UDC 347.73:336.22
DOI: 10.56215/naia-chasopis/3.2023.65

Offences in the sphere of virtual assets turnover and analysis of their qualification

Maksym Rafalskyi*
Postgraduate Student
Academy of Advocacy of Ukraine
01032, 27 Taras Shevchenko Blvd., Kyiv, Ukraine
https://orcid.org/0000-0001-9016-8613

Abstract
With the advent of new forms of interaction, virtual goods and services, a new field for committing offences in the field of virtual assets turnover is emerging. This encourages scientists and law enforcement agencies to actively research this area and develop effective mechanisms to respond to emerging challenges that have not yet been properly reflected in legislation. The purpose of this study was to explore the issue in depth by analysing specific offences related to virtual assets, including but not limited to theft, fraud, corruption, and tax evasion. The methods of scientific cognition employed for the study include analysis of legal regulation, modelling methods, analogies, systemic and structural, comparative legal, as well as methods of scientific abstraction and generalisation. Based on the results of the study, the study identified the main types of offences in the field of virtual assets and unifies them. The study identified the shortcomings in the current legal regulation that contribute to these problems. Proposals were formulated for amendments to the Criminal Code of Ukraine regarding the qualification of new types of offences committed in the field of virtual assets turnover based on research of current trends, international practices, and analysis of the current state of Ukrainian legislation. The study also showed that the available legal instruments often fail to ensure adequate detection and prosecution of new forms of offences, which makes it necessary to reform legislation to adapt to the current dynamic environment. The practical significance of this study was to identify the current problems of legal regulation of the circulation of virtual assets, and to develop recommendations for improving the qualification of offences in this area

Keywords:
cybersecurity; cybercrime; criminal law; criminal code; cryptocurrency

Article's History:
Received: 20.06.2023
Revised: 11.09.2023
Accepted: 26.09.2023

Suggest Citation:
Rafalskyi, M. (2023). Offences in the sphere of virtual assets turnover and analysis of their qualification. *Law Journal of the National Academy of Internal Affairs*, 13(3), 65-76. doi: 10.56215/naia-chasopis/3.2023.65.

*Corresponding author

Introduction

The problem of offences in the field of virtual assets is truly relevant in the modern world. The growing popularity of cryptocurrencies, blockchain technologies, and other decentralised networks leads to an increase in the number of offences committed in this area, where virtual assets can be both the means and the subject of such offences. The study of such offences is important for both practical applications and scientific research. Given that virtual assets are a new dimension in the life of Ukraine, which is not yet fully understood and developed, this leads to the fact that the methods of detecting and investigating offences in the field of circulation of such assets are still evolving and are not yet as effective as conventional methods of detecting offences. The absence of an effective system for detecting, investigating, and preventing such offences may lead to a lack of trust in virtual assets as tools for preserving and transferring value. The solution to this problem is only now becoming the subject of scientific research in various fields, including law, information security, economics, etc.

When reviewing global practice and trends in combating offences arising in the field of virtual assets, some international scholars or research teams have focused their efforts on investigating this topic. However, although they considered specific categories of offences, there is no comprehensive analysis and systematisation of the main groups of such offences, accompanied by proposals for modifying the current criminal legislation. This issue was discussed in the context of money laundering through virtual assets in B. Sanz-Bas *et al*. (2021), which identifies the close interaction between money laundering and cryptocurrencies, focusing on the use of these mechanisms by criminal organisations to legalise illicit funds. In another paper, A. Thommandru & B. Chakka (2022) discuss the problem of money laundering through virtual assets, but from the perspective of over-regulation. The authors note that a crypto asset market in need of regulation may suffer from excessive legal interference, which may encourage investors to seek more lenient jurisdictions, such as Asian markets. Another work is devoted exclusively to the financing of terrorism.

The authors D.-S. Cynthia *et al*. (2019) point out that the transition to innovative "fintech" solutions from traditional financial systems can significantly change counterterrorism financing strategies, despite current exaggerations about the role of cryptocurrencies in supporting terrorist organisations. In addition, the authors A. Trozze *et al*. (2022) emphasise that research into future challenges and potential scenarios arising from cryptocurrency fraud is still in its infancy, despite the rapid development in this area, both in terms of volume and scale. H.S. Zaytoun (2019) points out that the anonymity of crypto asset hijackers poses a major challenge for law enforcement agencies, which must spend significant resources to track down the attackers, especially considering new blockchain technologies that enhance this anonymity. V.V. Kovtun (2021) investigated the legal aspects of the circulation of virtual assets and contributed to the development of this topic in Ukraine.

Thus, as the above analysis suggests, researchers are focused on studying very particular areas such as money laundering through virtual assets, terrorist financing through such assets, etc. However, there has been no comprehensive investigation of diverse types of offences in the field of virtual assets turnover, so this paper is devoted to this area. The purpose of this study was to analyse various offences in the field of virtual asset trafficking to develop effective strategies to counteract them, improve their qualifications for legal regulation and protection from crime, and promote understanding of the technical aspects of decentralised networks for non-technical specialists.

During the study, both general scientific and special legal research methods were used. The modelling method was used to understand complex objects, processes, and relations connected to the turnover of virtual assets using other similar methods, which helped find the necessary ideas and options for solving the tasks. The method of analogy to establish similarity, equivalence of objects, processes, relations to establish other ones under study; the method of forecasting to improve counteraction and prevention of offences related to the turnover of virtual assets. The systemic-structural method was used to enable consideration of the criminal law characteristics of virtual assets as a whole and each element separately, as well as the interrelationships between them, their patterns, which helped identify problem areas and the means and methods of overcoming them. The author also used the formal legal method to clarify the essence, nature, and significance of objects, processes, and relations concerning the turnover of virtual assets in their connection with other processes.

Analysis of the issues and global trends in offences in the field of virtual assets turnover

Analysing the global practice and global trends in combating offences related to the turnover of virtual assets, several general trends in illegal activities can be identified related to the turnover of virtual assets. The main violations are fraud, theft, extortion, money laundering, tax evasion, smuggling, bribery, use of cryptocurrency in the shadow economy for the circulation of illegal products: weapons, drugs, human trafficking, etc. (in this case, cryptocurrency will be a means rather than an object); other offences, including various attacks in decentralised networks.

According to senior forensic experts K.S. Dmitrieva & O.V. Ivanova (2021), in criminal proceedings, offences committed with cryptocurrency include, first of all,

theft, fraud, corruption offences, as well as offences in the field of computer information. A survey conducted by Hartford Steam Boiler (HSB), a leading cyber insurance provider and part of the large German reinsurer Munich Re, found that 36% of small and medium-sized businesses in the United States accept bitcoin. Furthermore, there are large international corporations that also accept cryptocurrencies as payment, including technology corporations, retailers, restaurant chains, airlines, etc. (36% of SMEs accept..., 2020; Cryptocurrency financial crime..., 2022).

At the same time, the growing popularity of the benefits offered by cryptocurrencies has not gone unnoticed by criminals and entire criminal organisations. Criminals use cryptocurrencies such as bitcoin for a variety of purposes, including money laundering, extortion of funds from victims, defrauding investors, monetising ransomware, or purchasing illegal goods. For many years, intelligence reports have provided information that well-known terrorist organisations such as ISIS or al-Qaeda have used cryptocurrencies to obtain funding. In fact, the sale of illegal drugs and other types of lawbreaking on the so-called dark markets and payment for them with cryptocurrencies have increased dramatically since 2017 over the past few years (Risks of terrorism..., 2017).

According to the organisation, which tracks every bitcoin transaction and advises several government agencies, the amount of cryptocurrency spent on these dark markets increased by 60% to reach a new high of $601 million in the last quarter of 2019 (Cryptocurrency financial crime..., 2022). Even in the absence or insufficiency of regulation of the circulation of virtual assets, and until the Law of Ukraine "On Virtual Assets"[1] comes into force, these assets must meet all the features of someone else's property as the subject of property crimes. Thus, since virtual assets, according to the said law, are considered to be an intangible good that is an object of civil rights and has a value, they can be considered as the subject of property crimes, as they have the characteristics of property, which includes the right to own, use, and dispose of it. These signs can be proved, for example, through the existence of a corresponding account on a crypto exchange where cryptocurrency assets are stored or through the existence of a corresponding crypto wallet as an electronic or physical medium. Thus, in case of an offence involving virtual assets, all legal requirements relating to property offences should be followed in order to prove ownership and establish damages.

According to the provisions of Part 1 of Article 1 of the Criminal Code of Ukraine, the Criminal Code of Ukraine[2] is aimed at ensuring the protection of human and civil rights and freedoms, property, public order and public safety, the environment, the constitutional order of Ukraine from criminal offences, ensuring peace and security of mankind, as well as preventing criminal offences. To fulfil this task, part 2 of Article 1 of the Criminal Code of Ukraine defines which socially dangerous acts are criminal offences and what penalties are applied to the perpetrators[3].

As M.I. Panov (2019) points out, an adequate definition of the type of offence and its differentiation from others has a significant practical effect, which is manifested not only in the effective protection of public relations, but in the protection of the rights of persons who have committed the relevant violations. Decisive decisions on this extremely important practical issue are based on the general concept of a criminal offence, which includes not only the general features inherent in any violation, but special features that distinguish this offence from others. Among these features, one should consider criminal legality and social danger, which are innate characteristics of this offence and distinguish it from others. Therefore, it is necessary to determine what types of offences exist in the field of virtual assets.

Theft of virtual assets as a criminal offence

Unlike conventional money, virtual assets are not subject to centralised regulation. This brings some advantages for some holders of such assets, such as free, unregulated circulation, but also comes with certain disadvantages. Virtual assets can be stolen both in the blockchain itself, e.g., in decentralised networks, through diverse types of attacks or fraud, and from crypto wallets or crypto exchange accounts. For example, if virtual assets are stolen in the blockchain itself, it is impossible to cancel the transaction and return them.

Another way to steal virtual assets is to steal them from victims' wallets. If it is an electronic wallet, this is done, for example, by setting a PIN to the account or stealing the personal keys of such persons, including by downloading malware to computers or through social engineering. In the latter case, it can already be qualified as fraud. If it is a physical wallet, then such virtual assets are stolen along with the media. In society, it is not uncommon for such thefts to take place by law enforcement agencies during searches. For example, in 2017, the founder of a specialised cryptocurrency publication, A. Kaplan, had his cryptocurrency stolen during searches conducted by security forces. During the investigation, the Security Service of Ukraine (SSU) seized devices with cryptocurrency stored on them, a laptop and personal belongings at Kaplan's home in Odesa. According to the founder, during the search, one

[1] Law of Ukraine No. 2074-IX "On Virtual Assets". (2022, February). Retrieved from https://zakon.rada.gov.ua/laws/show/2074-20#Text.
[2] Criminal Code of Ukraine No. 2341-III. (2001, April). Retrieved from https://zakon.rada.gov.ua/laws/show/2341-14#Text.
[3] Ibidem, 2001.

of the special service officers tried to transfer Kaplan's cryptocurrency to his wallet, but the lawyer stopped this attempt by threatening to go to the police. However, the next day, all the Ethereum coins were transferred from the entrepreneur's cryptocurrency wallet to an unknown address, which, according to the founder, belonged to an SSU employee (Zavalniuk, 2023).

Thus, in the case of theft of virtual assets, the very object of theft is such virtual assets. However, with regard to the qualification of such offences, while in the case of theft of fiat money, law enforcement officers have no difficulty in their legal assessment, in the case of theft of virtual assets, the question arises as to the correct qualification of such offences, due to the lack of a legislative definition of their status, the absence of relevant articles in the criminal law, and the increasing number of criminal acts in this area.

In the current Criminal Code, liability for crimes against property is prescribed in Section VI "Crimes against Property" of its Special Part (Articles 185-191)[1]. The legal provision established in one of the sections of the Special Part of the Criminal Code guarantees all owners the same level of protection of their property rights against any encroachment, regardless of the form of this property, according to the requirements of the Constitution of Ukraine and national legislation. When qualifying crimes against property, the object plays a significant role. It may be someone else's property with a certain material value that is alien to the person guilty of the crime (e.g., movable and immovable property, cash, precious metals, securities, etc.), as well as the right to property and actions related to property, including the supply of electricity and heat (subpara. 1, para. 2 of the Resolution of the Plenum of the Supreme Court of Ukraine "On judicial practice in cases of crimes against property" of 6 November 2009, No. 10)[2].

Virtual assets that can be recognised as property by their characteristics may be subject to theft and fall under the relevant qualification of the article of the Criminal Code of Ukraine (Classification of crimes..., 2016). Given the above, as well as the fact that virtual assets can be defined as property by physical, legal, and economic characteristics, the theft of virtual assets can be qualified under Article 185 of the Criminal Code of Ukraine (Secret appropriation of another's property (theft))[3]. Another prominent issue is establishing the loss, as virtual assets, specifically cryptocurrencies, are highly volatile. The number of cryptocurrencies as of the beginning of March 2023 is about 23,000 distinct types (All cryptocurrencies, 2023). Each has its own exchange rate against the others, as well as the fiat currency. In general, the price of a cryptocurrency unit is determined by a social contract, i.e., people have agreed that a certain type of cryptocurrency has a certain value, there is a demand and a certain supply, and it exists as long as people will pay with it. If the cryptocurrency has been stolen, the law enforcement practice should be based on the principle of establishing damages.

Use of virtual assets for fraud and the purchase and sale of illicit goods

Marketplaces located in the darknet, using a separate set of Internet protocols, function as black markets where both illegal goods and legal products are sold. The darknet is used both through Internet browsers and through various software and mobile applications. For instance, DarkWallet is an app that prioritises anonymity. It uses various methods to protect user IDs and combines data from several synchronous transactions when making a payment, making it impossible to track account activity. Paying with cryptocurrency, one can buy more than just goods on the darknet. Darknet enables various operations, such as access to databases or confidential information, personal information about people, banking secrecy, forged documents, as well as cyberattack and terrorist services, hiring assassins (agreement on the physical elimination of a person), trafficking in human organs, narcotic and psychotropic substances, weapons, child pornography, counterfeit goods, information about social media accounts (including logins and passwords) (Hrebenkova, 2021).

The qualification of these offences depends on the particular features of a particular offence and their compliance with the provisions of the Criminal Code of Ukraine (CCU), which prescribe liability for such offences. For instance, Art. 199 of the CCU (Production, storage, acquisition, transportation, shipment, importation into Ukraine for use in the sale of goods, sale of counterfeit money, government securities existing in paper form, state lottery tickets, excise tax stamps or holographic security elements)[4] and Art. 204 of the CCU (Illegal production, storage, sale or transportation for sale of excisable goods)[5].

Y.P. Kalaida (2021) notes that there is another type of crime committed using cryptocurrency, and these are crimes against property, where the cryptocurrency itself becomes the object of the encroachment. Criminals who steal cryptocurrencies use fake e-wallets. Victims, when making purchases of goods or services on popular platforms, transfer funds to phishing wallets using viruses that have different addresses from the original ones. The creation of phishing sites of popular online

[1] Criminal Code of Ukraine No. 2341-III. (2001, April). Retrieved from https://zakon.rada.gov.ua/laws/show/2341-14#Text.
[2] Decision of the Plenum of the Supreme Court of Ukraine No. 10 "On Judicial Practice in Cases of Crimes Against Property". (2009, November). Retrieved from https://zakon.rada.gov.ua/laws/show/v0010700-09#Text.
[3] Criminal Code of Ukraine No. 2341-III. (2001, April). Retrieved from https://zakon.rada.gov.ua/laws/show/2341-14#Text.
[4] Ibidem, 2001.
[5] Ibidem, 2001.

resources can also be used. The use of cryptocurrencies in fraudulent schemes is also evident in crowdfunding projects. The development of a new model of collective investment has led to the emergence of fraudsters who collect money in cryptocurrencies from victims without intending to engage in business activities.

A common form of fraud is the pump and dump scheme in the context of cryptocurrencies (Nghiem *et al*., 2021). Pump-and-dump is a type of fraud where fraudsters act to lure unsuspecting traders into buying cryptocurrency at an artificially high price (pump) and then quickly selling their previous assets for a profit (dump). The anatomy of a pump-and-dump scheme typically involves abnormally high price and volume peaks in a particular cryptocurrency or coin, followed by sharp drops over very short periods of time, usually within minutes. The organisers of these schemes use social media platforms to engage their followers and communicate with them about the timing of upcoming pumps, as well as the performance of past pumps.

Phishing

Phishing is a form of cyberattack where attackers masquerade as well-known organisations or companies to steal personal data, such as credit card information, usernames, passwords, etc. Using psychological techniques and relying on human error rather than technical vulnerabilities, phishing is a social engineering technique. The level of user awareness of modern threats is quite low, and fraudsters take advantage of this – the ignorance of many users towards basic network security rules. According to IT experts, the weakest link in the security of any organisation is the average user, their lack of awareness, inattention, and, sometimes, simple curiosity (Demidov & Kolmyk, 2020).

Fraud involving cryptocurrencies, such as counterfeiting during sales, exchanges for fiat currency and other financial transactions, is a generic form of criminal activity. The recognition of cryptocurrencies as the object of criminal offences is a major step towards ensuring proper legal protection of ownership of these digital assets. In this regard, it is proposed to include cryptocurrency in the scope of criminal liability, as well as to consider the possibility of recognising it as the subject of certain criminal offences, depending on the specific criminal acts. Implementation of these measures requires proper legislative regulation of cryptocurrency relations and consideration of the specifics of the digital sphere, which will allow for effective combating of criminal activities related to cryptocurrency. In this regard, the position of V.V. Kovtun (2021) can be supported that before introducing cryptocurrency into civil circulation, it is necessary to recognise it as "property" in the context of the civil legislation of Ukraine, which will serve as the basis for further criminalisation of illegal actions with cryptocurrency. Prior to the entry into force of the Law of Ukraine "On Virtual Assets"[1], virtual assets may be treated in law enforcement and judicial practice as other property, and their theft should be qualified as theft of another's property. These offences can be classified under Article 190 of the Criminal Code[2]. If actions such as cryptocurrency phishing are prescribed, Article 362 of the Criminal Code[3] is also the correct qualification. It is also subject to Article 363-1 of the Criminal Code[4].

Corruption offences and tax evasion

Although virtual assets are not yet regulated by the Law on Virtual Assets[5] in the context of property rights and obligations, such assets, if accepted by an official as a reward for official actions or inaction, may be equated to the concept of "unlawful benefit" in the criminal law sense. The use of such assets may result in the acquisition of certain property rights that may be converted into cash in the future. In this regard, the transfer of virtual assets as a bribe may be qualified as an element of the objective side of criminal offences related to the provision or receipt of unlawful benefit. Even if the property is not included in civil circulation, it may be the subject of an unlawful benefit. The acceptance of an unlawful benefit in the form of virtual assets by an official performing an action (or inaction) in office is considered to be unlawful from the moment such assets are received. This applies even if the official did not later cash in or use the virtual assets for payment. The mere existence of a corresponding electronic record in the distributed register is enough to constitute the offence. The ownership of virtual assets as a subject of unlawful benefit must be expressed in terms of value, so the official must receive a pecuniary benefit.

In Ukrainian society, some public officials practice declaring virtual assets that do not actually exist. Some experts believe that virtual assets can only serve as a hiding place for bribes. In 2020, 46,351 bitcoins were accrued in the declarations of civil servants. As of 5 April 2021, this is almost UAH 75 billion. Declarations were submitted by 791,872 officials, and 652 officials registered cryptocurrencies (Bitcoin in declarations..., 2022).

As for the qualification of offences related to obtaining unlawful benefit in the form of virtual assets, Articles 368-370 of the Criminal Code of Ukraine can be applied here[6]. In this part, one can agree with

[1] Law of Ukraine No. 2074-IX "On Virtual Assets". (2022, February). Retrieved from https://zakon.rada.gov.ua/laws/show/2074-20#Text.
[2] Criminal Code of Ukraine No. 2341-III. (2001, April). Retrieved from https://zakon.rada.gov.ua/laws/show/2341-14#Text.
[3] Ibidem, 2001.
[4] Ibidem, 2001.
[5] Law of Ukraine No. 2074-IX "On Virtual Assets". (2022, February). Retrieved from https://zakon.rada.gov.ua/laws/show/2074-20#Text.
[6] Criminal Code of Ukraine No. 2341-III. (2001, April). Retrieved from https://zakon.rada.gov.ua/laws/show/2341-14#Text.

F.F. Fedchyshina (2022), A. Rosen & D. Ramirez (2022) that corruption with the use of cryptocurrencies poses a challenge due to its novelty and insufficient research in the field of criminal activity. One of the challenges is the difficulty of tracking cryptocurrency movements. Furthermore, the ease and re-conversion of cryptocurrencies into other types and their significant price fluctuations over a brief period of time make them attractive to criminals. This feature of cryptocurrencies facilitates money laundering, as transactions are executed quickly and are not recorded by a centralised authority, as no such authority exists. Therefore, countries, including Ukraine, should consider adopting suitable legislation to overcome these challenges and obstacles.

N.K. Siddiki & R.O. Movchan (2018) point out that according to the National Bank of Ukraine (NBU), the Security Service of Ukraine (SSU) and the National Police of Ukraine (NPU), the lack of control over the circulation of cryptocurrencies and the anonymity of payments creates potential prerequisites for their use for money laundering, payment for goods prohibited for free circulation (drugs, weapons), and enables the financing of terrorism, especially in the occupied territories of Ukraine. However, due to the existence of a terrorist threat in Ukraine, the introduction of cryptocurrencies has its own specific features. According to a report by the International Financial Action Task Force on Money Laundering (FATF), an intergovernmental organisation that develops global standards for combating money laundering and terrorist financing, the lack of legal regulations on bitcoin allows it to be used for criminal purposes, including the purchase of weapons. Experts from the Centre for Social and Economic Research "CASE Ukraine" confirmed that cryptocurrency can be seen as a way of concealing income and tax evasion. For instance, it is possible to justify some excessive costs in the future by a successful "investment" in cryptocurrency several years ago (Romaniuk, 2018).

In this area, the offence can be divided into tax evasion with the use of virtual assets and tax evasion for activities in the field of virtual asset turnover. The second category can be considered after the Law of Ukraine "On Virtual Assets"[1] enters into force and the relevant amendments to the Tax Code of Ukraine[2] are adopted, so it is worth focusing on the first category. Thus, since March 2023, cryptocurrency exchanges have stopped withdrawing money through Ukrainian cards (Cryptocurrency goes underground..., 2023). Following strict recommendations from the NBU, banks stopped processing high-risk transactions, including those related to gambling and cryptocurrencies. Investigators from the SSU and the Bureau of Economic Security (BES) suspect betting and gambling companies of tax evasion using cryptocurrencies (Tartachnyi, 2023). The funds were withdrawn through a miscoding scheme. Through various schemes, gambling companies created "quasi-cash" through card2account and account2card transactions, which are now effectively banned. The actual scheme of miscoding was that a player deposited money into the account of an operator (bank) that marked payments with a payment code of another industry. This helps disguise payments from gambling. The hryvnia is then exchanged for cryptocurrencies and transferred to foreign accounts of the gambling company. In gambling, the industry code 7995 is usually replaced by 7994. The bank receives a payment from a gambling customer, and if the player wins, the institution sends the winnings to the player without taxing them as a regular card-to-card transfer. These offences may be classified under Articles 212 and 209 of the Criminal Code of Ukraine (tax evasion on a particularly large scale and legalisation of the proceeds of crime)[3].

Mining and offences related to crypto exchanges

Cryptocurrency exchanges can also be used to commit cryptocurrency-related crimes, as there are many cryptocurrency varieties that are highly volatile. One of the most common cases is a "pump-and-dump" scheme, which involves a conspiracy between traders to convince third-party investors to purchase certain cryptocurrency coins using social media.

When a coin reaches a certain price, the participants in the manipulation sell their purchases and stop spreading information, which leads to a price drop. Persons who have purchased cryptocurrency under the influence of such manipulation will suffer financial losses. Such actions with cryptocurrencies can be qualified as a crime, which is the case with conventional currencies. Such manipulations should be recognised as criminal and classified under Article 222-1 (Manipulation of organised markets)[4], as well as under Article 192 (Causing property damage by deception or breach of trust)[5]. Many regulated cryptocurrency exchanges comply with laws requiring customer identification, but there are some that serve criminal customers without proper verification, and criminals can use both legal exchanges bypassing identification processes with fake documents and illegal ones where there is no identification.

The operation of creating (generating) cryptocurrency is called mining. In practice, mining is the formation of new blocks in the blockchain of each cryptocurrency. Furthermore, mining can also be described as the process of recording all cryptocurrency transactions

[1] Law of Ukraine No. 2074-IX "On Virtual Assets". (2022, February). Retrieved from https://zakon.rada.gov.ua/laws/show/2074-20#Text.
[2] Tax Code of Ukraine No. 2755-VI. (2010, December). Retrieved from https://zakon.rada.gov.ua/laws/show/2755-17#Text.
[3] Criminal Code of Ukraine No. 2341-III. (2001, April). Retrieved from https://zakon.rada.gov.ua/laws/show/2341-14#Text
[4] Ibidem, 2001.
[5] Ibidem, 2001.

in their blockchain, an open database of transactions. Mining is needed to support the operation of all existing cryptocurrencies, to ensure transparency of transactions and to create the blockchain structure (Kaznacheeva & Dorosh, 2020). It is important to understand its criminal law aspect. Offences related to mining are primarily cryptocurrency mining itself, provided that such activity is prohibited, or if unmetered electricity is used during mining, non-payment for such a network, or overloading of such a network.

Given that mining is not prohibited in Ukraine, it is worth considering the second type of offence. As of 2023, there are already many criminal proceedings related to mining. This is due to the availability of cheap electricity, often illegal. Illegal mining farms were discovered at the South Ukrainian NPP (Cryptocurrency was mined..., 2019) and at Vinnytsiaoblenergo (In Vinnytsia, a..., 2021). There have also been criminal proceedings in connection with mining at the Paton Institute (At the Paton..., 2017) and Ukrzaliznytsia (Employees of..., 2022). Such actions can be classified under Article 188-1 of the Criminal Code (Theft of water, electricity, or heat by unauthorised use)[1].

Although Ukrainian legislation does not prohibit cryptocurrency mining, such activities have all the hallmarks of a business activity that requires payment of taxes. If cryptocurrency mining is not prohibited by law and is performed based on the entrepreneur's free choice of business activity, it can be considered legal from the taxation standpoint. Thus, if this type of activity is not prohibited, it may be subject to taxation.

The conditions of liability for a person evading taxes from cryptocurrency transactions and property are regulated by the Resolution of the Plenum of the Supreme Court of Ukraine No. 15 of 08.10.2004 "On Certain Issues of Application of Legislation on Liability for Evasion of Taxes, Duties, and Other Mandatory Payments"[2]. According to the Resolution No. 15, liability under Article 212 of the Criminal Code may be applied only if the following conditions are met: 1) non-payment of taxes, duties, and other mandatory payments; 2) existence of an object of taxation; 3) identification of the payer; 4) establishment of a mechanism for payment of taxes and duties. Refusal to pay taxes for cryptocurrency mining may have consequences under Articles 209[3], 212[4] of the Criminal Code of Ukraine.

Hidden mining methods are also used. As of 2023, any user can do hidden mining. For this, one just needs to download the ready-made application, write their e-wallet number, and that is it. The program is modified in such a way that it is indistinguishable from a Trojan virus: it can spread on the network, copy itself to an external drive, hide its processes in the task manager and use the computer when no one is using it. As long as the user has a page with a malicious script open in the browser, the processor will perform mining unnoticed (Lyzunov & Vereshaka, 2018). These offences can be qualified under Article 362 of the Criminal Code[5] and Article 363-1 of the Criminal Code[6].

Financial offences in Initial Coin Offerings (ICOs)

Among the types of fraud in the sphere of virtual assets turnover, a special place is occupied by illegal Initial Coin Offerings (ICOs). Within the framework of an ICO, companies offer investors the sale of a fixed number of new units of virtual assets (tokens) that grant these investors certain rights, such as to cryptocurrency or certain goods/services. ICO fraud is often manifested through the creation of illegal ICOs that are difficult to recognise at the beginning of an investment. Investing in ICO projects on the Internet has no clear legal regulation. Consequently, investors who invest in such projects are left without adequate criminal law protection.

Blockchain technology allows private investors from all over the world to take part in ICOs for speculative purposes, but its cross-border and anonymous nature facilitates the expansion of pyramid schemes and the manipulation of token prices, which are traded on unregulated platforms with high volatility. As in other cases of virtual asset fraud, dumping, known as pump-and-dump, is a popular technique. The anonymity and untraceability of cryptocurrency transactions, specifically through ICOs, creates the risk of their use for money laundering, which can lead to serious conflicts with legislation on the prevention of terrorist financing (Zavalniuk, 2023).

In addition, one of the most common types of such offences is the so-called "Rug pulls" scheme, which is a "get-out scam" in which developers make promises and then quickly "leave" with investors' funds. "Rug pulls is a cryptocurrency fraud in which a developer attracts investors but withdraws before the project is completed, leaving buyers with a worthless asset. "Rug pulls" are commonplace for decentralised finance, or DeFi, projects that aim to displace conventional financial services such as banking and insurance, or non-fungible tokens (NFT) that grant digital ownership of art and other content. According to research firm Chainalysis, "Rug pulls" were worth more than $2.8 billion to investors in 2021 (Rosen & Ramirez, 2022).

[1] Criminal Code of Ukraine No. 2341-III. (2001, April). Retrieved from https://zakon.rada.gov.ua/laws/show/2341-14#Text.
[2] Resolution of the Plenum of the Supreme Court of Ukraine No. 15 "On Some Issues of Application of Legislation on Liability for Evasion of Taxes, Fees, Other Mandatory Payments". (2004, October). Retrieved from https://zakon.rada.gov.ua/laws/show/v0015700-04#Text.
[3] Criminal Code of Ukraine No. 2341-III. (2001, April). Retrieved from https://zakon.rada.gov.ua/laws/show/2341-14#Text.
[4] Ibidem, 2001.
[5] Ibidem, 2001.
[6] Ibidem, 2001.

Usually, fraudsters create a new cryptocurrency token, place it on a decentralised exchange, link it to a well-known platform, such as Ethereum, and then launch an active advertising campaign via social media. When the value of a token reaches its maximum due to the hype created, developers quickly give up their share of tokens, taking away investors' funds. In contrast to dumping, which is considered a mild "Rug pulling" scheme, as it can be a deliberate fraud or a side effect of an unstable crypto space, a more severe "Rug pulling" scheme is liquidity theft, which occurs when developers withdraw large amounts from the project's liquidity fund and intended to commit fraud from the very beginning. Typically, liquidity is first contributed by token creators and then by traders. Traders can contribute liquidity to decentralised exchanges, i.e., lend it tokens that it will use to execute other people's trades, and lenders are rewarded by reducing trading fees. It is envisaged that a sufficient liquidity pool will be available to ensure the programme's operation in case investors decide to withdraw their funds or execute large transactions. If the developer depletes this liquidity, the application may stop working, and investors will have a tough time recovering their investment. Despite the security measures in place in many crypto projects, there is a risk that unscrupulous developers can introduce vulnerabilities into the code (Mackenzie, 2022). After processing the data, it was discovered that an incredibly high number of liquidity pools were actually "Rug pulls". On the Binance Smart Chain (BSC) blockchain, 272,349 of the 332,265 (81.2%) liquidity pools under consideration have a Rug pulls pattern, including 21,742 of the 25,180 (86.3%) in Ethereum. This result shows that attackers use most coins as disposables to execute "Rug pulls". These transactions are organised by 116,516 different addresses in BSC and 16,539 different addresses in Ethereum (Cernera *et al*., 2022).

To establish the riskiness of ICO projects, it is necessary to understand who is behind the company conducting the ICO, where this company is located, how the funds will be used, what rights investors will receive, how and where they can be exercised, whether the investment can be returned or redeemed, whether the financial statements of the said company are provided for, etc. The qualification of these offences raises some difficulties. Given that the coin itself may have no value, its transfer may not constitute property damage from the legal standpoint, especially in the absence of legal regulation of such assets, which may indicate the absence of a crime. Therefore, in essence, the failure to comply with the terms of the ICO is a failure to comply with the terms of the contract by the person(s) who intended not to perform the obligations under it and to appropriate the property from the victims, and in this case, these actions can be qualified under Article 190 of the Criminal Code[1], namely, the seizure of another's property or the acquisition of the right to property by deception or breach of trust (fraud).

Apart from ICOs, there are other types of coin (token) offerings. For example, IDO (Initial DEX Offering) is a token launch during fundraising on a decentralised exchange; IGO (Initial Gaming Offering) is the placement of tokens in a game; SHO (Strong Holder Offering) is a fundraising campaign by the holders of a certain cryptocurrency; IEO (Initial Exchange Offering); LBP (Liquidity Bootstrapping Pool) is the sale of tokens in the form of an auction, when the offer price gradually decreases in the absence of demand and increases when buying. IFO (Initial Farm Offering) is the first offer of farming (growing) a new cryptocurrency – raising capital through the farming function of the proposed decentralised exchange. These types of coin (token) offerings can also be fraudulent schemes (Yatsyk, 2020).

Financing terrorism through virtual assets

Terrorist groups and their core (auxiliary) networks are exploring new financial technologies (FinTech) to further their efforts. Experts have identified cryptocurrency-based terrorist financing as a real risk that requires serious attention, and government agencies and organisations that monitor terrorist financing have begun to express alarm at the growing number of Islamist terrorist organisations experimenting with bitcoin and other digital coins (Zavalniuk, 2023). The use of cryptocurrencies for criminal activities, including terrorism, should be regulated, regardless of the lack of a clear legal status of cryptocurrencies. Experts recognise that virtual assets create new and sophisticated financing methods used by terrorist groups, and this real risk requires serious attention from law enforcement and regulatory organisations (Cynthia *et al.,* 2019). Afghanistan, facing financial difficulties after the Taliban seized power, has seen a rapid increase in the use of Bitcoin as a protection for financial assets (Wolf, 2021). Alongside the revival of the cryptocurrency sector, the country could become the epicentre of digital misconduct, including cyberattacks and online radicalisation campaigns instigated by the Taliban and affiliated terrorist groups.

Y.P. Kalaida (2021) notes that currently, a popular and new way to legalise criminal proceeds is to launder them through the use of online casinos. These services play a significant role in the laundering of more than a third of dirty virtual money. Criminals are increasingly using game currency to store valuables in cryptocurrencies. For this, they will purchase currency in popular virtual games, which is then converted on money platforms. The use of cryptocurrencies by the owners of terrorist organisations carries great risks, especially in the context of financing terrorist acts. As cryptocurrencies become more widespread and transactional

[1] Criminal Code of Ukraine No. 2341-III. (2001, April). Retrieved from https://zakon.rada.gov.ua/laws/show/2341-14#Text.

infrastructure develops, virtual currency may become an increasingly common tool for financing terrorist activities in the future. These offences can be qualified under Article 209-1[1], Article 258-3[2], Article 258-4[3], Article 258-5[4].

Problems of offences in the sphere of virtual assets turnover: Ukrainian and foreign aspects

As for the studies on this issue, in the Ukrainian legal literature, there has been virtually no systematic research on offences in the field of virtual assets, especially in the context of criminal law. There are some studies and articles that analyse the legal aspects of virtual asset circulation, including the analysis of their impact on criminal law. Studies in this area were conducted by M.O. Dumchikov & D.A. Repin (2020).

The study by N.K. Siddiki & R.O. Movchan (2018) examines the problems of controlling the circulation of cryptocurrencies in Ukraine, focusing on the potential use of these currencies for money laundering, payment for prohibited goods and terrorist financing. The author discusses the criminogenic properties of cryptocurrencies, such as anonymity, speed, and lack of legal regulation, which allow criminals to effectively use them for illegal activities. The paper analyses several high-profile detentions and crimes related to the use of cryptocurrencies, which have led to changes in legislation around the world and tightened control over the circulation of cryptocurrencies. Specifically, it covers attacks on computer systems for cryptocurrency mining, the use of cryptocurrencies for ransom, and various methods of fraud and money laundering using cryptocurrencies.

M.O. Dumchikov & D.A. Repin (2020) examined the spread of cryptocurrency use for illegal activities, including tax evasion, money laundering, and terrorist financing. The authors emphasise the prominent level of anonymity provided by cryptocurrencies, which makes it difficult to detect and track illegal transactions. They call for the need to study cryptocurrencies and their implications to determine the risks and threats they pose in the global economic space. The authors also warn that with the spread of cryptocurrencies and the development of transaction infrastructure, virtual currency will increasingly be used to finance terrorism.

Y.P. Kalaida (2021) carried out a study on criminal activity involving cryptocurrencies and found that these currencies are becoming more frequently used on the DarkNet for the acquisition of banned substances and drugs. The study investigated the specific types of cryptocurrencies used in this criminal scheme, the participants involved, and presented examples of how cryptocurrencies are laundered through criminal proceeds. Additionally, the study provided an overview of methods for investigating and countering such offences. V.V. Fedchyshina (2022) considers the problems and risks associated with the use of cryptocurrencies for corrupt practices, emphasising that the anonymity and difficulty of tracing such transactions make it difficult to combat this type of crime. The author discusses the lack of adequate legislation in the field of cryptocurrencies and the corresponding problems for users and governments. The study also outlines the European Union's ongoing efforts to create effective cryptocurrency legislation, including the adoption of the Markets in Crypto Assets Regulation (MiCA), which regulates cryptoasset-related activities in the EU.

As for foreign authors, D.-S. Cynthia *et al*. (2019) point out that while cryptocurrencies can provide new, more flexible transaction mechanisms, they can also open up new avenues for abuse, including use by terrorist groups, although many of them may not be technically proficient enough to use these systems effectively. While Bitcoin theft may not seem like a major issue, it is becoming increasingly prominent in the context of growing cybercrime, and the wider use of blockchain-based technologies can only increase the number of such cases. With this in mind, law enforcement should allow an appropriate amount of time to develop an appropriate approach to dealing with blockchain-related crimes (Zaytoun, 2019).

B. Sanz-Bas *et al*. (2021) notes that modern criminal groups are resorting to cryptocurrencies and specialised money laundering groups in an attempt to circumvent new methods of money laundering prevention. At the same time, the authors emphasise the need to create an international system of prevention and counteraction, which includes strict legislation on cryptocurrencies and active international cooperation to ensure effective information exchange and counteraction to money laundering. A. Thommandru & B. Chakka (2022) point out that the constant expansion and change of the legal framework, namely through the introduction of initiatives such as the MiCA regulation, can hinder technological advance. New companies may face increased costs and complications caused by these changes, prompting them to relocate their operations to regions with more favourable cryptocurrency laws. A. Trozze *et al*. (2022) note that many of the frauds identified in the study may be related to cyber networks, although new ways of committing them with the help of cryptocurrencies require further research. This paper also notes that there are no generally accepted or even existing definitions of different types of fraud described in the academic literature, so one of its main contributions is to define all types of fraud identified to date in

[1] Criminal Code of Ukraine No. 2341-III. (2001, April). Retrieved from https://zakon.rada.gov.ua/laws/show/2341-14#Text.
[2] Ibidem, 2001.
[3] Ibidem, 2001.
[4] Ibidem, 2001.

the academic and non-academic literature. Further harmonisation of these definitions could facilitate the development of common standards in the cryptocurrency sector, which would help prevent fraud in the future.

Thus, all of the articles reviewed focus on an overview of particular offences arising in the course of virtual asset circulation, or they provide a general overview of the topic, but only at a superficial level. They do not provide an in-depth analysis or a detailed description of the mechanism of each specific offence, nor do they contain particular proposals for modifying the Criminal Code of Ukraine to address these challenges. This paper, however, aims to address these shortcomings by offering a reasoned description of each virtual asset-related offence and recommendations on the necessary changes to the Criminal Code of Ukraine.

Conclusions

Thus, considering the above, it can be concluded that virtual assets can be used in various offences or can facilitate the commission of such offences. The anonymity of virtual asset transactions makes them an attractive form of illegal payment. There has been a considerable increase in the number of offences related to the theft of virtual assets. Given the lack of regulation, virtual assets may be classified as "other property" due to their economic value and the possibility of conversion into cash or use as a means of payment for goods and services.

Virtual assets exhibit the economic and legal features of the subject matter of these offences, but determining the physical feature is a more difficult task. In today's information society, property may be intangible. A more progressive interpretation of the object of theft involves considering financial interests and economic value. The growing popularity of virtual assets requires the state to ensure the protection of citizens' rights, including criminal law. Changes in the concept of property include intangible goods, which also require criminal law protection.

Considering virtual assets as an equivalent of property, it can be argued that criminal law should include virtual assets as a new object of criminal law protection, as they are already recognised by judicial practice and society, but not yet consolidated legislatively. As a result of the restrictions imposed by the current criminal law rules, there is a tendency that the range of objects of criminal law protection is not determined by civil law concepts, but rather the growing number of crimes related to virtual assets requires expanding the number of objects of civil rights and amending existing legislation.

Given the scope of this issue, a separate article will continue to consider offences in the field of virtual assets, especially such a broad topic as money laundering through virtual assets, and will also cover the topic of such specific offences arising in the field of ICOs, CBDCs, smart contracts, NFTs, DAOs, and meta-universes.

Research in the field of virtual asset trafficking offences can help to address various issues related to the development of effective methods for detecting, investigating, and preventing these offences. This problem is also an important incentive for the development of innovative technologies that will reduce the possibility of such offences.

Acknowledgements

None.

Conflict of Interest

The authors of this study declare no conflict of interest.

References

[1] 36% of SMEs accept payments in cryptocurrency. (2020). Retrieved from https://cryptodnes.bg/uk/36-ot-malkite-i-sredni-predpriyatiya-priemat-plashaniya-v-kriptovaluti/.

[2] All cryptocurrencies. (2023). Retrieved from https://coinmarketcap.com/all/views/all/.

[3] At the Paton Institute, they found a "factory" for generating bitcoin cryptocurrency. (2017). Retrieved from https://www.unian.ua/economics/finance/2075694-v-instituti-patona-znayshli-fabriku-generuvannya-kriptovalyuti-bitcoin.html.

[4] Bitcoin in declarations: Can officials prove bitcoin ownership. (2022). Retrieved from https://sud.ua/ru/news/publication/224972-bitkoin-u-deklaratsiyakh-chi-vdayetsya-chinovnikam-pidtverditi-pravo-vlasnosti-na-bitkoin-6b6cea.

[5] Cernera, F., La Morgia, M., Mei, A., & Sassi, F. (2022). Token spammers, rug pulls, and SniperBots: An analysis of the ecosystem of tokens in Ethereum and the Binance smart chain (BNB). *Computers and Society,* 1-16. doi: 10.48550/arXiv.2206.08202.

[6] Classification of crimes against property. (2016). Retrieved from https://arm.naiau.kiev.ua/books/kval-ok-zlochuniv-25-04-207/lectures/lecture_4.html.

[7] Cryptocurrency financial crime compliance bootcamp. (2022). Retrieved from https://www.udemy.com/course/blockchain-cryptocurrency-financial-crime-compliance/.

[8] Cryptocurrency goes underground: The NBU has banned the withdrawal of money from crypto wallets. Why is this a sign that the market is being prepared for strict regulation. (2023). Retrieved from https://mind.ua/publications/20254365-kriptovalyuta-jde-v-pidpillya-nbu-zaboroniv-vivoditi-groshi-z-kriptogamanciv-chomu-ce-oznaka-shcho-rino.

[9] Cryptocurrency was mined at the Yuzhno-Ukrainian NPP with the risk of disclosing a state secret. (2019). Retrieved from https://www.rbc.ua/ukr/news/sbu-obnaruzhila-mayning-kriptovalyuty-yuzhnoukrainskoy-1566462584.html.

[10] Cynthia, D.-S., Manheim, D., & Johnston, P.B. (2019). *Terrorist use of cryptocurrencies: Technical and organizational barriers and future threats*. Santa Monica: Rand Corporation.

[11] Demidov, Z.G., & Kolmyk, O.O. (2020). Phishing is like online fraud. In *The Vth international scientific and practical conference "Study of modern problems of civilization"* (pp. 448-450). Oslo: International Science Group. doi: 10.46299/ISG.2020.II.V.

[12] Dmitrieva, K.S., & Ivanova, O.V. (2021). Cryptocurrency as a research object of forensic economic expertise. *New Ukrainian Law*, 6, 156-160. doi: 10.51989/NUL.2021.6.23.

[13] Dumchikov, M.O., & Repin, D.A. (2020). Legalization of proceeds of crime through the use of virtual currency (cryptocurrency): Criminological and criminal law aspect. *Journal of East European Law,* 82, 32-37.

[14] Employees of "Ukrzaliznytsia" connected to the company's power grid and mined cryptocurrency. (2022). Retrieved from https://suspilne.media/277213-zaroblali-kriptovalutu-za-rahunok-ukrzaliznici-pravoohoronci-vikrili-pidpilnu-majning-fermu/.

[15] Fedchyshina, V.V. (2022). Cryptocurrency and blockchains cryptocurrencies as tools of corruption: Realities of institutionalization. In *Materials of the VII international scientific and practical conference* (pp. 101-110). Kyiv: Ministry of Internal Affairs of Ukraine, National Academy of Internal Affairs, National Academy of Legal Sciences of Ukraine.

[16] Hrebenkova, M. (2021). Current problems of electronic imagery in social networks as a source of evidence in criminal proceedings. *Criminal Procedural Law and Criminology*, 6, 251-257. doi: 10.32842/2078-3736/2021.6.36.

[17] In Vinnytsia, a mining farm was exposed that worked on the territory of regional energy. (2021). Retrieved from https://interfax.com.ua/news/general/754521.html.

[18] Kalaida, Y.P. (2021). Possibilities of blockchain technologies in the investigation of criminal offenses committed in cyberspace. *Information and Law,* 4(39), 170-178. doi: 10.37750/2616-6798.2021.4(39).249299.

[19] Kaznacheeva, D.V., & Dorosh, A.O. (2020). Cryptocurrency: Problems of legal regulation. *Bulletin of the Criminological Association of Ukraine,* 2(23), 171-176.

[20] Kovtun, V.V. (2021). Cryptocurrency vs criminal law. *Legal Scientific Electronic Journal,* 12, 345-347. doi: 10.32782/2524-0374/2021-12/86.

[21] Lyzunov, S., & Vereshaka, M. (2018). Hidden mining and protection against it. In V.V. Naumyk (Ed.), *Abstracts of reports of the scientific and practical conference* (pp. 910-911). Zaporizhzhia: ZNTU.

[22] Mackenzie, S. (2022). Criminology towards the metaverse: Cryptocurrency scams, grey economy and the technosocial. *The British Journal of Criminology*, 62(6), 1537-1552. doi: 10.1093/bjc/azab118.

[23] Nghiem, H., Muric, G., Morstatter, F., & Ferrara, E. (2021). Detecting cryptocurrency pump-and-dump frauds using market and social signals. *Expert Systems with Applications*, 182, article number 115284. doi: 10.1016/j.eswa.2021.115284.

[24] Panov, M.I. (2019). *Criminal offense and its types: Lecture*. Kharkiv: Pravo.

[25] Risks of terrorism and separatism. (2017). Retrieved from https://www.ipay.ua/media/files/tipolog_teror2017.pdf.

[26] Romaniuk, O. (2018). *Mysteries of cryptocurrencies: Why Ukrainian officials declare bitcoins.* Retrieved from https://economics.segodnya.ua/ua/economics/kriptovalyuta/zagadki-kriptovalyut-zachem-ukrainskie-chinovniki-deklariruyut-bitkoiny-1115821.html.

[27] Rosen, A., & Ramirez, D. (2022). *How to avoid "rug pulls", the latest cryptocurrency scam*. Retrieved from https://www.nerdwallet.com/article/investing/rug-pull.

[28] Sanz-Bas, D., del Rosal, C., Náñez Alonso, S.L., & Echarte Fernández, M.Á. (2021). Cryptocurrencies and fraudulent transactions: Risks, practices, and legislation for their prevention in Europe and Spain. *Laws*, 10(3), article number 57. doi: 10.3390/laws10030057.

[29] Siddiki, N.K., & Movchan, R.O. (2018). Cryptocurrencies and blockchain technologies in modern illegal activities. *Bulletin of the Donetsk National University named after Vasyl Stus*, 1(10), 78-83.

[30] Tartachnyi, O. (2023). *Due to the gambling business, crypto exchanges are now unable to accept and issue payments in hryvnias*. Retrieved from https://speka.media/kriptovalyutni-birzi-pripinili-vivoditi-grosi-cerez-ukrayinski-kartki-shho-vidbuvajetsya-z-binance-i-ne-tilki-9gqy8v.

[31] Thommandru, A., & Chakka, B. (2022). The globalization of cashless transactions using blockchain technology to preventing money laundering and the changing trends in the cryptocurrency market: A learning experience of polish and EU laws. *European Studies*, 9(2), 213-242. doi: 10.2478/eustu-2022-0021.

[32] Trozze, A., Kamps, J., Akartuna, E.A., Hetzel, F.J., Kleinberg, B., Davies, T., & Johnson, D. (2022). Cryptocurrencies and future financial crime. *Crime Science*, 11(1), 1-35. doi: 10.1186/s40163-021-00163-8.
[33] Wolf, S.O. (2021). Terrorism financing: Crypto-Taliban? *South Asia Democratic Forum*, 217, 1-6. doi: 10.48251/SADF.ISSN.2406-5617.C217.
[34] Yatsyk, T. (2020). Financial accounting of cryptotokens during the initial coin offering (ICO). *Young Scientist*, 2(78), 50-53. doi: 10.32839/2304-5809/2020-2-78-11.
[35] Zavalniuk, I. (2023). *The dark side of bitcoin: Top cryptocurrency crimes in Ukrainian history*. Retrieved from https://ua.news/ua/fintech-in-ukraine-30/obratnaya-storona-bytkoyna-opublykovan-top-prestuplenyj-s-kryptovalyutoj-v-ystoryy-ukrayny.
[36] Zaytoun, H.S. (2019). Cyber pickpockets: Blockchain, cryptocurrency, and the law of theft. *North Carolina Law Review*, 97(2), 395-431.

Правопорушення у сфері обігу віртуальних активів та аналіз їх кваліфікації

Максим Рафальський
Аспірант
Академія адвокатури України
01032, бульв. Тараса Шевченка, 27, м. Київ, Україна
https://orcid.org/0000-0001-9016-8613

Анотація
З появою нових форм інтерактивної взаємодії, віртуальних товарів і сервісів виникає нове поле для здійснення правопорушень у сфері обігу віртуальних активів. Це стимулює вчених і правоохоронні органи до активного дослідження цієї галузі та розроблення ефективних механізмів відповіді на виклики, що виникають, які ще не отримали належного відображення в законодавстві. Мета статті – ґрунтовно дослідити проблему, аналізуючи специфічні правопорушення, пов'язані з віртуальними активами, включаючи, але не обмежуючись крадіжкою, шахрайством, корупцією та ухиленням від податків. Використані для дослідження методи наукового пізнання охоплюють аналіз правового регулювання, методи моделювання, аналогії, системно-структурний, порівняльно-правовий, а також методи наукової абстракції та узагальнення. За результатами проведеного дослідження визначено основні види правопорушень у сфері віртуальних активів і здійснено їх уніфікацію. Встановлено недоліки в сучасному правовому регулюванні, що сприяють виникненню цих проблем. Сформовано пропозиції щодо внесення змін до Кримінального кодексу України в частині кваліфікації нових видів правопорушень, що відбуваються у сфері обігу віртуальних активів, на підставі досліджень сучасних тенденцій, міжнародного досвіду й аналізу поточного стану законодавства України. Також дослідження засвідчує, що наявні правові інструменти часто не забезпечують адекватного виявлення та притягнення до відповідальності за нові форми правопорушень, що актуалізує необхідність реформування законодавства для адаптації до сучасних динамічних умов. Практична значущість дослідження полягає у визначенні актуальних проблем правового регулювання обігу віртуальних активів, а також розробленні рекомендацій з удосконалення кваліфікації правопорушень у цій сфері

Ключові слова:
кібербезпека; кіберзлочинність; кримінальне право; кримінальний кодекс; криптовалюта