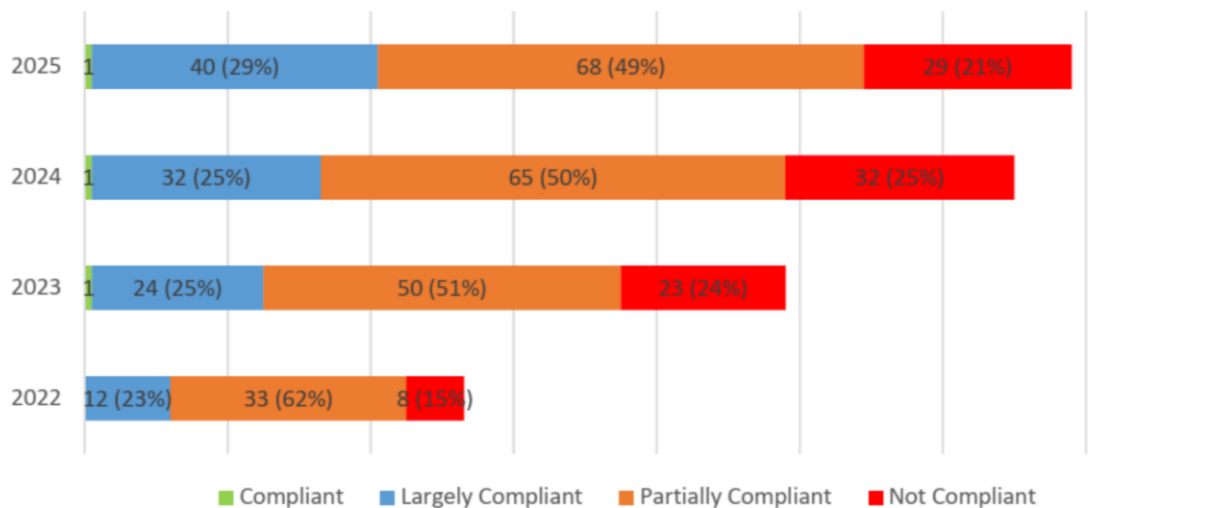


Figure 1. Assessment Results: Compliance with R. 15 (as of April 2025)

Source: Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs [6].

Moreover, Recommendation 16 “Wire Transfers” establishes the so-called *Travel Rule*. In particular, VASPs are required to transmit information on the originator and the beneficiary, including relevant identification data, together with a virtual asset transfer, and to ensure that such information is readily available to regulatory and law enforcement authorities.

The extent to which individual jurisdictions have implemented the Travel Rule is illustrated by the findings of recent empirical studies.

According to the 2025 FATF survey, 73% of jurisdictions (85 out of 117)—excluding those that prohibit or intend to prohibit VASP activities—have enacted legislation implementing the Travel Rule. This marks an increase compared to 2024, when only 65 jurisdictions had adopted the relevant legal framework. A further 14 jurisdictions are currently in the process of implementation, slightly fewer than the 15 out of 80 jurisdictions reported in 2024. At the same time, 42 of the 205 surveyed jurisdictions did not submit responses, which strongly indicates a lack of implementation and underscores that global compliance with the Travel Rule remains incomplete.

Despite notable legislative progress, enforcement practices remain limited. Among the 85 jurisdictions in which Travel Rule legislation is already in force, 59% (50 jurisdictions) have not yet issued supervisory findings, formal directives, or undertaken enforcement actions related to compliance. This situation can largely be explained by the relatively recent adoption of the relevant legislation, as competent authorities in many jurisdictions are still in the process of developing supervisory frameworks and enforcement mechanisms. In addition, certain jurisdictions may currently prioritize engagement with VASPs, the handling of ongoing cases, or the facilitation of remedial measures.

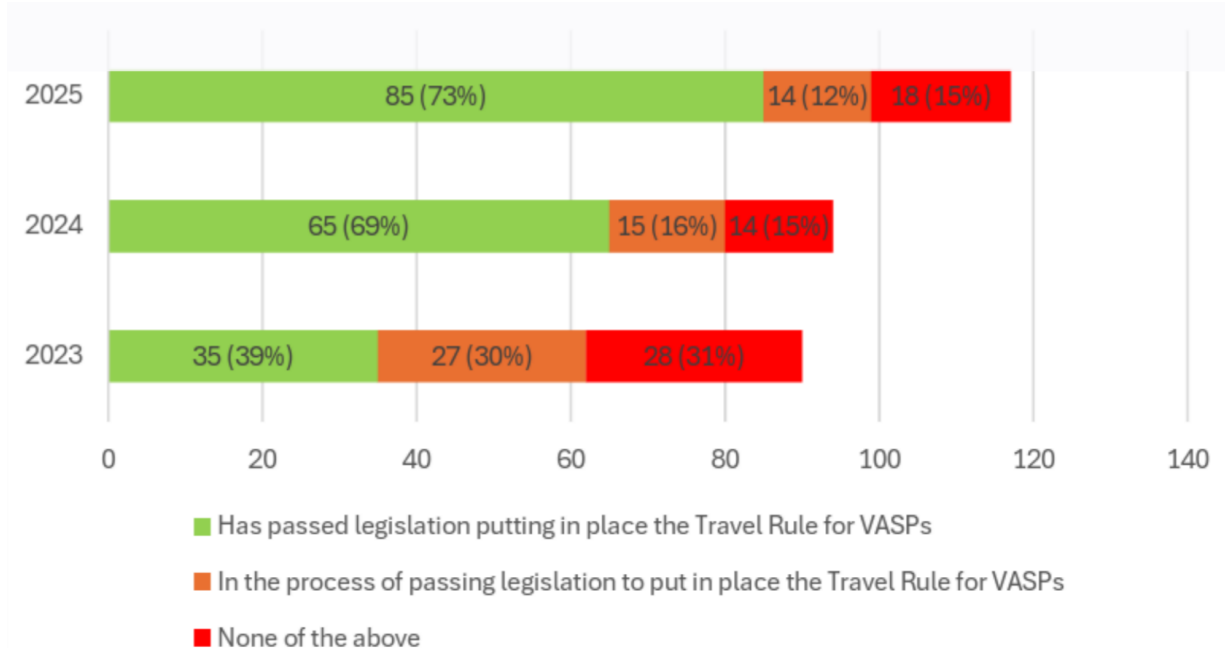


Figure 2. Jurisdictional Implementation of the Travel Rule  
Source: Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs [6].

In response to these challenges, the FATF has emphasized the urgent need for jurisdictions to fully operationalize the Travel Rule. To promote effective and consistent supervisory and enforcement practices, the FATF issued a dedicated guidance document entitled *Best Practices in Travel Rule Supervision* (FATF/PDG(2025)18).

The countries of the European Union, in turn, are gradually implementing the provisions of the Markets in Crypto-Assets Regulation (MiCA), which introduces comprehensive requirements regarding transparency, licensing, and financial monitoring of participants in the crypto-asset market [7]. In addition, the EU has adopted the Regulation on information accompanying transfers of funds and certain crypto-assets (TFR, 2023), which effectively obliges crypto-asset service providers to apply the Travel Rule, namely to provide data on the originator and the beneficiary of virtual assets during a transaction.

In particular, the MiCA lays down uniform transparency and disclosure rules on the issuance, offer to the public and admission to trading of crypto-assets; additionally, it governs the authorisation and supervision of crypto-asset service providers (CASPs). The Regulation intends to protect investors, promote innovation and competition, safeguard financial stability, ensure the smooth operation of payment systems, avoid monetary policy risks, prevent market abuse and insider dealing. In force of the technology neutrality principle, crypto-assets that are already covered by existing legislation, such as financial instruments, deposits, funds, or securitisations, fall outside the scope of MiCA and shall remain covered by existing regulation [10].

Among the key advantages of MiCA is the establishment of a single, harmonised regulatory framework for crypto-assets across the entire European Union. In practical terms, obtaining

authorisation in one Member State enables crypto-asset service providers to offer their services throughout all EU Member States, thereby ensuring regulatory certainty and facilitating cross-border market access.

Furthermore, the application of the MiCA Regulation enhances the protection of both crypto-asset projects and investors. In particular, compliance by CASPs with the regulatory obligations set forth under MiCA enables them to effectively defend their rights and legitimate interests against unlawful or excessive claims by various authorities and institutions. However, it should be emphasised that the actual effectiveness of any regulatory framework largely depends on the quality and consistency of its enforcement in practice.

It should also be noted that although the terms *Virtual Asset Service Provider* (VASP) and *Crypto-Asset Service Provider* (CASP) are often used interchangeably, there are significant differences between them (Table 1). The concept of VASP was introduced by the Financial Action Task Force and encompasses a broad range of crypto-related services, including the exchange and administration of virtual assets. CASPs, by contrast, are regulated under MiCA and include only those service providers operating within the European Union. While VASPs are required to comply with AML/KYC obligations in line with FATF's global standards, CASPs under MiCA are subject to additional regulatory requirements, including consumer protection measures and safeguards aimed at maintaining financial market stability. Accordingly, whereas VASPs may operate on a global scale, CASPs are strictly confined to the regulatory framework of the European Union.

*Table 1. Comparison of the Concept and Substance of the Terms VASP and CASP*

Criterion	VASP	CASP
Regulatory scope	AML/CFT (anti-money laundering and counter-terrorist financing)	Market regulation, licensing, supervision, and investor protection
Legal nature	FATF international standard (binding through national implementation)	EU Regulation, legally binding on all Member States
Definition of the asset	Virtual asset (broad concept)	Crypto-asset (narrower concept as defined by MiCA)
Main types of services	Exchange of virtual assets; transfer of virtual assets; custody and safekeeping services; participation in financial services related to virtual assets	Custody and administration; exchange; execution of orders; placement of crypto-assets; reception and transmission of orders; portfolio management; advisory services
Mandatory requirements	KYC, CDD, Travel Rule, reporting of suspicious transactions, PEP screening, ongoing monitoring	Licensing, operational resilience, corporate governance, disclosure obligations, safeguarding of clients' assets
Primary focus	Prevention of illicit financial flows	Market regulation and mitigation of risks to consumers
Status in the international context	Applied in all jurisdictions implementing FATF standards	Applicable exclusively within the European Union
Supervisory authorities	National financial intelligence and AML/CFT authorities	National financial regulators (central banks, market supervisory authorities)
Legal force	Standards implemented through national legislation	Direct applicability in the EU, mandatory for all market participants
Registration / licensing requirements	Requires registration or licensing of VASPs, without detailed procedural specifications	Detailed licensing procedures, capital requirements, compliance and risk-management obligations

*Source: compiled by the author*

It is also necessary to draw attention to another important aspect of financial monitoring of virtual assets. Despite the well-recognised attractiveness of cryptocurrencies for money laundering and terrorist financing, a number of inherent characteristics significantly reduce this level of attractiveness (Table 2).

Table 2. Characteristics of cryptocurrencies that reduce their attractiveness for ML/TF

No.	Characteristic	Substance and impact on ML/TF risk reduction
1	Public and transparent nature of blockchain	Data on all transactions are recorded in a public ledger, enabling real-time tracing of fund movements and thereby complicating the concealment of illicit activities.
2	Pseudonymity rather than full anonymity	Crypto wallets may be linked to real individuals through exchanges or analytical algorithms, making illicit schemes less covert.
3	Complexity of conversion into fiat currency	Exchanging cryptocurrencies into traditional currencies generally requires identity verification, leaving traceable records for law enforcement authorities.
4	Development of analytical tools	Chainalysis, TRM Labs, Elliptic, and similar tools enable the tracing of transaction chains, identification of mixers, and detection of monitoring evasion schemes.
5	Blacklists and reputational tagging	Addresses associated with criminal activity are blocked or flagged as high-risk, complicating the further use of such assets in subsequent transactions.
6	High market volatility	Price instability reduces the suitability of cryptocurrencies for long-term value storage within illicit schemes.

Source: compiled by the author.

Next, the current state of AML/CFT/CPF implementation in the field of virtual assets in Ukraine should be examined. According to the Global Cryptocurrency Adoption Index, Ukraine ranked 4th in terms of cryptocurrency transaction volume in 2021, 6th in 2024, and 8th in 2025 [4].

This situation is driven by a number of factors. In particular, transactions involving such assets are fast and offer a degree of anonymity, which makes them a potentially convenient instrument for laundering criminal proceeds and financing terrorism. Taking into account the need to regulate virtual assets and transactions conducted using them, on 8 September 2021 the Verkhovna Rada of Ukraine adopted, at second reading, the Law of Ukraine “On Virtual Assets”. The law was intended to regulate social relations arising in connection with the circulation of virtual assets in Ukraine, to define the rights and obligations of market participants, and to establish the principles of state policy in the field of virtual assets. However, the law was returned by the President for revision and ultimately never entered into force.

On 3 September 2025, the Verkhovna Rada of Ukraine took a significant step towards the development of the digital economy by adopting, at first reading, Draft Law No. 10225-d, which aims to legalise the virtual asset market and establish rules for their taxation. The draft law defines virtual assets as a specific type of digital property that does not constitute legal tender, while their legal regime is equated to that of movable property [5].

The draft law establishes a taxation rate on income derived from crypto-asset transactions at 18% personal income tax and 5% military levy, with a preferential rate of 5% applicable during the first year. It also provides for stringent financial monitoring requirements comparable to those applied in the banking sector and envisages harmonisation with the EU Markets in Crypto-Assets Regulation (MiCA).

The issue of designating the market regulator—either the National Bank of Ukraine or the National Securities and Stock Market Commission—remains unresolved and is expected to be determined prior to the second reading. The draft law also introduces liability for violations, including fines imposed on virtual asset service providers. In parallel with the legalisation of cryptocurrencies within the banking sector, the implementation of open banking is underway, regulating data exchange between banks and third-party payment service providers based on the user’s explicit consent. This development creates additional safeguards for the security and transparency of virtual asset transactions.

At the same time, experts emphasise the need to further refine the draft law in order to avoid excessive regulatory burdens on businesses and the risk of abuse by supervisory authorities. Overall, the legalisation of the cryptocurrency market could generate up to UAH 14–15 billion in

additional annual budget revenues and contribute to the development of Ukraine’s digital economy. At present, further work on Draft Law No. 10225-d is ongoing, with more than 2,000 amendments reportedly submitted.

Taking into account the above, it is possible to formulate the key regulatory tasks facing Ukraine at the current stage of development of the virtual asset market (Table 3).

Table 3. Key Tasks of Regulating the Virtual Asset Market

No.	Regulatory area	Content of the task
1	Transparency and accountability of market participants	<ul style="list-style-type: none"> <li>• Licensing and registration of VASPs/CASPs</li> <li>• Establishment of disclosure standards</li> <li>• Introduction of corporate governance requirements</li> </ul>
2	Anti-money laundering and counter-terrorist financing (AML/CFT)	<ul style="list-style-type: none"> <li>• Implementation of KYC/CDD procedures</li> <li>• Application of the FATF Travel Rule</li> <li>• Transaction monitoring and reporting of suspicious activities</li> </ul>
3	Consumer and investor protection	<ul style="list-style-type: none"> <li><input type="checkbox"/> Prevention of fraud and market manipulation</li> <li><input type="checkbox"/> Ensuring the security of asset custody</li> <li><input type="checkbox"/> Disclosure of risks associated with virtual assets</li> </ul>
4	Enhancement of financial stability	<ul style="list-style-type: none"> <li>• Prevention of fraud and market manipulation</li> <li>• Ensuring the security of asset custody</li> <li>• Disclosure of risks related to virtual assets</li> </ul>
5	Promotion of innovation in the blockchain sector	<ul style="list-style-type: none"> <li>• Creation of favourable conditions for Web3 companies</li> <li>• Support for the development of tokenisation and digital assets</li> <li>• Introduction of regulatory sandboxes</li> </ul>
6.	Cybersecurity and infrastructure protection	<ul style="list-style-type: none"> <li>• Cybersecurity requirements for exchanges and custodians</li> <li>• Prevention of hacking and cyberattacks</li> <li>• Cooperation with international cyber intelligence centres</li> </ul>
7.	Harmonisation with international standards	<ul style="list-style-type: none"> <li>• Implementation of FATF Recommendation 15</li> <li>• Alignment with EU regulation (MiCA, AML Package)</li> <li>• Unified approaches to cross-border operations</li> </ul>

Source: compiled by the author.

**Discussion.** Despite the introduction of legal regulation governing the circulation of virtual assets in Ukraine, significant gaps remain both in the normative regulation of certain aspects and in law enforcement practices aimed at countering the criminal use of cryptocurrencies [15].

Within the framework of financial monitoring of virtual assets in Ukraine, the key issues under discussion include the incomplete implementation of FATF standards (in particular Recommendation 15), deficiencies in the licensing of virtual asset service providers (VASPs), and the limited effectiveness of the State Financial Monitoring Service of Ukraine in providing data for the investigation of crypto-related transactions. These challenges are further exacerbated by the wartime context, in which virtual assets are frequently used for rapid transactions but are often flagged due to “tainted” funds or errors in AML systems.

FATF Recommendation 15 requires risk assessment, licensing of VASPs, and the implementation of the Travel Rule; however, in Ukraine these measures have been implemented only partially, with weak supervisory oversight and limited enforcement. Draft Law No. 10225-d, adopted at first reading, does not resolve issues related to coordination between the National Bank of Ukraine, the National Securities and Stock Market Commission, and the Ministry of Digital Transformation of Ukraine. Scholarly and policy debates also highlight the risks associated with

decentralised finance (DeFi) and decentralised exchanges (DEXs), where centralised control mechanisms are absent.

Particular attention is drawn to identification challenges and risk management issues, as AML/KYC systems frequently block bona fide users due to interactions with unregulated exchanges or suspicious transaction patterns, resulting in false positives. Although the State Financial Monitoring Service of Ukraine coordinates analytical efforts, law enforcement authorities still lack comprehensive information, especially with regard to anonymous wallets and cross-border transactions.

Issues related to institutional coordination, regulatory oversight of compliance in the virtual asset market, and the effective enforcement of AML requirements therefore remain unresolved.

**Conclusions.** The conducted research confirms that the rapid development of the virtual asset market is significantly transforming the financial system while simultaneously generating new and complex challenges for anti-money laundering and counter-terrorist financing systems. Combining substantial innovative potential with a high degree of technological complexity, virtual assets function both as instruments of economic development and as objects of heightened AML/CFT risk, particularly in the context of cross-border transactions, decentralised financial services, and the use of anonymisation technologies.

The article substantiates that international FATF standards—particularly Recommendation 15 and its associated requirements regarding VASP licensing, the application of a risk-based approach, and the implementation of the Travel Rule—constitute the core foundation for an effective financial monitoring system in the virtual asset sector. At the same time, the results of global FATF assessments demonstrate the fragmented and uneven implementation of these standards across jurisdictions, creating regulatory gaps and opportunities for regulatory arbitrage.

The study further demonstrates that, contrary to the widespread perception of cryptocurrencies as highly attractive tools for criminal activity, a number of their inherent characteristics—such as blockchain transparency, pseudonymity, difficulties in converting into fiat currency, the development of analytical tools, and reputational mechanisms—objectively reduce the effectiveness of virtual assets for money laundering and terrorist financing, provided that adequate regulatory and supervisory frameworks are in place.

An analysis of the European regulatory approach, particularly the Markets in Crypto-Assets Regulation (MiCA), allows the conclusion that the combination of FATF AML/CFT requirements with market and prudential regulation of CASPs forms a more comprehensive model of crypto-market oversight. This model is oriented not only towards preventing illicit financial flows but also towards investor protection and financial stability. The identified distinctions between VASPs and CASPs confirm the necessity of clearly separating AML functions from market supervision functions.

For Ukraine, the issue of financial monitoring of virtual assets is of particular importance in the context of wartime conditions, a high level of digitalisation, and the widespread use of cryptocurrencies by individuals and businesses. Despite existing legislative initiatives, including Draft Law No. 10225-d, the regulatory and supervisory framework governing virtual assets remains at a formative stage, with significant gaps persisting in institutional coordination, service provider licensing, and the practical enforcement of AML/CFT requirements.

In summary, effective financial monitoring in the virtual asset environment is achievable only through a comprehensive approach that combines the implementation of FATF international standards, harmonisation with EU law, the development of analytical and digital supervisory tools, and the strengthening of the institutional capacity of national regulators. The implementation of these measures constitutes a key prerequisite for ensuring Ukraine's financial security, reducing ML/TF risks, and fostering the sustainable development of the virtual asset market in the future.

### References

1. Verkhovna Rada of Ukraine. (2003). *Civil Code of Ukraine: Law of Ukraine № 435-IV*. Retrieved from: <https://zakon.rada.gov.ua/laws/show/en/435-15> [in Ukrainian]
2. Financial Action Task Force. (2025). *International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation. FATF Recommendations*. Retrieved from: <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html>
3. Chainalysis. (2024). *Money Laundering and Cryptocurrency*. Retrieved from: <https://go.chainalysis.com/cryptocurrency-money-laundering-report.html>
4. Chainalysis. (2025). *The 2025 Global Cryptocurrency Adoption Index: India and the United States Lead Cryptocurrency Adoption*. Retrieved from: <https://www.chainalysis.com/blog/2025-global-crypto-adoption-index/>
5. Verkhovna Rada of Ukraine. (2025). *On Amendments to the Tax Code of Ukraine and Certain Other Legislative Acts of Ukraine on the Regulation of the Circulation of Virtual Assets in Ukraine: Draft Law of Ukraine No. 10225-d*. Retrieved from: <https://itd.rada.gov.ua/billinfo/Bills/Card/56271> [in Ukrainian]
6. FATF. (2025). *Jurisdictions' Implementation of FATF Standards on Virtual Assets and Virtual Asset Service Providers (Recommendation 15): Targeted Update (Summary)*. Retrieved from: <https://www.21analytics.ch/blog/2025-fatf-targeted-update-summarised/>
7. European Securities and Markets Authority (ESMA). (2023). *Markets in Crypto-Assets Regulation (MiCA)*. Retrieved from: <https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/markets-crypto-assets-regulation-mica>
8. Kulyk, O. (2025). Virtual asset market participants. *Theory and Practice of Jurisprudence*, 2(26), 77–91. <https://doi.org/10.21564/2225-6555.2024.26.312466>
9. Ustyenko, V., Dzhabrailov, R., & Hudima, T. (2023). Priority directions for the formation of a legal framework for post-war economic recovery in Ukraine. *Law of Ukraine*, 9, 9–23. <https://doi.org/10.33498/louu-2023-09-009>
10. Cappai, M. (2023). The role of private and public regulation in the case study of crypto-assets: The Italian move towards participatory regulation. *Computer Law & Security Review*, 49, 105831. <https://doi.org/10.1016/j.clsr.2023.105831>
11. Popova, I., Liu, Y., & Yi, H. (2025). Anchoring on safe haven: Russia–Ukraine war effects on the cryptocurrency market. *Journal of Behavioral and Experimental Finance*, 48, 101122. <https://doi.org/10.1016/j.jbef.2025.101122>
12. Dote-Pardo, J., & Espinosa-Jaramillo, M. T. (2025). Money laundering risks of cryptocurrencies: Towards coordinated regulatory and technological strategies. *Latin American Journal of Central Banking*. <https://doi.org/10.1016/j.latcb.2025.100194>
13. Gupta, A., Dwivedi, D. N., & Shah, J. (2023). *Artificial Intelligence Applications in Banking and Financial Services*. Singapore: Springer Nature. <https://doi.org/10.1007/978-981-99-2571-1>
14. Horobets, N., Reznik, O., Maliyk, V., Vyhivskyi, I., & Bobrishova, L. (2025). Artificial intelligence technologies in banking: Challenges and opportunities for anti-money laundering in the context of EU regulatory initiatives. *Journal of Money Laundering Control*, 28(4–5), 593–608. <https://doi.org/10.1108/JMLC-03-2025-0041>
15. Yusupov, V. V., & Marchuk, R. P. (2025). Counteracting the illegal circulation of virtual assets in Ukraine: Issues of legal regulation. *Scientific Bulletin of Uzhhorod National University. Series: Law*, 90(4), 53. <https://doi.org/10.24144/2307-3322.2025.90.4.53> [in Ukrainian]

Received: 10.11.2025

Accepted: 02.03.2026

Received after review: 30.01.2026

Published: 31.03.2026

**Утенкова Каріна**

доктор економічних наук, професор  
професор кафедри банківського бізнесу та фінансових технологій  
ННІ «Каразінський банківський інститут»  
Харківський національний університет імені В.Н. Каразіна  
майдан Свободи, 4, м. Харків, 61022, Україна  
e-mail: [utenkova@karazin.ua](mailto:utenkova@karazin.ua)  
ORCID ID: [0000-0001-9097-5431](https://orcid.org/0000-0001-9097-5431)

**Фінансовий моніторинг віртуальних активів: міжнародні стандарти та виклики імплементації в Україні**

**Анотація.** Стаття присвячена дослідженню фінансового моніторингу у сфері обігу віртуальних активів. Стрімкий розвиток цього сегмента фінансового ринку створює нові можливості для економіки, водночас формуючи підвищені ризики відмивання доходів, фінансування тероризму та обходу санкцій, що зумовлює необхідність ефективного регуляторного та наглядового реагування.

**Постановка проблеми.** Основною проблемою є недостатня узгодженість національних механізмів фінансового моніторингу віртуальних активів з міжнародними стандартами FATF та європейським регулюванням, а також фрагментарність правозастосовної практики в Україні в умовах високої динаміки крипторинку.

**Нерозв'язані аспекти.** Незважаючи на активне формування нормативної бази, залишаються нерозв'язаними питання ефективної імплементації Рекомендації 15 FATF, застосування Travel Rule, координації між національними регуляторами, а також нагляду за децентралізованими фінансовими сервісами та транскордонними операціями.

**Мета статті.** Метою дослідження є комплексний аналіз міжнародних стандартів фінансового моніторингу віртуальних активів, оцінка актуальних ризиків відмивання коштів і фінансування тероризму та обґрунтування напрямів удосконалення регулювання в Україні з урахуванням стандартів FATF і підходів ЄС.

**Основний матеріал.** У статті проаналізовано правову природу віртуальних активів, вимоги FATF до VASP, особливості застосування Travel Rule, статистику незаконних криптооперацій за даними Chainalysis, а також європейську модель регулювання відповідно до Регламенту MiCA. Окрему увагу приділено порівнянню понять VASP і CASP та оцінці стану правового регулювання в Україні.

**Висновки.** Обґрунтовано, що ефективний фінансовий моніторинг віртуальних активів можливий лише за умови поєднання міжнародних стандартів FATF, гармонізації з правом ЄС, розвитку аналітичних технологій та посилення інституційної спроможності національних органів. Практичне значення результатів полягає у формуванні рекомендацій для підвищення фінансової безпеки України та зниження ризиків ML/TF у криптосекторі.

**Ключові слова:** віртуальні активи; фінансовий моніторинг; протидія відмиванню коштів (AML); фінансування тероризму (CFT); FATF; Travel Rule; VASP; CASP; Регламент MiCA; криптовалютний ринок; фінансова безпека.

**Формул:** 0; **рис.:** 2, **табл.:** 3, **бібл.:** 15.

**JEL Classification:** G 18, G28, F 38, K 22

**Для цитування:** Utenkova Karina. Financial monitoring of virtual assets: international standards and challenges of implementation in Ukraine. Фінансово-кредитні системи: перспективи розвитку. №1(20) 2026. С. 133-145. <https://doi.org/10.26565/2786-4995-2026-1-10>

**Список літератури**

1. Цивільний кодекс України: Закон України № 435-IV від 16 грудня 2003 р. URL: <https://zakon.rada.gov.ua/laws/show/en/435-15>
2. Financial Action Task Force (2025). International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation. FATF Recommendations. Retrieved from <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html>
3. Money Laundering and Cryptocurrency (2024). Chainalysis. Retrieved from <https://go.chainalysis.com/cryptocurrency-money-laundering-report.html>
4. The 2025 Global Adoption Index: India and the United States Lead Cryptocurrency Adoption (2025). Chainalysis. Retrieved from <https://www.chainalysis.com/blog/2025-global-crypto-adoption-index/>
5. Про внесення змін до Податкового кодексу України та деяких інших законодавчих актів України щодо врегулювання обороту віртуальних активів в Україні: Проект Закону України № 10225-д від 24 квітня 2025 р. URL: <https://itd.rada.gov.ua/billinfo/Bills/Card/56271>
6. Jurisdictions' Implementation of FATF Standards on VAs/VASPs (R.15). 2025 FATF Targeted Update Summarised. Retrieved from <https://www.21analytics.ch/blog/2025-fatf-targeted-update-summarised/>
7. Markets in Crypto-Assets Regulation (MiCA) (2023). ESMA. Retrieved from <https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/markets-crypto-assets-regulation-mica>

8. Kulyk, O. (2025). Virtual asset market participants . *Theory and Practice of Jurisprudence*, 2(26), 77–91. Retrieved from <https://doi.org/10.21564/2225-6555.2024.26.312466>
9. Ustymenko, V., Dzhabrailov, R. & Hudima, T. (2023). Priority directions for the formation of a legal framework for post-war economic recovery in Ukraine. *Law of Ukraine*, 9, 9-23. Retrieved from <https://doi.org/10.33498/louu-2023-09-009>.
10. Cappai, M. (2023). The Role of Private and Public Regulation in the Case Study of Crypto-Assets: The Italian Move Towards Participatory Regulation.” *Computer Law & Security Review*, 49, 105831. Retrieved from <https://doi.org/10.1016/j.clsr.2023.105831>.
11. Popova, I., Liu, Y. , Yi, H. (2025). Anchoring on safe haven: Russia–Ukraine war effects on the cryptocurrency market. *Journal of Behavioral and Experimental Finance*, 48, Page 101122. Retrieved from <https://doi.org/10.1016/j.jbef.2025.101122>
12. Dote-Pardo, J. & Espinosa-Jaramillo, M.T. (2025). Money laundering risks of cryptocurrencies: Towards coordinated regulatory and technological strategies. *Latin American Journal of Central Banking*, Retrieved from <https://doi.org/10.1016/j.lacsb.2025.100194>
13. Gupta, A., Dwivedi, D.N., Shah, J. (2023). Artificial Intelligence Applications in Banking and Financial Services. *Springer Nature Singapore, Singapore*. Retrieved from <https://doi.org/10.1007/978-981-99-2571-1>.
14. Horobets N, Reznik O, Maliyk V, Vyhivskiy I, Bobrishova L (2025), Artificial intelligence technologies in banking: challenges and opportunities for anti-money laundering in the context of EU regulatory initiatives. *Journal of Money Laundering Control*, Vol. 28 No. 4-5 pp. 593–608. Retrieved from <https://doi.org/10.1108/JMLC-03-2025-0041>
15. Юсупов В.В., Марчук Р.П. Протидія незаконному обігу віртуальних активів в Україні: питання правового регулювання. *Науковий вісник Ужгородського Національного Університету*. 2025. Серія «Право». Вип. 90: ч. 4. Retrieved from <https://doi.org/10.24144/2307-3322.2025.90.4.53>

Стаття надійшла до редакції 10.11.2025

Стаття надійшла після рецензування 30.01.2026

Статтю рекомендовано до друку 02.03.2026

Статтю опубліковано 31.03.2026