

UDC 346.1

DOI <https://doi.org/10.32782/chern.v1.2025.15>

*Starushchenko Ya. V.*  
Postgraduate Student  
Kyiv Aviation Institute  
[orcid.org/0009-0008-5164-5075](https://orcid.org/0009-0008-5164-5075)

## PREVENTION OF MONEY LAUNDERING FROM THE CIRCULATION OF VIRTUAL ASSETS: CURRENT LEGAL ASPECTS

**The purpose** of the article is to study the legal basis for preventing money laundering obtained from the circulation of virtual assets. **Research methods:** the chosen topic of scientific research requires the use of various scientific methods and approaches to obtain qualitative results. Therefore, the following research methods were used to solve the tasks: analysis; system method; analytical, etc. **Results:** the legal framework for preventing money laundering received from the circulation of virtual assets is in its infancy, and the current legislation of both the EU and other developed democracies in this area is still characterized by inconsistencies, contradictions, needs to eliminate gaps and does not provide optimal regulation of the digital market. However, for a comprehensive approach to eliminating gaps and inconsistencies in national legislation, the world The community has developed a number of recommendations to prevent money laundering received from the circulation of virtual assets. It is the preparation and implementation of the proposed norms that is the optimal step towards the development of appropriate national legal framework for the prevention of money laundering received from the circulation of virtual assets. **Discussion:** effective policies and legal frameworks for the prevention of money laundering derived from the circulation of virtual assets are key to the integrity and stability of both the international and national financial system and economy. Money laundering and related crimes (so-called “predicate crimes”) can threaten the integrity and stability of both the financial sector and the external stability of the country as a whole. They can lead to economic destabilization, banking crises, inefficient revenue collection, broader deficiencies in public administration, reputational risks to international financial centers, and the loss of correspondent banking relationships. In an increasingly interconnected world, the damage caused by these crimes is global and affects the integrity and stability of the international financial system.

Digital technology is an integral part of any modern economy due to its high degree of productivity and technological capabilities. A distinctive feature of the Ukrainian economy is the introduction of digital technologies into everyday life, both to accelerate management decision-making and to achieve the goal of their implementation. It is worth pointing out that in the digital age, there is a rapid development in the use of virtual assets, which, among other things, contributes to the development of illegal activities.

*Key words:* funds, virtual assets, digital age, prevention, money laundering.

### *Старущенко Я.В. ЗАПОБІГАННЯ ВІДМИВАННЮ КОШТІВ ВІД ОБІГУ ВІРТУАЛЬНИХ АКТИВІВ: АКТУАЛЬНІ ПРАВОВІ АСПЕКТИ*

**Метою** статті є дослідження правових засад запобігання відмивання коштів, отриманих від обігу віртуальних активів. **Методи дослідження:** обрана тема наукового дослідження потребує застосування різноманітних наукових методів і підходів для отримання якісних результатів. Тому для вирішення поставлених завдань використано такі методи дослідження: аналіз; системний метод; аналітичний тощо. **Результати:** правові засади запобігання відмивання коштів, отриманих від обігу віртуальних активів перебувають на стадії становлення, а чинне законодавство як ЄС, так й інших розвинених демократій, у цій сфері досі характеризується неузгодженістю, суперечностями, потребує усунення прогалин і не забезпечує оптимального регулювання цифрового ринку. Проте задля комплексного підходу до усунення прогалин та неузгодженостей національного законодавства світовою спільнотою розроблено низку рекомендацій щодо запобігання відмивання коштів, отриманих від обігу віртуальних активів. Саме підготовка та впровадження пропонованих норм є оптимальним кроком на шляху розроблення належних національних правових засад запобігання відмивання коштів, отриманих від обігу віртуальних активів. **Обговорення:** ефективна політика та правові засади запобігання відмивання коштів, отриманих від обігу віртуальних активів є ключем до цілісності та стабільності як міжнародної, так й національної фінансової системи та економіки. Відмивання грошей та пов'язані з ним злочини (так звані «предикатні злочини») можуть загрожувати цілісності та стабільності як фінансового сектору, так і зовнішній стабільності країни в цілому. Вони можуть призвести до дестабілізації економіки, банківських криз, неефективного збору доходів, більш широких недоліків публічного адміністрування, репутаційних ризиків для міжнародних фінансових центрів та втрати кореспондентських банківських відносин. У все більш взаємопов'язаному світі шкода, завдана цими злочинами, є глобальною та впливає на цілісність і стабільність міжнародної фінансової системи.

Цифрові технології є невід'ємною частиною будь-якої сучасної економіки завдяки своєму високому ступеню продуктивності та технологічним можливостям. Відмінною рисою української економіки є впровадження цифрових технологій у повсякденне життя, як для прискорення прийняття управлінських рішень, так і для досягнення мети їх впровадження. Варто вказати, що у цифрову епоху відбувається стрімкий розвиток використання віртуальних активів, що у тому числі сприяє розвитку незаконної діяльності.

*Ключові слова:* кошти, віртуальні активи, цифрова епоха, запобігання, відмивання коштів.

**Statement of the problem and its relevance.** Effective policies and legal frameworks to prevent money laundering derived from the circulation of

virtual assets are key to the integrity and stability of both the international and national financial system and economy. Money laundering and related

crimes (so-called ‘predicate offences’) can threaten the integrity and stability of both the financial sector and the external stability of the country as a whole. They can lead to economic destabilisation, banking crises, inefficient revenue collection, wider public administration failures, reputational risks for international financial centres and the loss of correspondent banking relationships. In an increasingly interconnected world, the harm caused by these crimes is global and affects the integrity and stability of the international financial system.

Digital technologies are an integral part of any modern economy due to their high degree of productivity and technological capabilities. A distinctive feature of the Ukrainian economy is the introduction of digital technologies into everyday life, both to accelerate management decision-making and to achieve the goal of their implementation. It is worth noting that in the digital age, the use of virtual assets is rapidly developing, which, among other things, contributes to the development of illegal activities.

**Analysis of research and publications on the issue.** The issue of regulating the virtual asset market is covered in the works of such scholars as D.Zetsche, M.Dinis Lucas, V.Ferrari, and others. The EU’s experience in the legal regime of cryptocurrencies is described in the works of V.A.Ustymenko, B.V.Derevyanko, O.I.Kulyk, I.P.Ustinova, etc.

**The purpose of the article** is to study the legal framework for preventing money laundering derived from the circulation of virtual assets.

**Summary of the main material.** The Law of Ukraine No. 361-IX dated 06.12.2019 ‘On Prevention and Counteraction to Legalisation (Laundering) of the Proceeds of Crime, Terrorist Financing and Financing of the Proliferation of Weapons of Mass Destruction’ stipulates that a virtual asset is a digital expression of value that can be traded in a digital format or transferred and can be used for payment or investment purposes (clause 13 of Article 1) [1]. It is worth noting that this Law adapts Ukrainian legislation to the provisions of the fourth EU Directive 2015/849 and EU Regulation 2015/847, as well as the standards of the Financial Action Task Force on Money Laundering and Terrorist Financing (FATF).

In order to understand the role of virtual assets in money laundering, it is important to understand the basics of this process. In particular, money laundering is a term used to describe actions aimed at disguising the source of funds and property obtained through criminal means and transferring them from criminal to legal circulation [2]. This process involves a series of transactions and actions that conceal the true source of funds, allowing criminals to avoid the attention of law enforcement agencies.

Traditionally, money laundering involved the circulation of cash through complex networks of intermediaries. However, with the rise of digital technology and the emergence of digital currencies, including cryptocurrencies, criminals have found new ways to launder money. Cryptocurrencies have also facilitated the operation of illegal online markets, commonly referred to as the ‘dark web’, where illegal goods and services are bought and sold. Virtual assets have become an attractive target due to their decentralised nature, which allows transactions to be conducted without revealing the identity of the owner. The anonymity provided by cryptocurrencies has made it difficult to trace and detain these individuals in the event of a criminal offence.

However, it is worth noting that not all cryptocurrencies are created equal in the field of illegal activities. Some of them are more popular among criminals due to specific features that help to conceal the origin and flow of funds. According to the Financial Crimes Academy, criminals mainly use Monero, Bitcoin, Ethereum, Ripple and Litecoin because of their ease of use, availability for sale and ability to conduct transactions with relative anonymity. Bitcoin in particular, due to its brand recognition and acceptance among darknet markets and other providers, remains the most commonly used cryptocurrency for illicit transactions. Monero is popular for its privacy and anonymity features, using technologies such as ring signatures and hidden addresses, which makes it much more difficult to trace transactions than Bitcoin. Ripple’s XRP can function as a bridge to facilitate exchanges between different cryptocurrencies quickly and with lower fees compared to traditional exchanges, thereby making it easy to launder the funds generated from the circulation of virtual assets. Ethereum smart contracts can also be used to create decentralised applications that facilitate money laundering through automated processes and transactions [3].

Indeed, understanding the appeal and use of these key cryptocurrencies in virtual asset laundering schemes is crucial to developing effective strategies to prevent financial crime in the digital currency sector. As we move into an increasingly digital age, it is vital that measures to prevent money laundering from virtual assets evolve in tandem with the development of virtual assets.

In order to prevent money laundering from virtual assets, regulators, financial institutions and law enforcement agencies are implementing measures to strengthen supervision and regulation. In particular, in response to the growing problem of money laundering, the Financial Action Task Force (FATF) was established in 1989 at a meeting of the Group of Seven leaders in Paris [4].

The Financial Action Task Force has been given the mandate to study money laundering methods and

trends, review measures already taken at the national or international level and identify measures that still need to be taken to prevent money laundering derived from the circulation of virtual assets.

The FATF has issued recommendations to address the risks associated with the laundering of funds derived from the circulation of virtual assets. These recommendations provide a consistent framework for states to regulate and supervise virtual asset service providers (VASPs) in the process of preventing money laundering.

In particular, one of the key recommendations is that VASPs should collect and store information about both the sender and the recipient of virtual asset transactions, which helps to create a transparent environment and prevent anonymous transactions that can be used to launder the proceeds of virtual assets.

It is worth noting that the global market capitalisation of virtual assets is currently more than USD 1 trillion, with the industry reaching USD 2.1 trillion in 2021 (the peak of its development). In 2023, the total capitalisation of the cryptocurrency market was over USD 1 trillion 143 billion. Currently, Ukraine ranks 3rd in terms of its propensity to use virtual assets [5].

Given the global nature of virtual assets and the challenges they pose to traditional anti-money laundering mechanisms, international cooperation and joint coordination of relevant authorities is essential. The vast majority of countries have recognised the importance of sharing information, best practices and intelligence to implement the best possible mechanism to prevent money laundering derived from the circulation of virtual assets.

Through initiatives such as the Egmont Group, Interpol and other international organisations, countries are working together to identify illicit financial flows facilitated by virtual assets. Increased cooperation allows for faster detection and response to new threats, providing a more robust global framework for preventing money laundering from virtual assets in the digital age.

It is worth noting that in order to keep pace with the changing landscape of virtual assets and money laundering schemes, countries are constantly updating their legal frameworks. Such legal reforms are aimed at ensuring that virtual assets are subject to effective regulation and supervision. To this end, for example, the European Union has taken steps to introduce regulation of cryptoasset markets (MiCA). The MiCA regulation is quite liberal and establishes certain requirements for a public offering of virtual assets, one of the main requirements of which is the publication of a white paper.

In particular, the Markets in Crypto Assets Regulation (MiCA) establishes common EU market rules for crypto assets. The regulation covers

crypto assets that are not currently regulated under existing financial services legislation. The key provisions for those issuing and trading crypto assets (including asset reference tokens and e-money tokens) cover transparency, disclosure, authorisation and transaction supervision. The new legal framework supports market integrity and financial stability by regulating public offerings of cryptoassets and ensuring that consumers are aware of the risks involved. Therefore, MiCA seeks to establish a comprehensive regulatory framework for digital finance and virtual assets, including rules to prevent money laundering derived from the circulation of virtual assets.

In particular, the Crypto Asset Markets Regulation (MiCA) entered into force in June 2023 and aims to provide regulators with the tools necessary to track cryptocurrencies used for money laundering, while ensuring that users are protected [6].

Similarly, countries such as the United States, the United Kingdom and others are implementing rules to monitor and control virtual asset transactions and prevent illegal activities such as money laundering derived from virtual assets [7].

By updating their legal frameworks, countries aim to ensure effective monitoring, regulation and compliance with relevant AML/CFT measures in virtual asset transactions. These measures provide a reliable basis for detecting, preventing and deterring money laundering activities derived from the circulation of virtual assets.

In our opinion, the implementation of regulatory measures, such as the FATF recommendations, MiCA provisions, international cooperation and coordination, and updated legal provisions, are crucial in the process of preventing money laundering from virtual assets. By working together, regulators and governments can mitigate the risks associated with virtual assets and contribute to a safer and more transparent financial system.

It is worth noting that criminals use a variety of methods and techniques to launder the proceeds of virtual assets. Understanding these methods is crucial to preventing the laundering of proceeds of crime from virtual assets in the digital age. In particular, the five most popular methods used by criminals to launder money on the blockchain include:

1. Nested services are a broad category of services that operate within one or more exchanges. These services use the addresses listed on the exchanges to tap into the liquidity of the exchanges and exploit trading opportunities. Some exchanges do not require high compliance standards for nested services, allowing bad actors to use them for money laundering. In the blockchain landscape, these nested service transactions appear to have been conducted by their host counterparties (i.e. exchanges) rather



than the hosted nested services or individual addresses. The most common and notorious type of nested service is the over-the-counter (OTC) broker. OTC brokers allow traders to trade large amounts of cryptocurrency easily, securely and anonymously. OTC brokers facilitate direct cryptocurrency trading between two parties without the intermediation of an exchange. These trades can be made between different cryptocurrencies (e.g. Ethereum and Bitcoin) or between cryptocurrencies and fiat currencies (e.g. cryptocurrencies such as Bitcoin and fiat currencies such as the euro). OTC brokers find counterparties for a transaction in exchange for a commission, but are not involved in the negotiation. Once the terms are agreed upon, the parties transfer custody of the assets to the broker. In particular, in August 2020, the US Department of Justice (DOJ) filed a complaint for the confiscation of 280 cryptocurrency addresses involved in the laundering of approximately \$28.7 million worth of cryptocurrency stolen from the exchange by hackers linked to North Korea known as the Lazarus Group. The complaint details two crypto exchange hacks by North Korean actors that stole millions of dollars worth of cryptocurrency and ultimately laundered the funds through Chinese over-the-counter (OTC) cryptocurrency traders, and follows related actions involving the theft of \$250 million in cryptocurrency through other exchange hacks by North Korean actors [8]. Lazarus Group continues to use OTC traders for money laundering. In April 2023, the U.S. Treasury Department's Office of Foreign Assets Control (OFAC) imposed sanctions on three individuals, including two OTC crypto traders, for assisting the North Korean group [9].

2. Gambling platforms are popular among cryptocurrency money launderers. Gambling services were mentioned in the FATF report 'Virtual Assets Red Flag for Money Laundering and Terrorist Financing' issued in September 2020 [10]. In this report, the FATF identified two situations in which gambling platform services can be considered as money laundering, in particular: 1) funds deposited or withdrawn from a virtual asset or wallet address with direct and indirect links to known suspicious sources, including dubious gambling sites; 2) transactions originating from or destined for online gambling services.

3. Mixers are services that combine digital assets from multiple addresses together before releasing them at random intervals to new destination addresses or wallets, thereby increasing anonymity. They are often used to hide the trail of funds before they are transferred to legitimate businesses or major exchanges. It is worth noting that in March 2023, the US Department of Justice announced a joint international takedown of ChipMixer, a cryptocurrency mixing service on the

darknet responsible for laundering more than \$3 billion in cryptocurrency. The operation allowed the German authorities to withdraw more than \$46 million in cryptocurrency from the servers [11]. Another example is Tornado Cash, a mixer that laundered more than \$7 billion from 2019 to 2022 until the service developer was arrested by Dutch authorities [12].

4. Fiat exchanges exchange cryptocurrencies for cash and can be mainstream, peer-to-peer (P2P) or non-compliant (exchanges that do not obey or are not subject to the rules). For example, exchanges used such addresses to cash out almost \$23.8 billion in cryptocurrency in 2022, which is 68% more than in the previous year [13].

5. Services headquartered in high-risk jurisdictions are services in jurisdictions identified as having strategic deficiencies in their AML or counter-terrorist financing (CFT) regimes. In particular, the FATF identifies jurisdictions with weak AML/CFT measures, often referred to as the 'Black and Grey List' [14]. The FATF's measures to publicly publish a list of countries with weak AML/CFT regimes have proved effective. On 18 January 2024, Commission Delegated Regulation (EU) 2024/163 [15] amending the EU list was published. As of June 2024, the FATF has reviewed 133 countries and jurisdictions and publicly identified 108 of them as having a weak AML/CFT regime. As a result, 84 countries have implemented the necessary reforms to address their AML/CFT weaknesses and have been removed from the list. The European Commission also identifies countries that have strategic deficiencies in their AML/CFT regimes and pose a significant threat to the financial system of the European Union [16].

Thus, the global community is constantly facing new challenges in the process of preventing money laundering from the circulation of virtual assets due to the increasingly complex methods of this process. However, it should be emphasised that measures are constantly being taken to prevent the laundering of funds derived from the circulation of virtual assets. In particular, the Commonwealth Secretariat developed and presented a new Model Law on 8 July 2024 in London to help countries regulate the rapidly growing virtual asset industry.

This law takes a principled approach to regulating virtual assets in line with the international standards set by the FATF and provides for a broad set of provisions, including licensing of virtual assets such as virtual currencies, defining issuer obligations, supervising financial activities and enforcing fines for non-compliance, etc. In addition, the Model Law proposes rules to prevent money laundering from the circulation of virtual assets, while protecting owners and providing them with legal clarity and stability. At the current stage, 19 Commonwealth countries

are in the process of using the Model Law to develop new or amend existing domestic legislation.

At the same time, on 30 May 2024, the Council of the European Union adopted a package of new rules to prevent money laundering derived from the circulation of virtual assets, which included EU Directive 2024/1640 of 31 May 2024 amending and repealing EU Directive 2015/849. EU Directive 2024/1640 sets out the mechanisms that Member States must implement to prevent the laundering of funds derived from the circulation of virtual assets in the financial system at the national level. Member States must implement this Directive by 10 July 2027.

In addition, EU Regulation 2024/1620 of 31 May 2024 establishing a body for the fight against money laundering and the financing of terrorism, also known as AMLA, which sets out the rules for preventing the laundering of funds derived from the circulation of virtual assets, should be added to this list. The Regulation will come into force on 10 July 2027, except for certain provisions that will come into force on 10 July 2029. As well as EU Directive 2024/1654 of 31 May 2024, which amends EU Directive 2019/1153 and establishes new rules for access to bank account registers by authorities and facilitates the use of transaction records.

The objectives of this package are to strengthen cooperation and coordination between national authorities, create a separate mechanism for this purpose, and create a single European AML/CFT regulation that could combine all the rules governing this area. That is, to make a transition from a model based solely on directives to a model based on a single regulation. The European Parliament emphasises that the new acts include enhanced due diligence and identity verification measures, after which the so-called obliged persons must report suspicious activities to the competent authorities [17].

**Conclusions.** The legal framework for the prevention of money laundering derived from the circulation of virtual assets is still in its infancy, and the current legislation of both the EU and other developed democracies in this area is still characterised by inconsistencies and contradictions, requires the elimination of gaps and, at the present stage, does not ensure optimal regulation of the digital market. However, as part of a comprehensive approach to eliminating gaps and inconsistencies in national legislation, the international community has developed a number of recommendations to prevent money laundering from the circulation of virtual assets. It is the preparation and implementation of the proposed rules that is the best step towards the development of an appropriate national legal framework for the prevention of money laundering derived from the circulation of virtual assets.

## Bibliography

1. Про запобігання та протидію легалізації (відмивання) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення: Закон України від 06.12.2019 № 361-IX URL: <https://zakon.rada.gov.ua/laws/show/361-20#Text>
2. Енциклопедія сучасної України URL: <https://esu.com.ua/article-3439>
3. Most Relevant Cryptocurrencies For Criminals: Tracing the Evolution of Criminal Money Finances URL: <https://financialcrimeacademy.org/relevant-cryptocurrencies-for-criminals/>
4. Група з розробки фінансових заходів боротьби з відмиванням грошей – FATF URL: <https://fiu.gov.ua/content/uk/fatf.htm>
5. CoinGeko. URL: <https://www.coingecko.com/uk>
6. What Is Markets in Crypto-Assets (MiCA)? URL: <https://www.investopedia.com/what-is-market-in-crypto-assets-6751039#toc-markets-in-crypto-assets-titles>
7. Cryptocurrency Regulations Around the World URL: <https://www.investopedia.com/cryptocurrency-regulations-around-the-world-5202122>
8. United States Files Complaint to Forfeit 280 Cryptocurrency Accounts Tied to Hacks of Two Exchanges by North Korean Actors URL: <https://www.justice.gov/usao-dc/pr/united-states-files-complaint-forfeit-280-cryptocurrency-accounts-tied-hacks-two>
9. Treasury Targets Actors Facilitating Illicit DPRK Financial Activity in Support of Weapons Programs URL: <https://home.treasury.gov/news/press-releases/jy1435>
14. FATF report Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing URL: <https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Virtual-Assets-Red-Flag-Indicators.pdf>
15. Justice Department Investigation Leads to Takedown of Darknet Cryptocurrency Mixer that Processed Over \$3 Billion of Unlawful Transactions URL: <https://www.justice.gov/usao-edpa/pr/justice-department-investigation-leads-takedown-darknet-cryptocurrency-mixer-processed>
16. Suspected developer of crypto mixer Tornado Cash arrested URL: <https://techcrunch.com/2022/08/12/suspected-tornado-cash-developer-arrested-in-amsterdam/>
17. The Chainalysis 2024 Crypto Crime Report URL: <https://go.chainalysis.com/crypto-crime-2024.html>
18. “Black and grey” lists URL: <https://www.fatf-gafi.org/en/countries/black-and-grey-lists.html>
19. Commission Delegated Regulation (EU) 2024/163 of 12 December 2023 URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R0163>
20. Anti-money laundering and countering the financing of terrorism at international level URL: [https://finance.ec.europa.eu/financial-crime/anti-money-laundering-and-countering-financing-terrorism-international-level\\_en](https://finance.ec.europa.eu/financial-crime/anti-money-laundering-and-countering-financing-terrorism-international-level_en)
21. New EU rules to combat money-laundering adopted URL: <https://www.europarl.europa.eu/news/en/press-room/20240419IPR20586/new-eu-rules-to-combat-money-laundering-adopted>
22. Устинова І. Е-гривня як крок до реформ у фінансовій системі України: зарубіжний досвід. *Наукові праці Національного авіаційного університету. Серія: Юридичний вісник «Повітряне і космічне право»*. 2024. № 1. С. 70–77.