Ashdin Publishing
Journal of Drug and Alcohol Research
Vol. 15 (2026), Article ID 236529, 09 pages
DOI: 10.4303/JDAR/236529

Research Article

Countering the Laundering of Drug Proceeds through Cryptocurrencies in Ukraine: Theoretical Foundations, Administrative Mechanisms and Criminal-Law Means

Maksym Maksimentsev[1*], Yuliia Khrystova[2], Halyna Tatarenko[3], Denys Yuriev[4], Yevhen Yakovykh[5]

[1]*Research Department of Criminal law and Process, State Tax University, Irpin, Ukraine*
[2]*Department of Criminal Law and Criminology, Dnipro State University of Internal Affairs, Dnipro, Ukraine*
[3]*Department of Public and Private Law, Volodymyr Dahl East Ukrainian National University, Kyiv, Ukraine*
[4]*Department of Criminal Procedure, Dnipro State University of Internal Affairs, Dnipro, Ukraine*
[5]*Department Criminal Procedure and Criminalistics, Odesa State University of Internal Affairs, Odesa, Ukraine*

**Address Correspondence to: Maksym Maksimentsev, Email: m.h.maksimentsev@dpu.edu.ua*

Received: 24 Aug 2026; Manuscript No: JDAR-26-195159; **Editor assigned**: 26 Aug 2026; PreQC No: JDAR-26-195159 (PQ); **Reviewed:** 09 Sep 2026; QC No: JDAR-26-195159; **Revised:** 16 Sep 2026; Manuscript No: JDAR-26-195159 (R); **Published:** 23 Sep 2026; DOI: 10.4303/JDAR/236529

Copyright © 2026 Maksym Maksimentsev, et al. This is an open access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Abstract

Aim: Over the past few years, retail drug selling in Ukraine has migrated to Telegram storefronts and darknet platforms where buyers settle in crypto, above all in dollar-pegged stablecoins. Sellers then turn these tokens back into hryvnias through Peer-to-Peer (P2P) deals, cash desks that trade over the counter and rented ("drop") bank accounts. Ukrainian legislation addresses only separate links of this chain: Since 2020 the anti-money laundering statute has counted crypto-service providers as obliged entities, the 2022 law on virtual assets is still not in force, and Article 306 of the criminal code continues to speak of banks, enterprises and privatised property. The paper examines how theoretical concepts, administrative tools and criminal-law means can be combined so that drug money moving through virtual assets is detected, stopped and recovered.

Methods: Doctrinal, comparative and typological methods were applied. The legal material comprised the substantive and procedural criminal codes, the administrative offences code, the Anti-Money Laundering (AML) statute of 2019, the dormant 2022 statute on virtual assets, civil code provisions on digital things, the statute on the asset recovery agency and bills Nos. 10225-д and 16013. International material included Financial Action Task Force (FATF) standards, Markets in Crypto-Assets Regulation (MiCA) and the other European Union (EU) acts on crypto-asset transfers, money laundering and confiscation, together with four confiscation judgments of the Strasbourg court. Empirical data came from typology studies, official statistics, blockchain-analytics reports and enforcement cases of 2024-2026.

Results: Drug money typically enters crypto at the moment of payment, is layered through P2P trades, token swaps and self-custody wallets, and is integrated via rented accounts, cash and offshore platforms. The points at which value changes form and an identifiable person must appear-conversion nodes-are where the law can intervene. Administrative rules nominally cover these nodes (customer due diligence from Ukrainian Hryvnia (UH) 30,000, wallet data accompanying transfers, suspension powers), yet without a licensing regime for domestic providers they bite mainly on banks. Criminal law is inconsistent: The general laundering offence (Article 209 CC) applies to virtual assets as property, but Article 306, the specific offence on drug proceeds, does not capture conversion into crypto, and the October 2026 offence on supplying accounts to fraudsters is limited to fraud and silent on crypto wallets. Seizing virtual assets has become common, whereas their custody, sale and restitution still hinge on foreign exchanges and on divergent judicial approaches.

Conclusion: Virtual assets need to be recognised as a separate object of both Anti-Money Laundering (AML) regulation and criminal-law protection. The paper offers a model with three tiers-control at the gateway, interruption of flows, and response with asset recovery-and proposes changes to Article 306, to the new account-supply offence, to the suspension and covert-investigation rules and to the procedure for seizing, holding and realising virtual assets, including a rebuttable presumption, compatible with the convention, concerning crypto-assets of persons convicted of drug trafficking.

Keywords: Money laundering, Drug proceeds, Virtual assets, Cryptocurrencies, Stablecoins, Financial monitoring, Administrative liability, Criminal liability, Confiscation, Ukraine

Introduction

Drug markets were among the first to treat cryptocurrency as a means of payment rather than an investment. Foley, et al. estimated that about a quarter of bitcoin users and some 46% of bitcoin transactions were associated with illegal activity, a phenomenon they described as "black e-commerce" [1]. The market has since changed its form but not its direction. Crypto flows to darknet markets and drug vendors slightly exceeded United States Dollar (USD) 2.5 billion in 2025 despite the closure of large platforms [2]; stablecoins accounted for 84% of illicit cryptocurrency volume in the same year [3]; and the Financial Action Task Force (FATF) has reported two years running that drug traffickers are among the illicit actors relying increasingly

on stablecoins, which are now involved in most identified on-chain illicit activity [4,5].

Ukraine is more exposed to this shift than most European states. Transactions linked to the country reached about USD 206.3 billion over the year to mid-2025, and the head of the securities regulator, citing blockchain-analytics data, noted that Ukraine ranks first in the world for crypto adoption once the figures are adjusted for population [6]. Drug crime is not declining either: 47,617 Drug offences were registered in 2024 [7] and 48,629 in 2025 [8]. Retail sales have moved to messengers and stash drops paid in cryptocurrency. In December 2025, for example, the police dismantled a production site in a Kyiv garage whose output, worth over UAH 95 million at black-market prices, was sold through Telegram channels with payment accepted exclusively in cryptocurrency [9]. In February 2025, the state tax service reported its contribution to uncovering a scheme built around amphetamine precursors: Revenue was gathered on the accounts of over one thousand nominee holders ("drops"), more than UAH 200 million was then shifted within a year to a pair of crypto deposit wallets, and the money was finally withdrawn in Cyprus; some participants face charges under Part 3 of Article 209 of the criminal code [10]. According to the 2025 typology study of the State Financial Monitoring Service, which serves as Ukraine's Financial Intelligence Unit (FIU), drugs on darknet platforms are paid for mainly in cryptocurrency, and splitting P2P transfers into numerous small payments is a widespread laundering technique [11].

Ukraine's legal answer to this problem is scattered. It was the 2019 statute on preventing money laundering (hereinafter, the Anti-Money Laundering (AML) law) that first introduced the notion of a virtual asset and placed crypto-service providers under reporting duties [12]. A separate law on virtual assets followed on 17 February 2022 to build a licensed market; however, the legislator made its commencement conditional on tax changes that are still pending, and the Law remains a dead letter [13]. The tax-and-supervision bill No. 10225-д was approved at first reading on 3 September 2025 [14]. In November 2026 the Rada's tax committee recommended it for second reading, scheduling commencement for 1 July 2027 [15], but the bill did not appear on the plenary agenda of 9-13 November 2026 [16]. Meanwhile, the civil code has recognised "digital things" since 2023 [17], and the Criminal Code contains a general laundering offence (Article 209) and a special one for drug money (Article 306) [18].

International scholarship has shown how cryptocurrencies fit the classical stages of laundering. Albrecht, et al. explain that by removing financial intermediaries they let value move peer to peer, outside the institutions on which AML law relies [19]. Dupuis and Gleason, applying Kane's regulatory dialectic, identify "open doors"-tumblers, over-the-counter trading, privacy coins and decentralised exchanges-through which illicit funds still pass as regulators close others [20]. Wronka finds that the (European Unions) EU's fifth AML Directive left non-custodial wallet providers and mixing services outside its scope [21], while Benson, et al., surveying experts from five European countries, report that no unified national framework for crypto-asset transactions exists and that current crypto regulation is dictated by AML recommendations [22]. Studies of drug supply complete the picture: Moyle, et al. describe how social media and encrypted messaging apps connect buyers with commercial suppliers [23], and Barratt, et al. analyse Televend, which combined a darknet back end with a Telegram storefront [24].

Ukrainian research has approached the problem from separate angles. Voronkin analyses the arrest of cryptocurrency in criminal proceedings and criticises the practice of seizing it merely to preserve physical evidence [25]; Kuzmenko, et al. point out that criminal legislation hardly mentions virtual assets expressly [26]; Shevchenko examines the qualification of drug sales through electronic resources [27]; and Yepryntsev, et al. analyse cyber-enabled drug crime at regional and local levels from both administrative and criminal-law perspectives [28]. The broader drug-enforcement context has been examined in studies on police tactics [29], on how investigations of drug offences are organised [30], on cross-border cooperation in covert operations [31], on the boundary between administrative and criminal liability for drug offences [32], on preventing such offences among minors [33] and on regulatory models abroad [34].

Methodologically, the paper draws on three further lines of work. Halunko, et al. examine the administrative, financial and criminal-law aspects of regulating social relations in government bodies within one theoretical and

methodological framework [35]; Maksimentseva, et al. link the exercise of judicial power in administrative proceedings to compliance with the principles of administrative procedure law [36]; and Khrystova, et al. compare how European states implement international standards on the criminological and criminal-law protection of justice [37]. Work on international legal standards for documenting and investigating war crimes [38] and on restorative justice in plural normative settings [39] adds two perspectives rarely found in AML scholarship: The evidentiary quality of digital traces and the question of whom recovered assets should serve. No study has yet examined financial-monitoring rules, the emerging market regulation and criminal law as one interacting set of tools applied to drug proceeds held in virtual assets; the present paper addresses this gap.

Purpose and objectives: The aim is to show how theory, administrative regulation and criminal law can work together against the laundering of drug money through cryptocurrencies in Ukraine. To this end, the paper (1) defines what kind of legal object a virtual asset is in laundering cases and models the mechanism of crypto-laundering; (2) describes the typical schemes through which Ukrainian drug proceeds pass via crypto; (3) assesses the administrative toolkit-financial monitoring, supervision, bank-side restrictions and administrative liability; (4) tests the criminal-law and procedural toolkit-Articles 209 and 306 of the criminal code, the new offence on supplying accounts, seizure, special confiscation and asset management-against the Strasbourg standards; and (5) formulates a model and draft amendments.

Methods

Four methods were used: Doctrinal, comparative, typological and formal-logical. Doctrinal analysis covered the criminal code [18], the criminal procedure code [40], the code on administrative offences [41], the AML law [12], the law on virtual assets [13], the civil-law rules on digital things [17], the framework drug statute [42], the statute on operational and search activity [43] and the asset-management statute in its original and reformed versions [44,45]. The legislative process was traced through Bill No. 10225-д [14-16] and Bill No. 16013 on drop accounts [46,47].

For comparison, the study drew on international treaties-the 1988 United Nation (UN) convention against drug trafficking [48] and the council of Europe's Warsaw convention [49]-and on soft-law standards: The FATF Recommendations [50], the two most recent FATF targeted updates on virtual assets and its 2026 report on stablecoins [4,5,51], as well as a Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL) typology study [52]. EU law was represented by Markets in Crypto-Assets Regulation (MiCA), the regulation on information accompanying transfers, the AML Regulation and the 2024 confiscation directive, which Ukraine must transpose as a candidate country [53-56]. From the case law of the European Court of Human Rights (ECtHR), four confiscation judgments were chosen in which either drug money or a presumption of criminal origin was at stake: Welch [57], Phillips [58], Grayson and Barnham [59] and Gogitidze [60].

The empirical part relied on the FIU's typology study and annual report [11,61], the national drug reports [7,8], the EU drug markets analysis [62], blockchain-analytics reports [2,3,63], official statements on drop accounts and payment limits [64-66], enforcement cases [9,10] and court practice on the arrest of virtual assets as summarised by practitioners and the Bar [67-69]. Scholarly literature was searched mainly in Scopus and Web of Science, the two databases on which bibliometric studies of Ukrainian research output also rely [70], and was supplemented by Ukrainian law journals. Laundering schemes were broken down into the classical stages of placement, layering and integration. All quotations from Ukrainian legal acts and reports are given in our own translation, and Tables 1-3 present the results of the analysis and modelling.

Results and Discussion

What is laundered: The legal character of virtual assets

Three definitions of the same object coexist in Ukrainian legislation. Borrowing the FATF formula, the AML law describes a virtual asset as "a digital expression of value that can be traded in digital form or transferred and that can be used for payment or investment purposes" [12,50]. The law on virtual assets, by contrast, conceives of it as a valuable intangible good capable of being an object of civil rights, yet this definition has never become operative [13]. Since 2023, the civil code has recognised digital things-goods that are created and exist only in the digital environment and have property value-and virtual assets fall within this category [17]. For criminal law the sequence matters, because Article 209 speaks of "property" [18]. The civil-

law category settles the question whether cryptocurrency can be laundered or confiscated as property, and the High anti-corruption court, in a verdict of 14 November 2024 (case No. 991/3227/24), likewise treated cryptocurrency as a virtual asset [67].

The gap lies elsewhere. Beyond these general notions, criminal legislation hardly mentions virtual assets expressly [26], and Article 306 still lists the forms of using drug money that were typical of the economy of 2001 [18]. As Section 4 shows, the special norm on drug proceeds therefore does not fit the main conversion technique used by today's drug markets.

Two features of virtual assets shape any theory of countermeasures. First, blockchain ledgers are public while their users are pseudonymous: Every transfer can be traced, but a wallet becomes evidence against a person only when it is linked to an identity. Second, value can change form-from hryvnias to stablecoins, from one network to another, from tokens back to cash-faster than any court can act. The place where laundering can be stopped is therefore not the asset as such but the conversion node: The point at which value enters or leaves the crypto ecosystem or changes custodian, and at which some actor has to know the customer. Dupuis and Gleason's regulatory dialectic explains why these nodes keep moving: Each new control redirects launderers to the next open door [20]. A law that lists specific nodes will lag behind; a law that obliges every professional node to know its customer, to report and to freeze on request will keep pace.

This perspective also clarifies how administrative and criminal law relate to each other. Administrative law shapes the conduct of gatekeepers before any crime is proven: It imposes due diligence, reporting and suspension duties and punishes their breach. Criminal law acts afterwards: It qualifies the laundering, establishes the predicate drug offence and recovers the proceeds. The two branches meet at the referral of financial intelligence to law enforcement and at the arrest of assets, which is why they should be designed as one system rather than as separate branches [28,35]. At both meeting points the quality of documentation decides the outcome. Blockchain evidence-transaction hashes, wallet clustering, captures of a Telegram storefront, exchange records-has to be collected with the discipline that international standards demand for documenting war crimes: A traceable chain of custody, verifiable methods and preservation of the original data [38]. Practitioners stress that the window for freezing crypto is often a matter of hours, while identifying the perpetrator can take months or years, so recovery and prosecution have to be treated as separate tasks [69].

International law defines the floor below which national regulation must not fall. Under Article 3 of the 1988 convention, each party must make a criminal offence of "the conversion or transfer of property" derived from drug trafficking where it is committed "for the purpose of concealing or disguising the illicit origin of the property", and Article 5 obliges it to enable confiscation of the proceeds [48]. The Warsaw convention broadens these obligations and, among other things, empowers financial intelligence units to postpone a suspicious transaction [49]. Within the FATF system, Recommendation 15 extends AML duties to virtual assets and their providers, while Recommendation 16, the so-called travel rule, demands that information about the sender and the recipient accompany each transfer [50].

Typology: The route of drug money through crypto in Ukraine

The EU drug markets analysis stresses that drug markets intersect with money laundering and depend on brokers and facilitators, money launderers among them [62]. The Ukrainian cases and typologies analysed here show a recurring pattern (Table 1). At the placement stage, the buyer pays a Telegram shop or a darknet market in USDT, usually on the TRON network, or in bitcoin, either from an exchange account or after buying crypto from a P2P trader with a bank card. Shops that also accept card payments route them to borrowed accounts whose funds are then converted into stablecoins. The same FIU study notes that sellers on darknet drug platforms receive payment chiefly in anonymous cryptocurrencies and that launderers favour P2P transfers divided into a multitude of minor amounts [11]. According to TRM labs, Russian-language darknet markets accounted for over 97% of global drug trafficking volume via crypto in 2024 [63], and Chainalysis places several such platforms in the billion-dollar range, particularly in synthetic drugs [2]. Much of this infrastructure lies outside Ukrainian jurisdiction, so tracing it turns into a matter of international cooperation [31].

Table 1: Stages of laundering drug proceeds through virtual assets and the corresponding legal levers.

Stage	Typical technique in drug cases	Conversion node where identity surfaces	Administrative lever	Criminal-law lever
Placement	Buyer pays a Telegram shop or darknet market in United States Dollar Tether (USDT) (TRON network) or Bitcoin (BTC); card payments go to borrowed accounts and are converted into stablecoins by P2P traders	Buyer's exchange account; bank card of the buyer or of the drop; P2P trader	Customer due diligence by exchanges and banks; limits on P2P card transfers; drop indicators	Article 307 CC (sale); Article 209 CC for account holders aware of the origin; new offence of Bill No. 16013
Layering	Chain-hopping, token swaps, mixers and bridges; couriers, laboratories and precursor suppliers paid in stablecoins	Swap or exchange service applying Know Your Customer (KYC); stablecoin issuer able to freeze an address	Information accompanying transfers; suspension of transactions; freeze requests to issuers	Article 306 CC where funds continue trafficking; Article 209 CC; arrest of virtual assets (Article 170(10) CPC)
Integration	Sale of crypto to P2P buyers for hryvnias; Over-The-Counter (OTC) cash desks; cash-out abroad; purchase of real estate and vehicles	Bank account receiving hryvnias; OTC desk; foreign exchange	Bank reporting; supervision of providers (once licensed); exchange of financial intelligence abroad	Article 209(2)-(3) CC; special confiscation (Articles 96-1, 96-2 CC); transfer to the asset-management agency

Source: Authors' elaboration based on [9-12,18,40,51].

At the layering stage, revenue moves through chains of wallets, is swapped between tokens and networks, sometimes passes through mixers or cross-chain bridges, and is partly spent inside the business: Couriers who leave stash drops, chemists and suppliers of precursors are paid in stablecoins. The FIU lists among its risk indicators crypto mixers and cross-chain bridges, crypto "mules", platforms without customer identification and unlicensed exchangers, including those operating in the occupied territories [11]. The FATF regards P2P transfers of stablecoins through unhosted wallets as a key vulnerability, because no obliged intermediary takes part in them [51].

At the integration stage, crypto is sold for hryvnias to P2P buyers paying from personal bank cards, exchanged for cash at over-the-counter desks or cashed out abroad, while borrowed accounts carry the hryvnia leg. Drops are recruited through social-media offers of "quick earnings" [11], which target people whose economic position has been weakened by the war-a setting in which the legislator has had to revisit even the basic guarantees of workers' rights [71]. The scale of this infrastructure is considerable: In the first five months of 2025 alone, the FIU analysed over 29,000 accounts involving more than 80,000 persons and over UAH 30 billion in transactions used for laundering [64]. The amphetamine case mentioned above shows the whole cycle: More than a thousand drops collected the proceeds, which were then funnelled into two crypto deposit wallets and later withdrawn in Cyprus [10] (Table 1).

Table 1 shows that each stage has at least one node where a regulated actor can identify a person: The exchange that sells USDT to the buyer, the issuer that can freeze the token, the bank that receives the hryvnias. Laundering succeeds where these nodes are missing-P2P trades between unhosted wallets, unlicensed exchangers, foreign platforms that ignore Ukrainian requests-or where they are present but not legally obliged to act. Cross-border legs of a scheme-deposits on foreign exchanges, cash-out abroad-also call for risk assessment that is modelled rather than merely listed, along the lines of the approaches developed for international trade contracts [72].

Administrative mechanisms: A framework without a perimeter

Financial monitoring: Formally, every conversion node is already covered by the AML law. Its Article 1(1)(51) names four activities that make a person a crypto-service provider-exchanging virtual assets, transferring them, keeping or administering them, and taking part in their issuance-and Article 6(2)(8) adds such providers to the list of obliged entities. Any operation with virtual assets worth UAH 30,000 or more triggers customer due diligence (Article 11(3)). The travel rule is transposed by Article 14: A payment, crypto transfers included, must carry data on both parties–as a minimum, the numbers of their accounts or wallets-and a transfer without these data may not be executed. Article 23 regulates suspension: The obliged entity halts an operation bearing signs of a criminal offence for two working days, the FIU can prolong the halt by up to seven working days, and once materials go to law enforcement the overall period may reach thirty working days. The Ministry of Digital Transformation (MDT) is

designated as the supervisor of providers (Article 18(1)) [12].

In practice, this framework lacks a perimeter. Without a licensing regime there is no register of domestic providers to supervise, while most Ukrainian crypto trading takes place outside the Ukrainian legal framework [6]. The FIU itself acknowledges that Ukraine has no dedicated law and no full licensing or supervision of providers [11]. Reporting therefore falls almost entirely on banks at the fiat edge of the chain. The FIU's 2025 annual report records 1,957,278 reports received and 1,441 referrals to law enforcement concerning transactions worth UAH 272.7 billion, but it contains no breakdown for drug proceeds or virtual assets [61]. Without such figures neither the legislator nor the supervisor can measure the problem it has to solve.

Bank-side measures: The National Bank of Ukraine (NBU) responded to the drop economy with a temporary limit of UAH 150,000 per month on outgoing card-to-card transfers from 1 October 2024 [65]. The limit was not extended beyond its six-month term; the regulator relied instead on a memorandum on the transparency of the payment market signed by banks in December 2024 [66]. Such measures reduce the capacity of drop networks but do not reach crypto-to-crypto layering, and they can be bypassed by spreading transfers across banks.

Administrative liability: The sanction for gatekeepers who fail is set by Article 166-9 of the Administrative Offences Code (AOC), which provides for a fine on officials of obliged entities "from three hundred to two thousand tax-free minimum incomes of citizens" for, among other things, defective due diligence, failure to report or to keep records, violation of the suspension procedure and breach of the requirement to accompany transfers with data on their originator and recipient [41]. Its addressees are thus limited to officials of regulated institutions. A private individual who, without any registration, regularly buys and sells crypto for third parties on P2P platforms-precisely the person who turns drug cash into stablecoins-falls outside it, and the Code has no separate offence of unregistered virtual-asset exchange. Administrative liability therefore ends where the regulated perimeter ends, and for virtual assets that perimeter is still empty.

Market regulation in waiting: Bill No. 10225-д would define virtual assets as a special kind of property that is not money, make the national securities and stock market commission the main regulator and the NBU the supervisor of electronic money tokens, require authorisation of exchanges and custodians, tighten financial monitoring and the verification of the origin of funds, and enter into force on 1 July 2027 [14,15]. This would create the missing perimeter along the lines of the EU authorisation regime for crypto-asset service providers [53]. Three issues should, however, be addressed when the bill and the AML law are aligned. First, supervision under Article 18 of the AML law has to follow the new regulator; otherwise the AML supervisor and the market regulator will diverge. Second, the Ukrainian threshold of UAH 30,000 for full transfer information departs from the EU approach, under which crypto-asset transfers carry originator and beneficiary information regardless of amount and transfers above EUR 1,000 to self-hosted addresses require an assessment of who owns or controls the address [54]. Third, EU law will prohibit anonymous crypto-asset accounts and anonymity-enhancing coins from July 2027 [55]; a candidate state that legalises its market in the same year should adopt the same rule from the outset.

Procedural principles: Administrative measures in this field-suspension of transactions, refusal of service, freezing on request, exclusion from the market-restrict property and economic activity. They must comply with the principles of administrative procedure, including legality, proportionality, a reasoned decision and access to judicial review, which also form the yardstick of review by administrative courts [36]. Strasbourg case law points the same way: In Gogitidze, confiscation of unexplained property was found compatible with Article 1 of Protocol No. 1 because the owners had a reasonable opportunity to put their case in adversarial proceedings [60]. The FATF's encouragement of stablecoin issuers to be able to freeze and withdraw tokens [51], and the practice of requesting such freezes through law enforcement [69], need a statutory basis that specifies who may request a freeze, for how long and under what judicial control (Table 2).

Table 2: Administrative instruments against crypto-laundering of drug proceeds: Coverage and gaps.

Instrument	Legal basis	Coverage of virtual assets	Main gap
Reporting duties of providers	AML law, Arts. 1(1)(51), 6(2)(8)	Formally complete	No licensing regime and no register; most providers used by Ukrainians are foreign
Customer due diligence	AML law, Article 11(3)	Transactions with virtual assets of UAH 30,000 or more	Splitting below the threshold; individual P2P traders outside the perimeter
Information accompanying transfers	AML law, Article 14	Wallet numbers required; full data above the threshold	Threshold-based; no verification of unhosted wallets, unlike the European Union (EU) transfer-of-funds rules
Suspension of transactions	AML law, Article 23	Any reporting entity; up to 30 working days in total	Ineffective where no domestic provider holds the asset; issuer freeze has no statutory basis
Limits on P2P card transfers	NBU Resolution No. 102 of 27.08.2024; banks' memorandum	Hryvnia leg only	Bypassed by spreading transfers across banks; no effect on crypto layering
Administrative liability	Code of Ukraine on Administrative Offences (CUAO), Article 166-9	Officials of reporting entities	No offence for unregistered, systematic exchange of virtual assets
Market licensing and supervision	Bill No. 10225-д	Securities regulator and National Bank of Ukraine (NBU); authorisation of exchanges and custodians	Not adopted; planned entry into force on 1 July 2027

Source: Authors' elaboration based on [12,15,41,54,65,66].

Criminal-law means: A general norm, a special norm and a new offence

Article 209: Since 2019, Article 209 has punished the acquisition, possession, use or disposal of property where factual circumstances indicate its criminal origin, including financial transactions and deals with such property, its movement and change of form (conversion), and acts aimed at concealing its origin, location or ownership, if the person knew or should have known of that origin. The penalties are three to six years' imprisonment under part 1, five to eight years under part 2 (repetition, group, large amount) and eight to twelve years under part 3 (organised group, especially large amount), each with confiscation [18]. The wording comfortably covers virtual assets: A swap of United States Dollar Tether (USDT) for bitcoin is a "change of form" and a transfer to a fresh wallet is "movement". The difficulty lies not in the object but in the mental element and the proof of the predicate. Speaking at a forum on anti-laundering policy in September 2026, the President of the supreme court admitted that judicial practice under Article 209 lacks uniformity. He underlined that a special purpose of legalisation is an obligatory element of the offence and that, although liability for laundering is not ruled out merely because nobody has yet been convicted of the predicate crime, the presumption of innocence must still be respected [73]. Drug cases usually avoid this difficulty because the predicate trafficking offence is proved in the same proceedings, and laundering is charged cumulatively with it; the amphetamine scheme described above was qualified under Part 3 of Article 209 [10].

Article 306: This is the specific offence for drug money. It covers the use of funds derived from illicit trafficking in narcotic drugs and similar substances in three ways: Their placement in banks, enterprises, institutions or organisations; the purchase of privatised property or equipment with them; and their use to continue illicit trafficking. Part 1 provides for seven to twelve years' imprisonment; part 2, applicable to repeated conduct, a group acting by prior conspiracy or a large amount (200 tax-free minimum incomes or more), raises the range to eight to fifteen years; confiscation is mandatory in both [18]. The provision was designed for a cash economy in which drug money had to enter a bank or a firm. Buying stablecoins from a P2P trader, depositing them on a foreign exchange or swapping them in an unhosted wallet is not "placement in a bank or enterprise" and is not the purchase of privatised property, and Article 3(4) of the criminal code prohibits applying criminal law by analogy [18]. Article 306 therefore reaches crypto only through its last form-use "to continue" trafficking-when stablecoins pay couriers, rent laboratories or buy precursors.

Two anomalies follow: First, qualification turns on how the money is used rather than on the laundering technique: Reinvesting crypto in the drug business falls under Article 306, with a minimum of seven years, whereas converting the same crypto into a flat or a car falls under Article 209(1), with a minimum of three. Second, the aggravated form of Article 306 starts at 200 tax-free minimum incomes, whereas Article 209 reserves its most severe part for property exceeding 18,000 such minimums [18], so the same wallet may be valued against two very different scales depending on what its owner did with it. Neither norm mentions virtual assets, and courts must reconstruct their application from general concepts-a source of the inconsistency that the supreme court has already identified [26,73].

Drop accounts: On 28 October 2026, the Verkhovna Rada adopted Bill No. 16013, which implements Directive (EU) 2019/713 "on combating fraud and counterfeiting of non-cash means of payment". According to press reports, the law extends Article 200 to payment orders and other tools giving access to bank and e-wallet accounts and adds a new article that penalises handing over, receiving, acquiring or storing payment instruments, account credentials or account access for the purpose of fraud; repeated or organised conduct is punishable by up to six years' imprisonment, while a first-time holder who reports the offence and helps to uncover it may be released from liability [46,47]. This is progress for anti-laundering work, since most schemes move their hryvnia leg through borrowed accounts. The new offence, however, is built around fraud and speaks of bank accounts and electronic wallets without mentioning virtual-asset wallets or exchange accounts [46,47]. Consequently, an account rented out to a drug shop, or an exchange account handed over to its treasurer, must still be pursued under Article 209, where the prosecution has to establish that the account holder was or ought to have been aware that the funds were criminal.

Arrest of virtual assets: In this area procedure has outpaced substance. Part 10 of Article 170 of the Criminal Procedure Code (CPC) explicitly mentions virtual assets among the property that may be arrested [40,67]. By the count of members of the Bar, the Unified State Register of Court Decisions already holds over two thousand rulings on arresting crypto-assets issued between 2020 and 2026 [69]. Judicial approaches nevertheless diverge. In 2025, one and the same district court in Kyiv treated cryptocurrency held on an exchange account as physical evidence in one case, yet in another case lifted an arrest because, in its view, cryptocurrency did not meet the criteria of physical evidence [68]; Voronkin criticises the habit of arresting crypto merely to preserve evidence rather than to secure confiscation [25]. Since judicial precedent plays a growing role in the Ukrainian legal system, as it does in EU law [74], a legal position of the supreme court on the arrest of virtual assets would be the quickest way to settle this divergence. An arrest only prohibits disposal, so a ruling that leaves out the network, the address or user identifier, the token, the amount, the custodian and the manner of execution gives an exchange nothing to act upon [69].

Asset management: The asset-management agency may manage arrested assets above a statutory value threshold [44], and its powers were revised by the 2025 reform [45]. In April 2025, an investigating judge in Kyiv for the first time authorised the transfer of USDT on the TRON network to the agency for management or sale (case No. 757/17710/25-к), and in May 2025 another judge ordered the same assets to be sold [67]. Three obstacles remain: A foreign exchange is not formally bound by a Ukrainian ruling and may require a request for mutual legal assistance; there is no official methodology for valuing virtual assets; and the references to virtual-asset wallets and exchange accounts contained in the reform bill were dropped from the final text [67]. Volatile tokens may lose value before a case ends, whereas stablecoins can be frozen by their issuer within the smart contract itself [69]. For that reason, the law should first of all say how seized tokens are moved to a wallet controlled by the State.

Special confiscation and Strasbourg standards: Under Articles 96-1 and 96-2 CC, the State may specially confiscate "money, valuables and other property" that were "obtained as a result of the commission of a criminal offence" [18]; virtual assets, as digital things, fall within this formula. The missing element is a mechanism that would lighten the burden of proving the criminal origin of crypto in the hands of a person already convicted of drug trafficking. The Strasbourg court tolerates such mechanisms, but only within defined limits. Welch classified a drug-trafficking confiscation order as a "penalty" and barred its retroactive application [57]. In Phillips, the court found no breach of Article 6 where a statutory assumption that a convicted

trafficker's property derived from drug trafficking was applied at the sentencing stage, could be rebutted and was subject to judicial assessment [58]. Grayson and Barnham accepted that a convicted trafficker may be required to show that his realisable assets are smaller than the assessed benefit [59], and Gogitidze accepted confiscation of unexplained property in proceedings that allowed the owners to rebut the presumption [60]. Directive (EU) 2024/1260 moves in the same direction by providing for extended confiscation and, under conditions, confiscation of unexplained wealth linked to criminal conduct [56]. A rebuttable presumption for virtual assets acquired by a person convicted under Article 306 or 307 within a defined period before the offence, applied by a court in adversarial proceedings, would meet these standards.

A three-tier model and proposals: The analysis suggests that counteraction should be organised around conversion nodes rather than around the asset or the offence. Three tiers can be distinguished (Table 3): Gateway control, which brings every professional node within the regulated perimeter; interruption, which allows suspicious value to be stopped while it is still in the crypto ecosystem; and response and recovery, which qualifies the conduct correctly and turns frozen tokens into confiscated and realised assets.

Table 3: Three-tier model of countering the laundering of drug proceeds through virtual assets.

Tier	Administrative-law measures	Criminal-law and procedural measures	International benchmark
Gateway control	Licensing of providers; regular P2P exchange treated as a provider activity; transfer information without threshold and verification of unhosted wallets; ban on anonymous accounts and anonymity-enhancing coins	Liability for supplying accounts and virtual-asset wallets to launderers (extension of the offence introduced by Bill No. 16013)	Financial Action Task Force (FATF) R.15-R.16; Markets in Crypto-Assets Regulation (MiCA); Regulation (European Union) 2023/1113; Regulation (European Union) 2024/1624
Interruption	Suspension under Article 23 of the AML law extended to freeze requests to issuers and foreign providers; drug- and crypto-specific risk indicators and statistics; public-private information exchange	Analysis of blockchain and open-source data named as an operational-search measure under judicial control; standards for documenting blockchain evidence	FATF report on stablecoins and unhosted wallets; Warsaw convention
Response and recovery	Procedure for custody, valuation and sale of virtual assets by the asset-management agency; allocation of part of recovered assets to prevention and treatment	Article 306 CC amended to cover operations with virtual assets; content standard for arrest rulings; rebuttable presumption for virtual assets of convicted traffickers	1988 United Nation (UN) convention, Article 5; Directive (European Union) 2024/1260; ECtHR: Welch, Phillips, Grayson and Barnham, Gogitidze
Source: Compiled by the authors on the basis of [12,18,40,43,44,48,50,51,54-56].			

The model requires legislative support, which we formulate as six proposals. (1) Adoption of Bill No. 10225-д should be accompanied by amendments to the AML law: Article 18 ought to make the new market regulator the AML supervisor of crypto-service providers; the UAH 30,000 threshold in Article 14 should no longer apply to virtual-asset transfers; and, following the EU model, providers should check transfers involving self-hosted wallets once they exceed a fixed value [12,53,54]. Exchanging crypto for third parties on a regular basis, P2P platforms included, should be listed expressly as a provider activity, and the Code on Administrative Offences should penalise carrying it on without registration [41]. (2) The suspension rules in Article 23 of the AML law need an express reference to operations with virtual assets; in addition, the FIU should be able, through law-enforcement channels and under ex post judicial review, to ask foreign providers and the issuers of stablecoins to block addresses for as long as the suspension lasts [51]. (3) The catalogue of operational-search measures in Article 8 of the operational-search statute should include analysis of public blockchain records and open-source data, with prior court authorisation required whenever such analysis is combined with personal data received from providers [43,75]. (4) The disposition of Article 306 CC should be supplemented by "conversion into virtual assets, exchange, transfer or other operations with virtual assets" and by "payment for goods, works or services connected with illicit trafficking, including in virtual assets", and its monetary thresholds should be aligned with Article 209 [18]. (5) The offence created by Bill No. 16013 should also cover virtual-asset wallets and exchange accounts and should apply whatever the predicate crime, not only fraud,

while the release clause for first-time holders who cooperate should be preserved [46]. (6) The criminal procedure code and the asset-management statute should specify the mandatory content of a ruling arresting virtual assets, the procedure for moving them to a wallet under State control, the method of valuation and the grounds for sale, and should introduce a rebuttable presumption of criminal origin for virtual assets of convicted drug traffickers consistent with Phillips and Grayson and Barnham [40,44,58,59].

Two further points concern the purpose of recovery and its measurement. Restorative justice, examined by Sarmadi, et al. in a setting where Islamic law and customary practice interact, asks whom a legal response should repair [39]. Drug proceeds have no individual victim, but they harm communities. Allocating part of the funds realised from confiscated drug-related virtual assets to prevention and treatment would link asset recovery with the health-oriented goals of the state drug policy strategy to 2030 [76]. As for measurement, Financial Intelligence Unit (FIU) reports should show drug proceeds and virtual assets as separate categories [61]. We share the view of Predmestnikov, et al. that the number of registered cases is a poor indicator of success [77]; the amount of virtual assets frozen, confiscated and actually realised would be a better one. The comparative experience of European states in implementing international standards [37] and the operational channels of international cooperation that Ukraine already uses [31] provide a basis for building such indicators.

Conclusion

Virtual assets have become a regular channel for laundering drug proceeds in Ukraine. Drug shops take payment in stablecoins, couriers and suppliers are paid in them, and the proceeds return to hryvnias through P2P trades, borrowed bank accounts and foreign platforms. Effective counteraction has to be node-centric: It must concentrate on the points at which value enters or leaves the crypto ecosystem or changes custodian and at which an identifiable person has to appear.

The administrative layer is formally in place-virtual asset service providers are reporting entities, due diligence applies from UAH 30,000, transfers must carry wallet information and suspicious transactions can be suspended-but it lacks a perimeter, because the market law of 2022 has not entered into force and no domestic provider is licensed. Bill No. 10225-д would supply that perimeter from 1 July 2027 if adopted; its alignment with the AML law, with the EU rules on information accompanying crypto-asset transfers and with the forthcoming EU ban on anonymous crypto-asset accounts will decide whether it closes the gap or merely moves it.

The criminal-law layer is uneven. Article 209 covers virtual assets as property, but the drug-money provision of Article 306 fits crypto only when it finances further trafficking, and the new offence concerning drop accounts adopted in October 2026 does not name virtual-asset wallets. Arrest of virtual assets has become routine, yet what happens to the seized tokens afterwards-custody, sale or return-is determined by foreign platforms, by the precision of court rulings and on rules that the 2025 reform of the asset-management agency left out.

The proposed three-tier model-gateway control, interruption, and response and recovery-and the six amendments derived from it would join these layers into one system. They respect Strasbourg limits: Confiscation remains a penalty that cannot be applied retroactively, and any presumption of illicit origin must be rebuttable and applied by a court. Further research should test the model on court files and on blockchain data from Ukrainian cases once drug-specific and crypto-specific statistics become available.

Acknowledgement

None.

Conflict of Interest

Authors have no conflict of interest to declare.

References

1. S. Foley, J.R. Karlsen, T.J. Putniņš. Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies? Rev Financ Stud, 32(2019):1798-1853.
2. Chainalysis. From fentanyl to fraud: On-chain activity highlights illicit market evolution, 2026 Crypto Crime Report, (2026).
3. The block. Crypto crime topped $150 billion in 2025 as state-backed actors scaled onchain: Chainalysis, (2026).
4. Financial Action Task Force (FATF). Targeted update on implementation of the FATF standards on virtual

assets and virtual asset service providers, (2025).

5. Financial Action Task Force (FATF). Targeted update on implementation of the FATF standards on virtual assets and virtual asset service providers, (2026).
6. B. Aris. Ukraine tops the world for crypto use per person as volumes hit $206bn, bne IntelliNews, (2026).
7. Public health center of the ministry of health of Ukraine. Report on the drug and alcohol situation in Ukraine (data for 2024), (2025).
8. Public health center of the ministry of health of Ukraine. National report on the drug and alcohol situation in Ukraine (data for 2025), (2026).
9. The public. National Police liquidates large-scale psychotropic drugs trafficking channel worth UAH 95 million, (2025).
10. 7eminar. An inter-regional drug cartel that used money mules was exposed with the help of the State Tax Service (STS), (2025).
11. State financial monitoring service of Ukraine. Risks and threats of money laundering and terrorist financing amid the military aggression of the Russian Federation-2025, Typology Study, approved by SFMS Order No. 116, (2025).
12. Law of Ukraine. On prevention and counteraction to legalisation (laundering) of the proceeds of crime, financing of terrorism and financing of proliferation of weapons of mass destruction, No. 361-IX, (2019).
13. Law of Ukraine. On virtual assets, No. 2074-IX, 17 February 2022 (not yet in force). (2022).
14. Forbes Ukraine. Legalisation of cryptocurrencies: The Verkhovna Rada supported the relevant bill in the first reading, (2025).
15. Mind.ua. The parliamentary tax committee supported the bill on the circulation of virtual assets, (2026).
16. TechnoFan. The crypto law in Ukraine has been put on hold: Why the National Bank of Ukraine (NBU) is opposed and what taxes are proposed, (2026).
17. Law of Ukraine. On amending the civil code of Ukraine on expanding the range of objects of civil rights, No. 3320-IX, (2023).
18. Law of Ukraine. Criminal code of Ukraine, No. 2341-III, (2001).
19. C. Albrecht, K.M. Duffin, S. Hawkins, V.M. Morales Rocha. The use of cryptocurrencies in the money laundering process, J Money Laundering Control, 22(2019):210-216.
20. D. Dupuis, K. Gleason. Money laundering with cryptocurrency: Open doors and the regulatory dialectic, J Financ Crime, 28(2021):60-74.
21. C. Wronka. Money laundering through cryptocurrencies-analysis of the phenomenon and appropriate prevention measures, J Money Laundering Control, 25(2022):79-94.
22. V. Benson, B. Adamyk, A. Chinnaswamy, O. Adamyk. Harmonising cryptocurrency regulation in Europe: Opportunities for preventing illicit transactions, Eur J Law Econ, 57(2024):37-61.
23. L. Moyle, A. Childs, R. Coomber, M.J. Barratt. #Drugsforsale: An exploration of the use of social media and encrypted messaging apps to supply and access drugs, Int J Drug Policy, 63(2019):101-110.
24. M.J. Barratt, F.R. Lamy, L. Engel, E. Davies, C. Puljević, et al. Exploring Televend, an innovative combination of cryptomarket and messaging app technologies for trading prohibited drugs, Drug Alcohol Depend, 231(2022):109243.
25. A.O. Voronkin. Arrest as a type of restriction of ownership of cryptocurrency assets in criminal proceedings, Anal Comp Juris, 5(2025).
26. O.V. Kuzmenko, P.Y. Kravchuk. Virtual assets as the object of a criminal offence: Problems of definition and proof, Anal Comp Juris, 6(2025).
27. T. Shevchenko. Illegal sale of narcotic drugs using electronic information resources: Problems of qualification, Sci Bull Uzhhorod Natl Univ Ser Law, 84(2024):408-413.
28. P. Yepryntsev, A. Nikitin, M. Maksimentsev, A. Korenev, R. Mrochko. Administrative and criminal law analysis of countering cybercrimes in the field of illicit drug trafficking at the regional and local levels, J Drug Alcohol Res, 15(2026):1-7.
29. R. Kushnirenko, Y. Kitsul, V. Tulinov, O. Karpenko, D. Chernolutskyi. Tactical actions of police officers in the fight against drug offenses as a direct route to information and national security, J Drug Alcohol Res, 14(2025):1-7.
30. M. Korniienko, A. Desyatnik, G. Didkivska, Y. Leheza, O. Titarenko. Peculiarities of investigating criminal offenses related to illegal turnover of narcotic drugs: Criminal law aspect, Khazanah Hukum, 5(2023):205-215.
31. V. Davydenko, M. Korniienko, A. Radchuk, A. Babiak, Y. Leheza. International cooperation in operational and search activities: A comparative analysis of foreign experience, Cadernos de Dereito Actual, 28(2025):83-102.
32. O. Volobuieva, Y. Leheza, V. Pervii, Y. Plokhuta,

R. Pichko. Criminal and administrative legal characteristics of offenses in the field of countering drug trafficking: Insights from Ukraine, Yustisia, 12(2023):262-277.

33. T. Voloshanivska, I. Pozihun, S. Losych, O. Merdova, Y. Leheza. Administrative and criminal law aspects of preventing offenses committed by minors in the sphere of illegal circulation of narcotic drugs, J Drug Alcohol Res, 12(2023):1-6.

34. Y. Leheza, V. Shablystyi, I. Aristova, I. Kravchenko, T. Korniakova. Foreign experience in legal regulation of combating crime in the sphere of trafficking of narcotic drugs: Administrative and criminal aspect, J Drug Alcohol Res, 12(2023):1-8.

35. V. Halunko, N. Maksimentseva, O. Poltoratskyi, M. Maksimentsev, I. Tsareva. Administrative, financial, criminal-legal and theoretical-methodological aspects of regulating social relations in government bodies, Cuest Polit, 41(2023):502-511.

36. N. Maksimentseva, M. Maksimentsev, N. Ilchyshyn. Exercise of judicial power in administrative proceedings through compliance with the principles of administrative procedure law of Ukraine, J Law Polit Sci, 34(2022):376-388.

37. Y. Khrystova, S. Miroshnychenko, I. Kurbatova, O. Titarenko, M. Maksimentsev. Legal regulation experience of individual countries of the European region regarding implementation of international standards for ensuring criminological and criminal-legal protection of justice, Jurnal Cita Hukum, 12(2024):293-308.

38. M. Loshytskyi, O.S. Yunin, D.P. Kyslenko, B. Tychna, O. Dotsenko. International legal standards for documentation and investigation of war crimes, Clio J Hist Hum Sci Crit Thought, 10(2025):1818-1855.

39. A.S. Sarmadi, A. Hafidzi, Mohlis, O.S. Yunin, M.V. Korniienko. Negotiating Islamic law and customary practice: Fiqh al-Aqalliyyat and restorative justice in Banjar inheritance disputes, J Ilm Al-Syir'ah, 23(2025):279-296.

40. Law of Ukraine. Criminal procedure code of Ukraine, No. 4651-VI, (2012).

41. Law of Ukraine. Code of Ukraine on administrative offenses, No. 8073-X, (1984).

42. Law of Ukraine. On measures to counter illicit trafficking in narcotic drugs, psychotropic substances and precursors and their abuse, No. 62/95-VR, (1995).

43. Law of Ukraine. On operational and search activity, No. 2135-XII, (1992).

44. Law of Ukraine. On the national agency of Ukraine for detection, search and management of assets derived from corruption and other crimes, No. 772-VIII, (2015).

45. Law of Ukraine. On amendments to the Law of Ukraine "On the national agency of Ukraine for the identification, search and management of assets derived from corruption and other crimes" regarding strengthening the institutional capacity of the National Agency and improving asset management mechanisms, No. 4503-IX, (2025).

46. Debet-Kredyt. Fines for handing over payment cards for drop schemes: The Verkhovna Rada adopted the law, (2026).

47. Forbes Ukraine. Up to six years in prison: The Verkhovna Rada adopted a law on criminal liability for "money mules", (2026).

48. United Nations (UN). United Nations convention against illicit traffic in narcotic drugs and psychotropic substances, adopted in Vienna on 20 December 1988, (1988).

49. Council of Europe. Convention on laundering, search, seizure and confiscation of the proceeds from crime and on the financing of terrorism, CETS No. 198, opened for signature in Warsaw on 16 May 2005, (2005).

50. Financial Action Task Force (FATF). International standards on combating money laundering and the financing of terrorism & proliferation: The FATF recommendations, (2025).

51. Financial Action Task Force (FATF). Targeted report on stablecoins and unhosted wallets: Peer-to-peer transactions, (2026).

52. Money laundering and terrorist financing risks in the world of virtual assets, typologies report, Ukrainian translation issued by the State Financial Monitoring Service of Ukraine (SFMS), (2023)

53. European parliament and council of the European Union (EU). Regulation European Union (EU) 2023/1114 of 31 May 2023 on markets in crypto-assets (MiCA), (2023):40-205.

54. European parliament and council of the European Union (EU). Regulation European Union (EU) 2023/1113 of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849, (2023):1-39.

55. European parliament and council of the European Union (EU). Regulation European Union (EU) 2024/1624 of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, (2024).

56. European parliament and council of the European

Union (EU). Directive European Union (EU) 2024/1260 of 24 April 2024 on asset recovery and confiscation, (2024).

57. European Court of Human Rights (ECtHR). Welch *vs*. the United Kingdom, application No. 17440/90, Judgment of 9 February 1995, (1995).

58. European Court of Human Rights (ECtHR). Phillips *vs*. the United Kingdom, application No. 41087/98, Judgment of 5 July 2001, (2001).

59. European Court of Human Rights (ECtHR). Grayson and Barnham *vs*. the United Kingdom, applications Nos. 19955/05 and 15085/06, Judgment of 23 September 2008, (2008).

60. European Court of Human Rights (ECtHR). Gogitidze and Others *vs*

61. . Georgia, application No. 36862/05, Judgment of 12 May 2015, (2015).

62. State Financial Monitoring Service of Ukraine (SFMS). Annual report of the state financial monitoring service of Ukraine for 2025, (2026).

63. European Monitoring Centre for Drugs and Drug Addiction (EMCDDA) and Europol. European Union (EU) Drug Markets Analysis 2024: Key insights for policy and practice, Luxembourg: Publications Office of the European Union, (2024).

64. TRM Labs. In wake of Department of Justice (DOJ) indictment of Iranian operator of darknet market nemesis, TRM Labs Shares New Data on Darknet Markets (DNMs), (2025).

65. Debet-Kredyt. The problem of "money mules" in Ukraine: How much money has been laundered according to the State Financial Monitoring Service (SFMS)? (2026).

66. Buhplatforma. From 1 October, the national bank of Ukraine introduces a monthly limit of UAH 150,000 on Card-to-Card (C2C) transfers by individuals, 1 October 2024. Based on national bank of Ukraine resolution No. 102 of 27 August 2024, (2024).

67. Mind.ua. Card-to-Card (C2C) Transfer limits: The national bank of Ukraine did not extend the restrictions, (2025).

68. K. Hupalo, T. Bihun. Arrest of crypto: New rules of the game for businesses and individuals, Mind.ua, (2026).

69. Ukrainian national bar association. Cryptocurrency in the courts' sights: From seizure to division of property, (2025).

70. Ukrainian national bar association. Seizure does not mean return: How to get an exchange to return stolen crypto-assets, (2026).

71. T.V. Sych, V.O. Boniak, V.V. Dokuchaieva, Y.M. Khrykov, N.S. Vasynova. Publication of education management research in Ukrainian issues from Scopus and Web of Science (WOS) databases, Asia Life Sci, 22(2020):127-142.

72. K. Rezvorovych, P. Gorinov, M. Sokol, K. Kutsyk, R. Opatskyi. Peculiarities of the legislative regulation of the protection of workers' rights against the background of Russian military aggression (The Ukrainian Experience), Rev Econ Finance, 21(2023):584-591.

73. O. Sokhatska, I. Bashynska, T. Stepanova, M. Malanchuk, S. Rybianets, et al. Modelling the risks of international trade contracts, Int J Innov Technol Explor Eng, 8(2019):2815-2820.

74. Supreme court of Ukraine (press service). New approaches to combating money laundering: Follow the money, report on the panel discussion at the "follow the money: New approaches to combating money laundering" forum, (2026).

75. V. Beschastnyi, S. Shkliar, A. Fomenko, N. Obushenko, L. Nalyvaiko. Place of court precedent in the system of law of the European Union (EU) and in the system of law of Ukraine, J Leg Ethical Regul Issues, 22(2019):1-6.

76. R. Byba. The concept of Open-Source Intelligence (OSINT) in the field of public order and safety, Sci Bull Uzhhorod Natl Univ Ser Law, 92(2025):38-43.

77. Cabinet of ministers of Ukraine. The government adopted the state drug policy strategy until 2030 and approved the operational plan for its implementation, (2025).

78. O. Predmestnikov, S. Skrebovska. The system of preventing and countering the illegal circulation of narcotic drugs in Ukraine: Effectiveness and prospects, Naukovi Zapysky. Seriia Pravo, 17(2024):176-184.