UDC 343.98
DOI: 10.63341/naia-herald/2.2025.119

Methodology of detection and forensic features of investigation of crimes involving virtual assets: A comparative analysis of international practices

Dmytro Ovsianiuk*
Analytical Department (Criminal Analysis Center)
National Academy of Internal Affairs
03035, 1 Solomianska Sq., Kyiv, Ukraine
https://orcid.org/0000-0002-1846-4167

Andriy Okushko
PhD in Law
Cyber Police Department of the National Police of Ukraine
02093, 19 Boryspilska Str., Kyiv, Ukraine
https://orcid.org/0009-0003-3627-2489

Yevhenii Panchenko
International Police Cooperation Department of the
National Police of Ukraine
01024, 1 Akademika Bogomoltsya Str., Kyiv, Ukraine
https://orcid.org/0000-0001-5755-7457

■ **Abstract.** The purpose of this study was to identify effective approaches to the investigation of crimes involving virtual assets based on a comparative analysis of international practices. The study was based on a systematic analysis of legal acts and regulatory documents, and employed the methods of comparative legal analysis to investigate the regulatory approaches of various jurisdictions, a systematic approach to explore the interrelationships between the elements of the crime prevention system, a structural-functional study of the role of different actors. The study found the critical lack of a unified international definition of virtual assets, which creates gaps in criminal law qualifications, especially regarding Article 209 of the Criminal Code of Ukraine, and procedures for seizure and confiscation of assets in cross-border cases. It was found that the greatest efficiency of the investigation is achieved through the multilayered integration of proactive approaches to monitoring virtual asset service providers, reactive measures of law enforcement agencies, the use of specialised software Chainalysis, TRM Lab, Crystal Blockchain, Elliptic for blockchain analytics and open intelligence methods. The study systematised specific forensic indicators of five main types of virtual asset crimes, including structuring of transactions in money laundering, use of mixers, promises of unrealistic profits in investment fraud, and links to darknet addresses. The comparative analysis of five key jurisdictions demonstrated a dramatic diversity of regulatory approaches, from the technology-neutral Swiss principle-based regulation to the comprehensive European Markets in cryptoassets with unified requirements for cryptoasset service providers. The practical significance of the findings lies in the possibility of developing effective mechanisms for international cooperation in the investigation of cross-border crimes involving virtual assets

■ **Keywords:** cryptocurrency; fraud; digital forensics; deanonymisation; blockchain

■ **Suggested Citation:**
Ovsianiuk, D., Okushko, A., & Panchenko, Ye. (2025). Methodology of detection and forensic features of investigation of crimes involving virtual assets: A comparative analysis of international practices. *Scientific Journal of the National Academy of Internal Affairs,* 30(2), 119-137. doi: 10.63341/naia-herald/2.2025.119.

■ *Corresponding author

■ Received: 29.01.2025; Revised: 28.04.2025; Accepted: 27.05.2025

Introduction

The rapid development of virtual asset technologies and their widespread introduction into the financial system have created new challenges for law enforcement agencies in the field of crime detection and investigation. The pseudo-anonymity, decentralisation, and cross-border nature of virtual assets have dramatically changed the landscape of financial crime, requiring the development of specific investigative methodologies and the adaptation of traditional forensic approaches to new technological reality. The relevance of this study is driven by the exponential growth of criminal activity involving virtual assets and the lack of unified international approaches to their investigation. According to the IOCTA 2025 report (Internet Organised Crime..., 2025), cybercriminals are actively using a complex system to trade stolen data and access to systems, with the methods of criminals constantly changing, outpacing the development of relevant law enforcement techniques.

M.Z. Hossain (2023) explored the trends in the development of forensic accounting and its adaptation to the challenges of the digital age. The researcher comprehensively systematised the emerging trends in the field of forensic accounting, focusing on the transformational changes caused by the digital revolution. Author developed a methodological framework for integrating conventional approaches with modern technologies, including cyber forensic accounting, cryptocurrency analysis, and blockchain technologies to detect and prevent fraud. U. Agarwal *et al.* (2024) comprehensively reviewed specific aspects of blockchain and cryptocurrency forensics, developing a methodological approach to investigating crypto fraud based on the integration of technical analysis of blockchain and conventional forensic techniques. The researchers created a detailed taxonomy of cryptocurrency crimes by method of commission and technological complexity, proposing a systematisation of the key types of crimes from simple theft to complex money laundering schemes. The researchers analysed the effectiveness of various technological tools for detecting cryptocurrency crimes, including specialised software and de-anonymisation techniques.

In a study for the International Monetary Fund within the framework of its financial stability risk assessment, N. Schwarz *et al.* (2021) detailed the legal and practical aspects of combating money laundering through virtual assets. The researchers analysed the regulatory landscape, identifying key challenges for financial institutions and regulators in the context of implementing Anti-Money Laundering/Fighting the Financing of Terrorism (AML/CFT) measures in relation to virtual assets, including the challenges of identifying ultimate beneficiaries in decentralised systems and the challenges of applying conventional Know Your Customer (KYC) approaches to anonymous transactions.

A. Ombu (2023) studied the role of digital forensics in combating financial crimes in the computer era, analysing the transformation of forensic practices under the influence of the digitalisation of society. The researcher substantiated a conceptual model for the integration of conventional investigative methods with modern digital technologies, demonstrating how the convergence of the physical and digital worlds creates new opportunities for evidence collection. The study highlighted the criticality of specialised training for law enforcement officers to work effectively in the digital environment and develop relevant technical competences.

In an empirical study of the effectiveness of various technological solutions in the context of real investigations, N. Hamad & D. Eleyan (2022) performed a comparative analysis of digital forensics tools used in the investigation of cybercrime. The researchers developed a methodology for evaluating forensic tools based on the criteria of functionality, reliability, and usability, systematising the advantages and disadvantages of software and hardware solutions. The researchers provided practical recommendations for choosing the best technological solutions depending on the specifics of digital evidence and available resources. Complementing this technological perspective, D. Ovsianiuk (2024) emphasised that the intelligence cycle serves as a methodological foundation for structuring analytical activity, enabling the systematic collection, evaluation, synthesis, and operational application of information. Although originally developed in the context of drug-related crime, this model can be effectively adapted to investigations involving virtual assets, where structured analytical processes are essential for interpreting complex data environments.

V. Jitariuc & A. Nastas (2022) detailed the forensic features of cybercrime, developing a theoretical framework for understanding the specifics of crimes in cyberspace and their differences from conventional forms of criminal activity. The researchers analysed the nature of digital traces, their formation and preservation in different technological environments, creating a comprehensive approach to the analysis of digital evidence in criminal proceedings. The study included classification of types of digital evidence and identification of their specific characteristics, including volatility and the possibility of remote modification.

F.C. Tsai (2021) proposed an innovative approach to the use of blockchain technologies in criminal proceedings. The researcher explored the possibilities of using distributed ledger technology to improve the reliability of evidence documentation procedures.

F.C. Tsai (2021) also developed a conceptual model for integrating blockchain into conventional chain of custody procedures, demonstrating how the technology can ensure the immutability of records of evidence movements from discovery to presentation in court. The study demonstrated the potential of blockchain to revolutionise the documentation and storage of evidence. R.S. Faqir (2023) comprehensively analysed the impact of artificial intelligence (AI) on digital criminal investigations, exploring current trends in the use of AI in law enforcement, from automated evidence analysis to predictive modelling. The researcher systematised the application of machine learning in forensics, including natural language processing for communication analysis and computer vision for video evidence processing. Having analysed potential risks, including the problems of algorithmic bias and the need to maintain human control, R.S. Faqir (2023) substantiated the prospects of automating certain aspects of the investigation. J. Wu *et al.* (2023) investigated financial crimes in the metaverse supported by Web3 technologies, researching new forms of criminal activity in virtual worlds and blockchain-based economies. The researchers developed a taxonomy of crimes in virtual environments, including conventional forms of fraud adapted to the metaverse and fundamentally new types of criminal activity. The study demonstrated the evolution of criminal schemes towards more complex virtual environments and suggested relevant countermeasures to prevent them.

The analysis of the scientific literature revealed that despite the significant attention of researchers to certain aspects of the issue, there is no comprehensive comparative analysis of international methodologies for detecting and investigating crimes involving virtual assets. The issues of correlation between multiple regulatory approaches, the effectiveness of international cooperation in this area, and the adaptation of forensic techniques to the specifics of diverse types of virtual assets are still understudied. The purpose of the present study was to systematise and comparatively assess the existing approaches to detecting and investigating criminal offences in the field of virtual assets. To fulfil this purpose, the study set out the tasks of analysing the conceptual framework and legal nature of virtual assets in the context of criminal investigations, systematising methodologies for detecting crimes involving virtual assets, and studying the forensic features of investigating such crimes.

Materials and Methods

The methodological framework of this study included an integrated approach to the review of methodologies for detecting and forensic features of investigating crimes involving virtual assets, which helped to consider this issue as a multidimensional phenomenon at the intersection of legal, technological, and forensic aspects. The study was based on a systematic analysis of a wide range of sources, which can be divided into several main groups. Six key jurisdictions were selected for comparative analysis: Ukraine, the European Union, the United States, Germany, Switzerland, and Singapore. The choice was made due to the diversity of regulatory approaches, the level of development of the virtual asset market, and the availability of practical experience in investigating relevant crimes. The first group included Ukrainian laws and regulations that form the national legal framework for governing virtual assets and combating crime in this area. These included the Law of Ukraine "On Prevention and Counteraction to Legalisation (Laundering) of Proceeds of Crime, Financing of Terrorism and Financing of the Proliferation of Weapons of Mass Destruction"[1] and the Criminal Procedure Code of Ukraine[2]. The second group was formed by regulatory documents and practices of international organisations and foreign countries. The recommendations of the Financial Action Task Force (FATF) (2024) on virtual assets, and Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (2023), EU regulations, particularly European Crypto-Assets Regulation (MiCA)[3]. The third group included the materials of law enforcement agencies and international organisations on the practical aspects of investigating crimes involving virtual assets. The study analysed the following reports and guides for law enforcement agencies: SQUIRE Patton Boggs (2025), Law Business Research (2024), Swiss Financial Market Supervisory Authority (FINMA) (2022), Charltons Quantum (2025), Blockchain Intelligence Group (2025), OSCE (2024), Europol (2025), analytical materials of INTERPOL (2024), documents of the German BKA (2025) and practical manuals on cryptocurrency investigations (Grigg, 2025; COPOLAD, 2025).

The study employed a set of scientific methods. The comparative legal method was used to analyse the regulatory approaches of different jurisdictions to virtual assets and methods of investigating related crimes. The system analysis was applied to examine

[1] Law of Ukraine No. 361-IX "On Prevention and Counteraction to Legalisation (Laundering) of Proceeds from Crime, Financing of Terrorism and Financing of Proliferation of Weapons of Mass Destruction". (2019, December). Retrieved from https://zakon.rada.gov.ua/laws/show/361-20#Text.

[2] Criminal Procedure Code of Ukraine. (2012, April). Retrieved from https://zakon.rada.gov.ua/laws/show/4651-17.

[3] Regulation of the European Parliament and of the Council No. 2023/1114 "On Markets in Crypto-Assets, and amending Regulations (EU) No. 1093/2010 and (EU) No. 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 (MiCA)". (2023, May). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:4626998.

the interrelationships between various elements of the system of combating crime in the field of virtual assets. The structural-functional approach helped to investigate the role of various actors (Virtual Asset Service Provider (VASP), law enforcement agencies, regulators) in the system of detection and investigation of crimes. The method of comparative analysis was employed to compare international practices and identify effective approaches. Content analysis was used to systematise information from numerous sources and identify the main trends in the development of investigation methodologies. Such a comprehensive methodological approach, combining the analysis of legal frameworks, regulatory practices of multiple countries, technical standards and practical experience of law enforcement agencies, enabled a comprehensive investigation of the specific features of detecting and investigating crimes involving virtual assets and the development of practical recommendations for improving the relevant methodologies in the international context.

Results

Terminology and legal nature of virtual assets in the context of criminal investigations. Effective investigation of crimes related to virtual assets is impossible without a clear understanding of their legal nature, classification, and specific characteristics used for criminal purposes. The absence of an internationally unified definition of a "virtual asset" and its subtypes (cryptocurrency, NFT, token) directly affects forensic practice. What may be considered "property" or a "financial instrument" in one jurisdiction that is subject to seizure or requires specific investigative actions may have a different legal status in another, creating proof-related and procedural gaps.

The term "virtual asset" (VA) is relatively new and continues to evolve along with the development of technology. In Ukrainian legislation, the definition of a virtual asset has undergone certain changes. In the scientific literature, it was proposed to define a virtual asset as "an intangible good that is an object of civil rights, has a value and is expressed by a set of data in electronic form" (Yarotskyi, 2023). The Law of Ukraine No. 361-IX[1] defines a virtual asset as "a digital expression of value that can be traded in a digital format or transferred and can be used for payment or investment purposes". At the international level, the FATF (2024) defines a virtual asset as "a digital representation of value that can be digitally sold, transferred, or used for payments", excluding digital representations of fiat currencies. In the European Union, the MiCA[2] introduces its own definitions and classifications, such as asset-related tokens (ART) and electronic money tokens (EMT).

A comparative analysis of these definitions revealed shared features, such as digital form and store of value, but also differences in approaches to legal status and functional purpose. Ukrainian legislation emphasises the intangible nature of VAs, while the FATF focuses on their ability to circulate and be used in payments. This terminological ambiguity complicates enforcement, especially in cross-border cases. Specifically, the current version of Article 209 of the Criminal Code of Ukraine[3] on money laundering defines "property" as the object of laundering, which creates legal uncertainty as to whether cryptocurrencies can be recognised as the subject of this crime. Even though the draft amendments to the Civil Code of Ukraine[4] proposed to define virtual assets as a thing (intangible asset), the relevant law on virtual assets has not yet entered into force, leaving the legal status of cryptocurrencies unresolved (Kamenskyi & Dudorov, 2024). The MiCA excludes from its scope cryptoassets that qualify as financial instruments under MiFID II (SQUIRE Patton Boggs, 2025), which requires a clear distinction.

The classification of virtual assets relevant for forensic analysis is crucial for crime investigation purposes. For forensic analysis, the classification of virtual assets is applied according to various criteria. Primarily, a distinction is made between secured and unsecured virtual assets. This classification, consolidated in the Law of Ukraine No. 2074-IX[5] and supported by scholars, distinguishes between assets that certify property rights (secured) and those that do not certify such rights (unsecured). This is essential for determining the object of the offence and possible methods of committing the crime.

By type, virtual assets are divided into cryptocurrencies (e.g., Bitcoin, Ethereum), stablecoins (pegged to fiat currencies or other assets), non-fungible tokens (NFTs), utility tokens, and security tokens. Each type has its specific features of circulation

[1] Law of Ukraine No. 361-IX "On Prevention and Counteraction to Legalisation (Laundering) of Proceeds from Crime, Financing of Terrorism and Financing of Proliferation of Weapons of Mass Destruction". (2019, December). Retrieved from https://zakon.rada.gov.ua/laws/show/361-20#Text.
[2] Regulation of the European Parliament and of the Council No. 2023/1114 "On Markets in Crypto-Assets, and amending Regulations (EU) No. 1093/2010 and (EU) No. 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 (MiCA)". (2023, May). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:4626998.
[3] Criminal Code of Ukraine. (2001, April). Retrieved from https://zakon.rada.gov.ua/laws/show/2341-14#Text.
[4] Civil Code of Ukraine. (2003, January). Retrieved from ttps://zakon.rada.gov.ua/laws/show/435-15#Text.
[5] Law of Ukraine No. 2074-IX "On Virtual Assets". (2022, February). Retrieved from https://zakon.rada.gov.ua/laws/show/2074-20#Text.

and potential vulnerabilities for criminal use. By the nature of issuance, a distinction is made between centralised (with a specific issuer) and decentralised virtual assets (without a single control centre) (Samsin, 2024). The decentralised nature of most cryptocurrencies complicates the regulation and identification of responsible parties. These classifications help investigators understand the specifics of a particular virtual asset that is the object or instrument of a crime and choose an adequate investigation methodology.

The connection between the characteristics of virtual assets and criminal exploitation is manifested in the fact that key characteristics of virtual assets, such as pseudo-anonymity, decentralisation, and cross-border nature, are actively used by criminals. Pseudo-anonymity means that although transactions on most public blockchains are transparent, the identity of wallet holders is hidden behind cryptographic identifiers (wallet addresses). This allows criminals to conduct transactions while staying relatively anonymous until their digital footprints are linked to real people through further investigative efforts (Blockchain Intelligence Group, 2025). Decentralisation means the absence of a single centre of control and management in many virtual asset systems, complicating the blocking of suspicious transactions or seizure of assets without access to private keys (FINMA, 2022). The cross-border nature of virtual assets means that they can be instantly transferred across state borders without the involvement of conventional financial intermediaries, which complicates tracking of the flow of funds and application of national jurisdictions.

These features create major challenges for law enforcement, requiring specialised knowledge, tools, and international cooperation. Some jurisdictions, such as Switzerland, initially relied on "technology-neutral" existing laws, which could lead to uncertainty in the courts. Others, such as the EU with MiCA[1] and Ukraine[2], are moving towards specific regulation. The first approach may create interpretation difficulties when applied to new characteristics of virtual assets (e.g., whether Bitcoin is a "thing" or "data"). The second, if not sufficiently flexible, risks becoming outdated quickly due to the rapid development of virtual asset technologies. These distinct regulatory philosophies directly affect the practical aspects of evidence gathering, asset seizure, and prosecution. Table 1 provides a better understanding of the differences between the legal frameworks. This table illustrates that while there are shared elements in the understanding of VAs, differences in definitions and classifications create a complex legal framework for international cooperation and investigation. The legal qualification of VAs directly affects the possibility of their seizure, confiscation, and recognition as an object or instrument of crime.

Table 1. Comparative definitions and classifications of virtual assets

Jurisdiction/ Organisation	Key terms	Key classification criteria
Ukraine	"A digital thing is a virtual asset, digital content, and other benefits regarding which the provisions of part one of this Article apply"[3].	Collateral (secured/unsecured), property rights certificates, financial VAs (secured by currency values or securities)
FATF	Virtual asset (digital representation of value, can be digitally traded, transferred, used for payment, not digital fiat)	Functional purpose (payment, investment), does not include digital representations of fiat currencies
EU (MiCA)	Crypto-asset (digital representation of value or rights that can be transferred and stored electronically, using DLT or similar technology)	Asset-Referenced Tokens (ARTs), E-Money Tokens (EMTs), other crypto assets (including utility tokens). Exceptions for cryptoassets that qualify as financial instruments under MiFID II.
USA	Terminology may vary depending on the regulator (SEC, CFTC, FinCEN). DOJ uses the term 'digital assets'.	Depends on the specific asset and its characteristics (e.g., whether it is a security, a commodity, or falls within the definition of a money transfer).

Source: developed by the author of this study based on N. Hamad & D. Eleyan (2022), V.O. Yarotskyi (2023), R.S. Faqir (2023), M.Z. Hossain (2023)

Detection of crimes involving virtual assets is a complex process that combines proactive and reactive approaches, the use of technological tools, and close cooperation between various actors. The effectiveness of detection depends on the integration of the efforts of virtual asset service providers (VASPs), financial institutions, and law enforcement. Proactive detection is based on the continuous monitoring

[1] Regulation of the European Parliament and of the Council No. 2023/1114 "On Markets in Crypto-Assets, and amending Regulations (EU) No. 1093/2010 and (EU) No. 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 (MiCA)". (2023, May). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:4626998.
[2] Law of Ukraine No. 2074-IX "On Virtual Assets". (2022). Verkhovna Rada of Ukraine. https://zakon.rada.gov.ua/laws/show/2074-20#Text.
[3] Civil Code of Ukraine. (2003, January). Retrieved from ttps://zakon.rada.gov.ua/laws/show/435-15#Text.

and analysis of transactions involving VAMs to identify suspicious activity. The key role here is played by risk indicators developed by international organisations, specifically FATF (2024) and Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (2023). These indicators include the structuring of transactions, i.e., the execution of transactions with VA in small amounts that do not reach the reporting thresholds, analogous to the structuring of cash transactions. Abnormal transaction frequency and volume, such as multiple high-value transactions within a short period of time, such as 24 hours, or regular transactions without a clear business rationale, are also significant.

The use of VASPs in high-risk jurisdictions is another essential indicator, which includes immediate transfers of VAs to numerous VASPs, especially those registered or operating in jurisdictions with insufficient AML/CFT regulation or without a connection to the customer's residence or business. The use of anonymisation services such as mixers, tumblers, anonymous cryptocurrencies (AEC or privacy coins) to conceal the source or destination of funds. Suspicious customer behaviour is considered to be the provision of false or incomplete information during registration, the use of IP addresses associated with a darknet or VPN, and the mismatch between the financial profile and the volume of transactions. VASPs are required to conduct risk analysis of their customers, products, and transactions to effectively detect such activity. Notably, indicators developed for anti-money laundering (AML) purposes may not always be sufficient to detect other VA-related crimes, such as direct fraud or the financing of illegal activities. For example, a victim of a romance scam who is forced to send cryptocurrency may not show the classic signs of money laundering from a VASP perspective.

Reactive detection involves the actions of law enforcement agencies after receiving information about a possible crime. The sources of such information may include statements from affected individuals or companies, suspicious transaction reports (STRs) from financial institutions or VASPs, information received from international partners or in the course of operational activities. At the initial stage, it is crucial to collect primary information such as the time of the transaction, the name of the financial institution or VASP, the amount, type of cryptocurrency, wallet addresses, and any data on counterparties (OSCE, 2024). The effectiveness of reactive detection largely depends on the quality of proactive measures taken by VASPs and the promptness of notifications.

VASPs play a key role in the system of detecting VA-related crimes. Following FATF standards and national laws, they must perform Customer Due Diligence (CDD), or KYC, i.e., identify and verify the identity of their customers and beneficial owners. They also must keep records, keep track of transactions and CDD data for a specified period. A significant obligation is to report Suspicious Transaction Reports (STRs), i.e., to inform the relevant Financial Intelligence Units (FIUs) of transactions that are suspected of being related to money laundering or terrorist financing. Furthermore, VASPs must follow the Travel Rule, receive, store, and transmit information about the initiator and beneficiary of transactions with VAs during their transfer between VASPs. Failure of VASPs to follow these obligations considerably complicates the detection and investigation of crimes, creating blind spots for law enforcement agencies.

Modern technology forms an integral part of the process of detecting VA offences. Blockchain analysis software developed by companies such as Chainalysis, TRM Lab, Crystal Blockchain, Elliptic, allows tracking transactions in public blockchains, clustering wallet addresses, identifying links to known criminal actors, such as darknet markets, sanctioned addresses, mixers, and assessing risks. AI and machine learning are increasingly being used to detect abnormal patterns of behaviour that may indicate fraud or money laundering (Grigg, 2025). The IOCTA report confirmed that AI not only accelerates crime but also requires the development of relevant AI-based defence mechanisms (Europol, 2025b). In the future, the role of AI may extend beyond simple anomaly detection to include predictive analysis to identify potential victims or new types of fraud, as well as automating the initial comparison of evidence. Detection methodologies should be multilayered, combining VASP compliance procedures, technological tools, victim reporting channels, and intelligence gathering. Excessive reliance on a single detection vector is insufficient for effective counteraction.

Forensic features of investigating crimes with virtual assets. Investigation of crimes involving virtual assets is described by a series of specific forensic features driven by the intangible nature of virtual assets, their pseudo-anonymity, cross-border nature, and technological complexity. These features affect all stages of the investigation – from establishing the crime to collecting and evaluating evidence. Establishing *corpus delicti* in VA-related crimes is one of the key issues, as it requires determining the legal status of VAs as the subject of a criminal offence. The intangible nature of VAs and the differences in their legal qualification in different jurisdictions, such as property, data, financial instrument, etc., create challenges. Various types of VA crimes have their unique distinctive forensic indicators. Money laundering is characterised by the use of mixers, such as ChipMixer, tumblers, "chain hopping" – transferring funds through different cryptocurrencies and blockchains to confuse the traces, transferring VAs through

numerous wallets and exchanges, exchanging for anonymous cryptocurrencies Monero, Zcash, using unregulated or offshore VASPs (Europol, 2025a). Fraud is manifested through investment scams with promises of super-profits from investing in VAs, phishing attacks to steal credentials to wallets or exchanges, *pig butchering* schemes that combine romantic scams and investment fraud (INTERPOL, 2024). Ransomware involves a demand for a ransom in VAs, usually Bitcoin or Monero, for decrypting data or not disclosing stolen information. Financing of terrorism and other illegal activities includes the use of VAs to finance terrorist organisations, purchase weapons, drugs due to their relative anonymity and speed of transactions. Crimes on Darknet markets are characterised by the payment for goods and services, including drugs, weapons, stolen data, child pornography, on shadowy online platforms using VAs.

Tracking the flow of virtual assets is based on the analysis of transactions in public blockchains such as Bitcoin, Ethereum, etc., as the principal method of tracking VAs. Specialised software allows visualising the flow of funds, identifying clusters of addresses belonging to the same entity, and identifying links to known risky addresses. However, there are major challenges. Private blockchains and anonymous cryptocurrencies, such as Monero, Zcash, Dash, use technologies of increased anonymity, such as ring signatures, zk-SNARKs, which makes it difficult or impossible to track transactions. Services mixers/tumblers mix VAs of different users, breaking the connection between incoming and outgoing transactions. De-anonymisation of users is a key task, which lies in establishing the real identity of the owner of the wallet address. Methods include analysis of KYC/CDD data from VASP, IP logging, OSINT, analysis of network behaviour, and other investigative measures.

Identification and attribution of perpetrators is a central challenge in investigating VA-related crimes due to the problem of attribution – definitively linking a wallet or transaction to a concrete, legally identifiable person or organisation. This requires a combination of online and offline methods. Data from VASPs, including obtaining KYC/CDD information from exchanges where a criminal may have registered or exchanged VAs for fiat money, is critical. This is why FATF standards, particularly the Travel Rule, which requires VASPs to collect and transmit sender and recipient information, are so critical. Digital traces include the analysis of IP addresses used to access wallets or exchanges, file metadata, data from suspects' computers and mobile devices. OSINT (Open-Source Intelligence) involves collecting information from open sources – social networks, forums, publications – where the criminal could have left traces linking them to certain IP addresses. Conventional methods include interrogating witnesses, victims, conducting searches, and covert investigative actions.

The collection, recording, examination, and evaluation of digital evidence in VA-related offences is based on the fact that such offences leave predominantly digital traces. Sources of such evidence may include crypto wallets, including hardware USB devices, software wallets installed on a PC or smartphone, online wallets with access through a web interface, paper wallets with printed private keys (TRM, n.d.). Their extraction and analysis require specialised knowledge and tools. Data from exchanges includes transaction history, KYC data, and IP logs. Computers, mobile devices, and servers may contain wallet software, private keys, browser history, correspondence, and files related to criminal activity. Methods of seizure and preservation of digital evidence must ensure its integrity, authenticity, and immutability for further use in court (Hlynska & Klepka, 2024). According to Part 1 of Article 99 of the CPC of Ukraine1, electronic evidence falls in the category of documents (Supreme Court Judge Spoke about..., 2021). For their admissibility, proper procedural execution and, in some cases, certification with an electronic digital signature are necessary (Fennych, 2022). Conducting computer and technical examinations, software examinations, and in the future, specialised examinations of virtual assets, is an integral part of the investigation.

The so-called "digital-physical nexus" in forensic investigations is significant. Although VA-related offences are digital, their investigation often requires a combination of the digital and physical worlds. Seizure of hardware wallets, identification of the physical location of servers or suspects through IP address analysis, as well as conventional police work, including surveillance and interrogation, are crucial to the successful crime-solving. The Silk Road case is an example of this, where digital traces led to physical arrests and seizures, including physically hidden private keys (TRM, n.d.).

Virtual assets can include both proceeds of crime, such as stolen cryptocurrency, and instrumentalities of crime, such as cryptocurrency used to pay for illegal goods on the darknet. This duality affects the seizure, confiscation, and even the qualification of the crime. The legal characterisation of VAs as property, data, etc., further exacerbates this issue (Cryptocurrency Bitcoin: Means…, 2019). For instance, in the ChipMixer case, VAs were used as a tool for money laundering. Ukrainian court practice demonstrates difficulties with recognising VAs as "material

[1] Criminal Procedure Code of Ukraine. (2012, April). Retrieved from https://zakon.rada.gov.ua/laws/show/4651-17.

objects" for the purposes of proof (Salamakha, 2024). To systematise information on typical VA-related crimes and their indicators, Table 2 presents a summary of the types of VA crimes.

Table 2. Typologies of virtual asset crime and key forensic indicators

Type of crime	Modus operandi with VAs	Key forensic/red flag indicators
Money laundering	Use of mixers/tumblers, chain-hopping, exchange for anonymous cryptocurrencies, use of unregulated VASPs, rapid turnover through multiple wallets/exchanges.	Structuring of transactions, illogical or overly complex transfer schemes, communication with high-risk addresses (mixers, darknet), use of VASPs in jurisdictions with weak AML/CFT, sudden activity on previously inactive accounts.
Fraud (investment, phishing, pig butchering)	Creation of fake investment platforms, ICOs; theft of private keys/credentials via phishing sites/messages; manipulation of victims to voluntarily transfer VAs.	Promises of unrealistically high profits, pressure to make quick decisions, requests to transfer VAs to unknown wallets, use of fake websites, unverified personal data of "investment managers".
Ransomware	Encryption of the victim's data and demand for a ransom in VAs (often Bitcoin, Monero) for its decryption or non-disclosure.	Receipt of a ransom note with instructions on how to pay the ransom in VA, specifying a concrete wallet address for the ransom, and a short time frame for payment.
Trading on the Darknet	The use of VAs (mainly Bitcoin, Monero) for the anonymous purchase/sale of drugs, weapons, stolen data, malware, and other illegal goods/services.	Transactions leading to or from known addresses of darknet markets, use of Tor or other anonymising networks to access platforms, communication with mixers to conceal the source of funds.
Terrorist financing	Raising and transferring funds for terrorist organisations or individual terrorists using VAs to conceal the source and purpose of payments.	Transactions related to individuals or organisations on sanctions lists, the use of VASPs in regions with high terrorist activity, and the collection of donations in VAs through online platforms related to extremist propaganda.

Source: developed by the author of this study based on D. Ovsianiuk & O. Ustymenko (2024), V.P. Fennych (2022), A. Schmidt (2021)

Anonymity issues and jurisdictional challenges continue to be among the primary hindrances. Overcoming the anonymity provided by some VAs and services, including mixers and private coins, is a major challenge. The cross-border nature of VA offences raises major jurisdictional issues, including obtaining evidence from abroad, extradition of offenders, and enforcement of court decisions. Forensic techniques should be comprehensive, combining online analysis with offline investigation. Legal frameworks should clearly define AML to support seizure and confiscation procedures, while international cooperation is essential for effective attribution in cross-border cases. Pseudo-anonymity and decentralisation create an attribution challenge that increases the reliance on VASP data and international cooperation and leaves the system vulnerable if VASP compliance is weak or cooperation fails.

Analysis of international practices in the investigation of crimes involving virtual assets. Analysis of international practices in detecting and investigating crimes involving virtual assets revealed both shared approaches and substantial differences conditioned by national legal systems, the level of technological development, and law enforcement priorities. Legislative regulation of the circulation of virtual assets and the activities of service providers in this area underlies effective investigation of crimes.

In Ukraine, the adoption of the Law "On Virtual Assets"[1] was a crucial step towards legalising the virtual assets market and defining the rights and obligations of its participants. However, this law has not yet entered into force, which leaves the legal regulation of virtual assets in Ukraine fragmented. The law prescribes the definition of the concept of the VAs, their classification (secured/unsecured, financial VAs), determination of the legal regime of ownership of the VAs, and regulation of the activities of service providers related to the circulation of the VAs, including requirements for obtaining permits. There are significant problems with the implementation of this law and its harmonisation with the current criminal and criminal procedural legislation. Specifically, there is an inconsistency between the

[1] Law of Ukraine No. 361-IX "On Prevention and Counteraction to Legalisation (Laundering) of Proceeds from Crime, Financing of Terrorism and Financing of Proliferation of Weapons of Mass Destruction". (2019, December). Retrieved from https://zakon.rada.gov.ua/laws/show/361-20#Text.

conceptual framework of the draft AML Law and the Criminal Code of Ukraine, which may complicate the qualification of crimes where AML is an object or instrument, especially in the context of Article 209 of the Criminal Code (money laundering)[1]. This is despite the fact that according to the amendments to the Civil Code of Ukraine[2], VAs are considered property (intangible asset), and the absence of a special law in force creates legal uncertainty regarding the procedures for their seizure and confiscation in criminal proceedings.

In the European Union, the key document is the MiCA[3]. The MiCA establishes unified rules for cryptoasset issuers and cryptoasset-related service providers (CASPs), including requirements for authorisation, prudential supervision, consumer protection, and prevention of market manipulation. The regulation aims to harmonise approaches across EU member states and introduce "passporting" for CASPs, enabling them to operate across the EU under a single licence. MiCA also factors in the FATF recommendations, particularly on Travel Rules. The implementation of MiCA is being phased in and is expected to substantially affect the ability to investigate AML crimes by increasing market transparency and enhancing supervision of market participants. This regulation is a significant attempt to harmonise AML regulation in a large economic bloc. Its interaction with existing national laws, such as the early rules for VASPs in Germany (SQUIRE Patton Boggs, 2025), will be a key aspect to observe. It is yet to be seen whether MiCA will spur global convergence or whether other major jurisdictions, such as the US, will continue to follow distinctive paths, creating challenges for international VASPs and investigations (Tran & Matthews, 2025).

In the United States, AML regulation is fragmented and is carried out by different agencies at the federal and state levels (SEC, CFTC, FinCEN, OFAC). The Department of Justice (DOJ) plays a key role in the prosecution of AML crimes. In April 2025, the DOJ issued a memorandum entitled "Ending Regulation by Prosecution"[4], which changed the DOJ's approach by prioritising investigations into cases involving financial harm to investors and the use of VAs for other criminal activities (drug trafficking, terrorism, etc.) and limiting prosecutions for purely regulatory violations unless there is evidence of intent. This indicates an attempt to avoid "regulation by prosecution" and focus on the most socially dangerous manifestations.

Switzerland follows a principle-oriented and technology-neutral approach, applying existing financial legislation to the use of VAs. The FINMA (2022) classifies crypto assets based on their economic function and applies the relevant regulations (e.g., on banking, financial market infrastructure, anti-money laundering). The adoption of the so-called DLT Bill in 2020 amended existing laws to integrate crypto assets and distributed ledger technologies, making the Swiss regulatory framework one of the most progressive. In Germany, the Federal Financial Supervisory Authority (BaFin) has been regulating certain cryptoasset-related services (e.g., crypto storage) since 2020 (SQUIRE Patton Boggs, 2025). Germany is actively implementing the MiCA, endowing the BaFin with the relevant supervisory powers. The BKA also plays a vital role in the investigation of AML crimes. In Singapore, the Monetary Authority of Singapore (MAS) is the key regulator. The Payment Services Act (PSA) sets out the framework for the licensing and supervision of digital payment token service providers (DPTSPs), including AML/CFT requirements. Singapore is committed to following the FATF standards (Charltons Quantum, 2025). The FATF (2024) Recommendations, particularly No. 15 on emerging technologies and the Travel Rule, are fundamental to global efforts to combat money laundering and terrorist financing through VAs. The Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (2023) reports assess the progress of member states in implementing these standards and identify crime typologies.

Most regulatory frameworks (MiCA, FATF) focus on identified intermediaries (VASP/CASP). However, the growth of decentralised finance (DeFi), decentralised autonomous organisations (DAOs) and non-custodial wallets poses a considerable challenge to this intermediary-focused regulatory model. The FATF (2021) guidance mentions DeFi as an area of ongoing monitoring. MiCA is mainly aimed at CASPs. The nature of DeFi is to eliminate intermediaries, which creates a fundamental tension: regulators seek to impose obligations on entities, while DeFi aims to eliminate these entities. This could become a serious gap in the future. Table 3 summarises the regulatory approaches to virtual assets and VASPs in selected jurisdictions.

[1] Criminal Code of Ukraine. (2001, April). Retrieved from https://zakon.rada.gov.ua/laws/show/2341-14#Text.
[2] Civil Code of Ukraine. (2003, January). Retrieved from ttps://zakon.rada.gov.ua/laws/show/435-15#Text.
[3] Regulation of the European Parliament and of the Council No. 2023/1114 "On Markets in Crypto-Assets, and amending Regulations (EU) No. 1093/2010 and (EU) No. 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 (MiCA)". (2023, May). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:4626998.
[4] Memorandum of the Deputy Attorney General of the Ministry of Justice of U.S. (2025, April). Retrieved from https://www.justice.gov/dag/media/1395781/dl?inline.

Table 3. Overview of regulatory approaches to virtual assets and VASPs in selected jurisdictions

Jurisdiction/ Organisation	Key regulation(s)	Requirements for licensing/ registration of VASPs	Key AML/CFT obligations (incl. Travel Rule)	Supervisory authority(ies)
Ukraine	Law of Ukraine No. 361-IX[1]	Permit to provide services related to the turnover of VAs (4 types of activities)	General AML/CFT requirements apply; implementation of the Travel Rule is expected with the full launch of the market	NSSMC, NBU
EU	MiCA[2]	Authorisation as a Crypto-Asset Service Provider	Comprehensive AML/CFT requirements, including Travel Rule, capital requirements, risk management	National Competent Authorities (NCA), ESMA, EBA
USA	Bank Secrecy Act (BSA), SEC, CFTC, FinCEN regulations, DOJ policy[3]	Registration as a Money Services Business (MSB) for certain VASPs; licensing at the state level	AML programme requirements, STR, KYC/CDD, Travel Rule implementation	FinCEN, SEC, CFTC, DOJ, IRS
Switzerland	DLT Bill (amendments to existing laws), Anti-Money Laundering Act[4]	FinTech licence or banking licence for certain activities (e.g., custody services)	AMLA, KYC/CDD compliance, joining a self-regulatory organisation (SRO) for AML supervision	FINMA, SROs
Germany	Implementation of MiCA, Act on the Supervision of Markets for Crypto-Assets[5]	BaFin licence for cryptocustody and other crypto services	AML/CFT requirements under German law and MiCA	BaFin
Singapore	Payment Services Act (PSA), Financial Services and Markets Act[6]	Major Payment Institution (MPI) licence for Digital Payment Token Service Providers (DPTSP)	Strict AML/CFT, KYC/CDD, STR requirements, implementation of the Travel Rule	Monetary Authority of Singapore (MAS)
FATF	FATF (2024) recommendations (particularly R.15)	VASP licensing or registration	Risk-based approach, CDD, record retention, STR, Travel Rule	National supervisory authorities

Source: developed by the author

The most significant difference is between comprehensive regulatory frameworks and fragmented approaches. The European Union with MiCA represents the most comprehensive approach, creating uniform rules for all member states and introducing detailed capital and risk management requirements, which is in stark contrast to the US model, where regulation is distributed among multiple federal agencies without a single coordinating structure. The differences in licensing of VASPs are particularly noteworthy. Singapore requires a Major Payment Institution licence, which indicates high barriers to entry and strict controls, while the US relies on registration as a Money Services Business with additional licensing at the state level, creating a complex multi-tiered system. Switzerland demonstrates the most flexible approach, allowing a choice between a FinTech licence and a banking licence depending on the type of activity. The difference in supervisory structures is critical. Germany and Singapore have centralised supervisory authorities (BaFin and MAS, respectively), which ensures fast decision-making and policy coherence. In contrast, the US has the most fragmented system with five different federal agencies, which can lead to conflicts of jurisdiction and inconsistent enforcement.

The implementation of the Travel Rule reveals differing speeds of adaptation to international standards. While the EU, the US, and Singapore have already fully implemented the rule, Ukraine is only planning to implement it with a full market launch, which may create gaps in international transaction tracking. This is of critical significance for law enforcement agencies, as the effectiveness of cross-border crime investigations directly depends on the existence of unified standards for the exchange of information between VASPs from different countries.

[1] Law of Ukraine No. 361-IX "On Prevention and Counteraction to Legalisation (Laundering) of Proceeds from Crime, Financing of Terrorism and Financing of Proliferation of Weapons of Mass Destruction". (2019, December). Retrieved from https://zakon.rada.gov.ua/laws/show/361-20#Text.

[2] Regulation of the European Parliament and of the Council No. 2023/1114 "On Markets in Crypto-Assets, and amending Regulations (EU) No. 1093/2010 and (EU) No. 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 (MiCA)". (2023, May). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:4626998.

[3] Memorandum of the Deputy Attorney General of the Ministry of Justice of U.S. (2025, April). Retrieved from https://www.justice.gov/dag/media/1395781/dl?inline.

[4] Anti-Money Laundering Act of Switzerland. (1997, October). Retrieved from https://www.fedlex.admin.ch/eli/cc/1998/892_892_892/en.

[5] Law on the Supervision of Markets for Crypto Assets of the Federal Republic of Germany. (2024, December). Retrieved from https://www.gesetze-im-internet.de/kmag/BJNR1B60B0024.html.

[6] Payment Services Act of Singapore. (2019, January). Retrieved from https://sso.agc.gov.sg//Act/PSA2019.

Law enforcement agencies and specialised units. The effectiveness of investigating VA-related offences largely depends on the availability of specialised units in law enforcement agencies and their interaction. National approaches are characterised by distinct organisational models. In the United States, historically, different agencies, such as Homeland Security Investigations (HSI), Internal Revenue Service-Criminal Investigation (IRS-CI), and Federal Bureau of Investigation (FBI), have had specialised teams to combat cryptocurrency crime. The National Crypto Enforcement Team (NCET) was created to coordinate efforts but was subsequently disbanded and its functions transferred to the Computer Crime and Intellectual Property Section (CCIPS) of the DOJ Criminal Division. This move may reflect a strategy to integrate cryptocurrency expertise into broader cybercrime structures rather than isolate it, although the effectiveness of this approach is yet to be seen.

In Germany, the BKA has specialised departments, such as the Serious and Organised Crime Division and the Cybercrime Division, which are dedicated to investigations related to VA. The BKA (2025) also conducts research projects, such as BITCRIME, to investigate the use of virtual currencies in financial crime (Forschungsprojekte zu Cybercrime..., n.d.). There is close cooperation between the BKA and BaFin (Cryptonovaint.net: BaFin..., 2025). In Singapore, the Commercial Affairs Department (CAD)[1] is the principal agency for investigating white-collar crimes, including those related to VAs. It cooperates closely with the MAS. CAD has specialised units such as the Investment Fraud Investigation Unit and the Financial Crimes Investigation Unit.

In Ukraine, the Cyber Police Department of the National Police of Ukraine, the State Bureau of Investigation (SBI), the National Anti-Corruption Bureau of Ukraine (NABU), the Security Service of Ukraine (SSU), the Bureau of Economic Security of Ukraine (BES), the State Bureau of Investigation (SBI) and the State Investigation Service (SIS) are involved in investigating VA crimes. The effectiveness of their work depends on the level of specialisation, technical equipment, and interagency coordination.

International organisations also play a vital role. Europol, through the European Cybercrime Centre (EC3) and the European Financial and Economic Crime Centre (EFECC), supports EU Member States in the fight against cybercrime and financial crime related to VAs. Europol publishes significant analytical reports, such as SOCTA (Serious and Organised Crime Threat Assessment) and IOCTA (Internet Organised Crime Threat Assessment), which analyse trends in VA crime (Europol, 2025a; Europol, 2025b). INTERPOL (2024) through the Financial Crime and Anti-Corruption Centre (IFCACC), coordinates international efforts to combat financial crime, including those related to cryptocurrencies. Interpol develops guidelines for law enforcement and facilitates information exchange. These organisations play a crucial role in coordinating cross-border investigations, sharing intelligence and best practices, and providing training for law enforcement. The critical role of public-private partnerships is also evident. Many sources emphasise the cooperation of law enforcement agencies with blockchain analytics firms, exchanges, and other private sector entities (Grigg, 2025). This suggests that law enforcement agencies cannot handle AML crime alone due to rapid technological development and private sector control over key data and infrastructure.

Investigation cases, methods, and tools. The arsenal of methods and tools used to investigate VA crimes is constantly expanding. Blockchain analysis software includes tools such as Chainalysis, TRM Lab, Crystal Blockchain, Elliptic, which are key to tracking transactions in public blockchains. They allow visualising VA flows, identifying clusters of addresses likely to belong to the same entity, identifying links to known risky entities (darknet markets, mixers, sanctioned addresses), and assessing the risks of individual transactions or wallets. OSINT (Open-Source Intelligence) methods involve collecting and analysing information from open sources (social networks, forums, publications, websites), which can help identify links between real people and their activities on the Internet, find advertisements for the sale of illegal goods on the Internet, or identify participants in fraudulent schemes (OSINT Industries Team, 2025).

Undercover operations are also used when law enforcement agencies conduct covert operations by infiltrating criminal groups operating on the Internet or conducting controlled purchases on darknet markets to collect evidence and identify criminals. An example is Operation Dark Gold in the United States (HSI New York..., 2019). VAs is physically seized because private keys to VAs can be stored on physical media (hardware wallets, computers, paper-based media, flash drives), and therefore their detection and seizure during searches is an essential element of the investigation. This requires investigators to know where to look for such media and how to safely seize them. Interaction with VASPs involves obtaining data from VASPs (KYC information, transaction history, IP logs) through official requests (subpoenas, warrants) is critical to de-anonymising users and

[1] Joint Statement by Commercial Affairs Department, Singapore Police Force (CAD) & Monetary Authority of Singapore (MAS). (2025, June). Retrieved from https://www.mas.gov.sg/regulation/enforcement/enforcement-actions/2025/civil-penalty-action-taken-against-gui-boon-sui-for-false-trading-and-unauthorised-trading.

tracing the flow of funds, especially when VAs are transferred to a monetary market for exchange for fiat money or other assets. Notably, the "toolkit" is broader than just software. An effective investigation requires a combination of OSINT (OSINT Industries Team, 2025), covert methods, digital forensics for device analysis, legal tools (requests, warrants) and international cooperation mechanisms (MLAT) (COPOLAD, 2025). There is a kind of "arms race" in the field of de-anonymisation. Criminals are using mixers, tumblers, private coins, and chain-hopping for obfuscation. Investigators use advanced analytics, cross-chain tracing, and attempt to link pseudonymous activity to real individuals through VASP data or other means. The success of de-anonymisation often depends on identifying a "weak link", such as a transaction that passes through a compliant VASP that stores KYC data.

American authorities have the broadest powers, including civil forfeiture and access to advanced blockchain analytics technologies, while Ukrainian investigators face limitations due to incomplete implementation of legislation and limited access to specialised tools. The European model focuses on coordination and information exchange between national authorities, striking a balance between sovereignty and efficiency, while the German approach combines systematic cooperation with regulators and participation in research projects to develop the methodological framework for investigations.

The cross-border nature of VA offences makes international cooperation an essential element of effective investigation. Jurisdictional issues and mutual legal aid treaties (MLATs) pose major challenges, as determining jurisdiction in cases where criminals, victims, VASPs, and servers may be located in different countries is a complex task. Conventional MLATs are often slow and bureaucratic, which is incompatible with the speed of VA-related operations. Criminals can move VAs across multiple jurisdictions in minutes, while an MLAT request can take months to process. This creates a "speed mismatch" that is actively exploited by criminals. To accelerate the exchange of operational information, mechanisms for exchanging information through Europol channels (e.g., SIENA – Secure Information Exchange Network Application) and Interpol (I-24/7 secure communication system) are used. These platforms allow law enforcement agencies from different countries to exchange data and coordinate actions in a near real-time mode. Approaches and standards are being harmonised through the efforts of the FATF, MONEYVAL, and the EU (through MiCA), which are aimed at harmonising legislation, regulatory requirements for VASPs, and investigation standards. This should facilitate international cooperation. Speed of response continues to be a challenge, as even with information exchange channels in place, the speed of response to cross-border requests, especially for freezing or seizure of the VAs, is still problematic. This requires not only formal but also informal channels of cooperation. Considering the limitations of formal channels, there is a growing reliance on informal law enforcement networks and direct cooperation with foreign VASPs (where legally permitted) to expedite urgent requests (e.g., freezing of accounts). The role of financial intelligence units (FIUs) and their networks (e.g., Egmont Group) is also critical here. Best practices include the establishment of Joint Investigation Teams (JITs), the use of direct channels of communication between law enforcement agencies, the development of standardised request forms, and the active use of Europol and Interpol.

The analysis of concrete criminal proceedings offers a better insight into the methods of investigating VA offences, the challenges faced by law enforcement agencies, and the success factors. Analysis of international cases demonstrates different approaches. The Silk Road case was one of the first high-profile cases involving the use of Bitcoin in the darknet market to trade drugs and other illicit goods. The investigation conducted by the FBI, IRS-CI, and other US agencies demonstrated the ability to track Bitcoin transactions, the significance of identifying operational security errors (OPSEC failures) on the part of criminals (e.g., Ross Ulbricht's use of the same pseudonym in different forums, which allowed linking him to Silk Road), as well as the effectiveness of combining digital forensics with conventional investigative methods, including undercover work and physical seizure of evidence (e.g., Ulbricht's laptop with keys to Silk Road wallets, seizure of physical media with keys hidden in a popcorn tin in another related case) (IVPN, 2025). Many successful VA investigations, like the Silk Road case, hinge on OPSEC errors made by criminals, rather than solely on encryption or blockchain anonymity breaches.

The case of ChipMixer, mentioned in the EU report (Europol, 2025a), illustrates the struggle against large cryptocurrency mixing services. ChipMixer was suspected of laundering billions of dollars in Bitcoin, much of which was linked to darknet markets, ransomware, and other criminal activity. The investigation required sophisticated blockchain analysis to de-anonymise the flow of funds passing through the mixer and international cooperation to shut down the service. The German BKA's investigation of Chemical Revolution, a large online drug trafficking platform (Lott, 2025), showed that significant amounts of customer data were seized during the operation, leading to numerous subsequent proceedings. Interestingly, as one analysis noted, the investigation showed that the creation of such a platform required only an "informal association of the necessary experts", which

indicated a reduction in the barriers to entry into cybercrime (Arzt *et al.*, 2021).

Operation Dark Gold (USA) was an undercover operation conducted by Homeland Security Investigations (HSI), which lied in infiltrating the darknet to identify sellers of drugs and other illegal goods who used cryptocurrencies for payments (HSI New York..., 2019). The operation resulted in numerous arrests and seizures of significant amounts of cash, cryptocurrencies, weapons, and drugs, demonstrating the effectiveness of undercover methods in the fight against cryptocurrency crime. The "follow the money" principle still applies, but with new nuances. Tracking VAs is the digital equivalent of tracking conventional cash flows. However, the "money" can be transformed (channelling), pass through unregulated entities, and instantly cross borders, requiring new tools and international cooperation on an unprecedented scale.

Relevant Ukrainian judicial practice and investigative experience show that the judicial practice on VA offences in Ukraine is still being developed, but there are already some precedents. The cases cited in the source (Salamakha, 2024) handled the use of cryptocurrencies to launder the proceeds of theft and fraud, as well as fraud schemes exploiting banking system vulnerabilities to illegally obtain funds and convert them into VAs. The key problems in Ukrainian practice include the qualification of crimes, particularly the challenges with defining the VAs as an object of crime under the current Criminal Code, the proof, i.e., the collection and presentation to the court of relevant and admissible evidence confirming the movement of VAs, their connection with criminal activity and the identity of the perpetrators, as well as the seizure and confiscation of VAs due to the lack of clear legislative procedures for the seizure, storage, and confiscation of VAs. In some cases, courts have recognised VAs as material evidence, which is controversial considering their intangible nature, while seizure to ensure possible confiscation of property is considered a more reasonable approach. These cases highlight the urgent need to adapt Ukrainian legislation and forensic techniques to the specifics of VA offences.

Discussion

The findings of the study on the methodologies for detecting and forensic features of investigating crimes with virtual assets demonstrated convergence with current trends in the development of digital forensics, which was confirmed by a series of international studies in related fields. This convergence indicated the development of a new paradigm of forensic analysis that extends beyond conventional investigative methods.

The specific features of collecting and analysing digital evidence in crimes involving virtual assets identified in the present study showed a significant correlation with the findings of S. Seo *et al.* (2023) on the development of a framework for digital forensic investigations in the metaverse. The structural correspondence is manifested in the five-stage approach (identification, preservation, collection, analysis, and presentation of evidence), which fully coincided with the conclusions obtained regarding the need for a multi-stage approach to working with virtual assets. Of particular significance is the correlation between the problems of preserving volatile digital traces and the challenge of identifying users through pseudonymous profiles, which directly corresponds to the identified challenges of anonymisation in the field of virtual assets. The rationale for the need to develop specialised tools for working with immersive technologies extrapolates to the need to create specific methodologies for the different types of virtual assets identified in the current study.

The identified problems of standardisation of approaches to investigating crimes with virtual assets were fully confirmed in the study by M. Saleh *et al.* (2023), who developed a meta-modelling approach for forensic investigations of IoT. Methodological compliance is manifested in the creation of a comprehensive taxonomy with four main categories, which structurally coincides with the classification of methods of working with virtual assets developed in the present study. The fundamental significance of a unified methodological framework based on ISO/IEC 27043 (2015) directly correlates with the present study's conclusions on the critical need for standardisation of approaches to virtual assets. The problem of terminological inconsistency between different jurisdictions identified in the current study was fully supported by the rationale for the need for international harmonisation of standards.

The value of preserving the integrity of digital evidence identified in the present study was strongly supported by C. Karagiannis & K. Vergidis (2021) in their research on legal challenges in the field of digital evidence and cloud forensics. The systemic correlation is manifested in the key challenges of ensuring the chain of custody of evidence in distributed systems, which directly corresponds to the specifics of blockchain technologies for virtual assets. The problems of data authentication in the absence of centralised control and the issue of territorial jurisdiction when storing evidence in cloud services of different countries are directly related to the identified problems of seizure and confiscation of virtual assets. The proposed legal model of a "forensic exceptional situation" correlated with the conclusions of the present study regarding the need to develop special procedural mechanisms for handling virtual assets.

Through an empirical analysis of twelve popular applications, M.M. Mirza *et al.* (2022) detailed the

features of mobile forensics in the context of Web3 wallets identified in the current study. Then technical correlation is manifested in the identified critical differences in private key storage between operating systems: the use of an encrypted keystore in Android with the possibility of rooting-based recovery compared to Secure Enclave in iOS. The conclusions regarding the specific challenges of mobile forensics, including the problems of obtaining root/jailbreak access and the complexity of decryption through hardware security modules, directly complemented the findings of the present study on the value of understanding the technological specifics of different types of virtual asset wallets and the need for differentiated approaches depending on the platform.

The developed approaches to digital forensics in virtual worlds were further substantiated by T. Al Ali *et al.* (2023), which creates a fundamentally new type of digital trace through the identification of unique sources of evidence in VR environments. The conceptual correlation lies in the need for technological adaptation of investigative techniques to the evolution of virtual assets towards more complex ecosystems, which is fully consistent with the present study's conclusions on the need for constant adaptation of tools.

The established significance of computer forensics was confirmed by a systematic study by S. Drobotov *et al.* (2023), which included an analysis of more than 200 software solutions and technology platforms. The results of a comparative analysis of the effectiveness of various technical tools, including an assessment of processing speed, detection accuracy, and usability, directly correlated with the current study's conclusions on the critical need to use specialised blockchain analytics software, such as Chainalysis, TRM Lab, Crystal Blockchain, and Elliptic. The identified trends in the automation of data collection processes and the integration of artificial intelligence to identify patterns of criminal behaviour are fully consistent with the findings on the significance of constantly updating the technological arsenal.

The identified trends in the modernisation of forensic tools were confirmed in the comprehensive systematisation presented by D. Rawtani & C.M. Hussain (2023), which included an analysis of more than 500 technological solutions from 45 countries. The concept of a "technological arms race" between criminals and law enforcement, where the success of investigations critically depends on the ability to adapt tools faster than criminals, is fully consistent with the findings of the present study on the need to constantly adapt tools to the evolution of virtual assets, including anonymisation technologies, decentralised finance, and private cryptocurrencies.

The developed principles of validation of the reliability of forensic techniques were theoretically substantiated in the Reliability Validation Enabling Framework (RVEF) by R. Stoykova & K. Franke (2023). The Framework with four key components (methodological validation, technical verification, procedural standardisation, and legal admissibility) creates a methodological basis for standardising approaches to the investigation of crimes involving virtual assets. The proposal to create an international accreditation system for forensic laboratories working with digital evidence directly complements the present study's findings on the need to harmonise international approaches.

The identified factors influencing the implementation of IT forensic tools correlated with the empirical analysis of H. Alshurafat *et al.* (2024) based on the extended Technology Acceptance Model (TAM). The identified key determinants of successful implementation and the biggest barriers (high staff training costs, complexity of integration with existing systems, insufficient technical support) are fully consistent with the identified problems of implementing specialised tools for working with virtual assets. The significant regional differences in readiness to implement the latest technologies correlate with the current study's conclusions on the need for specialised training.

The prospects for the use of emerging technologies in digital forensics were developed in a comprehensive analysis by A.K. Mishra *et al.* (2024), who created a roadmap for technological development until 2030. The revolutionary potential of quantum algorithms for decrypting complex cryptographic systems can dramatically change the landscape of investigating crimes involving anonymous cryptocurrencies, which is directly in line with the trends predicted in the current study. The concept of federated machine learning systems for forensic analysis, which allow training models on distributed datasets without violating confidentiality, directly complements the study's conclusions on future areas for the development of virtual asset investigation methodologies.

The developed approaches to mitigating cybercrime were confirmed by a systematic review presented by A.A. Kazaure *et al.* (2023), which analysed 156 scientific publications for 2018-2023. The developed taxonomy of digital forensic approaches with reactive, proactive, and hybrid models demonstrated a 35% greater efficiency of hybrid approaches in detecting complex multi-stage attacks. The conclusions on the effectiveness of a multi-layered security architecture and the significance of integrating technical and organisational measures are fully correlated with the results of the present study on the need for a multi-layered approach to detecting crimes with virtual assets.

The established significance of natural language processing technologies was substantiated by D. Sun *et al.* (2021), who developed a platform for

digital forensic investigations based on NLP. The demonstrated 87% accuracy in detecting suspicious communications and 82% accuracy in identifying money laundering schemes through the analysis of linguistic patterns provided a strong basis for expanding the capabilities of AI in the investigation of virtual asset crimes, especially in the context of analysing communications on cryptocurrency forums and darknet markets. The predicted trends in the development of cybercrime correlate with the futuristic analysis of S. Saharan *et al.* (2024) on the evolution of cyber threats in the metaverse. The forecast of a 15-20 – fold increase in cybercrime over the next decade underscored the criticality of adapting law enforcement strategies. The recommendations for the development of proactive approaches, including predictive policing based on big data analysis and international platforms for the exchange of information on cyber threats, are fully consistent with the findings of the current study on the development of proactive approaches to detecting crimes with virtual assets.

The developed theoretical framework for the integration of payment systems and forensic accounting was practically embodied in the "3M" theory (Money, Method, Motive) presented by A.O. Efuntade & O. Efuntade (2023) based on an empirical study of 1,247 cases of financial crime in 34 countries. The multi-dimensional analysis matrix, which combines quantitative financial data with qualitative analysis of behavioural patterns, provides a powerful methodological framework for a comprehensive approach to the analysis of virtual asset crime, especially in the context of complex international money laundering schemes. Summarising the results of the comparative analysis, it was found that the conclusions obtained are not only in line with the current trends in the development of digital forensics but also correlate with the findings of leading international studies in all key aspects of the issue. The identified convergence of the conclusions of different research groups regarding the need for technological modernisation of law enforcement agencies, development of international cooperation, and creation of unified standards for handling digital evidence confirmed the validity of the findings obtained and their relevance to the global scientific discourse in the field of virtual asset forensics.

Conclusions

The present study offered a comprehensive analysis of the methodologies for detecting and forensic features of investigating crimes involving virtual assets through a comparison of international practices. The study found a critical absence of a unified international definition of virtual assets, which creates significant gaps in criminal law qualifications, especially regarding Article 209 of the Criminal Code of Ukraine and complicates the procedures for seizure and confiscation of assets in cross-border cases. It was found that high efficiency of investigation is achieved through the multilayered integration of proactive approaches to monitoring Virtual Asset Service Provider (VASP), reactive measures of law enforcement agencies, the use of specialised software Chainalysis, TRM Lab, Crystal Blockchain, Elliptic for blockchain analytics and Open Source Intelligence (OSINT) methods. The study demonstrated the criticality of combining digital and traditional forensic methods for effective user de-anonymisation. Specific forensic indicators of five main types of virtual asset crimes were systematised: structuring transactions in money laundering, promises of unrealistic returns in investment fraud, ransom demands in Bitcoin or Monero in ransomware, connections to darknet addresses in illicit trafficking, and transactions with sanctioned lists in terrorist financing. This systematisation creates a practical toolkit for quickly classifying criminal activity. The comparative analysis of five key jurisdictions demonstrated a dramatic diversity of regulatory approaches, from the technology-neutral Swiss principle-based regulation to the comprehensive European MiCA with unified requirements. Ukrainian legislation must be improved in terms of harmonisation with criminal law.

Prospects for further research include the development of unified international standards for the qualification of crimes with virtual assets, the creation of automated systems for detecting criminal patterns based on artificial intelligence, the study of the specifics of investigating crimes involving decentralised finance (DeFi), and the development of methods for working with new types of virtual assets in the meta-universe.

Acknowledgements

None.

Funding

The study was not funded.

Conflict of Interest

None.

References

[1] Agarwal, U., Rishiwal, V., Tanwar, S., & Yadav, M. (2024). Blockchain and crypto forensics: Investigating crypto frauds. *International Journal of Network Management*, 34(2), article number e2255. doi: 10.1002/nem.2255.

[2] Al Ali, T., Alfulaiti, S., Abuzour, M., Almaqahami, S., & Ikuesan, R. (2023). Digital forensic in a virtual world: A case of metaverse and VR. In *ECCWS 2023 22nd European conference on cyber warfare and security* (pp. 12-21). Reading: Academic Conferences and Publishing Limited.
[3] Alshurafat, H., Shbail, M.O.A., & Almuiet, M. (2024). Factors affecting the intention to adopt IT forensic accounting tools to detect financial cybercrimes. *International Journal of Business Excellence*, 33(2), 169-190. doi: 10.1504/IJBEX.2024.139917.
[4] Arzt, C., Hirschmann, N., Hunold, D., Lüders, S., Meißelbach, C., Schöne, M., Sticher, B. (Eds.). (2021). *Perspectives on police research. FÖPS Berlin*. Berlin: Arbeitskreis Empirische Polizeiforschung. doi: 10.4393/opushwr-3370.
[5] BKA. (2025). *Accessible organisational chart of the Federal Criminal Police Office*. Retrieved from https://www.bka.de/DE/DasBKA/OrganisationAufbau/Organigramm/organigramm_node.html.
[6] Blockchain Intelligence Group. (2025). *Law enforcement resource guide for cryptocurrency investigations*. Retrieved from https://blockchaingroup.io/wp-content/uploads/2025/02/Law-Enforcement-Resource-Guide-for-Cryptocurrency-Investigations-.pdf.
[7] Charltons Quantum. (2025). *An overview of the regulation of virtual assets in Singapore*. Retrieved from https://charltonsquantum.com/wp-content/uploads/docs/singapore-crypto-guide.pdf.
[8] Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism. (2023). *Typologies report on money laundering and terrorist financing risks in the world of virtual assets*. Strasburg: Council of Europe.
[9] COPOLAD. (2025). *Navigating cryptocurrency-driven crime: A guide for law enforcement*. Retrieved from https://copolad.eu/en/cryptocurrency-law-enforcement/.
[10] Cryptocurrency Bitcoin: Means of payment or financial instrument from the perspective of BaFin? (2019). Retrieved from https://www.roedl.de/themen/rechtsberatung/kryptowaehrung-bitcoin-zahlungsmittel-finanzinstrument-bafin.
[11] Drobotov, S., Pertsev, R., Hrab, M., Fedytnyk, V., Moroz, S., & Kikalishvili, M. (2023). Forensic research of the computer tools and systems in the fight against cybercrime. *Journal of Information Technology Management*, 15(1), 135-162. doi: 10.22059/jitm.2023.90741.
[12] Efuntade, A.O., & Efuntade, O. (2023). Internet payment system, forensic accounting and forensic investigation: 3M theory in the financial frauds. *Journal of Accounting and Financial Management*, 9(7), 115-130. doi: 10.56201/ijssmr.v8.no1.2022.pg32.40.
[13] Europol. (2025a). *The changing DNA of serious and organised crime*. Retrieved from https://fiaumalta.org/app/uploads/2025/03/Mar-2025-Serious-and-Organised-Crime-Threat-Assessment-SOCTA-2025_Part1.pdf.
[14] *Europol*. (2025b). Internet Organised Crime Threat Assessment (IOCTA). Retrieved from https://www.europol.europa.eu/cms/sites/default/files/documents/Steal-deal-repeat-IOCTA_2025.pdf.
[15] Faqir, R.S. (2023). Digital criminal investigations in the era of artificial intelligence: A comprehensive overview. *International Journal of Cyber Criminology*, 17(2), 77-94.
[16] FATF. (2021). *Updated guidance for a risk-based approach for virtual assets and virtual asset service providers*. Paris: FATF.
[17] Fennych, V.P. (2022). Evaluation of electronic evidence in civil proceedings (on examples of specific categories of court cases). *Scientific Bulletin of Uzhhorod National University. Law Series*, 71, 370-375. doi: 10.24144/2307-3322.2022.71.63.
[18] Financial Action Task Force. (2024). *Virtual assets: Targeted update on implementation of the FATF standards on virtual assets and virtual asset service providers*. Paris: FATF.
[19] FINMA. (2022). *Fact sheet: Cryptoassets*. Retrieved from https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/faktenblaetter/faktenblatt-kryptobasierte-vermoegenswerte.pdf.
[20] Grigg, G. (2025). *Law enforcement in the age of cryptocurrency*. Retrieved from https://www.police1.com/investigations/law-enforcement-in-the-age-of-cryptocurrency.
[21] Hamad, N., & Eleyan, D. (2022). Digital forensics tools used in cybercrime investigation-comparative analysis. *Journal of Xi'an University of Architecture & Technology*, 14(4), 113-127.
[22] Hlynska, N., & Klepka, D.I. (2022). Digitization of criminal proceedings: current aspects of conceptualization (part 1). *Issues of Crime Prevention*, 1(43).
[23] Hossain, M.Z. (2023). Emerging trends in forensic accounting: Data analytics, cyber forensic accounting, cryptocurrencies, and blockchain technology for fraud investigation and prevention. *SSRN*. doi: 10.2139/ssrn.4450488.
[24] HSI New York hosts 1st Annual Cyber Crime Symposium. (2019). Retrieved from https://www.ice.gov/news/releases/hsi-new-york-hosts-1st-annual-cyber-crime-symposium.

[25] INTERPOL. (2024). *Global financial fraud assessment*. Retrieved from https://www.interpol.int/en/content/download/21077/file/24COM005563-01%20-%20CAS_Global%20Financial%20Fraud%20Assessment_Public%20version_2024-03%20v2.pdf.
[26] ISO/IEC 27043:2015 "Information technology – Security techniques – Incident investigation principles and processes". (2015). Retrieved from https://www.iso.org/standard/44407.html.
[27] IVPN. (2025). *Online privacy through OPSEC and compartmentalization – Part 3*. Retrieved from https://www.ivpn.net/privacy-guides/online-privacy-through-opsec-and-compartmentalization-part-3/.
[28] Jitariuc, V., & Nastas, A. (2022). Forensic features of cybercrime. *Romanian Journal of Forensic Science*, 4, 286-294.
[29] Kamenskyi, D.V., & Dudorov, O.O. (2024). Laundering criminal proceeds through virtual currency transactions: A new threat to economic security. *Analytical and Comparative Jurisprudence*, 1, 500-509. doi: 10.24144/2788-6018.2024.01.88.
[30] Karagiannis, C., & Vergidis, K. (2021). Digital evidence and cloud forensics: Contemporary legal challenges and the power of disposal. *Information*, 12(5), article number 181. doi: 10.3390/info12050181.
[31] Kazaure, A.A., Yusoff, M.N., & Jantan, A. (2023). Digital forensics investigation approaches in mitigating cybercrimes: A review. *Journal of Information Science Theory & Practice (JIStaP)*, 11(4), 14-39. doi: 10.1633/JISTaP.2023.11.4.2.
[32] Law Business Research. (2024). *Switzerland: Cryptoassets & blockchain*. Retrieved from https://mll-legal.com/wp-content/uploads/2024/01/Switzerland-Cryptoassets-Blockchain.pdf.
[33] Lott, R. (2025). *Darknet orders of narcotics: Criminal law risks in 2025 – specialist lawyer explains*. Retrieved from https://www.rechtsanwalt-lott.de/darknet-bestellungen-von-betaeubungsmitteln-strafrechtliche-risiken-2025-fachanwalt-klaert-auf/.
[34] Mirza, M.M., Ozer, A., & Karabiyik, U. (2022). Mobile cyber forensic investigations of Web3 wallets on Android and iOS. *Applied Sciences*, 12(21), article number 11180. doi: 10.3390/app122111180.
[35] Mishra, A.K., Hemamalini, V., & Tyagi, A.K. (2024). Digital forensics with emerging technologies: Vision and research potential for future. In *Conversational artificial intelligence* (pp. 675-697). doi: 10.1002/9781394200801.ch37.
[36] Ombu, A. (2023). Role of digital forensics in combating financial crimes in the computer era. *Journal of Forensic Accounting Profession*, 3(1), 57-75. doi: 10.2478/jfap-2023-0003.
[37] OSCE. (2024). *Decoding crypto crime: A guide for law enforcement (table of contents & excerpts)*. Vienna: OSCE.
[38] OSINT Industries Team. (2025). *What is dark web intelligence (DARKInt)? A beginner's guide*. Retrieved from https://www.osint.industries/post/what-is-dark-web-intelligence-darkint-beginners-guide
[39] Ovsianiuk, D., & Ustymenko, O. (2024). Exchange of information as a form of international cooperation in combating drug trafficking. *Novum Jus*, 18(1), 181-216. doi: 10.14718/NovumJus.2024.18.1.7
[40] Ovsianiuk, D. (2024). Intelligence cycle as the basis of analytical activity in combating drug-related crime. *Law Journal of the National Academy of Internal Affairs*, 14(2), 95-104. doi: 10.56215/naia-chasopis/2.2024.95.
[41] Rawtani, D., & Hussain, C.M. (Eds.). (2023). *Modern forensic tools and devices: Trends in criminal investigation*. Hoboken: John Wiley & Sons.
[42] Saharan, S., Singh, S., Bhandari, A.K., & Yadav, B. (2024). The future of Cyber-Crimes and cyber war in the metaverse. In *Forecasting cyber crimes in the age of the metaverse* (pp. 126-148). Hershey: IGI Global Scientific Publishing. doi: 10.4018/979-8-3693-0220-0.ch007.
[43] Salamakha, R. (2024). *Cryptocurrency and criminal proceedings: unusual cases of judicial practice*. Retrieved from https://yur-gazeta.com/dumka-eksperta/kript_ovalyuta-ta-kriminalni-provadzhennya-nezvichni-keysi-sudovoyi-praktiki.html.
[44] Saleh, M., Othman, S.H., Driss, M., Al-dhaqm, A., Ali, A., Yafooz, W.M., & Emara, A.H.M. (2023). A metamodeling approach for IoT forensic investigation. *Electronics*, 12(3), article number 524. doi: 10.3390/electronics12030524.
[45] Samsin, R.I. (2024). Classification of virtual assets. *Central Ukrainian Bulletin of Law and Public Administration*, 2(6), 90-98. doi: 10.32782/cuj-2024-2-12.
[46] Schmidt, A. (2021). Virtual assets: Compelling a new anti-money laundering and counter-terrorism financing regulatory model. *International Journal of Law and Information Technology*, 29(4), 332-363. doi: 10.1093/ijlit/eaac001.
[47] Schwarz, N., Chen, M.K., Poh, M.K., Jackson, M.G., Kao, K., Fernando, M.F., & Markevych, M. (2021). *Virtual assets and anti-money laundering and combating the financing of terrorism: Some legal and practical considerations*. Washington: International Monetary Fund.

[48] Seo, S., Seok, B., & Lee, C. (2023). Digital forensic investigation framework for the metaverse. *The Journal of Supercomputing*, 79(9), 9467-9485. doi: 10.1007/s11227-023-05045-1.
[49] SQUIRE Patton Boggs. (2025). *Update of German law aspects of crypto assets*. Retrieved from update-of-german-law-aspects-of-crypto-assets.pdf.
[50] Stoykova, R., & Franke, K. (2023). Reliability validation enabling framework (RVEF) for digital forensics in criminal investigations. *Forensic Science International: Digital Investigation*, 45, article number 301554. doi: 10.1016/j.fsidi.2023.301554.
[51] Sun, D., Zhang, X., Choo, K. K. R., Hu, L., & Wang, F. (2021). NLP-based digital forensic investigation platform for online communications. *Computers & Security*, 104, article number 102210. doi: 10.1016/j.cose.2021.102210.
[52] Supreme Court judge spoke about judicial practice regarding the evaluation of electronic evidence in criminal proceedings within the HELP course "Cybercrime and electronic evidence". (2021). Retrieved from https://supreme.court.gov.ua/supreme/pres-centr/news/1750192/.
[53] TRM. (n.d.). *Enhancing law enforcement's role in expanding the U.S. Strategic Bitcoin Reserve*. Retrieved from https://www.trmlabs.com/resources/blog/enhancing-law-enforcements-role-in-expanding-the-us-strategic-bitcoin-reserve.
[54] Tsai, F.C. (2021). The application of blockchain of custody in criminal investigation process. *Procedia Computer Science*, 192, 2779-2788. doi: 10.1016/j.procs.2021.09.048.
[55] Wu, J., Lin, K., Lin, D., Zheng, Z., Huang, H., & Zheng, Z. (2023). Financial crimes in web3-empowered metaverse: Taxonomy, countermeasures, and opportunities. *IEEE Open Journal of the Computer Society*, 4, 37-49. doi: 10.1109/OJCS.2023.3245801.
[56] Yarotskyi, V.O. (2023). Concepts and types of virtual assets that may be in circulation according to the legislation of Ukraine. *Scientific Notes of V.I. Vernadsky Ternopil National University. Series: Legal Sciences*, 34(3), 101-107. doi: 10.32782/TNU-2707-0581/2023.4/15.

Методологія виявлення та криміналістичні особливості розслідування злочинів, пов'язаних з віртуальними активами: порівняльний аналіз міжнародної практики

Дмитро Овсянюк
Аналітичний відділ (Центр кримінальної аналітики)
Національна академія внутрішніх справ
03035, пл. Солом'янська, 1, м. Київ, Україна
https://orcid.org/0000-0002-1846-4167

Андрій Онушко
Кандидат юридичних наук
Департамент кіберполіції Національної поліції України
02093, вул. Бориспільська, 19, м. Київ, Україна
https://orcid.org/0009-0003-3627-2489

Євгеній Панченко
Департамент міжнародного поліцейського співробітництва
Національної поліції України
01024, вул. Академіка Богомольця, 1, м. Київ, Україна
https://orcid.org/0000-0001-5755-7457

■ **Анотація.** Мета цього дослідження полягає у визначенні на основі порівняльного аналізу міжнародної практики найефективніших підходів до розслідування злочинів, пов'язаних з віртуальними активами. Дослідження базувалося на систематичному аналізі законодавчих актів і нормативних документів. Було використовувало методи порівняльного правового аналізу для дослідження регуляторних підходів різних юрисдикцій, систематичний підхід для вивчення взаємозв'язків між елементами системи запобігання злочинам, структурно-функціональне дослідження ролі різних суб'єктів. Дослідження виявило критичну відсутність єдиного міжнародного визначення віртуальних активів, що створює прогалини у кваліфікації кримінального права, особливо щодо статті 209 Кримінального кодексу України, та процедур арешту й конфіскації активів у транскордонних справах. Було встановлено, що найбільша ефективність розслідування досягається завдяки багаторівневій інтеграції проактивних підходів до моніторингу постачальників послуг з віртуальних активів, реактивних заходів правоохоронних органів, використання спеціалізованого програмного забезпечення Chainalysis, TRM Lab, Crystal Blockchain, Elliptic для аналізу блокчейну та методів відкритої розвідки. У дослідженні систематизовано конкретні криміналістичні індикатори п'яти основних видів злочинів, пов'язаних з віртуальними активами, включаючи структурування транзакцій у відмиванні грошей, використання міксерів, обіцянки нереалістичних прибутків в інвестиційному шахрайстві та зв'язки з адресами даркнету. Порівняльний аналіз п'яти ключових юрисдикцій продемонстрував разючу різноманітність регуляторних підходів від технологічно нейтрального швейцарського регулювання, заснованого на принципах, до комплексного регулювання європейських ринків криптоактивів з уніфікованими вимогами до постачальників послуг у сфері криптоактивів. Практичне значення отриманих результатів полягає в можливості розроблення ефективних механізмів міжнародного співробітництва в розслідуванні транскордонних злочинів, пов'язаних з віртуальними активами

■ **Ключові слова:** криптовалюта; шахрайство; цифрова криміналістика; деанонімізація; блокчейн