DOI: https://doi.org/10.30525/2256-0742/2026-12-5-110-123

CRYPTOASSETS, MONEY LAUNDERING AND CRIMINAL LIABILITY: ECONOMIC AND LEGAL CHALLENGES OF THE DIGITAL FINANCIAL SYSTEM

Andrii Borovyk[1], Andrii Poliushko[2], Andrii Lukashuk[3]

Abstract. The present article provides a comprehensive economic and legal analysis of the use of cryptoassets in mechanisms for the legalisation (laundering) of proceeds of crime. In addition, it examines the specific features of criminal-law responses to such practices within the digital financial system. The study's relevance is determined by the rapid expansion of the global cryptoasset market, the growth in the volume of illicit cryptocurrency transactions, and the increasing use of stablecoins, P2P and OTC channels, cryptocurrency mixers, and other technologies in schemes designed to transfer and conceal criminal proceeds. It is also determined by the need to adapt national financial monitoring and criminal justice systems to the technological transformation of financial relations. The purpose of the study is fourfold: to identify the economic mechanisms through which cryptoassets are used for money laundering; to assess the applicability of Article 209 of the Criminal Code of Ukraine to digital forms of economic value; to pinpoint the primary challenges of criminal law qualification and evidentiary assessment; and to provide recommendations for enhancing the national economic and legal mechanisms for combating illicit financial flows in the digital environment. The study establishes that, while cryptoassets do not alter the economic essence of money laundering, they do significantly transform the architecture of the financial trail. This is achieved by increasing transactional complexity, fragmenting financial flows, enabling the repeated conversion of digital value and combining decentralised and traditional financial infrastructures. It is argued that the current wording of Article 209 of the Criminal Code of Ukraine is sufficiently technology-neutral to encompass transactions involving cryptoassets. However, the main challenges lie in establishing the link between a digital asset and a predicate criminal offence, identifying the beneficial or actual controller of the asset, proving that the individual is aware of its criminal origin, and ensuring effective procedural control over virtual assets. The study also shows that the FATF's standards and the European Union's regulatory framework provide the conceptual basis for integrating crypto assets into the wider system of risk-based AML/CFT regulation. The study's scientific novelty lies in substantiating an integrated model of economic and legal counteraction to money laundering involving cryptoassets. This model incorporates technology-neutral criminal law, specialised criminal procedural mechanisms for dealing with digital assets, risk-based financial monitoring, blockchain analytics and international co-operation. The findings have the potential to improve law enforcement practice under Article 209 of the Criminal Code of Ukraine by developing procedures for the detection, seizure, custody, valuation and confiscation of cryptoassets. They could also strengthen the analytical capacity of financial intelligence and criminal justice authorities and harmonise national regulation with FATF standards and European Union law.

Keywords: cryptoassets, money laundering, criminal liability, digital financial system, financial monitoring, blockchain analytics, FATF, MiCA.

JEL Classification: K14, K24, G28, E42, O33

Received on: August 07, 2026 **Accepted on:** October 10, 2026 **Published on:** November 02, 2026

[1] Private Institution "Scientific Institute of Public Law", Ukraine *(corresponding author)*
E-mail: aborovychok@gmail.com
ORCID: https://orcid.org/0000-0003-1834-404X
[2] Sole Proprietor, Ukraine
E-mail: poliushko.an@gmail.com
ORCID: https://orcid.org/0009-0000-5343-2876
[3] Private Law Practice, Ukraine
E-mail: lukashuk.av@ukr.net
ORCID: https://orcid.org/0009-0008-1492-7583

This is an Open Access article, distributed under the terms of the Creative Commons Attribution CC BY 4.0

1. Introduction

The rapid development of digital financial technologies and the growing use of cryptoassets are transforming the modern financial system. Cryptocurrencies, stablecoins and other digital assets are being used more and more for exchange, investment, capital preservation and cross-border transfers. However, the technological characteristics of their circulation – including pseudonymous blockchain addresses, high transaction speeds, repeated conversion and decentralised financial infrastructure – create additional risks for systems designed to prevent and counter the laundering of criminal proceeds.

While cryptoassets do not alter the economic essence of money laundering, they do substantially transform the mechanisms used to transfer and conceal illicit value. The use of transaction structuring, crypto mixers, P2P and OTC channels, the multi-stage conversion of digital assets and the combination of crypto-based and traditional financial infrastructures makes it more difficult to detect illicit financial flows, identify their origin and determine the actual participants in relevant transactions.

For Ukraine, these issues are of particular importance due to the high level of cryptoasset adoption, the incomplete development of a dedicated legal framework governing their circulation, and the security challenges arising from the ongoing full-scale armed aggression. Digital assets have been found to be utilised not only in schemes involving the laundering of criminal proceeds, but also for the evasion of sanctions, the financing of unlawful activities and the cross-border transfer of value outside traditional channels of financial control.

The criminal law response to such practices is primarily associated with the application of Article 209 of the Criminal Code of Ukraine. The main challenges lie not so much in establishing whether cryptoassets can be considered property, but in demonstrating their link to a predicate criminal offence, tracing the digital transaction trail, proving the individual's knowledge of the assets' criminal origin, and ensuring effective procedural control over them.

The purpose of this study is to provide a comprehensive economic and legal analysis of the use of cryptoassets in mechanisms for laundering proceeds of crime. In addition, the study will determine the specific features of applying Article 209 of the Ukrainian Criminal Code to digital forms of economic value. Furthermore, the study will substantiate directions for improving the national framework for countering illicit financial flows in light of contemporary international AML/CFT standards and the technological characteristics of the digital financial system.

2. Literature Review

An analysis of the scientific literature reveals that the study of cryptoassets and their use in illicit financial activities, as well as the mechanisms for countering money laundering, has evolved into an interdisciplinary field. This field combines approaches from criminal and financial law, economics, financial monitoring and digital forensics. Researchers primarily focus on the legal nature of virtual assets, the mechanisms through which they are used in money laundering schemes, the criminal-law qualification of relevant conduct, the evidentiary assessment of blockchain transactions, and the effectiveness of AML/CFT regulation.

These issues are developing across several interconnected areas in Ukrainian legal scholarship. Zh. V. Udovenko's work on criminal procedure, evidentiary issues and the use of specialised knowledge provides a methodological basis for analysing digital evidence and technologically complex financial transactions. K. O. Cherevko's work focuses on methods of laundering the proceeds of crime, as well as the criminal-law aspects of using intermediaries in illicit financial flows. A. I. Demchuk has analysed the specific use of cryptocurrencies for money laundering and terrorist financing. More recent studies by A. S. Politova have categorised the various scholarly approaches to the criminal law countermeasures against the laundering of property through virtual assets. O. V. Kuzmenko and P. Yu. Kravchuk examine virtual assets as the subject matter of criminal offences, as well as the difficulties involved in identifying and proving them. Finally, O. P. Hetmanets investigates the financial law foundations of cryptocurrency regulation and their place within the modern monetary system.

Sean Foley, Jonathan R. Karlsen and Tālis J. Putniņš made a major contribution to the quantitative analysis of illicit cryptoasset use in the international literature. In 'Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed through Cryptocurrencies?', Foley et al. (2019) developed an empirical methodology for estimating the scale of illicit activity in the Bitcoin network, demonstrating its relationship with illegal markets. Donato Masciandaro and Raffaella Barone analyse the economic nature of traditional and emerging money laundering mechanisms, including the use of cryptocurrencies to transform illicit capital (Barone & Masciandaro, 2019). Albrecht et al. (2019), meanwhile, take a more specific look at the integration of cryptocurrencies into the money laundering process and the resulting regulatory challenges. Ferwerda (2009) addresses the broader economic effectiveness of AML regulation, whereas Unger and van Waarden (2009) compare rule-based and risk-based AML models, highlighting the problems

associated with excessive reporting and information overload.

Another area of research focuses on blockchain forensics and the technological traceability of illicit cryptoasset flows. Möser et al. (2013) conducted an early systematic study of transaction anonymisation and money laundering tools within the Bitcoin ecosystem. Meanwhile, Meiklejohn et al. (2013) demonstrated the potential of transaction graph analysis and address clustering to associate pseudonymous Bitcoin activity with identifiable entities. These studies have helped to dispel the idea that cryptocurrencies are inherently untraceable and have established important methodological principles for using blockchain data in financial intelligence and criminal investigations today.

Despite the substantial body of research on this topic, most studies remain focused on individual aspects of the problem. These include the economics of the circulation of illicit cryptoassets, the legal status of virtual assets, financial monitoring, the qualification of crimes under criminal law, and blockchain analytics. There is an insufficiently developed comprehensive analysis of the relationship between the economic mechanisms of laundering digital value, the application of Article 209 of the Criminal Code of Ukraine, the establishment of the origin of cryptoassets, the criminal procedural control of these assets, and international AML/CFT standards. The present study therefore focuses on the integration of these economic, legal and technological dimensions.

3. Methodology

The study's methodological framework is based on an interdisciplinary approach combining economic and legal perspectives, and utilising tools from criminal law, criminal procedure, financial monitoring, economic analysis and digital forensics. This approach enables cryptoassets to be examined simultaneously as a form of digital economic value, an element of modern financial infrastructure, and a potential instrument for transferring, concealing and laundering the proceeds of crime. Consequently, it allows for a thorough evaluation of the relationship between the economic mechanisms of digital circulation, the criminal law classification of relevant activities, and the institutional mechanisms of AML/CFT control.

The study uses a systemic approach to identify the relationships between the economic, legal and technological aspects of combatting the illicit use of crypto assets. The formal legal method is used to analyse Article 209 of the Criminal Code of Ukraine, criminal procedural legislation and the rules that govern the legal status of virtual assets. The comparative legal method is utilised to draw parallels between Ukrainian regulation and FATF standards, European Union legislation, including MiCA and the rules governing information accompanying transfers of cryptoassets, as well as selected examples of foreign judicial practice. The economic and legal analysis is used to examine the structure and dynamics of illicit cryptoasset circulation, transaction structuring, crypto mixing, P2P and OTC operations, the conversion of digital assets into fiat currency, and the formation of hybrid money laundering schemes.

The study is based on Ukrainian and European Union legislation, FATF standards, and analytical materials. It also draws on statistical and analytical data from Chainalysis, as well as materials from the State Financial Monitoring Service and the Bureau of Economic Security of Ukraine. Other sources include selected materials from foreign judicial practice and contemporary academic research in criminal law, economics, financial monitoring, and blockchain forensics.

The study's limitations stem from its predominantly theoretical and analytical nature, as well as its reliance on publicly available statistical and law enforcement data. The findings do not include econometric modelling of illicit cryptocurrency flows or the experimental validation of blockchain analytics tools. This underlines the importance of further research using quantitative methods, large-scale blockchain data analysis and an empirical assessment of the effectiveness of AML/CFT mechanisms in the digital financial system.

4. Results and Discussion

4.1. Concept and Classification of Cryptoassets as Objects of Economic and Legal Relations

According to the Law of Ukraine 'On Virtual Assets' of February 17, 2022, No. 2074-IX, a virtual asset is defined as an object of civil rights that has value and is expressed as a set of electronic data. It exists and circulates exclusively through information and communication technologies and certifies property rights, including rights of claim to other objects of civil rights (The Law of Ukraine 'On Virtual Assets' of 15.11.2024, No. 2074-IX). Although the law has been adopted, it has not yet come into force. Therefore, its definition reflects the legislatively adopted model of virtual asset regulation rather than the special regulatory regime currently in operation. From an economic perspective, cryptoassets can be considered a particular type of digital representation of value that can be used for exchange, accumulation and investment, and which can be transferred and stored in a digital environment. At the same time, a significant proportion of cryptoassets are neither issued nor guaranteed by a central bank or other public authority. Instead, their economic value is primarily determined by

market demand, the functional characteristics of the relevant digital network and the confidence of its users (Prystash, 2023).

From an economic standpoint, cryptoassets can be divided into several main categories based on their functions and circulation characteristics. Each category is associated with a specific risk profile in the context of illicit financial activity. Payment cryptocurrencies, such as Bitcoin and Litecoin, operate as a decentralised digital means of exchange and can be used to transfer value outside of traditional banking intermediation mechanisms. The absence of a single issuing authority, the cross-border nature of transactions and the possibility of direct, peer-to-peer transfers mean they can be used at various stages of laundering the proceeds of crime. This includes the initial introduction of illicitly obtained value into digital financial circulation.

Stablecoins constitute a separate category. These are digital tokens whose value is linked to a fiat currency or another asset, or maintained through a stabilisation mechanism. Compared with conventional cryptocurrencies, they are significantly more attractive for large-scale digital transactions due to their lower price volatility, high liquidity and technological suitability for rapid cross-border value transfers. According to the Chainalysis Team (2026), stablecoins accounted for 84% of the total volume of illicit cryptocurrency transactions worldwide in 2025. Their characteristics facilitate their use in complex chains of asset transfers and conversions designed to obscure the origin of funds and the identity of the ultimate beneficiary.

Another category comprises tokenised digital assets representing property, investments or other economically significant rights. This includes security and utility tokens, as well as certain digital assets operating within metaverses and online gaming platforms. These assets are primarily associated with illicit financial schemes due to the possibility of repeatedly converting value across different digital environments, which can substantially complicate the economic link between the original source of funds and the asset ultimately held by an individual.

There are particular risks in the field of countering money laundering that arise from cryptoassets and technological instruments designed to enhance transaction privacy. The former include so-called 'privacy coins', the technological architecture of which is intended to conceal or significantly hinder the identification of transaction participants and parameters. By contrast, crypto-mixing services (also known as mixers or tumblers) are not a distinct category of cryptoasset, but they can be used to transform the transaction trail by pooling, splitting and subsequently transferring digital assets across numerous addresses. This makes it considerably more difficult to establish the link between the original sender of an asset and its ultimate recipient.

The legal nature of cryptoassets is characterised by functional multidimensionality. On the one hand, they are independent objects of property capable of possessing economic value, and subject to possession, disposal, transfer and other legally significant transactions. On the other hand, their technological characteristics mean they can be used as an instrument of criminal activity, such as concealing the origin of criminal proceeds, transferring or converting them, or facilitating their subsequent use. Nevertheless, this potential does not affect the legal status of a cryptoasset as a property right; it merely reflects the specific way in which the asset is used in criminal activity.

4.2. Scale and Dynamics of Cryptoasset Use in Illicit Financial Activity

The contemporary dynamics of illicit cryptoasset use are characterised by a significant rise in the total volume of relevant transactions, despite their limited share of the overall cryptocurrency market. According to Chainalysis, addresses identified as being associated with illicit activity received at least 154 billion USD worth of cryptocurrencies in 2025, which is a 162% increase on the revised figure of 57.2 billion USD for 2024. A significant factor contributing to this growth was the substantial increase in the value of assets received by entities subject to international sanctions (Chainalysis Team, 2026).

At the same time, these absolute figures require careful economic interpretation. Despite the record volume of illicit transactions in 2025, they accounted for less than 1% of the total volume of attributed cryptocurrency transactions (Chainalysis Team, 2026). Accordingly, the sharp increase in the nominal value of illicit transactions does not necessarily indicate a proportional increase in the criminalisation of the cryptocurrency market. To a large extent, this reflects the wider growth of the digital financial ecosystem. However, the simultaneous growth in activity across most categories of crypto-related crime also shows that the associated risks are becoming increasingly significant.

Another distinctive feature of the current stage is the qualitative transformation of the infrastructure supporting the circulation of illicit cryptoassets. By 2025, professionalised networks offering all-encompassing services for the transfer and laundering of illicit funds had become particularly prevalent. These networks included Chinese-language money laundering organisations, which specialised in asset conversion, nominee accounts and wallets, and over-the-counter intermediaries (Chainalysis Team, 2026). This suggests a gradual shift from individual offenders

occasionally using cryptoassets towards a specialised market for professional money laundering services that combine traditional and digital financial mechanisms (Foley et al., 2019).

Another important trend is the use of tokenised instruments to circumvent international sanctions. Notable examples include the ruble-backed stablecoin A7A5, through which transactions totalling over 93.3 billion USD were conducted in less than one year (Chainalysis Team, 2026). The scale of such activity shows that cryptoassets are being used more and more not only in traditional schemes to conceal criminal proceeds, but also as an alternative infrastructure for cross-border payments. This could partially replace traditional financial channels for entities that are restricted from using them.

These developments are of particular economic and legal significance for Ukraine, given its exceptionally high level of cryptoasset adoption. According to Chainalysis's 2025 Global Crypto Adoption Index, Ukraine ranks eighth worldwide in terms of overall cryptocurrency adoption. In the population-adjusted ranking, however, Ukraine ranks first, ahead of Moldova and Georgia (Chainalysis Team, 2025). The intensive use of cryptoassets can be explained by a combination of economic and technological factors. These include macroeconomic uncertainty, high levels of technological literacy, widespread use of digital financial instruments, the need for cross-border transfers of value and alternative asset preservation mechanisms.

The adoption of cryptoassets does not necessarily indicate an increase in criminality within the relevant market. However, a substantial volume of legitimate digital transactions makes it more difficult to identify those that display indicators of money laundering, financing other unlawful activities or circumventing established financial restrictions. In the context of financial monitoring systems, this involves identifying a small number of high-risk transactions within a large volume of legitimate activity. This highlights the importance of risk-based analysis, blockchain analytics and the effective exchange of information between financial institutions, cryptoasset service providers and competent public authorities.

The increasing complexity of these risks is also reflected in the activities of Ukraine's State Financial Monitoring Service. In 2024, the Service received around 1.75 million reports on financial transactions, many of which required further analysis. As a consequence of its analytical operations, a total of 1,050 generalised and supplementary general materials pertaining to questionable financial transactions, amounting to a sum in excess of 62 billion UAH, were submitted to the relevant law-enforcement authorities. Concurrently, transactions exceeding 7.2 billion UAH were successfully blocked (State Financial Monitoring Service of Ukraine, 2025b). While these figures relate to financial monitoring as a whole and cannot be interpreted as direct statistics on cryptocurrency-related offences, they demonstrate the extent to which the national system is under strain in its efforts to detect and counter illicit financial flows.

The State Financial Monitoring Service of Ukraine's typological studies increasingly identify the cryptocurrency segment as a distinct area of financial risk. Typical patterns include converting funds of unidentified or suspicious origin through cryptoasset exchange services, followed by using bank accounts to launder the proceeds of cybercrime through cryptocurrency infrastructure. There are also fraudulent schemes involving soliciting funds from individuals under the guise of investing in cryptoassets or cryptocurrency trading (State Financial Monitoring Service of Ukraine, 2025a). Such schemes are characterised by their combination of traditional banking infrastructure and decentralised digital channels, creating a hybrid environment for illicit financial flows.

The global nature of this trend is also confirmed by the findings of the FATF. According to the organisation, stablecoins are being used more and more for money laundering, terrorist financing, evading sanctions, and financing the proliferation of weapons of mass destruction. They are attractive for illicit purposes because of the same economic characteristics that support their growth in legitimate markets: relative price stability, high liquidity, cross-border accessibility and the ability to transfer substantial amounts of value rapidly (Financial Action Task Force, 2026).

4.3. Economic Mechanisms of Money Laundering Involving Cryptoassets

The classical three-stage model of money laundering – comprising placement, layering, and integration – remains analytically relevant in the context of cryptoasset transactions. However, the technological characteristics of the digital financial environment significantly alter the economic nature and order of these stages. While they can generally be distinguished from one another with relative clarity in the traditional financial system, individual transactions in cryptocurrency-based schemes may simultaneously perform the functions of placement, concealment and subsequent introduction of assets into legitimate economic circulation (Barone & Masciandaro, 2019; Kamenskyi & Dudorov, 2024).

While they can generally be distinguished from one another with relative clarity in the traditional financial system, individual transactions in cryptocurrency-based schemes may simultaneously perform the functions of placement, concealment and subsequent introduction of assets into legitimate economic circulation (Barone & Masciandaro, 2019;

Kamenskyi & Dudorov, 2024). At the same time, declaring digital assets as proceeds from investment or trading activities, using them to acquire goods and services, or converting them into fiat currency may facilitate economic integration. Therefore, the distinctive feature of cryptoassets is not the disappearance of individual stages of money laundering, but rather their functional convergence and potential realisation within a single digital transaction cycle.

One common mechanism used to complicate financial monitoring is transaction structuring, also known as 'smurfing', which involves dividing substantial assets into smaller, more numerous transactions. This mechanism serves to reduce the informational visibility of individual transactions and make it more difficult to identify links between multiple transfers. In the digital environment, structuring can involve the fragmentation of transaction amounts and the use of multiple wallets, different service providers and blockchain networks, as well as successive exchange operations.

Ukrainian legislation addresses the increased risks associated with virtual asset transactions by setting out specific customer due diligence requirements and the information that must accompany relevant transfers. In particular, the legislation on the prevention and counteraction of money laundering sets out specific rules regarding virtual asset transfers up to the value of 30,000 UAH, whereas the general threshold for financial transactions designated by law as 'threshold transactions' is 400,000 UAH (The Law of Ukraine 'On Prevention and Counteraction to Legalisation (Laundering) of Criminal Proceeds, Terrorist Financing and Financing of Proliferation of Weapons of Mass Destruction' of June 26, 2026, No. 361-IX; Rudaia, 2026). These figures fulfil different regulatory functions and should not be considered as standard reporting thresholds for suspicious activity. The obligation to respond to a suspicious financial transaction is primarily determined by its risk indicators, rather than its absolute value alone.

Crypto mixing is a significant technological tool for concealing the origin of cryptocurrencies. Its purpose is to break or substantially complicate the establishment of the transactional link between the original source of the assets and their subsequent recipient. In centralised models, assets belonging to different users can be pooled and redistributed across numerous addresses. Decentralised protocols, on the other hand, use software-based mechanisms that make it difficult to reconstruct the sequence through which digital assets have been transferred.

The extent to which such instruments have been used demonstrates their considerable potential for concealing illicit financial flows. According to the U.S. Department of the Treasury, the Blender.io cryptocurrency mixer has facilitated the transfer of over 500 million USD in Bitcoin since its launch in 2017. This sum includes over 20.5 million USD associated with assets stolen in the attack on the Axie Infinity project (Udovenko & Karandas, 2026). With regard to the decentralised Tornado Cash protocol, U.S. authorities have estimated that over 7 billion USD in virtual assets have been used for money laundering since its launch in 2019 (Udovenko & Karandas, 2026). This also highlights the importance of distinguishing the overall transaction volume of privacy-enhancing services from the portion directly linked to criminal activity.

Another group of mechanisms consists of transactions aimed at minimising institutional oversight of participants in transactions. Examples include P2P transactions between cryptoasset holders, using certain over-the-counter intermediaries with ineffective KYC/AML procedures, and involving nominee holders of bank accounts and digital wallets. While P2P and OTC transactions are legitimate forms of digital asset circulation, when combined with anonymised or nominee accounts, they can create an infrastructure for the multi-stage transfer of illicit funds. Such arrangements fragment a single financial flow among formally unrelated participants and across different channels of circulation, thereby having an economic effect.

Crypto-to-fiat exit points play a particularly important role in money laundering mechanisms. Converting cryptoassets into fiat currency often results in the highest concentration of information that can be used to identify those involved in the transaction, including the bank accounts, payment instruments and intermediaries used, as well as the ultimate beneficiaries (Rudaia, 2026). From an economic perspective, such points act as a bridge between decentralised digital circulation and the regulated financial system. As such, they are a critical element of money laundering schemes and one of the most promising targets for financial monitoring and criminal investigation.

So-called conversion centres are a useful example of this interaction, as they integrate traditional and digital mechanisms for transferring value into a single illicit financial infrastructure. The Ukrainian Bureau of Economic Security uncovered an international scheme involving the conversion of funds into cash, the movement of cash between Ukrainian cities and EU countries, illegal currency exchange and cryptocurrency sales. During the course of an investigation, a sum of 152 million UAH in cash was seized (Bureau of Economic Security of Ukraine, 2023). This example shows that contemporary money laundering schemes are increasingly hybrid arrangements, rather than exclusively 'cryptocurrency-based' or 'cash-based'. In these schemes, cryptoassets serve as one of several channels for transferring and transforming economic value.

Thus, the economic mechanism of money laundering involving cryptoassets is characterised not by the emergence of a new laundering objective, but by a substantial expansion of the available technological means to achieve it. Methods such as transaction structuring, crypto mixing, repeated asset conversion, using P2P and OTC channels, nominee wallets and integrating cryptocurrency infrastructure with the fiat financial system can significantly increase the number of intermediary links between criminal proceeds and their final use. The growing complexity and fragmentation of transactions in the financial system is one of the main economic and legal challenges of the digital age. It complicates the detection of illicit financial flows and the identification of the link between the predicate offence, the specific asset and the conduct aimed at laundering it.

4.4. Objective and Subjective Elements of the Offence under Article 209 of the Criminal Code of Ukraine

The criminal law framework for combatting money laundering in Ukraine is primarily based on Article 209 of the Ukrainian Criminal Code. This covers the acquisition, possession, use and disposal of property where the circumstances suggest that it was obtained through a socially harmful illegal act. This includes carrying out a financial transaction or concluding a transaction involving such property, as well as transferring, transforming or taking other actions aimed at concealing or disguising its origin, ownership, location or other legally relevant characteristics (The Criminal Code of Ukraine). This legislative model encompasses various forms of the transformation and transfer of economic value, including those involving cryptoassets.

The main purpose of this criminal offence is to protect the social relations that ensure the lawful functioning of the financial and economic system, transparency regarding the origin of property and the prevention of criminal proceeds being introduced into legitimate economic circulation. In the context of the digital financial system, this legally protected interest takes on an additional dimension, as the illegal use of cryptocurrencies can facilitate the rapid transfer of value across borders, the fragmentation of financial flows, and their subsequent integration into traditional financial infrastructure.

The subject matter of the offence under Article 209 of the Criminal Code of Ukraine is property that has been obtained through an illegal act that endangers society prior to its laundering. The application of this concept to cryptoassets is consistent with contemporary private-law systems. According to Article 179-1 of the Ukrainian Civil Code, a digital asset is defined as a benefit created and existing exclusively in a digital environment that has property value. Virtual assets are expressly included among digital assets. At the same time, Article 190 of the Civil Code of Ukraine defines property as an individual thing, a collection of things, as well as property rights and obligations (The Civil Code of Ukraine; Prystash, 2023). Accordingly, given the current legal framework, there is sufficient basis to recognise cryptoassets as property for the purposes of applying Article 209 of the Criminal Code of Ukraine.

In this regard, it is not obvious that the wording of Article 209 needs to be amended to expressly refer to virtual assets. On the one hand, such a specification could enhance legal certainty and eliminate potential doubts in law enforcement practice. However, excessive detail concerning the subject matter of the offence could lead to the legislation becoming obsolete quickly in the context of the ongoing technological transformation of digital assets. Therefore, a more consistent approach is a functional one, in which decisive importance is attached not to the technological form of the asset, but to its property value and the established link between the asset and the preceding socially dangerous unlawful act.

The objective element of the offence under Article 209 can manifest in several different ways. In the context of cryptoassets, this may include acquiring or storing digital assets of criminal origin, transferring them between crypto wallets, converting one type of cryptoasset into another, exchanging them for fiat currency, using them for payments, transferring them to third parties, or using crypto-mixing mechanisms and other technologies intended to conceal the origin of a transaction. However, none of these operations constitutes money laundering in itself. It only acquires criminal-law significance where the criminal origin of the relevant property and the other statutory elements of the offence are established.

It is particularly important to establish the link between the asset involved in the relevant transaction and the preceding socially dangerous unlawful act. In the traditional financial system, this link can be demonstrated using banking records, accounting documents, contracts and records of funds moving through accounts, among other sources of information. By contrast, in a blockchain environment, a substantial proportion of transactions are publicly accessible and technically immutable. The main challenge lies in attributing the relevant addresses to specific individuals or legal entities (Meiklejohn et al., 2013). Therefore, the evidentiary challenge is not so much the absence of a transaction trail, but rather linking that digital trail to a specific person and proving that the asset originated from a predicate offence.

An offender under Article 209 of the Criminal Code of Ukraine is subject to general criminal liability. Whether or not the person directly participated in the predicate offence or became involved only at a later

stage in transactions concerning property of criminal origin, the criminal-law assessment does not depend on this. This is particularly important in the cryptocurrency ecosystem, where a variety of intermediaries may be involved in relevant transactions. These include wallet holders, exchange-service operators, OTC intermediaries, nominees of assets and other individuals.

The subjective element of money laundering is characterised by intent. The decisive issue is whether the person was aware of the factual circumstances that indicated the property they were dealing with had a criminal origin. In cases involving cryptoassets, establishing this element can present significant evidentiary challenges. The pseudonymous nature of blockchain addresses, automated interaction with smart contracts, use of decentralised protocols and multi-layered transaction chains do not always allow the scope of information available to a person regarding the source of their received assets to be determined directly.

At the same time, the technological complexity of a transaction should not automatically be taken as proof of the absence or presence of intent. The question of whether an individual has become aware of the criminal origin of cryptoassets is to be determined on the basis of the totality of the factual circumstances, including the nature and economic irrationality of the transactions, the systematic use of anonymising tools, interaction with addresses linked to unlawful activity, the use of numerous nominee wallets, artificial fragmentation of transactions, the absence of an apparent legitimate economic purpose, the person's conduct before and after receiving the assets, and other data capable of demonstrating actual awareness.

4.5. The Predicate Offence Problem and Other Challenges of Legal Qualification

One of the main challenges in applying Article 209 of the Criminal Code of Ukraine is establishing the link between the laundered property and the unlawful act that was socially dangerous and through which the property was obtained. This issue is particularly acute in criminal proceedings involving cryptoassets because their technological structure makes it possible to create complex, multi-layered transaction chains. This means that the original source of economic value can be significantly removed from the asset actually controlled by a person when it is identified.

Following the adoption of the Law of Ukraine No. 361-IX of December 6, 2019, Article 209 of the Criminal Code of Ukraine was revised, thereby changing the statutory manner in which the connection between laundered property and the preceding unlawful act is described (The Criminal Code of Ukraine; Sukhov, Chystiakova, & Merzliuk, 2025). The current wording of the provision stipulates that the factual circumstances must indicate that the relevant property was obtained through a socially dangerous unlawful act. Accordingly, although the scope and manner of its procedural establishment may be considered separately from the question of whether there is a distinct conviction for that predicate conduct, the predicate offence retains constitutive significance for the criminal-law assessment of money laundering.

In this context, it is important to distinguish between two issues. The first is the need to prove that the property has a criminal origin. The second is the need for a prior judicial finding that a particular person is liable for the predicate offence. The absence of a separate conviction for the underlying offence should not automatically disqualify someone from qualifying under Article 209 of the Criminal Code of Ukraine, provided that all the relevant and admissible evidence establishes the factual circumstances that demonstrate how the property was obtained as a result of a socially dangerous unlawful act. However, criminal liability for money laundering cannot be based solely on the assumption that the property has a 'suspicious' origin, unless there is a properly established evidentiary link between the property and the preceding unlawful activity.

Similar findings emerge from comparative European research, which demonstrates that the formal recognition of tax offences as predicate offences for money laundering does not necessarily ensure consistent implementation in practice. Substantial differences may arise between statutory regulation and law enforcement practices across jurisdictions (Rossel et al., 2022).

This approach reflects the temporal and causal nature of money laundering: the property in question must be the result of an earlier illegal act before any subsequent actions involving its acquisition, use, transformation, transfer, concealment or disguise can take place. Therefore, the predicate offence performs an evidentiary and structural function within the offence established by Article 209 of the Criminal Code of Ukraine.

In cases involving cryptoassets, establishing a causal and temporal link is considerably more complex. These assets can be transferred repeatedly between different blockchain addresses, converted into other tokens, moved across blockchain networks and routed through centralised and decentralised exchanges, mixers, cross-chain bridges and other technological services. Consequently, the evidentiary inquiry not only concerns the existence of a preceding offence, but also the reconstruction of the economic and technological chain through which value was transformed from its original criminal source into the particular cryptoasset being examined. Such analysis increasingly requires specialised blockchain

analytics tools and experts who can interpret digital transaction data.

Another issue is the distinction between money laundering and related criminal offences. Cryptoassets may be used to facilitate tax evasion, fraud, the unlawful appropriation of property, cybercrime, corruption offences and other criminal activities. However, the mere conversion or transfer of assets following a predicate offence does not automatically constitute money laundering. To qualify under Article 209 of the Criminal Code of Ukraine, proof of all the statutory elements of this separate criminal offence is required, rather than merely proof of the subsequent use of property of criminal origin.

Particular attention should be paid to the relationship between Articles 209 and 212 of the Criminal Code of Ukraine. Cryptoasset transactions may be used as one of the channels for withdrawing, transforming and subsequently returning funds to business or cash circulation in the operation of conversion centres. If the independent elements of tax evasion and subsequent money laundering are proven, it may be possible to impose cumulative criminal law sanctions (Bureau of Economic Security of Ukraine, 2023). However, such cumulative qualification should not be presumed simply because cryptocurrency was used. The objective and subjective elements of each offence must be established separately in each case, while ensuring that the same factual circumstances are not counted twice.

Significant difficulties also arise in relation to cryptoassets in the fields of criminal procedural evidence and the application of measures to secure criminal proceedings. Ukrainian criminal procedural legislation already expressly allows for the seizure of virtual assets. However, formally recognising them as assets capable of being seized does not eliminate the technological challenges associated with exercising effective control over them. Unlike traditional property, control over a cryptoasset is less dependent on physically seizing a particular object and more dependent on obtaining and securing access credentials to a digital wallet. These credentials can include private keys, seed phrases, hardware devices or other means of authentication (The Criminal Procedure Code of Ukraine).

This gives rise to specific procedural risks. Seizing a computer, mobile phone or hardware wallet does not guarantee effective control over the corresponding cryptoasset. Even after the physical device has been seized, the owner or another person who retains a copy of the private key or seed phrase may potentially transfer the asset to another address. Conversely, mishandling access credentials can result in the permanent loss of a crypto asset. In the digital environment, therefore, the traditional concept of 'seizure of property' becomes a matter of establishing exclusive cryptographic control over the asset.

Further issues arise concerning the custody and valuation of seized cryptoassets. The high price volatility of these assets can lead to substantial changes in their economic value during criminal proceedings. This raises questions about the most appropriate time, method and source for determining its value. This is particularly relevant for low-liquidity tokens, NFTs and other digital assets, as there may be no single transparent market quotation for them (Kuzmenko & Kravchuk, 2025). Another issue is whether to preserve the asset in its original form or allow it to be sold or converted to prevent substantial depreciation. This directly affects the balance between the interests of criminal proceedings and the property rights of the owner.

A separate set of challenges relates to evidence obtained from foreign cryptocurrency platforms and other service providers. Due to the cross-border nature of the cryptoasset market, data relating to user identification, transaction histories, IP addresses, payment instruments and asset movements may be held by entities registered in different jurisdictions. This raises issues relating to the speed of mutual legal assistance and the preservation of digital data. It also raises questions about the procedural form in which such information is obtained and its admissibility in domestic criminal proceedings.

The lack of a unified approach to the expert examination of blockchain transactions remains a significant concern. A proper evidentiary assessment requires more than just establishing that a cryptoasset has moved from one address to another. The economic substance of transactions must be interpreted, relationships between addresses identified, and the possible involvement of exchanges, mixers, smart contracts and other services determined. Technical transactions must also be distinguished from operations with legal significance. This creates a need for the further development of specialised methodologies for the computer-technical, economic and interdisciplinary forensic examination of digital assets (Kuzmenko & Kravchuk, 2025).

4.6. Law-Enforcement Practice: Examples of Investigations and Directions for Counteraction

An analysis of the law enforcement practices of Ukraine's Bureau of Economic Security indicates a gradual development of practical approaches to investigating criminal offences involving the use of cryptoassets in schemes for the transfer, conversion or laundering of funds. One example is the aforementioned criminal proceedings concerning the operation of a conversion centre, in which participants organised the movement of cash between Ukrainian cities and EU countries, as well as illegal currency exchange and the sale of cryptocurrency. A total of 152 million

UAH in cash was seized during the investigation, which was conducted on the basis of elements of the criminal offence provided for in Part 2 of Article 212 of the Criminal Code of Ukraine (Bureau of Economic Security of Ukraine, 2023).

From an economic perspective, this practice demonstrates how traditional conversion centres are evolving into hybrid financial structures that integrate cash transactions, currency exchange, bank transfers and cryptoassets into a single mechanism for transferring economic value. Consequently, investigating such offences requires a comprehensive reconstruction of financial flows combining traditional and digital channels, rather than an isolated analysis of cryptocurrency transactions.

At the same time, forensic economic and other expert examinations in cases of this category require a clear distinction to be made between the application of specialised knowledge and criminal law assessment. While an expert or other specialist can examine asset movements, establish the economic sequence of transactions and identify signs of artificial fragmentation, conversion or economic irrationality, conclusions about the presence of criminal offence elements and the final legal classification of relevant conduct are beyond the remit of expert examination (Rudaia, 2026).

This distinction highlights the interdisciplinary nature of tackling money laundering involving cryptoassets. The effectiveness of the criminal law response hinges on the coordinated interaction of financial intelligence units, blockchain analytics experts, investigators, prosecutors, forensic specialists and the judiciary. These groups each perform distinct functions, ranging from detecting anomalous financial flows and reconstructing digital transaction trails to securing evidence procedurally and subsequently assessing it in the context of criminal law.

4.7. International Standards for Countering Money Laundering in the Virtual Asset Sector and Foreign Experience

The Financial Action Task Force (FATF) primarily shapes the international regulatory framework for countering money laundering involving virtual assets. Following the extension of FATF requirements to virtual assets and virtual asset service providers (VASPs) in 2019, the Travel Rule became one of the key regulatory elements. Under this rule, transfers of virtual assets must be accompanied by a prescribed set of information concerning the originator and beneficiary (Financial Action Task Force, 2021). This approach aims to apply the fundamental principles of transparency applicable to traditional financial transfers to the digital environment, while also facilitating the identification of participants in high-risk transactions.

The FATF's red flag indicators for virtual asset transactions are also of considerable practical significance. Based on over one hundred real-life cases, the FATF has categorised risk indicators relating to the nature and structure of transactions, the use of anonymity-enhancing technologies, geographical factors, unusual transaction volumes or frequency, atypical participant profiles and the source of funds (Financial Action Task Force, 2020). Such indicators include the use of mixers and privacy-enhancing coins, repeated transfers of assets between VASPs without justification, transactions involving jurisdictions with weak AML/CFT supervision and transaction patterns that are inconsistent with the customer's economic profile.

These standards remain relevant as the cryptocurrency market continues to evolve. In its 2026 Seventh Targeted Update on the Implementation of the FATF Standards on Virtual Assets and VASPs, the Financial Action Task Force (FATF) reported further progress in the implementation of Recommendation 15 and the Travel Rule. However, it also emphasised continuing gaps in the practical application of regulatory, supervisory, and enforcement mechanisms. The FATF also highlighted the growing risks associated with stablecoins, P2P transactions involving unhosted wallets, VASPs operating offshore and outside effective supervision, and DeFi arrangements. By 2026, 83% of surveyed jurisdictions had adopted legislation to implement the Travel Rule, up from 73% in 2025. However, the effectiveness of practical supervision and enforcement remained uneven (Financial Action Task Force, 2026).

The European Union has developed a comprehensive regulatory model that combines rules governing the cryptoasset market with AML/CFT requirements. Most of the provisions of Regulation (EU) 2023/1114 on Markets in Crypto-Assets (MiCA) have been in force since 30 December 2024. This legislation introduced harmonised rules concerning the issuance of certain categories of cryptoassets, disclosure obligations, market organisation, and the authorisation of cryptoasset service providers (CASPs) (European Parliament & Council of the European Union, 2023). In general, providing cryptoasset services in the EU requires the appropriate authorisation. However, a transitional regime was available for entities that were already operating before MiCA became applicable.

The AML/CFT requirements relating to information accompanying cryptoasset transfers are set out directly in Regulation (EU) 2023/1113. These obligations impose a duty on CASPs to obtain, retain and transmit information about the originator and beneficiary of a cryptoasset transfer. The regulation also establishes specific rules for interactions with self-hosted addresses (European Parliament & Council of the European Union, 2023). The European model effectively combines

MiCA-based market regulation with a separate regime that governs the traceability and financial monitoring of cryptoasset transfers. This is consistent with the broader logic of FATF standards.

For Ukraine, adopting these approaches is significant in two ways. Not only is it necessary for developing an effective national system for countering the illicit use of cryptoassets, it is also necessary for gradually approximating Ukrainian financial legislation to the European Union's acquis. However, simply transplanting individual regulatory provisions is insufficient. The central task should be to establish a system that is capable of authorising, risk-based supervising, exchanging information and effectively monitoring cryptoasset service providers' compliance with AML/CFT requirements.

United States v. Costanzo, decided by the U.S. Court of Appeals for the Ninth Circuit in 2020, is a representative example of criminal-law practice in another jurisdiction. Thomas Costanzo engaged in P2P transactions involving the exchange of substantial amounts of cash for Bitcoin. During these controlled transactions, law enforcement officers repeatedly informed him that the funds were connected with illegal activities, including drug trafficking. Nevertheless, he continued to conduct the exchanges. Costanzo was convicted on five counts of money laundering under 18 U.S.C. § 1956 and sentenced to 41 months' imprisonment (United States v. Costanzo, 2020).

Upon review, the court confirmed that, in the specific circumstances of the case, the Bitcoin transactions had a sufficient nexus with interstate or foreign commerce for the purposes of federal law. While the case does not establish a new "cryptocurrency" money laundering offence, it does demonstrate the technological neutrality of the traditional criminal law prohibition. The digital form of economic value does not alter the nature of money laundering when the statutory elements of a transaction involving property connected with unlawful activity are met (United States v. Costanzo, 2020).

Thus, international experience demonstrates a gradual shift away from creating specific rules for cryptocurrencies, towards integrating cryptoassets into the broader financial regulatory and AML/CFT control architecture. The FATF provides functional standards for risk identification and transaction traceability. The European Union combines these principles with authorisation and supervision of the cryptoasset market. Meanwhile, criminal justice systems in individual jurisdictions adapt traditional money laundering offences to digital forms of economic value. For Ukraine, a technology-neutral criminal law model combined with the development of specialised financial and institutional regulation appears to be the most consistent approach to further reform.

4.8. Directions for Improving the Economic and Legal Mechanism for Countering Money Laundering Involving Cryptoassets

The analysis conducted has identified several interrelated areas for improving the national economic and legal mechanisms for countering the laundering of proceeds of crime through the use of cryptoassets.

Firstly, at the level of substantive criminal law, priority should be given to ensuring the consistent, technology-neutral application of Article 209 of the Criminal Code of Ukraine to digital forms of economic value, rather than to further casuistic expansion of its wording. Current civil legislation provides sufficient normative grounds for treating virtual assets as property, so an express reference to them in the criminal law provision is not necessary for effective legal classification. Instead, it is necessary to develop a stable law enforcement practice for establishing the link between a specific cryptoasset and the predicate criminal offence, as well as subsequent transactions aimed at laundering that asset.

Secondly, proving the criminal origin of property in proceedings under Article 209 of the Criminal Code of Ukraine requires further normative and doctrinal clarification. It is particularly important to distinguish between establishing the factual origin of an asset from a preceding socially dangerous unlawful act, and establishing that a separate conviction exists for that act. This issue is particularly important in the context of cryptoassets, given that multi-stage transactions, cross-chain transfers and anonymising technologies make it much more difficult to establish the causal and temporal link between the predicate offence and the property being laundered.

Thirdly, the procedures for detecting, seizing, establishing effective control over, storing, valuing and confiscating virtual assets require improvement at the criminal procedural level. While the current Criminal Procedure Code of Ukraine recognises the possibility of seizing such assets, their technological characteristics necessitate more detailed procedures for their actual control and preservation. This includes managing private keys and seed phrases, transferring assets to addresses controlled by public authorities, stopping them from being moved remotely, documenting relevant actions and creating mechanisms to manage the risk of significant changes in the market value of assets during criminal proceedings.

Fourthly, a priority task at the regulatory level is to finalise the development of a coherent legal framework for Ukraine's virtual asset market. This framework must consider not only the provisions of the Law of Ukraine 'On Virtual Assets', but also the evolving FATF standards, the European Union's regulatory framework under MiCA, and the particular AML/CFT requirements relevant to cryptoasset transfers. Its key elements should include transparent

authorisation procedures for professional market participants, a clear allocation of regulatory competences, risk-based supervision and effective interaction between cryptoasset service providers and the financial monitoring system.

Fifthly, it is important to strengthen the technological and analytical capacity of the State Financial Monitoring Service of Ukraine, law enforcement agencies and prosecuting authorities. Tools such as blockchain analytics and digital forensics can be used to reconstruct transaction chains, identify related addresses, detect transaction structuring and reveal the use of mixers, cross-chain bridges and other mechanisms for concealing the origin of assets. However, the effectiveness of such technologies depends not only on the availability of appropriate software, but also on the training of specialists, the development of methodological standards and the procedural use of analytical findings as evidence.

Sixthly, introducing a systematic, risk-based approach to analysing cryptoasset transactions appears to be a particularly promising idea. This approach should be based not only on formal threshold criteria, but also on behavioural and transactional indicators. Relevant indicators may include economically unjustified transaction fragmentation, interaction with high-risk addresses, frequent use of mixers, rapid movement of assets across multiple blockchain networks, the use of nominee wallets, and inconsistencies between transaction patterns and the customer's financial profile. This would enable the focus to shift from the formal control of individual transactions to the early identification of complex patterns of high-risk behaviour (Unger & van Waarden, 2009).

Finally, deeper international co-operation remains a strategic priority since the cross-border nature of cryptoassets limits the effectiveness of national control mechanisms alone. Particular importance should be attached to the rapid exchange of information between financial intelligence units within the Egmont Group, collaboration with foreign law enforcement and regulatory bodies, access to data held by overseas cryptoasset platforms and the development of cross-border seizure and confiscation mechanisms for digital assets.

Therefore, improving the economic and legal mechanisms for combatting money laundering involving cryptoassets should not be limited to extending criminal law prohibitions. A more promising approach would be to combine technology-neutral criminal law with specialised procedural mechanisms for handling digital assets, modern risk-based financial monitoring, the enhanced technological capacity of public authorities and international co-operation. This integrated architecture can effectively counter illicit financial flows while avoiding the unjustified restriction of legitimate digital financial systems.

5. Conclusions

The economic and legal analysis conducted in this study demonstrates that, as cryptoassets assume an increasingly significant role within the modern digital financial system, they simultaneously generate a new set of risks in the field of countering the laundering of proceeds of crime. While their technological and economic characteristics – decentralised circulation, pseudonymous blockchain addresses, high-speed cross-border value transfers, repeated automated conversion and multiple digital infrastructures – do not alter the economic essence of money laundering, they do substantially transform the architecture of the financial trail. As a result, the traditional mechanisms for structuring transactions, concealing the origin of assets, using intermediaries and subsequently integrating illicit value into legitimate circulation are implemented through significantly more complex digital processes. This is evidenced by the global dynamics of illicit cryptocurrency transactions, which amounted to at least 154 billion USD in 2025, as well as by the practices of Ukrainian financial intelligence and law enforcement authorities.

A criminal law analysis shows that the current wording of Article 209 of the Criminal Code of Ukraine is generally sufficiently technology-neutral to cover transactions involving cryptoassets. As contemporary civil legislation expressly recognises virtual assets as a type of digital asset with property value, their criminal law treatment as property does not require the creation of a separate 'cryptocurrency' offence. The main challenges in enforcement relate less to the normative definition of money laundering than to establishing the origin of a specific digital asset from a socially dangerous unlawful act, identifying its owner or controller, reconstructing a multi-stage transaction chain and proving that the person was aware of the criminal origin of the property in question.

The study also shows that digitalisation is changing the way traditional criminal procedures deal with property. While virtual assets may already be subject to seizure in criminal proceedings, the effective implementation of this measure requires the legal restriction of disposal rights and the establishment of exclusive cryptographic control over the asset. This highlights the need for further normative and methodological regulation of procedures for detecting, documenting, transferring into state control, storing, valuing, managing and confiscating cryptoassets. It also emphasises the importance of developing unified approaches to the use of blockchain analytics, as well as computer and economic forensic examinations, in criminal proceedings.

A comparative legal analysis of the FATF standards, European Union regulations and foreign judicial practices confirms a general trend towards

integrating cryptoassets into the existing AML/CFT framework, rather than creating a separate criminal law counteraction model. The FATF develops functional standards for risk-based supervision and transaction traceability. The European Union combines MiCA-based market regulation with specific requirements for information accompanying cryptoasset transfers. Meanwhile, United States v. Costanzo shows that traditional money laundering provisions can be applied to Bitcoin transactions effectively, even when the relevant economic value exists in digital form.

For Ukraine, the absence of a comprehensive regulatory framework for the virtual asset market continues to represent a significant challenge. The national legal system has effectively developed an asynchronous regulatory model in which mechanisms for monitoring cryptoasset-related financial risks are already in operation, while comprehensive rules governing market access, authorisation, taxation, and public supervision are still in the process of development. Further reform should therefore not only focus on bringing previously adopted provisions into force, but also on establishing a coherent regulatory model that is aligned with current FATF standards, European Union law and the contemporary technological structure of the cryptoasset market.

The practical improvement of the economic and legal mechanism for countering money laundering involving cryptoassets should be pursued comprehensively: through the development of consistent practice in the technology-neutral application of Article 209 of the Criminal Code of Ukraine; clarification of approaches to proving the predicate origin of digital assets; development of specialised procedural mechanisms for their seizure, custody, and confiscation; implementation of risk-based analysis of cryptoasset transactions; expansion of blockchain analytics and digital forensics capabilities; and deeper international exchange of financial intelligence and law-enforcement information. It is precisely the combination of criminal law, economic, technological, and institutional instruments that can ensure an effective response to illicit financial flows without unjustifiably restricting the development of the legitimate digital economy.

In the context of the ongoing armed aggression in Ukraine, the importance of these tasks is paramount. Cryptoassets have the potential to be utilised not only for conventional money laundering but also for terrorist financing, collaboration-related activities, sanctions evasion, and the maintenance of cross-border financial infrastructure involving entities connected with the aggressor state. In such circumstances, the efficacy of countering the illicit use of digital assets is not only a component of economic and financial stability, but also of Ukraine's broader national security framework.

References:

Albrecht, C., Duffin, K. M., Hawkins, S., & Morales Rocha, V. M. (2019). The use of cryptocurrencies in the money laundering process. *Journal of Money Laundering Control,* 22(2), 210–216. https://doi.org/10.1108/JMLC-12-2017-0074

Barone, R., & Masciandaro, D. (2019). Cryptocurrency or usury? Crime and alternative money laundering techniques. *European Journal of Law and Economics*, 47(2), 233–254. https://doi.org/10.1007/s10657-019-09609-6.

Bureau of Economic Security of Ukraine. (2023, January 3). BES exposed a cryptocurrency conversion centre and seized UAH 152 million. https://esbu.gov.ua/news/beb-vykrylo-konverttsentr-kryptovaliut-vylucheno-152-mln-hrn

Chainalysis Team. (2025). The Chainalysis 2025 global crypto adoption index. Chainalysis. https://www.chainalysis.com/blog/2025-global-crypto-adoption-index/

Chainalysis Team. (2026, January 8). Crypto crime reaches record high in 2025 as nation-state sanctions evasion moves on-chain at scale. Chainalysis. https://www.chainalysis.com/blog/2026-crypto-crime-report-introduction/

European Parliament & Council of the European Union. (2023). Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets. *Official Journal of the European Union*, L 150, 40–205. https://eur-lex.europa.eu/eli/reg/2023/1114/oj/eng

Ferwerda, J. (2009). The economics of crime and money laundering: Does anti-money laundering policy reduce crime? *Review of Law & Economics*, 5(2), 903–929. https://doi.org/10.2202/1555-5879.1421

Financial Action Task Force. (2020). Virtual assets: Red flag indicators of money laundering and terrorist financing. FATF. https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Virtual-Assets-Red-Flag-Indicators.pdf

Financial Action Task Force. (2021). Updated guidance for a risk-based approach to virtual assets and virtual asset service providers. FATF. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html

Financial Action Task Force. (2026). Seventh targeted update on implementation of the FATF standards on virtual assets/VASPs. FATF. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-updated-virtualassets-vasps-2026.html

Foley, S., Karlsen, J. R., & Putniņš, T. J. (2019). Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies? *The Review of Financial Studies*, 32(5), 1798–1853. https://doi.org/10.1093/rfs/hhz015

Kamenskyi, D. V., & Dudorov, O. O. (2024). Laundering of criminal proceeds through transactions with virtual currencies: A new threat to economic security. *Analytical and Comparative Jurisprudence*, 1, 500–509. https://doi.org/10.24144/2788-6018.2024.01.88

Kuzmenko, O. V., & Kravchuk, P. Yu. (2025). Virtual assets as the subject of a criminal offence: Problems of definition and proof. *Analytical and Comparative Jurisprudence*, 6(3), 194–198. https://doi.org/10.24144/2788-6018.2025.06.3.29

Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. M., & Savage, S. (2013). A fistful of bitcoins: Characterizing payments among men with no names. In Proceedings of the 2013 Conference on Internet Measurement Conference (pp. 127–140). ACM. https://doi.org/10.1145/2504730.2504747

Möser, M., Böhme, R., & Breuker, D. (2013). An inquiry into money laundering tools in the Bitcoin ecosystem. In 2013 eCrime Researchers Summit (eCRS) (pp. 1–14). IEEE. https://doi.org/10.1109/eCRS.2013.6805780

Prystash, S. S. (2023). Virtual assets as a subject of legalisation (laundering) of criminally obtained proceeds. *Journal of Kyiv University of Intellectual Property and Law*, 3, 9–13. https://doi.org/10.32782/chasopyskiivp/2023-3-2

Rossel, L., Unger, B., & Ferwerda, J. (2022). Shedding light inside the black box of implementation: Tax crimes as a predicate crime for money laundering. *Regulation & Governance*, 16(3), 781–800. https://doi.org/10.1111/rego.12407

Rudaia, M. I. (2026, April 25). Money laundering through cryptocurrency: Article 209 of the Criminal Code of Ukraine. Rudaia.com.ua. https://rudaia.com.ua/blog/vidmyvannia-koshtiv-cherez-kryptovaliutu/

State Financial Monitoring Service of Ukraine. (2025). Risks and threats of money laundering and terrorist financing in the context of the Russian Federation's military aggression – 2025. https://fiu.gov.ua/assets/userfiles/411/Типолог%20ДСФМУ/Typology%202025_UA.pdf

State Financial Monitoring Service of Ukraine. (2025). Report of the State Financial Monitoring Service of Ukraine for 2024. https://fiu.gov.ua/assets/userfiles/0350/2025/REPORT2024.pdf

Sukhov, Yu., Chystiakova, A., & Merzliuk, A. (2025, September 24). The problem of the predicate offence in the qualification of an act under Article 209 of the Criminal Code of Ukraine. *Judicial and Legal Newspaper*. https://sud.ua/uk/news/blog/341882-problema-predikata-pri-kvalifikatsii-deyaniya-po-state-209-uk-ukrainy

Udovenko, Zh. V., & Karandas, M. V. (2026). Counteraction to the laundering of criminally obtained property committed using cryptocurrency mixing technologies. *Ukrainian Political and Legal Discourses*, 23. https://doi.org/10.5281/zenodo.20755249

Unger, B., & van Waarden, F. (2009). How to dodge drowning in data? Rule- and risk-based anti-money laundering policies compared. *Review of Law & Economics*, 5(2), 953–985. https://doi.org/10.2202/1555-5879.1423

United States v. Costanzo, 956 F.3d 1088 (9th Cir. 2020). https://law.justia.com/cases/federal/appellate-courts/ca9/18-10291/18-10291-2020-04-17.html

The Criminal Code of Ukraine. *The Official Bulletin of the Verkhovna Rada (BVR)*, 2001, No. 25–26, Article 131. https://zakon.rada.gov.ua/laws/show/2341-14

The Civil Code of Ukraine. *The Official Bulletin of the Verkhovna Rada (BVR)*, 2003, No. 40–44, Article 356. https://zakon.rada.gov.ua/laws/show/435-15#Text

The Criminal Procedure Code of Ukraine. *The Official Bulletin of the Verkhovna Rada of Ukraine (BVR)*, 2013, No. 9–10, No. 11–12, No. 13, Article 88. https://zakon.rada.gov.ua/laws/show/4651-17

The Law of Ukraine 'On Virtual Assets' of 15.11.2024, No. 2074-IX. The *Official Bulletin of the Verkhovna Rada of Ukraine (BVR)*, 2023, No. 15, Art. 51. https://zakon.rada.gov.ua/laws/show/2074-20

The Law of Ukraine 'On Prevention and Counteraction to Legalisation (Laundering) of Criminal Proceeds, Terrorist Financing and Financing of Proliferation of Weapons of Mass Destruction' of June 26, 2026, No. 361-IX. *The Official Bulletin of the Verkhovna Rada of Ukraine (BVR)*, 2020, No. 25, Article 171. https://zakon.rada.gov.ua/laws/show/361-20#Text