Management (Montevideo). 2025; 3:253
doi: 10.62486/agma2025253
ISSN: 3046-4048

ORIGINAL

Legislative Categorization of Crimes Committed with the Help of Cryptocurrencies

Categorización legislativa de los delitos cometidos con la ayuda de criptomonedas

Kostiantyn Orobets[1], Vladyslav Shkolnikov[2], Tetiana Batrachenko[3], Tetiana Baranovska[4], Valeriy Sereda[5]

[1]Yaroslav Mudryi National Law University, Department of Criminal Law Policy. Kharkiv, Ukraine.
[2]National Academy of Internal Affairs, Department of Criminology and Information Technologies. Kyiv, Ukraine.
[3]University of Customs and Finance, Department of Law Enforcement. Dnipro, Ukraine.
[4]Zhytomyr Polytechnic State University, Department of Law and Law Enforcement. Zhytomyr, Ukraine.
[5]Institution of Higher Education "Lviv University of Business and Law", Educational and Scientific Institute of Law and Social and Humanitarian Sciences. Lviv, Ukraine.

Cite as: Orobets K, Shkolnikov V, Batrachenko T, Baranovska T, Sereda V. Legislative Categorization of Crimes Committed with the Help of Cryptocurrencies. Management (Montevideo). 2025; 3:253. https://doi.org/10.62486/agma2025253

Submitted: 16-06-2024 **Revised:** 10-01-2025 **Accepted:** 10-06-2025 **Published:** 11-06-2025

Editor: Ing. Misael Ron

ABSTRACT

Introduction: the legal regime of cryptocurrency in different countries of the world is heterogeneous. In some, it is not defined at all, which leads to legal conflicts, including when qualifying crimes committed with cryptocurrency use. The situation is further complicated because such crimes can occur in the territories of several states where cryptocurrency has a different legal regime. Traditional legislation and mechanisms for combating money laundering and terrorist financing are practically ineffective in the landscape of crimes involving the use of cryptocurrency.
Objective: the aim of the study is to systematise the main patterns of crimes related to the use of cryptocurrency, as well as analyse existing vectors of their legal assessment, appropriate design and application of effective methods of combating these crimes.
Method: based on the methods of analysis and synthesis, qualitative data analysis, using content analysis as the primary research tool, it is shown that the main problem in preventing the use of cryptocurrency in predicate crimes lies in the technical difficulty of identifying a person or group of persons who carry out cryptocurrency transactions for illegal purposes. Such goals may be aimed at legalising funds, i.e., concealing their illegal origin, making payments in a hidden network, organising various fraudulent schemes, financing terrorism, and other crimes.
Results: the article argues that given the technical specifics of cryptocurrency transactions and the technical capabilities of "masking" the origin of cryptocurrency funds, it is necessary to develop methods for studying trace formation and develop an algorithm for establishing and consolidating forensically significant information for this type of crime. The results indicate that the future of law enforcement in the fight against cryptocurrency-related crime will require a multifaceted approach. Agencies must adopt a proactive approach by foreseeing emerging criminal strategies. To protect the public from crimes using digital assets, law enforcement must be flexible, progressive, and technologically savvy as cryptocurrencies continue to develop. The development of provisions on cryptocurrency also determines the theoretical significance of the work as an object and means of committing crimes, a surrogate means of payment during the commission of certain crimes.
Conclusions: the practical significance of the work lies in the possibility of using its results to solve problems arising in the law-making activities of state authorities and law enforcement activities, as well as in developing recommendations for improving criminal legislation in the field of cryptocurrency-related crimes.

Keywords: Cryptocurrencies; Cybercrime; Money Laundering; Terrorist Financing.

RESUMEN

Introducción: el régimen jurídico de la criptomoneda en los diferentes países del mundo es heterogéneo. En algunos, no está definido en absoluto, lo que conduce a conflictos legales, incluso a la hora de calificar los delitos cometidos con el uso de criptodivisas. La situación se complica aún más porque tales delitos pueden ocurrir en los territorios de varios estados donde la criptomoneda tiene un régimen jurídico diferente. La legislación y los mecanismos tradicionales de lucha contra el blanqueo de dinero y la financiación del terrorismo son prácticamente ineficaces en el panorama de los delitos relacionados con el uso de criptodivisas.
Objetivo: el objetivo del estudio es identificar y sistematizar los principales patrones de delitos relacionados con el uso de criptodivisas, así como analizar los vectores existentes de su valoración jurídica, diseño adecuado y aplicación de métodos eficaces de lucha contra estos delitos.
Método: a partir de los métodos de análisis y síntesis, análisis cualitativo de datos, utilizando como herramienta primaria de investigación el análisis de contenido, se demuestra que el principal problema para prevenir el uso de criptodivisas en delitos precedentes radica en la dificultad técnica de identificar a una persona o grupo de personas que realizan transacciones de criptodivisas con fines ilícitos. Dichos objetivos pueden estar dirigidos a legalizar fondos, es decir, ocultar su origen ilegal, realizar pagos en una red oculta, organizar diversos esquemas fraudulentos, financiar el terrorismo y otros delitos.
Resultados: el artículo argumenta que dadas las especificidades técnicas de las transacciones de criptodivisas y las capacidades técnicas de "enmascarar" el origen de los fondos de criptodivisas, es necesario desarrollar métodos para estudiar la formación de rastros y desarrollar un algoritmo para establecer y consolidar información forense significativa para este tipo de delitos. Los resultados indican que el futuro de la aplicación de la ley en la lucha contra los delitos relacionados con las criptomonedas requerirá un enfoque multifacético. Las agencias deben adoptar un enfoque proactivo previendo las estrategias delictivas emergentes. Para proteger al público de los delitos que utilizan activos digitales, las fuerzas de seguridad deben ser flexibles, progresistas y tecnológicamente expertas a medida que las criptomonedas continúan desarrollándose. El desarrollo de las disposiciones sobre criptodivisas también determina la importancia teórica de la obra como objeto y medio para cometer delitos, un medio de pago sustitutivo durante la comisión de determinados delitos.
Conclusiones: la importancia práctica del trabajo radica en la posibilidad de utilizar sus resultados para resolver los problemas que surgen en las actividades legislativas de las autoridades estatales y en las actividades de aplicación de la ley, así como en el desarrollo de recomendaciones para mejorar la legislación penal en el ámbito de los delitos relacionados con la criptodivisa.

Palabras clave: Criptodivisas; Ciberdelincuencia; Blanqueo de capitales; Financiación del terrorismo.

INTRODUCTION

The world of crime has turned toward high-tech crime, just as every other aspect of society has improved and altered in tandem with technological advancements.[1] In this sense, the rise of cryptocurrencies has made it possible for high-tech crimes like money laundering, international drug and arms trafficking, theft, and blackmail. The most prevalent criminal activities that use Bitcoin is to proliferate.

Transnational criminal networks are using cryptocurrency to fuel illegal operations, including ransomware, terrorism, drug trafficking, pornography, and sanctions evasion. However, this illegal link is frequently ignored in popular Bitcoin writing. Cryptocurrency's transboundary and very recent character is reorganising illegal activity.[2] Hacking has become a modern-day bank robbery, stealing large amounts of money from exchange platforms. Cryptocrime is a dynamic phenomenon that has evolved from mainly transferring and accumulating the proceeds of earlier crimes into the financial system to a growing trend of virtual currency theft. Although Bitcoin is not a factor in every online financial crime, the number of cybercrimes made possible by it is growing at an exponential rate.[3,4,5,6,7]

Cryptocurrency's cross-border, unregulated, or at least underregulated, relatively recent features are revolutionising crime. For example, in 2021 and 2022, a state-sponsored hacker group in North Korea used ransomware attacks to obtain billions of dollars in cryptocurrency in order to finance its nuclear arsenal.[8] Additionally, it was alleged that North Korea stole $400 million worth of Bitcoin in 2021 alone; this amount has subsequently increased to an estimated $1,7 billion, and the entire amount of cryptocurrency stolen in 2022 is anticipated to be $3,8 billion.[9] With massive amounts of money being taken from exchange websites, hacking has become the cryptocurrency equivalent of bank robbery. In August 2016, Bitfinex, the leading cryptocurrency exchange programme, was hacked, losing over half its digital assets. The $3,6 billion worth of assets were linked to two crooks who used several cryptocurrencies to launder their earnings and enrich themselves.[10] Stated differently, the crime surrounding cryptocurrencies is dynamic and ever-evolving. In contrast, virtual

currencies have historically been utilised primarily to deposit profits into the financial system; the theft of real virtual currency is a crime expanding quickly.

Three forms of transnational crime - online child sexual exploitation and abuse (OCSEA), sanctions evasion, and ransomware - that are notable for their financial gain and specific societal harm, are compared by Hamilton and Leuprecht.[3] The use examples demonstrate how each person uniquely uses cryptocurrencies. OCSEA chooses its cryptocurrency for pseudonymity and utilises it for transactions. Criminals are switching to safer and anonymous transaction methods as technology advances to monitor the primary currency used in crimes, like Bitcoin. This helps to explain why Bitcoin has recently lost ground to other virtual currencies. For instance, Monero provides more security and privacy. Cryptocurrencies are employed for rent-seeking and value transfer in sanctions evasion, where an entity aims to acquire property without completing productive or reciprocal activities. Large sums of money may be transferred using cryptocurrencies without a conventional transaction. Lastly, because of the vast sums, Bitcoin is a favourite payment method for ransomware assaults. Bitcoin and other cryptocurrencies are used for payments, but because the money must be later laundered from the originating wallet, they frequently coexist with other currencies and mixers.

The study of cryptocurrencies as a subfield is still very young. Researchers are now evaluating the extent of cryptocurrencies and the legislative options to counter them. The United Nations Office on Drugs and Crime (UNODC), Interpol, and the Internet Watch Foundation have all highlighted the extent, scope, and effect of criminality involving cryptocurrencies on the black market. However, nothing is known about the connection between cryptocurrencies and criminal activity.[14] The illegal economy is not considered much in cryptocurrency legislation, which is still industry-independent. The guidelines are vague and mostly overlook how cryptocurrencies interact with illegal activity.

Dudani et al.[15] argue that forensic research on cryptocurrency (CC) is lagging and needs to improve interagency coordination. Based on 2011 exchange rate swings and a few reports of Bitcoin usage, these authors contend that the FBI expressed moderate confidence in its 2012 Intelligence Assessment Report that Bitcoin would develop into a profitable payment mechanism for cyber criminals. Based on the information available on criminal investigations involving the usage of e-Gold and WebMoney, the FBI also thinks there is a slim chance that Bitcoin may be used as a money laundering instrument in the future. Based on the crimes documented in the assessment, the FBI has discovered several intelligence gaps that present many difficulties for law enforcement, including details on actors trying to evade the US Bank Secrecy Act (BSA) regulations, other criminal actors, and Bitcoin services that facilitate illicit activity. Digital forensics is essential to answering these questions.

Furthermore, according to Dudani et al.,[15] trends suggest that cryptocurrencies will progressively integrate into international financial institutions because of their distinctive features and widespread user appeal. Because cryptocurrencies are anonymous and uncontrolled, criminals use them more often, resulting in a future of cybercrime powered by cryptocurrencies. The technology now accessible to scholars and law enforcement worldwide may not be enough and requires improvement.

Research on cryptocurrency crime has mainly focused on the regulation of the illicit use of cryptocurrency. In particular, Pocher and Veneris[16] emphasise that not only does technology help to achieve legal goals but also that some regulatory requirements need to be "built into" technology to achieve consistent outcomes and/or standards. Towne Morton's[17] study addresses the cybersecurity challenge for cryptocurrencies with inconsistent international regulation of this new international phenomenon of fraud, anti-money laundering and terrorist financing. Simser[18] argues that the challenge posed to society by money laundering mirrors the challenge posed by organised crime: a test of values and the importance of the rule of law. Furthermore, Simser[18] believes that financial intelligence units (FIUs) are an important mechanism for addressing this challenge in general, and there are important changes in the environment that need to be considered to achieve the FIU's future policy goals. Jenkins et al.[19] focus on cryptocurrency laundering and its significant differences from traditional money laundering.

More theoretical and empirical studies are conducted by Majumder et al.,[20] Desmond et al.,[21] Dupuis et al.,[22] and Lee and Choi.[23] Using the vector error correction model (VECM), Majumder et al.[20] found a statistically significant long-term relationship between terrorist attacks and Bitcoin transactions/turnover in a sample of 12 countries for 2010-2016. According to a systematic review of the literature by Desmond et al.,[21] no prior research has defined crypto-laundering as a complex socio-technical system or evaluated how law enforcement, regulators, or criminals comprehend the procedures and evaluate risk in crypto-laundering systems using a systems thinking framework approach. Dupuis et al.[22] conclude that digital space and digital assets can facilitate pseudonymous criminal activity in the current regulatory landscape. Lee and Choi[23] examine the relationship between Bitcoin, ransomware, and terrorist activity. Their results show correlations between the frequency of ransomware and terrorist action and a unidirectional association between ransomware prevalence and Bitcoin.

The study by Maurushat and Halpin[24] focuses on methods of investigating the illegal use of cryptocurrencies. In particular, the authors analyse the use of cryptocurrencies in Internet fraud and the problems encountered

in investigating cryptocurrency and cryptocurrency investment fraud. In addition, more attention has recently been paid to the geopolitical risk posed by cryptocurrencies and transnational crime. Long et al.[25] investigate the so-called "cross-pricing" of geopolitical risk in cryptocurrencies. At the same time, the studies in this field are rather scattered and narrow-directed.

Thus, the aim of this article is carrying out criminal law assessment of crimes related to the use of cryptocurrencies, since this is a critically important scientific and practical task in legal science and interdisciplinary discourse.

METHOD

The study' methodology is of qualitative nature, based on secondary sources analysis. The primary research tool is content analysis.

The source base of the study includes scientific publications in specialised journals presented in ScienceDirect, ResearchGate, Google Scholar, JSTOR, and materials from FATF and Interpol reports. The data published in the period 2022-2024 by Chainalysis, a blockchain data platform (the company provides data, software, services and research to government agencies, exchanges, financial institutions, insurance companies and cybersecurity companies in more than 70 countries; this data provides investigative, compliance and market analysis software that has been used to solve some of the world's most high-profile criminal cases and safely expand consumer access to cryptocurrencies), was also widely used.

The study's foundation is the constructivist paradigm, often called the interpretive paradigm, which holds that people create reality via their experiences and social interactions. Researchers working within these paradigms aim to comprehend people or groups' many intricate viewpoints by employing qualitative techniques. This paradigms was chosen taking into account the relative novelty of the topic under consideration, as well as the fact this is under-researched while being developed within complex and changing landscape.

RESULTS

National regulators have applied new and current AML regulations to the cryptocurrency ecosystem. Legal academics[26] have examined in detail how the rules and regulations of the nation that has been the most aggressive in pursuing money laundering and at the centre of worldwide AML efforts apply to cryptocurrencies, and they have been used in several court cases. For instance, the CEO of Bitinstant, Charlie Schram, pled guilty to aiding and abetting unlawful money transfers in 2014 after the US Department of Justice (DoJ) used the 1986 Money Laundering Act in its case. His two-year sentence "scared potential money launderers into using cryptocurrency", according to Schram.

The Financial Crimes Enforcement Network (FinCEN) of the U.S. Treasury Department filed its first-ever civil lawsuit against a cryptocurrency exchange in 2015, citing the Bank Secrecy Act of 1970. San Francisco-based Ripple Labs was fined USD 700 000 for not implementing efficient anti-money laundering programmes within two years of FinCEN's 2013 advice.[27] The US Department of Justice's case against the owners of the cryptocurrency exchange Coin.mx, who allegedly used the credit union to launder the proceeds of ransomware attacks against major high-profile financial institutions like JP Morgan Chase and the media company Dow Jones, was supported by a similar line of reasoning.[11]

At least $20 billion was made via crypto crime in 2022.[11] Profits are significantly larger, according to some projections.[12] Based on the quantity transmitted from illegal addresses to addresses hosted by services, cybercriminals laundered $8,6 billion worth of cryptocurrencies in 2021 (figure 1).

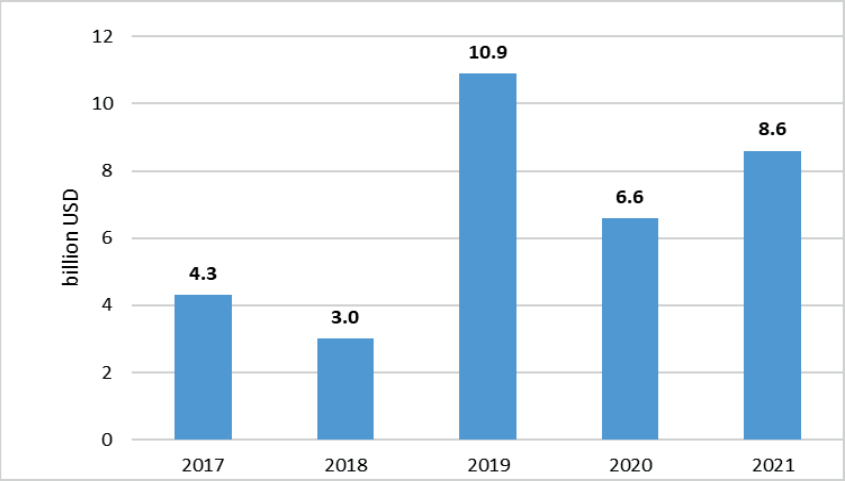

Figure 1. The total value of laundered cryptocurrency, 2017–2021, in billions of US dollars, USD
Source:Chainalysis[13]

Several fficial actions have been taken to curb cryptocurrency use outside the US. In certain nations, like Bangladesh, Bolivia, and Ecuador, "altcoins" are prohibited, while in others, like Thailand, their legality is still up for debate. Laws banning financial services firms and their staff from handling and carrying out cryptocurrency transactions were enacted by the State Bank of Vietnam in 2014 and the People's Bank of China in 2013. In a 2014 decision, the Central Bank of Iceland contended that buying cryptocurrency is against the nation's Foreign Exchange Act.

However, other governments, including New York State, have attempted to position themselves as authentic hubs for Bitcoin trading. Virtual currency exchanges operating in Singapore have been obliged since 2014 to confirm the identification of their clients and notify their questionable Transaction Reporting Unit of any questionable transactions.[28] To establish itself as a significant global hub for cryptocurrency transactions, the Channel Island of Alderney has established a collection of AML-compliant CC services.[29] The neighbouring Isle of Man is vying for the moniker "Bitcoin Island" and is creating comparable "innovative regulatory and funding schemes" after amending its primary anti-money laundering law to allow cryptocurrency.[30] However, such initiatives to establish genuine AML-compliant states have little effect on reducing the likelihood that money laundering would thrive in other jurisdictions.

Insufficient oversight and immature understanding provide terrorist groups with easy access to cross-border financial transfers using virtual currency.[31] Cryptocurrencies are not a significant source of terrorist financing. However, their growing importance requires increased attention and stronger partnerships between public authorities and private financial institutions, especially as groups shift to privacy-oriented currencies.[32]

In particular, virtual currency and decentralised finance (DeFi) are emerging as a new frontier in terrorist financing. According to a report prepared for Congress by the US Department of Homeland Security, cryptocurrencies have some appealing features that terrorists have already exploited. One can expect violent extremists to continue to use this tool to facilitate their terrorist activities, especially as the technology becomes more accessible and widely used in general commerce and the commercial sector.[33] Positive attributes include anonymity, decentralisation, worldwide reach, speed, indisputability, simplicity, affordability, the potential to enhance anonymity and security, and the flexibility to relocate networks to new locations, capitalising on the disparities in cryptocurrency regulations across nations.[34]

Compared to cryptocurrencies like Bitcoin, DeFi technology functions on peer-to-peer networks with higher anonymity.[3] Crypto provides a different financial system for terrorists to conduct cross-border transactions using pseudonyms. DeFi extends anonymity to capitalise on cryptocurrency. Cryptocurrencies are not as well-regulated or enforced as the traditional financial system. For example, they are not as susceptible to anti-terrorist financing (CTF) and anti-money laundering (AML) regulations as fiat currencies.[35] The virtual financial ecosystem is quickly emerging as a significant transnational terrorist financing channel in addition to more conventional methods like cash and wire transfers. Social media has been used by al-Qaeda, Jamaat al-Tawhid we'll-Jihad, and al-Nusra Front to acquire Bitcoin.[36] After that, their networks used multi-layered cryptocurrency transactions to launder the money.

Following the 9/11 attacks in New York City, FATF made counter-terrorism a top priority. This focus was re-emphasised in 2015 when attacks worldwide were linked to Al-Qaeda and the Islamic State (IS).[37] FATF mandates pertinent risk assessments and establishes the worldwide standard for CTF, AML, and counter-proliferation finance recommendations at domestic and international levels. It does not explicitly identify hazards, establish criteria for risk assessment, or create or enforce rules. Instead, it creates guidelines and offers particular suggestions to guide the creation of regulations by various authorities.

For many years, the FATF has released pertinent studies on funding terrorism but has also paid little attention to virtual currencies. FATF's suggestions centre on conventional methods of funding terrorism, especially in the Middle East and West Africa. The exception is a recent analysis of risk factors linked to terrorism and right-wing extremism. It notes that specific terrorist organisations have been encouraged to employ virtual assets, particularly Bitcoin, due to the recent decrease in credit card availability.[37] Virtual assets are noticeably missing from these studies, emphasising the importance of cash, foreign currencies, non-governmental organisations, hiring, and risk assessment.

Al-Qassam and al-Qaeda brigades' use of virtual assets for terrorist funding is compared in research by Burgess et al.[31] The standards created and suggested by the Financial Action Task Force on Money Laundering (FATF) are wholly inadequate to stop the proliferation of centralised virtual assets and decentralised financial technologies as forces behind the global illicit international political economy (IIPE), according to the comparison of the virtual assets used.

The FATF's suggestions for recognising, thwarting, and discouraging the connections between cryptocurrency, crime, and terrorism are neither thorough nor effective. Even worse, FATF members are failing to implement even the FATF standards that are inadequate to the current situation. According to the author's conclusions, the FATF ought to make the inclusion criteria more apparent by the current definition of virtual assets, broaden the regulations, enhance interagency collaboration, and develop more thorough recommendations that take

into account the various forms of criminal activity and criminogenic factors that are relevant to crypto-crime.

To evade identification and countermeasures against terrorist financing, terrorist organisations, including Hamas, Hezbollah, Palestinian Islamic Jihad (PIJ), and Islamic State of Khorasan (ISK), are increasingly using cryptocurrency as a fundraising tool. The Israeli Ministry of Defense declared after 7 October of this year that it had captured around $41 million in cryptocurrency from Hamas and $94 million from Palestinian Islamic Jihad between 2019 and 2023.[38]

Through its flagship Voice of Khurasan journal, ISK has shifted its attention from Bitcoin and Tether to Monero. This privacy-focused cryptocurrency makes sure that transactions cannot be tracked. Since privacy-focused cryptocurrencies like Monero and ISK are intended to hide the sender and receiver and the transaction value, their increasing use poses a significant threat to efforts to combat terrorist financing.

Virtual assets are becoming a more important source of funding for jihadist terrorist organisations. In particular, terrorist organisations like Hamas, Hezbollah, Palestinian Islamic Jihad (PIJ), and the Islamic State of Khorasan (ISK) are increasingly using social media to solicit cryptocurrency in order to evade counter-terrorism and terrorist finance detection. Blocking donations to terrorist organisations and the financing of terrorist attacks using decentralised and encrypted virtual currencies is still a problem, despite efforts by the US Treasury Department, the Israeli National Bureau for Combating Terrorist Financing, and other anti-terrorist financing authorities worldwide, including the Financial Action Task Force (FATF), to seize cryptocurrency wallets from terrorist organisations and destroy cryptocurrency addresses that have been used for years to finance terrorist organisations. Just prior to carrying out the murder that claimed 140 lives, the ISK assailants that attacked Crocus City Hall in Moscow in March 2024 collected about $2 000 in virtual assets.

The US Treasury Department sanctioned the Buy Cash virtual currency exchange in Gaza after the 7 October Hamas attack, which killed almost 1,200 people, for using a variety of cryptocurrencies to finance the Hamas military arm, al-Qassam Brigades. A Russian programmer named Alexey Pertsev was sentenced to five years in jail in the Netherlands in May of this year for developing the cryptocurrency mixer Tornado Cash, which was used to launder funds for terrorism and other illicit acts.[38]

The difficulty in prosecuting terrorist funding cases employing cryptocurrencies makes it impossible to determine the scope of their usage for terrorist financing, even if cryptocurrencies have been recognised as a way of financing terrorism.

Global sanctions regimes have evolved due to the entrance of cryptocurrencies into the global financial system. The efficiency of geopolitical objectives and economic stability is threatened by the capacity of sanctioned persons to avoid discovery and carry on trade thanks to cryptocurrencies. As a tool of international politics, sanctions have grown in popularity. Agencies, including the US Treasury Department's Office of Foreign Assets Control, have sanctioned cryptocurrency wallets, coin businesses, and mixers in recent years.[39] According to international law, sanctions are defined as follows: "Coercive measures taken [in response to a violation of international law] to implement a decision of a competent social authority, that is, a body legally authorised to act on behalf of a society or community governed by a legal system".[40]

The reasoning behind evading sanctions use Bitcoin for various purposes, such as rent-seeking, money transfer and subsequent laundering, or, in some political contexts, funding the spread of WMDs. Sanctions can be imposed at various levels and in various trade sectors, such as defence, food, medicine, and oil. Any actor has the authority to penalise another. Many parties prefer to apply sanctions through the United Nations or multilateral channels like the European Union for legitimacy concerns or when dealing with economies too tiny to act independently.

North Korea, Venezuela, Iran, Cuba, and Russia are among the nations currently under sanctions. To avoid dealing with currencies that they are not allowed to transact with, sanctioned companies might create virtual currencies using cryptocurrencies. Ten Bitcoin businesses and 400 addresses were subject to penalties in 2022.[9]

These numbers reflect the rising worry over the use of cryptocurrencies to circumvent sanctions. The number of payments for evading sanctions through virtual assets has increased with the number of sanctioned addresses and organisations. The number of Bitcoin-sanctioned organisations increased in 2021 and 2022, with 2022 seeing a record high. According to Chainalysis,[9] 100 addresses were sanctioned in 2021, while 350 addresses were sanctioned in 2022. Nine entities were sanctioned in 2021, and ten entities were sanctioned in 2022.

The availability of technology like mixers, cross-border payments, and the pseudonymous nature of cryptocurrencies allow sanctioned entities to benefit with little scrutiny from conventional regulations. Cryptocurrencies are revolutionary because they evade the regulations of the US Treasury's Office of Foreign Assets Control (OFAC), making it very simple to escape penalties. It is challenging to stop using cryptocurrencies to avoid sanctions as they are not covered by sanctions laws in many nations. To close the regulatory gap brought up by cryptocurrencies, OFAC has placed economic sanctions on several Bitcoin wallet addresses, businesses, and people, including BitRiver in Russia.

Virtual money has made the emergence of new crimes like cryptocurrency theft possible. Ransomware, software that encrypts files and prevents their owners from accessing critical information or services (such as

medical records), is a terrible illustration of an evolving crime. The owner usually has to pay a hefty ransom to unlock the encrypted files.

Ransomware attacks cause significant losses to governments, companies, and individuals, and these losses and social harms grow yearly. Criminals demand that victims pay a ransom in exchange for a decryption key. In 2022, ransomware attacks were among the top cryptocurrency-related crimes against US federal agencies, accounting for 11,9 of all virtual currency crimes.[3] The numbers are similar at the state and local levels: 11,3 of crimes were identified as ransomware attacks.[41] Ransomware attacks usually have three stages. The first stage is an infection, where the computer receives malware. Files, data, or personal information are encrypted in the second step, which prevents the owner from accessing the material. Ransomware is the third step, during which the attacker requests a ransom to unlock the compromised files. The files will either be restored or destroyed if the ransom is paid, and the attacker must launder the money.

Financially speaking, the blockchain's open nature has allowed vast amounts of data to be gathered. The flow of money from the wallet that received the ransom to its secondary destination is being tracked by recent trends. Typically, money is transmitted to key exchanges (like Binance) first, followed by high-risk exchanges, banned platforms, and mixers, frequently utilised as secondary outputs from wallets. Ransomware attacks frequently rely on money laundering in combination with the conventional banking system, even if they employ cryptocurrency to earn rent. Since the targeted organisations are usually in Western nations, ransomware's scope or methods usually demand more advanced, integrated laundering procedures. Criminal intelligence benefits from this. At the same time, relying on cryptocurrency to obtain ransom payments means inextricably linking cryptocurrency to ransomware crimes.

Ransomware attacks are dangerous, and their geopolitical ramifications for financing proliferation are especially evident. For example, the FATF postulates that state-sponsored ransomware attacks by North Korea have enabled "an unprecedented number of recent ballistic missile launches". Virtual currencies that have been stolen from decentralised exchanges, amounting to over $1,2 billion since 2017 alone, have been the primary source of funding for these launches.[42] Non-state actors are also making profits. Several criminal organisations have utilised cryptocurrencies and ransomware assaults to transfer money. Attacks using ransomware can bring in billions of dollars in revenue for terrorist organisations, criminal organisations, and dishonest state actors. Gaining a deeper understanding of how these many entities contribute to ransomware assaults in the global economy is crucial.

One of the most active and lucrative ransomware criminal organisations in 2022 was LockBit. Their network is transnational, decentralised, and worldwide. Lockbit has been paid $100 million since its founding. Lockbit alone generated $44 million in 2022.[43] According to the Canadian Cyber Security Centre, the LockBit Gang is "responsible for 22 per cent of ransomware incidents" in Canada and around 44 per cent of instances worldwide.[44] Mikhail Vasiliev, a Canadian citizen from Bradford, Ontario, who was born in Russia, was accused in the District of New Jersey of "knowingly extorting money in connection with damage to a protected computer" and "intentionally causing damage to a protected computer" between September 2019 and October 2022. Under the guidance of the National Cybercrime Coordination Centre, the RCMP conducted an investigation that led to the charges. According to the research, the LockBit ransomware strain, which surfaced in January 2020, was found to be owned and controlled by Vasilyev. Malware called LockBit is available for purchase and may be used to demand payments. Tens of millions of ransom threats resulted in ransom payments, and the firm is accountable for over $100 million worth of ransomware.[45]

For instance, Sault Ste. Marie, a little Ontario municipality of 7 700 residents with weak cybersecurity, was the target of LockBit. The city owned 67 terabytes of encrypted material, which included private citizen information and internal financial records. By demanding a ransom and threatening to post the city's data online if the city did not pay, the organisation committed double extortion.[46] The city responded by asking the city council, Stratford Police, a group of attorneys, and the Canadian Cyber Security Centre (CCCS) for help. The city council was advised by CCCS not to make the payment.[47] Before agreeing to pay the ransom, CCCS attempted to identify the offender and ascertain whether they may have backed up the data. The city shut down its servers to stop the data from being taken, but many of its computer systems were rendered useless, yet it is unknown if St. Mary's paid for the recovery of their files. Similar situations occurred when Frederick, Colorado, was threatened with a $200 000 ransom demand to recover its information, and Stratford, Ontario, paid $75 000 in Bitcoin.

According to Cherniei et al.,[48] the establishment of criminal liability for operations related to cryptocurrency circulation and effective counteraction to criminal offences in this area remain urgent issues because of the legal uncertainty surrounding the status of cryptocurrencies at the legislative level in the global environment. The Blockchain Claims Database (BLD), established by the financial legal firm Murphy & McGonigle in New York, is mentioned by Cherniei et al.[48] Law enforcement organisations utilise this commercial initiative to investigate crimes, including establishing bogus ICOs and cryptocurrencies. The overall number of fraud instances in this region, their trends, details on criminal or civil proceedings, and the generalised circumstances of one or a

group of cases that may be related to new initiatives or startups are all included in the BLD tracking data. Furthermore, some commentators argue that cryptocurrencies are commodities (property) or a type of currency. These characteristics of cryptocurrencies allow for the classification of criminal offences involving their usage into two categories: 1) "real" offences, which are crimes where cryptocurrency is the topic of the offence or where cryptocurrency is used as payment; 2) "virtual" offences, which are offences performed only online with computer equipment and information impact.

Compared to $3,1 billion in 2021, cryptocurrency transactions on illegal marketplaces and fraudulent stores were over $1,5 billion in 2022. The primary cause of the fall was the collapse of Hydra Market, the highest-earning darknet marketplace in 2022, which was shut down in April 2022 following a combined operation by US and German law enforcement. Since Hydra owns over 93 of the darknet's market value, its demise has allowed other markets to grow, so authorities may now have to look into additional significant players without a monopoly. Terra USD and Luna tokens - two crypto tokens that peaked just two months ago - fell in May 2022, wiping out more than $40 billion in consumer funds. Many believe the currency is a pyramid scheme, and in early 2022, the US Securities and Exchange Commission accused the blockchain protocol's inventors of securities fraud.[49]

Meanwhile, in 2022, non-banking financial sector (NBFS) enforcement in Asia and the Pacific (APAC) included 164 penalties, 37 limitations, 31 license revocations, and 17 warnings (figure 2).

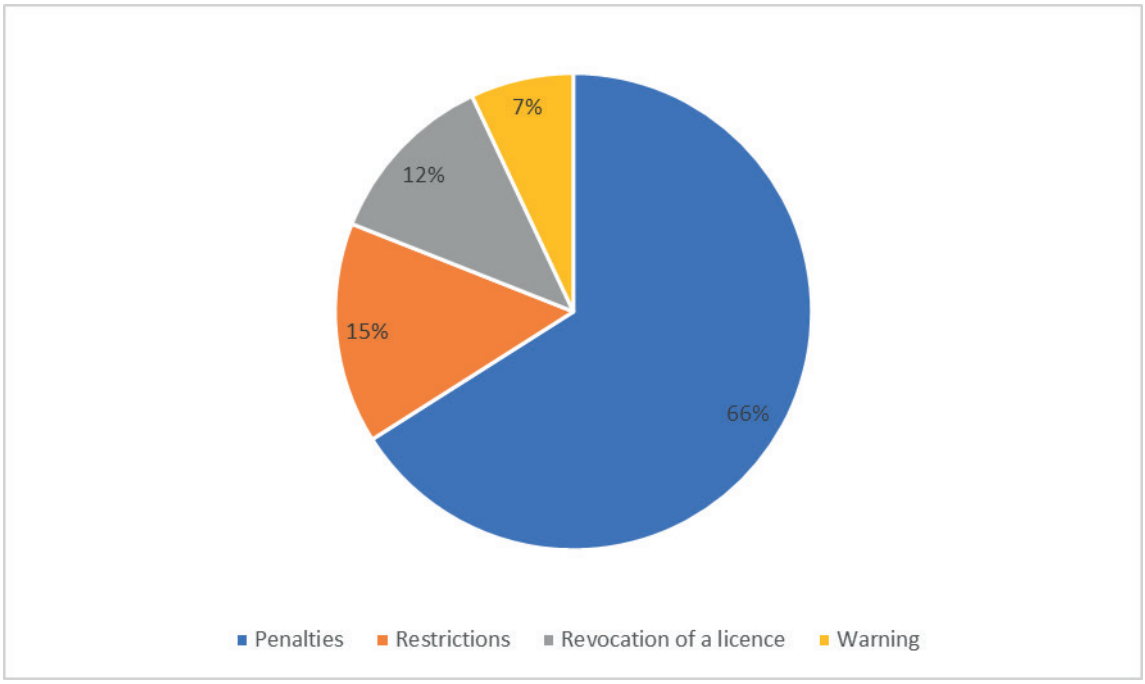

Figure 2. Enforcement of the Asia-Pacific non-banking financial industry in 2022
Source: Widyatmoko et al.[49]

When combined, Bitcoin transactions' decentralised and quasi-anonymous characteristics provide significant theoretical obstacles to anti-money laundering initiatives. Table 1 below provides a more thorough summary of the money laundering risks associated with cryptocurrency transactions in the three conventional "stages."

Table 1. Risks of money laundering through cryptocurrency transactions

Common risk factors	Possibility of exploiting weaknesses at every level		
	Accommodation	Layering	Integration
Quasi-anonymity	Associations and criminals can utilise cryptocurrencies	Suspicious names that are hard to identify, mainly when money mules are involved	Permission to cash in proceeds of crime that will be transferred anonymously to untraceable persons
Transactions in real-time	Crime proceeds can be moved to a different cryptocurrency in a different nation.	Since transactions happen instantly, there is little time to halt them if money laundering is detected.	The international banking system makes it easy for criminal proceeds to be transferred and withdrawn in another nation.

Source: Choo[28]

Blockchain-based intelligence helps investigators map crypto transactions and present them in a format that can be easily understood and analysed. For example, the diagram below (figure 3) shows the transactional relationships between eight drug buyers and sellers, each connected to the same darknet marketplace. Blockchain-based intelligence helps law enforcement advance investigations, apprehend criminals, present cases for prosecution, and pave the way for the recovery and return of crypto funds to victims whenever possible.

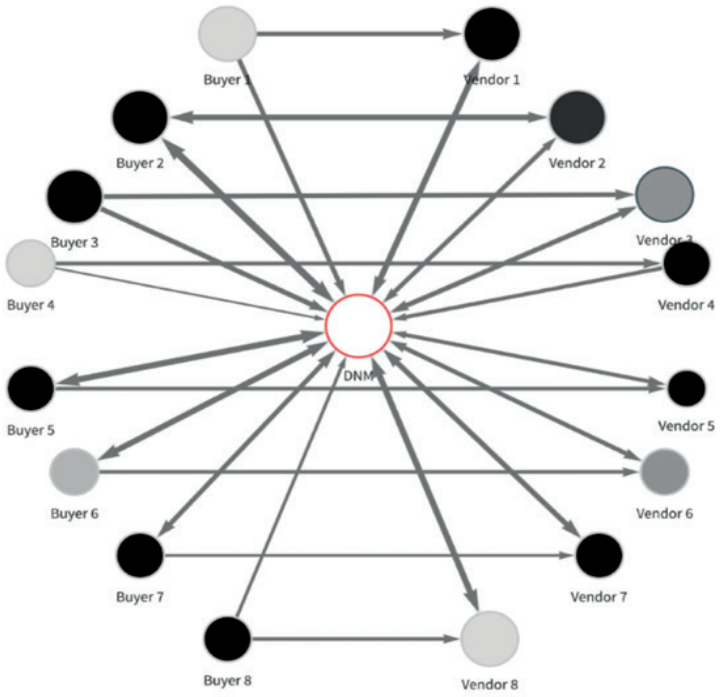

Figure 3. Graph of cryptocurrency transactions
Source: Chainalysis[54]

The development of the legal system's structure, content, and culture must undoubtedly be in line with the reform of the criminal justice system as a whole, given the complex issues that the public and law enforcement agencies face about the phenomenon of the digital financial system's development. Criminal law (judicial policy) plays an important role in crime prevention. It, therefore, needs to be supported by government policy aimed at preventing criminal behaviour through criminal law enforcement agencies operating on the ground by issuing a law, which passes through several phases: legislative policy, judicial policy, and executive/ administrative policy.

Crimes related to cryptocurrencies can take on rather unexpected forms. In particular, cryptocurrencies require electricity to function. Some criminals mine cryptocurrency by stealing energy. Several noteworthy examples of comparable crimes include the February 2021 arrest of six Malaysians on allegations of stealing around $2 million in electricity to run cryptocurrency mining operations. In July 2021, Malaysia demolished 1 069 mining rigs allegedly stealing power as part of a series of crackdowns on cryptocurrency mining activities. An underground cryptocurrency farm that was unlawfully stealing around $259 000 worth of power per month was discovered by the Ukrainian authorities later in July 2021.[12]

Additionally, a scam known as "Rug pull" is used to mislead investors by asking them to "pump it up" by investing in a new non-fungible token (NFT) or other digital currencies. When the money grows, and the scammers can access the victims' accounts, they abandon them and steal the money. Investors are left with illiquid cash once the scammers encrypt it to prevent them from selling it. This scam occurred in the Squidcoin case when the cryptocurrency rose from a cent to around $90 and then peaked at about $2 856. The scammers stole almost $2,5 million from the victims when the price peaked, and the money vanished, making the token worthless.[50]

Cryptocurrencies may continue challenging traditional law enforcement models, but law enforcement agencies can stay one step ahead with the right resources, strategies and cooperation. The war on crypto crime is about responding to crimes and building robust systems to prevent them, creating a safer environment for individuals and financial systems worldwide.

DISCUSSION

Money laundering across national borders has historically been linked to large international banks specialising in cross-border financial transactions. Therefore, international banks have historically been "substituted"[51] by global anti-money laundering (AML) initiatives as centralised "bottlenecks"[52] for reporting transactions suspected of laundering illegal monies. Nevertheless, decentralised networks of users located all over the world conduct cryptocurrency transactions. Cryptocurrencies rely on these decentralised user networks rather than centralised organisations like banks to confirm the legitimacy of transactions and prevent duplicate spending. Cryptocurrencies "deliberately circumvent the myriad of anti-money laundering regulations developed over the past 25 years" by not depending on centralised financial institutions.[53] No set of institutions can implement AML regulations without centralised organisations "in charge" of cryptocurrencies.

The quasi-anonymity of cryptocurrency transactions challenges traditional global AML efforts to identify money laundering participants. At least two issues impede such efforts. First, quasi-anonymity makes it more difficult for financial institutions like banks to comply with Know Your Customer (KYC), a requirement that forms the basis of worldwide AML regulation. Identifying "evasive or defensive responses to questions" is a challenge for financial experts, who must decide who to ask questions of. The conventional issue with anti-money laundering operations is shifting from "parties known - transactions unknown" to "transactions known - parties unknown" due to cryptocurrencies.[33]

Blockchain intelligence facilitates faster and more efficient collaboration between law enforcement departments and government agencies during an investigation. Using the same dataset fosters a shared understanding, leading to better investigative outcomes. And while blockchain intelligence helps fight crime, it can also help law enforcement agencies proactively prevent crime. Illegal activity can be detected early by analysing transaction patterns on the network and connections that may indicate criminal behaviour. Here are some examples:

- Observing an unusual increase in the volume of transactions or patterns typically associated with money laundering or fraud.
- Interrupting criminal networks by mapping the financial flows of criminal organisations, which can disrupt their operations and prevent future crimes.
- Targeting darknet markets. Proactive monitoring of transactions related to known darknet markets allows law enforcement to gather information about buyers and sellers, identify new threats, and take action before illegal transactions become more intense.

For local governments wishing to engage in cryptocurrency crime investigations, creating a comprehensive knowledge base across all teams and departments is important. This shared understanding ensures smooth cooperation and communication across the organisation and between agencies, from field officers to judges. Leadership support for these initiatives is crucial in building the foundation to begin combating cryptocurrency crime, requiring a commitment to capacity building and ongoing training to stay abreast of trends and develop effective policies, regulations, and operational strategies. The significant seizure of over £2 billion worth of Bitcoin by the UK Metropolitan Police in March 2024 is an example of the potential success of these operations. In 2021, the UK police seized cryptocurrencies totalling £294 million in connection with an international money laundering investigation.[54] These developments, along with significant seizures over the past few years, highlight the global scale of the problem and the critical impact of skilled measures.

Government agencies continue to invest more resources in preventing crimes related to cryptocurrency. On 17 February 2022, during the Munich Cybersecurity Conference, the FBI officially recognised a Crypto Task Force. The task force has been dubbed the Virtual Asset Exploitation Unit (VAXU) to investigate Bitcoin crimes better and seize virtual assets. The task force released a statement that clarified its objectives: "Like many other cryptocurrency-fuelled crimes, ransomware and digital extortion only function when the criminals are 'compensated'. The message to businesses is clear even though the currency is virtual: if you inform us, we can trace the money and not only assist you, but we also aim to stop the next victim".[12]

The UN and cooperation at the international level have made sound efforts to reduce the financing of crypto-terrorism through the Global Coordinated Programme on the Identification, The United Nations Counter-Terrorism Centre (UNCCT), which is part of the United Nations Office for the Suppression of Terrorism (UNOCT), and other approaches are used in the Prevention and Combating of Terrorism (CFT Programme).[55] With the international community's assistance, the UN has enacted several resolutions to combat terrorism financing, most notably Resolution 2462 (2019). UN researchers examined terrorist incidents, including crypto-financing, and determined that the number has grown dramatically.[56]

The Market Integrity and Major Fraud Division (MIMF) is a national leader in prosecuting cryptocurrency-related fraud and market manipulation in the United States. Since 2019, the unit has charged investors from around the world in cryptocurrency fraud cases in which investors from around the world have been intentionally defrauded of more than $2 billion. Prosecutors employ conventional law enforcement methods and blockchain

data analysis to find and prosecute intricate cryptocurrency investment schemes, cryptocurrency price and market manipulation, unregistered cryptocurrency exchanges engaged in fraudulent schemes, and insider trading schemes impacting cryptocurrency markets. Prosecutors from the Division frequently collaborate with the Commodity Futures Trading Commission and the U.S. Securities and Exchange Commission. For instance, in a cryptocurrency enforcement case in 2022, the MIMF's actions indicted six individuals, including a CEO, founder, trader, and executive. Law enforcement partners included the FBI, the Board of Governors of the Federal Reserve System, IRS-CI (the US federal law enforcement agency responsible for investigating potential criminal violations of the US Internal Revenue Code), and Homeland Security Investigations (HSI).

Nonetheless, the FATF is committed to addressing the more nuanced connection between crime and cryptocurrency. Investigators might broaden their scope to stay ahead of the criminals' adaption. Wallets may be analysed as forensic evidence using various methods, including blockchain-based investigations and ongoing content monitoring. Red lines can be drawn with the use of stricter laws governing harmful material instructions and more severe sanctions for businesses that sell illicit goods like malware, hardware, and child pornography. Criminals are searching for rent; crimes have become easier and more profitable due to cryptocurrency. The technology, law enforcement's acceptance and a deeper comprehension of the socioeconomic and psychological factors contributing to cryptocurrency crime highlight the dangers of untethered cryptocurrency as malicious individuals and geopolitical players want to utilise it for illegal purposes. There is a significant financial, social, and political risk when the FATF fails to give governments timely, comprehensive information about alternative financial ecosystems like cryptocurrency.[57,58]

It is necessary to update the FATF requirements. Nonetheless, it is also the duty of member states to guarantee that their domestic standards are suitable. Even while the FATF is in a good position to lead the charge in establishing rules for cybercrime, it cannot accomplish this independently or without further assistance. The FATF depends on its members to carry out, oversee, and enforce its rules, and member nations are now failing to do so about virtual currencies.[59] The FATF is lagging in virtual currencies in general and in particular about emerging cryptocurrency crimes.

The decentralised nature of cryptocurrencies creates significant legal challenges for law enforcement. Jurisdictional issues are common, as criminals can operate in multiple countries with relative ease. A criminal can reside in one country, use an exchange in another, and route funds through various offshore services. Law enforcement agencies in individual countries must improve their cooperation with international bodies such as Interpol, Europol, and the FATF. International treaties and agreements on dealing with digital asset crime, especially those relating to countries that do not have strict cryptocurrency regulation, will play a key role in future investigations.

However, legislative updates are also needed. Many laws are outdated and were written before the advent of digital currencies. Law enforcement agencies should work with policymakers to ensure that legislation aligns with cryptocurrency advancements. In addition, the acquisition and preservation of digital evidence, such as private keys, transaction records and digital wallets, should align with the applicable legal framework while respecting individual privacy rights.

As this study demonstrates, cryptocurrencies such as Bitcoin, Ethereum, and a growing number of anonymous cryptocurrencies (including Monero) are often used in illicit activities due to their anonymity and ease of transferring value across borders. Criminal networks, including human traffickers, drug cartels and ransomware operators, are using these assets to circumvent traditional financial systems, where rules such as Know Your Customer (KYC) and anti-money laundering (AML) protocols are strict. The quasi-anonymity and decentralised nature of cryptocurrency transactions make it impossible to effectively use standard anti-money laundering mechanisms tested in the "traditional" financial system. In particular, the low accessibility of cryptocurrency transactions for regulatory and criminal law control is due to the multi-stage nature of money laundering operations. In addition, cryptocurrency transactions take place in real-time, which leaves little time to stop them, even if there are suspicions of money laundering.

Another important conclusion of the study is that cryptocurrency-related crimes can also take on combined and rather unexpected forms, making combating them even more difficult.

CONCLUSIONS

According with the aim of the article - carrying out criminal law assessment of crimes related to the use of cryptocurrencies – it was revealed that as cryptocurrencies and digital assets become increasingly entrenched in global financial systems, law enforcement agencies face an increasingly complex challenge in dealing with the rise of related crimes. The pseudonymous nature of blockchain technology, the global reach of cryptocurrency exchanges and the rapid pace of innovation in digital finance have made these assets attractive to criminals for activities such as money laundering, drug trafficking, ransomware and fraud. To effectively combat such crimes, law enforcement agencies must evolve, acquiring new skills, tools and resources to stay one step ahead. Innovations and changes should be implemented at all levels - law enforcement agencies from the top

to the patrol level should understand blockchain technology and cryptocurrency transaction tracking well. Ongoing investigations of cryptocurrency-related crimes require combining traditional investigative skills and new, tech-savvy approaches. Investigators must learn how to identify patterns in blockchain data, track funds across multiple wallet addresses, and analyse the complex flow of funds on decentralised exchanges (DEX) or peer-to-peer platforms. In addition, the study showed that close cooperation with stakeholders is an important factor, as evidenced by the investigation and development of Chainalysis and other similar platforms, which are a source of important data for law enforcement agencies in solving cryptocurrency crimes and blocking criminal schemes involving cryptocurrency transactions.

Based on the study, it is possible to formulate vectors for developing national measures to respond to cryptocurrency risks. In our opinion, the relevant measures should include the following components:

- understanding: raising awareness and building a knowledge base among policymakers, law enforcement and supervisors who understand how cryptocurrencies work;
- investigations: increasing the capacity of law enforcement agencies to track cryptocurrencies;
- seizure and confiscation;
- regulation and supervision.

It should also be noted that further theoretical and empirical research into the multifactorial links in the criminal "ecosystem" of cryptocurrency transactions, including those carried out for terrorist financing, is critically needed, given the sharp increase in geopolitical tensions and the expansion of military conflict zones.

REFERENCES

1. Azad I. An Introduction to Cryptocurrency Investigations. In: Montasari R, Carroll F, Mitchell I, Hara S, Bolton-King R. (Eds.):Privacy, Security and Forensics in the Internet of Things (IoT). (pp. 97–129). Springer, Cham, 2022. https://doi.org/10.1007/978-3-030-91218-5_5

2. Orobets K. Concept, signs and types of criminal offence in legislation and practice of the US and Ukraine. Pakistan Journal of Criminology [Internet]. 2022 [cited 29 May 2025];14(2):47–62. Available in: http://www.pjcriminology.com/wp-content/uploads/2022/08/4-Concept-Signs-and-Types-of-Criminal.pdf

3. Hamilton R, Leuprecht C. The Crime-Crypto Nexus: Nuancing Risk Across Crypto-Crime Transactions. In: Goldbarsht D, de Koker L. (Eds.):Financial Crime and the Law. Ius Gentium: Comparative Perspectives on Law and Justice. Vol. 115. Springer, Cham, 2024. https://doi.org/10.1007/978-3-031-59543-1_2

4. Holovkin BM, Tavolzhanskyi OV, Lysodyed OV. Corruption as a cybersecurity threat in the New World Order. Connections 2021;20(2):75–87. https://doi.org/10.11610/Connections.20.2.07

5. Holovkin B, Cherniavskyi S, Tavolzhanskyi O. Factors of cybercrime in Ukraine. Relacoes Internacionais no Mundo Atual 2023;3(41):464–488.

6. Kravtsov S, Orobets K, Shyshpanova N, Vovchenko O, Berezovska-Chmil O. Progress and challenges in combating corruption in Ukraine: Pathways forward. Journal of Strategic Security 2024;17(2):28–43. https://doi.org/10.5038/1944-0472.17.2.2223

7. Orlovskyi R, Kharytonov S, Samoshchenko I, Us O, Iemelianenko V. Countering cybercrime under martial law. Journal of Cyber Security and Mobility 2023;12(6):893–910. https://doi.org/10.13052/jcsm2245-1439.1264

8. NCC Group. The Lazarus Group: North Korean scourge for +10 years responsible for some of the largest cyber attacks worldwide. [Internet]. 2023 [cited 29 May 2025]; Available in: https://www.nccgroup.com/us/the-lazarus-group-north-korean-scourge-for-plus10-years/group-north-korean-scourge-for-plus10-years/

9. Chainalysis. 2022 Biggest year ever for crypto hacking with $3.8 billion stolen, primarily from DeFi protocols and North Korea-linked attackers. [Internet]. 2023 [cited 29 May 2025]; Available in: https://blog.chainalysis.com/reports/2022-biggest-year-ever-for-crypto-hacking/

10. Bilton N. The ballad of Razzlekhan and Dutch, Bitcoin's Bonnie and Clyde. VanityFair. [Internet]. 2022 [cited 29 May 2025]; Available in: https://www.vanityfair.com/news/2022/08/the-ballad-of-razzlekhan-and-dutch-bitcoins-bonnie-and-clyde

11. Carlisle D. The crypto launderers: Crime and cryptocurrencies from the Dark Web to DeFi and beyond.

Wiley, 2023.

12. Brown A. The criminal side of cryptocurrency. Arkansas State University, Faculty Publications [Internet]. 2023 [cited 29 May 2025];5. Available in: https://arch.astate.edu/clac-scrim-facpub/5

13. Chainalysis. DeFi takes on bigger role in money laundering but small group of centralised services still dominate. [Internet]. 2022 [cited 29 May 2025]; Available in: https://www.chainalysis.com/blog/2022-crypto-crime-report-preview-cryptocurrency-money-laundering/

14. Interpol General Secretariat. Interpol Global Trend Summary Report. [Internet]. 2022 [cited 29 May 2025]; Available in: https://www.interpol.int/en/content/download/18350/file/Global%20Crime%20Trend%20Summary%20Report%20EN.pdf

15. Dudani S, Baggili I, Raymond D, Marchany R. The current state of cryptocurrency forensics. Forensic Science International: Digital Investigation 2023;46. http://doi.org/10.1016/j.fsidi.2023.301576

16. Pocher N, Veneris A. Privacy and transparency in CBDCs: a regulation-by-design AML/CFT scheme. In: 2021 IEEE International Conference on Blockchain and Cryptocurrency. (pp. 1–9). Sydney, Australia, 2021. https://doi.org/10.1109/ICBC51069.2021.9461090

17. Towne Morton D. The future of cryptocurrency: an unregulated instrument in an increasingly regulated global economy. Loyola University Chicago International Law Review [Internet]. 2020 [cited 29 May 2025];16(1):8. Available in: https://lawecommons.luc.edu/cgi/viewcontent.cgi?article=1219&context=lucilr

18. Simser JR. Canada's financial intelligence unit: FINTRAC. Journal of Money Laundering Control 2020;23(2):297–307. https://doi.org/10.1108/JMLC-10-2019-0079

19. Jenkins C. Canadian Cryptocurrency Conundrums: A Socio-Technical Systems Analysis of Crypto Laundering in Canada Caitlyn Jenkins, Rhianna Hamilton, and Christian Leuprecht. Dirty Money: Financial Crime in Canada 2023;27. https://doi.org/10.1515/9780228019886-014

20. Majumder A, Routh M, Singha D. A conceptual study on the emergence of cryptocurrency economy and its nexus with terrorism financing. In The Impact of Global Terrorism on Economic and Political Development. (pp. 125–138). Emerald Publishing Limited, 2019. https://doi.org/10.1108/978-1-78769-919-920191012

21. Desmond DB, Lacey D, Salmon P. Evaluating cryptocurrency laundering as a complex socio-technical system: A systematic literature review. Journal of Money Laundering Control 2019;22(3):480–497. https://doi.org/10.1108/JMLC-10-2018-0063

22. Dupuis D, Smith D, Gleason K. Old frauds with a new sauce: digital assets and space transition. Journal of Financial Crime 2023;30(1):205–220. https://doi.org/10.1108/JFC-11-2021-0242

23. Lee H, Choi KS. Interrelationship between Bitcoin, ransomware, and terrorist activities: Criminal opportunity assessment via cyber-routine activities theoretical framework. In: The New Technology of Financial Crime. (pp. 82–103). Routledge, 2022. https://doi.org/10.4324/9781003258100-5

24. Maurushat A, Halpin D. Investigation of cryptocurrency enabled and dependent crimes. In: Financial Technology and the Law: Combating Financial Crime. (pp. 235–267). Cham: Springer International Publishing, 2022. https://doi.org/10.1007/978-3-030-88036-1_10

25. Long H, Demir E, Sojka B, Zaremba A, Shahzad S. Is geopolitical risk priced in the cross-section of cryptocurrency returns? Finance Research Letters 2022;49:103131. https://doi.org/10.1016/j.frl.2022.103131

26. Elwell CK, Murphy MM, Seitzinger MV. Bitcoin: questions, answers, and analysis of legal issues. Washington: Congressional Research Service, 2015.

27. Hudak S. FinCEN fines Ripple Labs Inc. in first civil enforcement action against a virtual currency exchanger. Washington, DC: United States Department of the Treasury, Financial Crimes Enforcement Network, 2015. https://www.fincen.gov/news_room/nr/html/20150505.html

28. Choo K-KR. Cryptocurrency and virtual currency: Corruption and money laundering/terrorism financing risks? In D. L. K. Chuen (Ed.):Handbook of digital currency: Bitcoin, innovation, financial instruments, and big data. (pp. 283–307). London: Academic Press, 2015.

29. Connell J. Alderney: gambling, Bitcoin and the art of unorthodoxy. Island Studies Journal 2014;9(1):69–78. https://doi.org/10.24043/isj.294

30. Nicholls J. Isle of man sees Blockchain through the prism of e-gaming triumphs. Blockchain Briefin, 2016.

31. Burgess A, Hamilton R, Leuprecht C. Terror on the Blockchain: The Emergent Crypto-Crime-Terror Nexus. In: Goldbarsht D, de Koker L. (Eds.):Financial Crime, Law and Governance. Ius Gentium: Comparative Perspectives on Law and Justice. Vol. 116. Springer, Cham, 2024. https://doi.org/10.1007/978-3-031-59547-9_9

32. Campbell-Verduyn M. Bitcoin, crypto-coins, and global anti-money laundering governance. Crime, Law and Social Change 2018;69:283–305. https://doi.org/10.1007/s10611-017-9756-5

33. Furneaux N. Investigating cryptocurrencies: Understanding, extracting, and analysing Blockchain evidence. Wiley, 2018. https://doi.org/10.1002/9781119549314

34. Wang S, Zhu X. Evaluation of potential cryptocurrency development ability in terrorist financing. Policing: A Journal of Policy and Practice 2021;15(4):2329–2340. https://doi.org/10.1093/police/paab059

35. Leuprecht C, Cockfield A, Simpson P, Haseeb M. Tracking transnational terrorist resourcing nodes and networks. Florida State University Law Review 2019;46(2):289–344.

36. Leuprecht C, Skillicorn DB, McCauley C. Terrorists, radicals and activists: distinguishing between countering violent extremism and preventing extremist violence, and why it matters. In: Countering violent extremism and terrorism: assessing domestic and international strategies. (pp. 18–46). McGill-Queen's University Press, Montreal, 2020. https://doi.org/10.1515/9780228000600-005

37. FATF. Ethnically or racially motivated terrorism financing. FATF, Paris, France. [Internet]. 2021 [cited 29 May 2025]; Available in: https://www.fatf-gafi.org/publications/methodsandtrends/documents/ethnically-racially-motivatedterrorism-financing.htm

38. IntelBrief. Blockchain and Bloodshed: The Role of Cryptocurrencies in Terrorist Financing. [Internet]. 2024 [cited 29 May 2025]; Available in: https://51.159.195.58/intelbrief-2024-october-16/?__cpo=aHR0cHM6Ly90aGVzb3VmYW5jZW50ZXIub3Jn#:~:text=Cryptocurrencies%20are%20not%20the%20main,oriented%20currencies%20such%20as%20Monero

39. Office of Foreign Assets Control (OFAC). Sanctions programmes and country information. [Internet]. 2023 [cited 29 May 2025]; Available in: https://ofac.treasury.gov/sanctions-programs-and-country-information

40. Abi-Saab G. Keynote address the concept of sanction in international law. In: United Nations sanctions and international law. (pp. 29–41). Brill, Leiden, 2001. https://doi.org/10.1163/9789004502871_005

41. Greenberg A. Lords of crypto crime: The race to bring down the world's invisible kingpins. Monoray, 2024.

42. FATF. Targeted update on implementation of the FATF standards on virtual assets/VASPs. FATF, Paris. [Internet]. 2023 [cited 29 May 2025]; Available in: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2023.html

43. Petkauskas V. Why individual arrests will not shut down lockbit. Cybernews. [Internet]. 2022 [cited 29 May 2025]; Available in: https://cybernews.com/editorial/arrests-wont-shut-down-lockbit/

44. Tunney C. Intelligence agency says ransomware group with Russian ties poses 'enduring threat' to Canada. CBC News. [Internet]. 2023 [cited 29 May 2025]; Available in: https://www.cbc.ca/news/politics/cse-lockbit-threat

45. United States District Court for the District of New Jerse. United States of America v. Mikhail Vasiliev, Mag. No. 22-12370. [Internet]. 2022 [cited 29 May 2025]; Available in: https://cdn.prod.website-files.com/6082dc5b670562507b3587b4/673773106dcf79486142430c_USA%20v.%20Vasiliev%20Complaint.pdf

46. Trevithick M. St. Marys, Ont. grapples with cyberattack as ransomware group threatens to publish stolen data. Global News. [Internet]. 2022 [cited 29 May 2025]; Available in: https://globalnews.ca/news/9009347/st-marys-ont

47. Faife C. A small Canadian town is being extorted by a global ransomware gang. The Verge. [Internet]. 2022 [cited 29 May 2025]; Available in: https://www.theverge.com/2022/7/22/23274372/st-marys-canada-lockbit-ransomware-cyber-incident

48. Cherniei V, Cherniavskyi S, Babanina V, Tykhonova O. Criminal liability for cryptocurrency transactions: Global experience. European Journal of Sustainable Development 2021;10(4):304–316. https://doi.org/10.14207/ejsd.2021.v10n4p304

49. Widyatmoko U, Atmasasmita R, Susanto A, Purwanto B. Law enforcement against cryptocurrency abuse. Journal of Social Research 2024;3(2):1–11. https://doi.org/10.55324/josr.v3i2.1941

50. Dickens S. Squid Game meme coin crashes by 99.9% after developers pull the plug. Yahoo! [Internet]. 2021 [cited 29 May 2025]; Available in: https://www.yahoo.com/now/squid-game-meme-coin-crashes-131908065.html

51. Roberge I. Misguided policies in the war on terror? The case for disentangling terrorist financing from money laundering. Politics 2007;27(3):196–203. https://doi.org/10.1111/j.1467-9256.2007.00300.x

52. Shields P. When the 'information revolution' and the US security state collide: money laundering and the proliferation of surveillance. New Media Society 2005;7(4):483–512. https://doi.org/10.1177/1461444805054110

53. Stokes R. Anti-money laundering regulation and emerging payment technologies. Banking Financial Services Policy Report 2013;32(5):1–10.

54. Chainalysis. How To Use Blockchain Intelligence to Investigate Crypto Crime. [Internet]. 2024 [cited 29 May 2025]; Available in: https://www.chainalysis.com/blog/investigate-crypto-crime-blockchain-intelligence/

55. Dion-Schwarz C, Manheim D, Johnston PB. Terrorist use of cryptocurrencies: Technical and organisational barriers and future threats. Rand Corporation, 2019. https://doi.org/10.7249/RR3026

56. Shukla S. UN says crypto use in terror financing likely to soar. Bloomberg. [Internet]. 2022 [cited 29 May 2025]; Available in: https://www.bloomberg.com/news/articles/2022-10-31/un-finding-more-cases-where-crypto-involved-in-terror-financing

57. Gonzalez-Argote J, Maldonado E, Maldonado K. Algorithmic Bias and Data Justice: ethical challenges in Artificial Intelligence Systems. EthAIca. 2025; 4:159. https://doi.org/10.56294/ai2025159

58. Juárez GE, Gambino N. Professionalization and Artificial Intelligence in Family Businesses. EthAIca. 2024; 3:139. https://doi.org/10.56294/ai2024139

59. de Koker L, Ocal T, Casanovas P. Where's Wally? FATF, virtual asset service providers, and the regulatory jurisdictional challenge. In: Financial technology and the law, law, governance and technology series 2022; 47:151–183. Springer, Cham. https://doi.org/10.1007/978-3-030-88036-1_7

FINANCING

The authors did not receive financing for the development of this research.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest.

AUTHORSHIP CONTRIBUTION

Conceptualization: Kostiantyn Orobets.
Data curation: Tetiana Batrachenko.
Formal analysis: Tetiana Baranovska.
Research: Tetiana Batrachenko, Valeriy Sereda.
Methodology: Kostiantyn Orobets, Vladyslav Shkolnikov.
Project management: Tetiana Baranovska.
Resources: Tetiana Baranovska, Valeriy Sereda.
Software: Tetiana Batrachenko.
Supervision: Valeriy Sereda.
Validation: Valeriy Sereda.
Display: Valeriy Sereda.
Drafting - original draft: Kostiantyn Orobets.
Writing - proofreading and editing: Vladyslav Shkolnikov.