

Cryptocurrency as an Enabling Instrument of Transnational Organized Crime: A Criminological Analysis

Bohdan M Holovkin^{1†}, Oleksii V Tavalzhanskyi¹, Roman V Shapoval¹, Sergiy O Kharytonov¹ and Hanna M Zaikina²

¹Yaroslav Mudryi National Law University, Kharkiv, Ukraine

²Ukrainian State University of Railway Transport, Kharkiv, Ukraine

Received: 21st August 2025; revised: 25th February 2026

Transnational organized crime now has new structural capabilities as a result of the rapid development of digital financial technologies. Instead of treating cryptocurrencies as a separate cause of crime, this article sees them as a tool that promotes illegal financial ecosystems. The study identifies the main ways to include digital assets in drug trafficking, cyber fraud, money laundering and terrorist financing schemes through doctrinal analysis, criminological interpretation and the study of 56 court decisions related to cryptocurrencies in Ukraine. According to the study, cryptocurrency primarily serves as an accumulation and transaction tool that complements traditional illegal financial mechanisms and improves cross-border financial concealment. Although it accounts for a relatively modest percentage of illegal financial flows in the world, the technological flexibility of cryptocurrency-related crime increases the complexity of investigations and the fragmentation of regulations. A study of Ukraine's case demonstrates how institutional weakness and legal ambiguity create weaknesses that transnational criminal networks can exploit. The article proposes specific institutional and regulatory changes, such as improved international cooperation in blockchain analytics, stricter AML/KYC requirements, and clarification of the legality of digital assets. The ability of cryptocurrencies to reorganize the international logistics architecture of illegal financing gives them criminological relevance.

Keywords: Cryptocurrencies, Transnational Crime, Crime Fighting, Blockchain, Financial Security

Due to the forced transition to remote work caused by the spread of the pandemic around the world, the number of crimes using complex information technology and the digital economy has increased. The pandemic has exacerbated negative trends, including the rise of populism, protectionism, and international rivalries, which have reduced interpersonal connections and population mobility, and contributed to the development of new avenues for spreading crime, particularly on the Internet. Against this background, cryptocurrencies are rapidly spreading around the world as advanced financial and economic tools built on blockchain technology. This encourages criminals to commit crimes and implement illegal cryptocurrency exchange schemes, regardless of their location or jurisdiction. In the modern world, the law enforcement system should investigate and prevent a number of crimes, including fraud with payment cards, theft of a cryptocurrency wallet, distribution of computer viruses, theft of personal information of citizens by hackers, drug trafficking on the Internet, and distribution of illegal content.

In addition to the rapid development of complex information technologies and the government's desire to fully digitize every aspect of public life, technological progress also facilitates the commission of crimes, which leads to a sharp increase in the frequency of such crimes. That is, regarding the sustainable development of innovative technologies, the introduction of modern methods of preventing criminal offenses related to the circulation of cryptocurrencies, the development of algorithms for preventing the use of cryptocurrencies in illegal activities, and the strengthening of criminal liability for all such actions are considered relevant in law enforcement.

With the legal status of cryptocurrencies still unclear in many countries, criminal encroachments on cryptocurrency circulation are becoming more common as new payment methods gain popularity. Recently, these encroachments have become significant and systemic. Generally speaking, criminals who use cryptocurrencies as payment methods transfer large amounts of money online, neglecting traditional financial institutions, which leads to huge financial losses and undermines the

[†]Corresponding author: Email: b.m.golovkin@nlu.edu.ua

national security of the state. In light of the above, it is appropriate and appropriate to examine the criminological dangers associated with the circulation of cryptocurrencies and their use for illegal activities. International cooperation in preventing and combating corruption is crucial because corruption is no longer a local problem, but rather a global phenomenon that affects the economies and societies of all countries.¹

Several scholars have investigated the topic of crime in the field of cryptocurrency. Shulhun² investigated the use of cryptocurrencies for criminal offenses such as fraud and money laundering, and also noted that cryptocurrency is not property by law and cannot be recovered as a fine. He pointed out the lack of separate legislation in Ukraine regarding cryptocurrencies, although they can be qualified under the Criminal Code. Dolianovska and Kryvenko³ investigated criminal offenses in the circulation of virtual assets, their classification, and methods of struggle. The main types of crimes have been identified, in particular the seizure of assets and their use for the legalization of income. Analyzed violations and precautions, such as legal regulation and international cooperation.

Hres⁴ investigated the legal nature of cryptocurrency, its status as an object of criminal offenses, and the possibility of attribution to civil law relations. Different views on its legal status, comparison with property, and methods of use in crimes are considered. The need to adopt a legislative act to regulate cryptocurrency has been determined. Kutera⁵ investigated cryptocurrencies in the context of fraud, in particular money laundering and pyramid schemes. It is determined that this is a new, but rapidly growing area that requires improved legal regulation. Trozze, Davies and Kleinberg⁶ have studied cryptocurrency scams, investigating existing types of scams and potential future threats. 47 unique types of fraud were identified, among which Ponzi schemes and high-income programs were most discussed. It was found that cryptocurrency scams are developing rapidly, but require better cross-sector cooperation and harmonization of terminology to effectively combat them.

The aim of the study is to analyze the criminological aspects of the use of cryptocurrencies in transnational organized crime and to develop effective approaches to prevent crimes related to electronic currencies in the context of the rapid development of information technology and cashless assets.

The main emphasis of this study is on transnational organized crime, which is defined as organized criminal groups operating internationally and using cryptocurrency infrastructure to support cyber fraud, money laundering, drug trafficking and terrorist financing. Instead of viewing Ukraine as a separate national phenomenon, it is being investigated as a case study reflecting broader global patterns. This method allows you to find systemic criminological trends that are relevant outside a certain jurisdiction.

To study the criminological aspects of the fight against the use of cryptocurrencies in transnational organized crime, a comprehensive methodology was used that combines general scientific and special methods of knowledge. This approach allows us to comprehensively investigate the problem, given its interdisciplinary nature and the depth of the impact of cryptocurrencies on criminal activity on a global scale.

The analysis was the basic method of research aimed at isolating the components of the problem. A detailed study of the nature of cryptocurrencies, their technical features, legal status in different countries, as well as the characteristics that contribute to their use in criminal activities was carried out. In particular, analysis of anonymity, transaction speed, lack of regulation, and decentralization revealed their significant potential as a means of criminal activity.

The synthesis method allowed combining the results of the analysis of individual aspects of cryptocurrencies into a holistic system of knowledge that highlights their impact on transnational organized crime. The synthesis ensured the integration of information on the ways of criminal use of cryptocurrencies, such as money laundering, terrorist financing, drug trafficking, and cybercrime. Thanks to this, it was possible to formulate general ideas about the scale of the problem and the mechanisms of its functioning.

The induction method was used to form conclusions based on the collected empirical data, such as examples of criminal schemes using cryptocurrencies, statistics on the scale of criminal activity, and international studies on the use of cryptocurrencies in illegal activities. At the same time, the deduction method helped to apply the general patterns of the development of cryptocurrencies and crime to specific cases, for example, the impact of anonymity on money laundering or the use of the darknet for illegal operations.

The dialectical method made it possible to identify contradictions arising in the process of interaction of the cryptocurrency industry, state regulation, and the underworld. Particular attention is paid to the study of the impact of new technologies, which are both a driving force of progress and an instrument of criminal activity. The dialectical approach also helped to determine the dynamics of changes in the field of crime under the conditions of the development of cryptocurrencies.

The analytical method provided an in-depth study of the legal aspects of regulating cryptocurrencies and their use in criminal schemes. International and national regulations governing the circulation of cryptocurrencies were investigated, as well as practical approaches to combating crimes related to cryptocurrencies. This method made it possible to identify shortcomings in the legislation that facilitate the use of cryptocurrencies in criminal activity.

The analogy method was used to compare cryptocurrencies with traditional financial instruments and other digital technologies used in criminal activities. This allowed us to identify common features and differences in the mechanisms of use, risks, and possibilities of counteraction.

Abstraction made it possible to distinguish the key characteristics of cryptocurrencies as a phenomenon that promotes criminal activity. In particular, attention was focused on such aspects as anonymity, speed of transactions, and lack of regulatory control. The method of abstraction allowed us to avoid unnecessary detail and focus on key issues.

The generalization method helped formulate general conclusions about the criminological features of the use of cryptocurrencies in criminal activity and develop recommendations to increase the effectiveness of the fight against this phenomenon. Generalization of the obtained results became the basis for the formation of strategic approaches to countering the use of cryptocurrencies in criminal activities.

Thus, the use of a comprehensive methodology made it possible to comprehensively study the criminological aspects of the use of cryptocurrencies in transnational organized crime and develop recommendations to increase the effectiveness of the fight against this phenomenon. The applied methods ensured the scientific validity of the obtained results and their practical significance.

Results

A decentralized payment system completely automatically (without the need for internal or external management) produces and accounts for cryptocurrency, a kind of digital money. A fundamental feature of cryptocurrencies is the storage of information on the blockchain, where asymmetric encryption is used to verify credentials, and other cryptographic methods are used as evidence of work done and/or Proof of stake.

In general, the use of electronic currency is not illegal. On the contrary, this is significant progress in the fields of IT and the financial system. If it were not for the procedures for obtaining, extracting, and using these financial resources, nothing dangerous b. Today in the world there are many electronic currencies, both active and popular for investment, and inactive and unloved. We are interested in the first group.⁶

Consider Bitcoin, the most famous electronic money, the value of which has increased significantly in recent years. Text files and digital currency, especially Bitcoin, are comparable. You just need to know the electronic wallet number to complete the transaction, as the relevant transactions occur in the form of an electronic message. Therefore, the advantages of this currency include decentralization, the absence of a single owner, anonymity and speed of transactions, and significant simplicity of financial activity.

Electronic currencies are now a convenient way to pay, earn, and finance criminals who commit crimes in various spheres of public life, such as cyberbullying, terrorism, and the legalization (laundering) of money earned illegally.⁷ Electronic currencies have become popular not only because of their high market value or high transaction speed but also because their owner is unknown, which makes crime in this space, in particular, using cryptocurrencies, naturally prone to delays.⁸

The first to discuss the criminal threats associated with the use of cryptocurrency was Europol. In his 2015 study, he determined that new financial instruments are more popular in the criminal sector (corruption crimes, drug trafficking, psychotropic drugs, and pornography) by analyzing bitcoin turnover patterns. Cryptocurrency is most often used to purchase goods that have been withdrawn from circulation on the illegal Internet, sometimes known as the "dark net." Even though by the end of 2018

the number of illegal uses of cryptocurrency has increased significantly, the most common use of cryptocurrency remains payment in underground markets.

The main reasons that cryptocurrency, and above all its most popular representatives - Bitcoin, Ethereum, Monero, and others, become the subject of criminal offenses are, firstly, its unreasonably high value in monetary terms, which is characterized by volatility, and secondly, constant coverage of the situation around it in public space. Although Ukraine has not yet established responsibility for the illegal seizure of cryptocurrency, since its legal status is still unknown, criminal crimes against property (such as theft, robbery, and extortion) are quite common in the world. These crimes involve the theft of computer equipment, hard drives, or portable cryptocurrency wallets, together with the corresponding passwords, to seize the cryptocurrency and receive money from its subsequent conversion.²

The main characteristics of cryptocurrencies that make them criminogenic are: the anonymity of transactions and users, which makes it impossible to identify them; complete decentralization, when money is stored in the wallets of millions of users around the world; lack of control over payments and transactions; independence from financial systems; lack of state regulation; as well as the ease and speed of transactions, since they only require a computer or smartphone and a reliable Internet connection. Now you can buy a variety of illegal products and services with bitcoins.

Cryptocurrencies have structural advantages over traditional financial instruments, making them particularly suitable for global organized crime. First, in cross-border transfers, aliasing reduces the danger of early detection and eliminates the need for intermediaries. Second, independent of correspondent banking networks, blockchain-based transfers allow for fast money transfers between jurisdictions.

Most importantly, cryptocurrencies work alongside traditional money laundering methods, rather than completely replacing them. Cryptocurrency assets are commonly used by criminal organizations along with traditional money laundering strategies, including offshore accounts, fictitious corporations, and high-cash businesses. Through inter-chain switching, service combination, and the use of privacy-focused coins, cryptocurrencies are mostly used in the layering phase of this hybrid architecture to increase transaction complexity.

Moreover, criminal organizations are quickly adapting to changes in legislation. Offenders switch to decentralized exchanges, peer-to-peer platforms, or privacy-enhancing technologies when exchanges provide rigorous AML/KYC processes. This adaptive dynamic shows that cryptocurrency-backed crime does not exist as a static phenomenon, but changes in response to judicial pressure. According to criminology, the appeal of cryptocurrencies lies not only in their anonymity, but also in their ability to reorganize illegal financial transactions on a global basis.

Investigations into drug trafficking, cyber fraud, ransomware and some cases related to terrorist financing are increasingly revealing cryptocurrency. However, international studies now available indicate that traditional cash and banking systems continue to dominate global illicit financial movements, with crypto-assets currently accounting for a small portion of these flows. So, instead of being the main driving force behind larger illegal financial ecosystems, cryptocurrencies should be seen as an evolving tool within them.

The following types of use of cryptocurrency during the commission of crimes can be distinguished:

1. The use of cryptocurrency for criminal purposes as a tool or means of criminal encroachment (as cash when buying weapons, narcotic drugs, psychotropic substances, and other prohibited items, legalization (laundering) of criminal proceeds, terrorist financing, etc.).

2. Criminal encroachments on cryptocurrencies include cryptocurrency extortion, online fraud, and bitcoin theft from accounts. Phishing sites for cryptocurrency exchanges are now very common. These sites ask users to enter a secret key or transfer money to the fraudster's electronic wallet. When attackers gain access to a user's wallet, they move the cryptocurrency stored there to other wallets.

3. Use of cryptocurrency in information warfare. The pricing of cryptocurrencies is influenced by additional aspects that are not characteristic of traditional fiat money, since they are decentralized and do not directly depend on any currency or other goods, especially gold. The cryptocurrency exchange rate is influenced, in particular, by the number of its users, so there may be cases of manipulation of public opinion or interference with strategic information systems of the state to influence the cryptocurrency exchange rate, and therefore the security of the state.

4. Mining for cryptocurrency. The process of mining bitcoins involves the creation of so-called "farms," which are huge networks of computers that are constantly working and used to perform computational calculations that lead to mining and accumulation of cryptocurrency. For continuous operation, farms need a stable power supply in large volumes. Now there are many cases when people use electricity without permission or create these farms based on business, especially the state.⁹

Since it is known that crime coexists with technological progress, the question arises of how to combat criminal activity and stop it in a certain place. Consider the following offenses that occur when receiving cryptocurrency without falling into criminal schemes that use it as a reward or a tool for committing a crime: theft of electricity, unauthorized connection to energy networks, unauthorized use without accounting tools, interference with computer systems and interference with public and private electronic systems. Since the production of the same bitcoin requires a significant amount of electricity, the aforementioned criminal activity largely threatens the country's energy security.

Theft of electricity for the productive work of mining farms in recent years has become the main topic of news in the media and press centers of law enforcement agencies. The problem is that criminal offenses involving various forms of electronic currencies pose a transnational risk, including the potential for financing various criminal illegal activities secretly and anonymously to undermine the political and civil situation in any country. This threat goes beyond the economic security of Ukraine.

There is not a single example of control over the circulation, production, exchange, and conversion of these currencies if we look at many countries. State bodies have no authority over them when it comes to controlling the circulation of money and securities. These structural characteristics help explain why organized criminal networks continue to find cryptocurrencies attractive.¹⁰

The use of this kind of money is risky because it is a cloud asset that can be used as a payment, not banknotes or other monetary assets. It is important to note that according to the results of a statistical study conducted by the international IT services company Triple-A, Ukraine is in the top 10 countries in terms of the number of cryptocurrency owners. This

indicates that there is a significant concentration of assets that can be converted for certain needs.¹¹

Since all trade in drugs and precursors in Ukraine, for example, is carried out through electronic wallets, which are paid in local currency before conversion into any cryptocurrency, it is possible to track the movement of assets, but it is impossible to identify the person who made the transaction. Another problem is that the darknet system is used to buy and sell a variety of restricted or prohibited drugs. A darknet is an overhead network that can only be accessed using certain software, configurations, or permissions; it often uses unconventional communication protocols and ports.¹²

A system of disconnected virtual tunnels that provides encrypted data transmission is known as an anonymous network. Unlike other distributed peer-to-peer networks, the darknet allows users to interact without fear of government interference, since file sharing occurs anonymously (since IP addresses are not publicly available). For this reason, the darknet is often seen as a means of communication for a variety of illegal and covert operations. In a broader sense, the phrase "darknet" can refer to any "underground" Internet communications and technologies that are mainly associated with illegal activities or protests, or it can refer to non-profit "nodes" of the Internet. Anonymous buyers, who often pay with bitcoins, buy goods and services on black markets on the darknet.

Alphabet in Market is one of the largest darknet marketplaces. About 70% of different types of drugs are also available on the darknet. In addition, you can buy profiles on social networks, scans of your passport and personal data, as well as several other documents, such as driver's license and passport numbers. Scanned copies of credit cards are widespread on the darknet, where they are used to steal cards or steal money from credit cards. The popularity and relative openness of the darknet service contribute to the widespread use of cryptocurrencies, which makes it easy to legalize money earned illegally.³

Take, for example, the ability of any user on the Bitcoin network to generate an infinite number of addresses without revealing their identity. Operations with two addresses managed by one person are identical to transactions with addresses controlled by individuals. Accordingly, theoretically, attackers can make 100,000 Bitcoin transactions between addresses that are under their control before transferring the

cryptocurrency to another format. Reconstructing such a transaction line would take too long if at all, to do, especially if done manually.

This method can be used in a complex money laundering plan that involves virtual currency and multiple people. Secondary trading of virtual currencies, such as through online auctions or other trading platforms, offers advantageous opportunities to increase the complexity of conducting transaction investigations in addition to the primary trading that occurs with virtual currency administrators or on exchanges.¹³ The results of a one-year UN study show that from 800 billion to 2 trillion US dollars, or 2-5% of global gross domestic product, is laundered worldwide as a result of numerous criminal acts.

It should be noted that this assessment does not mean that cryptocurrency is the main channel of money laundering; rather, it refers to money laundering around the world in general. According to available data, cryptocurrency-related money laundering accounts for a relatively small but growing part of criminal finance worldwide.

If we describe cryptocurrencies from a criminological point of view as a means of committing a criminal offense, then it is worth noting the following features:

- operation processing speed;
- anonymity of the owner or the person who operates the data;
- a significant number of chains of intricate transactions;
- access to assets from anywhere in the world via the Internet;
- convenience in transportation;
- lack of full control and regulation by the authorities of many countries.¹⁴

From a criminological point of view, cryptocurrency contributes to circumstances that can significantly contribute to certain phases of criminal activity, including cross-border transfers and the concealment of financial data. To legalize the proceeds from crime, most of which are received in cash, recently there have been tendencies to popularize the use of virtual currencies in illegal financial schemes. As a result, organized criminal organizations especially often use cryptocurrency as a tool for illegal operations related to fraud in the IT technology sector of the so-called "pyramid schemes."

Due to the rapid growth of cryptocurrencies in the global financial system and the development of digital

technologies, the criminological elements of counteracting their use in transnational organized crime are becoming increasingly significant. Bitcoin, Ethereum, and other cryptocurrencies have emerged as technology that creates new avenues for financial transactions that are not directly regulated by the government. This allows criminal organizations to avoid traditional banking supervision and detection of illegal flows during illegal financial transactions on a global scale. The use of cryptocurrency in organized crime can take many forms, ranging from trafficking in drugs, weapons, and people to money laundering and supporting terrorist groups.¹⁵

The fight against money laundering has become much more difficult with the development of cryptocurrency. Since cryptocurrencies are decentralized and anonymous, organized criminal groups can transfer money between countries without sufficient control. This allows them to evade established banking institutions and launder the proceeds of illegal activities. In addition, the use of cryptocurrencies significantly increases risks for legal and financial institutions, since many transactions can occur without access to proper customer information.¹⁶

The use of cryptocurrency to finance violent crimes such as terrorism is another major concern. Because cryptocurrencies allow anonymous cross-border transactions, terrorist groups can use them to fund their operations without involving state regulators. Such operations can be carried out without identifying the final recipients or the source of cash, which greatly complicates the work of law enforcement agencies.¹⁷ There is a significant problem with the lack of a single legal framework to regulate cryptocurrencies around the world, as they are not governed by the usual rules. Cryptocurrency wallets and exchanges are exempt from the same rules that apply to traditional financial institutions when it comes to identifying users or identifying questionable transactions. This creates several gaps in the system that criminals can use to transfer illegal payments.

Strengthening international cooperation is a crucial step in the fight against this problem. It is necessary to develop effective methods for tracking and identifying cryptocurrency transactions to successfully prevent their use for illegal actions. International organizations should, in particular, create a unified policy that will limit the use of cryptocurrencies in illegal financial schemes. In addition, it is important to strengthen the interaction

between financial institutions and law enforcement agencies to identify and block cryptocurrency transactions that may be associated with organized crime.¹⁸

The creation of new technologies that allow in-depth research of cryptocurrency transactions and identify criminals is now a crucial component in the fight against the use of cryptocurrencies for illegal purposes. To detect suspicious behavior and investigate, law enforcement agencies can use tools such as analytical systems that can monitor the flow of cryptocurrencies through the blockchain. However, to achieve real success, it is necessary to integrate these technologies into international legal supervision systems and ensure effective legal responsibility for the use of cryptocurrencies for criminal purposes.

It should be noted that martial law is currently in force in Ukraine, which was introduced by Decree of the President of Ukraine on 24.02.2022 No64/2022 and approved by the Law of Ukraine "On Approval of the Decree of the President of Ukraine" On the Introduction of Martial Law in Ukraine "24.02.2022 No. 2102-IX. The restriction, and in some cases the outright prohibition of cross-border foreign exchange transactions from Ukrainian banks to the accounts of foreign financial institutions, as well as transactions related to the purchase, exchange, and replenishment of electronic wallets - that is, any exchange of foreign currency in swap mode, P2P-perekazi, and quasi-cash transactions - was decided to stop the flight of capital. In addition to preserving Ukraine's economic security and stability, these restrictions also stop financing terrorist fronts and hostile subversive organizations.¹⁸

The decision of the NBU Board dated March 4, 2022 No. 36, as amended by the decision of the Board of the National Bank of Ukraine dated March 21, 2022 No. 58, dated April 4, 2022 No. 68, dated April 20, 2022 (Kyiv No. 78), was able to significantly suspend the capital flow from Ukraine. From the beginning of Russia's full-scale invasion of Ukraine until April 20, 2022, according to NBU estimates, about 3 billion US dollars were withdrawn from Ukraine.

The Unified State Register of Court Decisions has checked all currently available court verdicts in proceedings in which cryptocurrency was used to highlight the current situation and trends in the spread of criminal offenses using cryptocurrency in Ukraine. Some conclusions were drawn from this analysis. On December 8, 2017, the first sentence in Ukraine was

passed in the case of 755/17724/17. In this case, the accused paid 1800 UAH for the online purchase of a particularly dangerous cannabis drug, which he then transferred to an electronic wallet in the form of cryptocurrency, namely "Bitcoin."

Currently, 56 court decisions are registered in the Unified State Register of Court Decisions, where bitcoin is used mainly as a means to commit crimes, and in a small number of cases as the subject of these crimes. So, from the statistical data of the above table, it is clear that the bulk of criminal offenses are associated with the illegal trafficking of narcotic drugs, psychotropic substances, their precursors, and equivalents. In all documented cases, bitcoins are used as a way to commit a crime, namely as payment for illegal drugs, by this category of crimes. As for criminal offenses under Article 209 of the Criminal Code of Ukraine, the legalization of property obtained by criminal means (mainly from the sale of narcotic drugs) was carried out by exchanging money from electronic wallets for cryptocurrency – bitcoin.¹⁹

According to the structural analysis, most of these 56 cases concern activities related to drug trafficking, where cryptocurrency was mostly used as a form of payment. Fraud, illegal interference in computer systems and terrorist financing account for a smaller percentage. In almost all cases, cryptocurrency served as a transactional tool rather than a primary criminal purpose. This shows that instead of creating completely new types of crime, cryptocurrencies in the Ukrainian context usually serve to strengthen already existing illegal markets.

The mechanism of crimes under Article 361-1 of the Criminal Code of Ukraine is the development of malicious programs that infect users' computers and use their resources to mine cryptocurrency without their knowledge. You can also use "stiller" apps that steal your Bitcoin wallet login credentials. Cryptocurrency was used to obtain confidential data under Article 361 of the Criminal Code and to pay for restricted materials under Article 361-2 of the Criminal Code. Pornography was bought using cryptocurrency in violation of Article 301 of the Criminal Code.

Using cryptocurrency to pay for drugs on websites is also considered drug trafficking (Articles 255, and 256 of the Criminal Code). Cryptocurrency fraud occurs when thieves obtain wallets or bitcoins by deception. Cryptocurrency was used to help terrorists in eastern Ukraine finance terrorism (Article 110 of

the Criminal Code). The inability to quantify the amount of damage caused makes it difficult for the scientific community to qualify crimes related to cryptocurrencies. Since cryptocurrency does not have a clearly defined status and mechanism for converting it into a monetary equivalent, forensic examinations cannot accurately assess the material consequences, which complicates the qualification of such crimes.²⁰

Given the constant development of digital financial technologies and the growing threat posed by criminal organizations that use cryptocurrencies for illegal operations, the criminological elements of the fight against the use of cryptocurrencies in transnational organized crime in Ukraine are decisive. One of the countries where cryptocurrencies are now widely used by both ordinary people and organized criminal groups is Ukraine. Criminals use cryptocurrency for money laundering, terrorist financing, drug and arms trafficking, and other forms of transnational criminal activity because of its anonymity and decentralized structure.²¹

The lack of clear legal control over cryptocurrencies in national legislation is one of the biggest problems faced by Ukrainian law enforcement agencies. Even though cryptocurrencies have been used in Ukraine since the 2010s, it is still unclear how they stand legally. This creates legal gaps that allow criminals to use cryptocurrencies for various illegal financial transactions without proper control and supervision. In this regard, law enforcement agencies face difficulties in identifying criminals who use cryptocurrency for money laundering, since the blockchain provides transparency of operations, but does not allow identifying real participants in transactions.²²

Transnational organized crime in Ukraine actively uses cryptocurrencies to carry out cross-border financial transactions, which complicates cooperation between law enforcement agencies of different states. Criminal groups can use these technologies to hide the source of funds, move them, and legalize them through cryptocurrency platforms and exchanges that are not always subject to national legislation. In addition, there is a threat that Ukraine could become a haven for international criminal groups that use the country's territory for anonymous financial transactions, which greatly complicates the fight against this phenomenon.⁴

To combat financial crimes, Ukrainian law enforcement officers have already begun to use

modern technologies, in particular analytical systems that analyze Bitcoin transactions. Unfortunately, the lack of specific standards in the criminal and civil legislation of Ukraine makes it extremely difficult to effectively implement these technologies in real scenarios. Since cryptocurrencies are not legally recognized as a form of payment, law enforcement agencies cannot investigate cryptocurrency transactions and implement clear policies to prevent such crimes.

International cooperation is crucial in the fight against the illegal use of cryptocurrencies, especially with the United States, the European Union, and other countries that have created legal frameworks to track bitcoin transactions. To exchange information on transactions and dubious cash flows, Ukraine already regularly cooperates with international law enforcement organizations, in particular Interpol and Europol. However, the integration of Ukrainian law enforcement agencies into the international cryptocurrency regulatory system is also an important prerequisite for a successful fight, as it will allow early detection and suppression of illegal activities.²³

Another important factor is the need to create and apply special laws in Ukraine that would regulate the use of cryptocurrencies. Determining the current state of cryptocurrencies is crucial, but it is also important to develop effective controls to limit their use. This covers the need for cryptocurrency exchanges to deploy user identification and transaction systems in addition to complying with anti-money laundering and terrorist financing regulations.

Strengthening the participation of financial institutions in tracking and prohibiting suspicious transactions with bitcoins is one of the potential ways to counter the use of cryptocurrencies for illegal purposes. To quickly detect and stop illegal financial transactions conducted through cryptocurrencies, Ukrainian banks, payment systems, and cryptocurrency exchanges must work closely with law enforcement agencies. Thus, to address the criminological elements of countering the use of cryptocurrency in transnational organized crime in Ukraine, a comprehensive strategy is needed that includes technological progress, improved legal framework, and international cooperation. Only by using the latest methods of tracking cryptocurrency transactions and creating unambiguous regulatory standards can Ukraine successfully withstand this modern danger.²⁴

Discussion

The EU, US, and Ukraine should take comprehensive legislative efforts and practical steps to more effectively combat the use of cryptocurrency in transnational organized crime. The first step in regulating the cryptocurrency market is to create standardized rules that would clearly define the status, circulation, and accounting of cryptocurrencies. It will be possible to prevent legal gaps that give criminals an advantage if such standards are agreed upon between countries.

The United States, Ukraine, and the EU should work together to create interstate channels to exchange information about dubious cryptocurrency transactions. This involves signing international agreements that will give countries "financial intelligence services access to the data they need, including information about the origin and purpose of transactions. Ukraine's inclusion in international organizations such as the Financial Action Task Force (FATF), which sets global standards for combating money laundering, is a significant step in this direction.

To track and evaluate blockchain transactions, it is necessary to use the latest technological methods. The use of tools such as blockchain analytics allows you to track the movement of cryptocurrencies and identify suspicious schemes. To do this, it is necessary to create state or private-state competence centers that will develop and implement such technologies.²⁵ The key component is strengthening control over cryptocurrency exchange platforms. All cryptocurrency exchanges must obtain licenses and adhere to standards similar to those applied to banks, including know-your-customer (KYC) and anti-money laundering (AML) procedures. Exchanges must notify the relevant authorities of suspicious transactions.

The following changes to the law are proposed:

- (i) Provide cryptocurrencies with an accurate legal definition as a type of property that can be seized and confiscated.
- (ii) Make it mandatory for Bitcoin exchanges operating in national jurisdictions to obtain a license and register.
- (iii) Force centralized storage and storage service providers to comply with legally binding AML/KYC requirements.
- (iv) Establish legal procedures to locate, freeze and seize digital assets in criminal matters.

(v) Create specialized financial and cyber investigation teams equipped with technical knowledge of blockchain analytics.

These steps will address the regulatory loopholes currently being exploited by organized criminal groups.

In addition, it is advisable to expand the powers of law enforcement agencies to conduct operational search activities in the field of digital currencies. This involves the creation of specialized units that will have access to technological tools and will cooperate with international partners to investigate crypto crimes.²⁶ It is worth stepping up work to popularize information among the population and businesses about the risks of using cryptocurrencies in criminal schemes. It is necessary to introduce mandatory training programs for bank employees, law enforcement officers, lawyers, and judges to identify and counter the illegal use of cryptocurrencies. This will increase the overall level of awareness and reduce the vulnerability of society to criminal manipulation.

Using the darknet for illegal purposes is a serious problem. To counter this, investment is needed in creating tools to identify darknet users. In addition, it is worth strengthening responsibility for operations on the dark network associated with illegal Bitcoin transactions. Another area is the creation of methods to reduce the harm caused by crimes related to cryptocurrency. This involves creating a reserve fund to compensate victims of theft or fraud in this region.⁵

Given the global nature of cryptocurrencies, only close international cooperation can combat their use in transnational crime. To monitor threats, share best practices, and plan actions to prevent the illegal use of digital currencies, it is necessary to create permanent international working groups. To successfully prevent the use of cryptocurrencies in transnational organized crime, it is imperative to harmonize laws, introduce new technologies, strengthen international cooperation, and implement educational programs.

Conclusions

This study shows that cryptocurrency, instead of serving as the structural basis of international organized crime, mostly serves as a facilitating tool. Its flexibility of adaptation to variable regulatory bases, rapid cross-border transfer, technological decentralization and pseudonymity – all contribute to its criminogenic potential. These traits drastically change the financial and logistical basis used by

organized crime to function, but they do not create entirely new types of criminal activity.

According to a study of the Ukrainian case, cryptocurrency most often serves as an addition to already existing illegal markets, especially those related to drug trafficking, cyber fraud, unauthorized interference in information systems, and some types of terrorist financing. Rather than being the primary target of the crime, Bitcoin has been used as a transactional tool in the vast majority of documented cases. This means that instead of replacing established criminal structures, digital assets are integrated into already existing criminal ecosystems. Although global illicit cash-based and bank-based financial flows still account for a larger share of crime, technological flexibility and transnational cryptocurrency outreach are leading to increased investigative complexity and fragmentation of jurisdiction.

By promoting transaction obfuscation strategies such as chain switching, the use of multiple wallets, decentralized exchanges, and privacy-enhancing technologies, cryptocurrencies improve the layering and concealment steps of money laundering from a criminological perspective. As the rules tighten, organized crime groups adapt, changing their platforms and technological tools. The need for continuous institutional adaptation is highlighted by the dynamic interaction between technological innovation and regulatory intervention.

Therefore, a number of interrelated components are necessary to effectively counter: (1) legal clarification of the status of digital assets as property subject to seizure and confiscation; (2) stricter and more enforceable AML/KYC requirements for cryptocurrency service providers; (3) development of specialized investigative capabilities in blockchain analytics; and (4) improved international cooperation in financial intelligence sharing and digital asset tracking. In the absence of coordinated cross-border processes, organized criminal networks will continue to enjoy regulatory asymmetries.

The ability of cryptocurrencies to change the global logistics basis of illegal money ultimately gives them criminological relevance. Cryptocurrency should be seen as a technologically sophisticated intermediary integrated into larger organized criminal groups, rather than as a separate criminal economy. To address this challenge, in addition to legislative reform, international harmonization of regulatory standards, institutional coordination and strategic integration of technological skills are needed.

References

- 1 Holovkin B M, Semenyshyn M, Tavolzhanskyi O V, Lysodyed O V & Smetanina N V, Fight against corruption-related crimes in wartime in Ukraine, *International Annals of Criminology*, 61 (3-4) (2023) 384, <https://doi.org/10.1017/cri.2023.31>.
- 2 Shulhun D V, Criminalization of offenses related to cryptocurrencies, in *Reforming the Legal System in the Context of Euro-Integration Processes: Proceedings of the VII International Scientific and Practical Conference* (Sumy, 18-19 May 2023) (Sumy State University, Sumy), 2023, 320.
- 3 Dolianovska I M & Kryvenko K O, Global experience in counteracting criminal offenses related to the circulation of virtual assets, *Legal Bulletin*, 2024, 79, <https://doi.org/10.31732/2708-339X-2024-12-A12>.
- 4 Hres D O, Cryptocurrency as an object of criminal offenses against property, *Scientific Papers Collection of Kharkiv National Pedagogical University Named After H. S. Skovoroda "Law"*, (37) (2023) 29, <https://doi.org/10.34142/23121661.2023.37.04>.
- 5 Kutera M, Cryptocurrencies as a subject of financial fraud, *Journal of Entrepreneurship, Management and Innovation*, 18 (4) (2022) 45, <https://doi.org/10.7341/20221842>.
- 6 Trozze A, Davies T & Kleinberg B, Explaining prosecution outcomes for cryptocurrency-based financial crimes, *Journal of Money Laundering Control*, 26 (1) (2023) 172, <https://doi.org/10.1108/JMLC-10-2021-0119>.
- 7 Holovkin B, Cherniavskiy S & Tavolzhanskyi O, Factors of cybercrime in Ukraine, *Relações Internacionais no Mundo Atual*, 3 (41) (2023) 464, <https://doi.org/10.21902/Revrima.v3i41.6401>.
- 8 Budik I M, Determinants of crimes committed by participants of criminal organizations in the sphere of trafficking narcotic substances, psychotropic substances, their analogs, and precursors, *Analytical and Comparative Legal Studies*, (5) (2024) 672, <https://doi.org/10.24144/2788-6018.2024.05.104>.
- 9 Topchii V V & Svintsytskyi A V, Methodological principles of ensuring participation of persons during criminal proceedings, *Irpın Legal Journal*, 2 (9) (2022) 204, [http://dx.doi.org/10.33244/2617-4154-2\(9\)-2022-204-213](http://dx.doi.org/10.33244/2617-4154-2(9)-2022-204-213).
- 10 Leonov B, Criminal law counteraction to the financing of terrorism in the context of ratifying the Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism, *Information and Law*, 4 (47) (2023) 177, [https://doi.org/10.37750/2616-6798.2023.4\(47\).291660](https://doi.org/10.37750/2616-6798.2023.4(47).291660).
- 11 Nolasco Braaten C & Vaughn M S, Convenience theory of cryptocurrency crime: A content analysis of U.S. Federal Court decisions, *Deviant Behavior*, 42 (8) (2021) 958, <https://doi.org/10.1080/01639625.2019.1706706>.
- 12 Kabachna O V, Current trends in criminal policy to combat financial crime, *Irpın Legal Journal*, 1 (14) (2024) 97, [https://doi.org/10.33244/2617-4154-1\(14\)-2024-97-104](https://doi.org/10.33244/2617-4154-1(14)-2024-97-104).
- 13 Huang S, *Cryptocurrency and crime*, In A Lui & N Ryder (Eds.), *FinTech, Artificial Intelligence and the Law: Regulation and Crime Prevention* (Routledge, London), 2021, 125.
- 14 Malov B Y, Strategies for preventing an increase in crime rates in the country during military aggression, *Irpın Legal Journal*, 3 (12) (2023) 318, [https://doi.org/10.33244/2617-4154-3\(12\)-2023-318-326](https://doi.org/10.33244/2617-4154-3(12)-2023-318-326).

- 15 Wahrstätter A, Gomes J, Khan S & Svetinovic D, Improving cryptocurrency crime detection: Coinjoin community detection approach, *IEEE Transactions on Dependable and Secure Computing*, 20 (6) (2023) 4946, <https://doi.org/10.1109/TDSC.2023.3238412>.
- 16 Pravdyuk A L, Constitutional guarantees of informational security of individuals and citizens, *Legal Scientific Electronic Journal*, (12) (2021) 303, <https://doi.org/10.32782/2524-0374/2021-12/75>.
- 17 Omelchuk O M, Haiur I Y, Kozyt'ska O G, Prysiashna A V & Khmelevska N V, Analysis of the activities of law enforcement authorities in the field of combating crime and corruption offences, *Journal of Money Laundering Control*, 25 (3) (2022) 700, <https://doi.org/10.1108/JMLC-07-2021-0073>.
- 18 Kozii V V, Copying, archiving, and hashing files when recording data from the Internet during the investigation of crimes in the cryptocurrency sphere, in *Current Issues and Prospects for the Use of Operational and Investigative Means in Solving Crimes in Martial Law Conditions: Materials of the Interdepartmental Scientific and Practical Conference* (Kyiv, 30 March 2023) (National Academy of Internal Affairs, Kyiv), 2023, 73.
- 19 Orlovskyi R, Kharytonov S, Samoshchenko I, Us O & Iemelianenko V, Countering cybercrime under martial law, *Journal of Cyber Security and Mobility*, 12 (6) (2023) 893, <https://doi.org/10.13052/jcsm2245-1439.1264>.
- 20 Samoylenko O A & Titunina K V, Typical forensic tools for investigating criminal offenses related to the use of cryptocurrencies, *Actual Issues in Modern Science*, 7 (13) (2023) 409, [https://doi.org/10.52058/2786-6300-2023-7\(13\)-409-420](https://doi.org/10.52058/2786-6300-2023-7(13)-409-420).
- 21 Haltsova V V, Kharytonov S O, Khramtsov O M, Zhytniy O O & Vasyliiev A A, The criminal law as a means of protecting human rights and freedoms in the modern world, *Bulletin of the National Academy of Legal Sciences of Ukraine*, 28 (3) (2021) 248, [https://doi.org/10.37635/jnalsu.28\(3\).2021.248-256](https://doi.org/10.37635/jnalsu.28(3).2021.248-256).
- 22 Movchan A, Shliakhovskiyi O, Kozii V & Fedchak I, Investigating cryptocurrency financing crimes related to terrorism and armed aggression, *Social & Legal Studies*, 6(4) (2023) 123, <https://doi.org/10.32518/sals4.2023.123>.
- 23 Cherevko V V & Dufeniuk O M, Cryptocurrency as an object of forensic research, in *Procedural and Forensic Support of Pre-Trial Investigation: Abstracts of the Scientific and Practical Seminar* (Lviv, 2 December 2022) (Lviv State University of Internal Affairs, Lviv), 2022, 121.
- 24 Maurushat A & Halpin D, *Investigation of cryptocurrency-enabled and dependent crimes*, In D Goldbarsht & L de Koker (Eds.), *Financial Technology and the Law: Combating Financial Crime* (Springer International Publishing, Cham), 2022, 235.
- 25 Bohdan E, The use of cryptocurrency for the legalization of funds obtained illegally: A bibliometric analysis, *Development Service Industry Management*, (3) (2024) 213, [https://doi.org/10.31891/dsim-2024-7\(31\)](https://doi.org/10.31891/dsim-2024-7(31)).
- 26 Trozze A, Kamps J, Akartuna E A, Hetzel F J, Kleinberg B, Davies T & Johnson S D, Cryptocurrencies and future financial crime, *Crime Science*, 11 (2022) 1, <https://doi.org/10.1186/s40163-021-00163-8>.