Cryptocrime in the Context of Digital Transformation

Submitted: 15 October 2025
Reviewed: 9 December 2025
Revised: 23 December 2025
Accepted: 25 December 2025

Evgheni Florea*
https://orcid.org/0000-0001-7236-0695

Article submitted to peer blind review

DOI: https://doi.org/10.26512/lstr.v18i2.60028

Abstract

[Purpose] The purpose of this study was to investigate the quantitative and qualitative characteristics of crypto-crime in the context of digital transformation.

[Methodology/approach/design] The methodological framework of this study included comparative analysis, criminological approach, statistical research, and case studies (using Silk Road, Hydra, Monopoly Market, CryptoLocker, PlusToken, ransomware viruses and pump-and-dump schemes, as examples).

[Findings] The study systematised the principal forms of crypto-crime – from financial pyramids and extortion to money laundering, crypto-banking fraud, and romantic deception schemes. Their key features were identified: high level of anonymity of transactions, transnational nature of activity, legal uncertainty, and rapid development of technological methods of crime. A separate place was given to the analysis of the dynamics of crypto-crime growth: if in 2015 there were less than 2 thousand incidents with a total damage of 2 million dollars, by 2024 the number of complaints approached 150 thousand, while the cumulative losses exceeded USD 9.3 billion. The losses from investment fraud (USD 5.8 billion with 41.5 thousand complaints), romance schemes (USD 237 million with less than 4 thousand complaints), and crypto-banking scams (USD 189 million with 5.5 thousand incidents) are particularly pronounced.

[Practical implications] It is shown that digital literacy plays a dual role: on the one hand, the high level of technical knowledge of criminals favours the emergence of increasingly sophisticated schemes, while on the other hand, the lack of awareness of users makes them particularly vulnerable. It concludes that a balanced legal approach is needed, combining effective controls with support for innovation, and emphasises the significance of digital literacy as a tool for crypto-crime prevention.

[Originality/value] This study offers a comprehensive synthesis of both quantitative data and case-based analysis to map the evolving landscape of crypto-crime, highlighting underexplored correlations between digital illiteracy and victimisation. By integrating

*Senior Compliance Officer at Payme Swiss. PhD and Associate Professor at the Department of Law, Cooperative-Commercial University of Moldova (UCCM), Chisinau, Republic of Moldova. E-mail: floreaevgheni9@gmail.com.

criminological insights with technological trends, it provides a novel interdisciplinary perspective on the risks posed by crypto-crime in the era of digital transformation.

Keywords: Anonymity. Fraud. Terrorism. Digital literacy. Legal regulation.

INTRODUCTION

The relevance of the study is conditioned by the fact that the development of digital technologies and the rapid spread of various crypto-assets have radically transformed the sphere of financial and cybercrime. Crypto-crime has become one of the most dynamic and challenging to control forms of unlawful activity. The high level of anonymity and decentralisation inherent in crypto-assets creates a favourable environment for financial crimes, such as money laundering, fraud, embezzlement, and the financing of illegal activities, often facilitated through the wide web. In this context, the need to study the quantitative and qualitative characteristics of crypto-asset crime becomes particularly relevant.

The problematic of the study centres on the fact that law enforcement and regulatory authorities around the world face a series of serious challenges, including limited access to verified information, the lack of a unified database on crypto-assets, the difficulty in interpreting anonymised transactions and lack of expertise in emerging blockchain technologies. Data analysis is hampered by a high degree of technological variability and complexity, the constant emergence of new forms of fraud and the use of tools that make tracking challenging. Under these conditions, it becomes necessary to systematically and thoroughly investigate the quantitative and qualitative characteristics of crypto-crime as a basis for developing more effective mechanisms for detecting, preventing, and suppressing crime in the digital economy.

Many researchers have investigated crypto-crime from different methodological perspectives, focusing both on its structural features and on the dynamics of its development. Zhao et al. (2023) investigated the nature of illegal transactions in blockchain networks, emphasising that cryptocurrencies are actively used to conceal financial activity. The researchers noted that due to the anonymity of crypto-asset turnover, criminals have obtained tools that considerably complicate conventional financial monitoring mechanisms. Carletti et al. (2024) focused on the typology of cryptocurrencies, tracing how the methods of illegal activity evolved from simple fraudulent schemes to multi-level structures with international reach. The researchers noted the trend towards the professionalisation of criminals and the development of stable communities using cryptocurrencies as a basis for organising operations.

Cong et al. (2025) proposed to consider crypto-crime as a distributed ecosystem that uses digital technologies to decentralise risks. W. Cong et al. specifically highlighted the consistent correlation between the degree of technology advancement and the proliferation of novel forms of illicit behaviour. The researchers' analysis focused on intermediary links – such as cryptocurrency exchanges and anonymous wallets – that act as buffers between criminals and the ultimate recipients of funds. Iordachi (2023) approached the problem from a sociological standpoint, analysing how legal and economic instability contributes to an increase in the number of individuals involved in crypto schemes. The researcher emphasised that the growth of crypto-crime cannot be explained by technical factors alone – societal processes, including digital ignorance and a prominent level of trust in innovative financial technologies, must also be considered.

Krishnan et al. (2023) proposed a conceptual model of crypto-crime classification based on the degree of complexity of its detection and investigation. The researchers argued that it is the qualitative aspect of criminal activity that comes to the forefront – intellectualisation of approaches, active use of software tools to hide traces, and integration into legal financial flows. Otero and Diaz (2025) considered the transnational nature of cryptocurrencies, pointing out that the lack of a unified international legal mechanism enables criminals to move freely between jurisdictions. Otero and Diaz emphasised that cryptocurrencies have exacerbated the problem of so-called "digital extraterritoriality" when activities cannot be localised within a single country.

Costea et al. (2024) analysed the state regulatory response to the threat of crypto crime. The researchers considered both prohibitive and adaptive measures, demonstrating the heterogeneity of legal approaches. A reactive regulatory model based on delayed response cannot effectively handle the constantly transforming threats. Ogele (2024) also emphasised the use of crypto-assets in financing extremist and terrorist groups. The researcher emphasised that cyberspace has become not only a medium for economic crimes, but also a tool of ideological struggle.

Rahman et al. (2024) addressed forensic aspects, specifically, the possibilities of recovering digital traces. The researchers showed that the use of machine learning and graph analysis methods can significantly improve the accuracy of identification of suspicious transactions and participants in criminal networks. Rustamaji and Faisal (2024) reviewed international cooperation in the fight against crypto-crime. Rustamaji and Faisal concluded that despite the existence of a series of agreements and platforms for data exchange, the interaction between countries is still fragmented, while law enforcement practice

– uncoordinated. As a result, the effectiveness of the fight against crypto-asset crime is limited at both the national and global level.

Gottschalk (2018) introduced the convenience theory as a comprehensive framework for understanding white-collar crime, examining how convenience serves as a primary motivation for criminal behaviour among professionals and executives. The theory posits that individuals commit crimes when illegal activities provide a more convenient path to achieving desired goals compared to legal alternatives (Nuridin et al., 2025). Gottschalk (2019) further developed the convenience theory by identifying three key dimensions that contribute to criminal convenience: financial motive, organizational opportunity, and personal willingness. The author argued that white-collar criminals are driven by the desire to achieve financial goals through the most efficient means available, often leveraging their organizational positions to minimize effort and risk.

Cohen and Felson (1979) developed the foundational routine activity theory, which examined how crime occurs through the convergence of three essential elements: motivated offenders, suitable targets, and the absence of capable guardians. The authors argued that crime rates are influenced more by opportunity structures than by criminal motivations alone, revolutionizing criminological thinking about crime causation. Maimon and Louderback (2018) examined routine activity theory's application to cybercrime prevention, demonstrating how understanding online routine activities can inform the development of effective digital guardianship strategies. Their research emphasized the importance of capable guardianship in virtual environments.

Thus, the accumulated body of research reflects a wide range of views and approaches, but at the same time demonstrates the absence of a holistic picture combining quantitative parameters and qualitative features of crypto-crime. The problem of interaction between criminal networks and digital infrastructures has also not received due attention. The issue of adaptation of crypto-criminal schemes to new legal conditions, as well as the impact of the level of technological literacy of the population on the involvement in illegal activities with crypto-assets has not been sufficiently covered. This points to the need for a comprehensive analysis that accounts for both structural patterns and the dynamics of digital threats on a global scale.

This study addresses a significant gap in the existing literature and criminological research on the rapidly growing issue of crypto-crime, particularly within the context of digital transformation. While previous studies have explored general trends in cybercrime, few have delved into the unique technological characteristics of crypto-assets and the specific forms of fraud that exploit these innovations. Moreover, the rapid expansion of crypto-crime, marked by the increasing sophistication of fraud schemes and the significant rise in financial

losses, has not been adequately examined in terms of its correlation with users' digital literacy and law enforcement's limited capabilities.

The purpose of this study was to identify the most widespread patterns of crypto-crime, as well as the quantitative and qualitative characteristics of this phenomenon in the digital economy, to contribute to a better understanding of its scale, forms, and mechanisms of functioning. The objectives of the study were to analyse the characteristics and transnational nature of crypto-crime, including its technological complexity and methods of concealing traces in the digital space; to examine the dynamics and structure of crypto-crime; and to investigate the impact of the level of digital literacy and legal regulation on the vulnerability of users and the effectiveness of the fight against crypto-crime.

MATERIALS AND METHODS

The study employed both quantitative and qualitative methods of analysis aimed at a comprehensive study of the phenomenon of crypto-crime in the context of digital transformation. The methodological framework included a combination of comparative, criminological, statistical approaches (analysis of dynamics and trends), and case studies. Of particular significance were the data for 2015-2024, which helped to trace the dynamics of crypto-crime in retrospect and record qualitative changes in the manner, scale, and legal responses to such crimes. The structure of crypto-crime as of 2024 was analysed. For this, data from the Internet Crime Complaints Centre (IC3) (2024) was used. Attention was also paid to assessing the share of the total volume of crypto-asset transactions related to illegal activity for 2021-2024, which helped to identify consistent trends and determine the degree of crypto-infrastructure involvement in criminal circulation. The assessment was conducted based on materials from Transaction Monitoring Labs (2025).

To assess the effectiveness of different criminal strategies, a comparative analysis was conducted for key types of crypto-crime: investment fraud, pump-and-dump schemes, extortion using ransomware, romance schemes, crypto-banking schemes, money laundering, fake application schemes, and phishing. Chainalysis (2025) were used as the main source of data. The case study method was applied within the research, including analyses of key incidents such as Silk Road (2025; Spagnuolo et al., 2014), CryptoLocker (Kelion, 2013; How much did…, 2013), and Hydra (Tidy, 2022). These cases were selected based on their notorious status and their ability to represent distinct forms of crypto-crime, including marketplace operations, ransomware attacks, and illicit trading platforms. Additional cases, including Monopoly Market (Europol, 2023) and PlusToken (PlusToken scammers didn't…, 2019), were also included to examine the diversity of criminal models in the crypto space. The selection was intentional

to encompass a wide range of incidents, showcasing different criminal strategies and operational scales. Each case was analysed through a document analysis approach, utilizing investigative reports, court documents, and authoritative news sources to assess their modus operandi, scale, and legal outcomes. This systematic approach allows for a comparative understanding of the common features and differences among these crypto-crime incidents.

The study analysed crypto-crime cases covering the regions with the greatest concentration of reported incidents involving the illicit use of crypto-assets (Iran (Bayena, 2025), Venezuela (Erazo, 2020), Israel (Reuters, 2023)). Cases reflecting the specifics of crypto-crime in Moldova were also considered. A case study of two incidents was used: a scheme of fictitious investments through call centres uncovered in February 2025 (Fraudulent cryptocurrency investment…, 2025), and a transnational fraud involving an organised group, stopped in a joint operation between Romania and Moldova in 2023 (European Union Agency for Criminal Justice Cooperation, 2023).

Additionally, the study investigated the impact of the digital literacy level of the population on the prevalence of crypto-assets. For this, data on the types of crime victims, the nature of fraudulent schemes used, and the frequency of successful attacks using social engineering methods were analysed. This allowed a correlation to be established between the low level of digital competence of users and their high vulnerability to fraudulent activities, particularly phishing, fake investment platforms and romance fraud schemes, which further exacerbated by the limited expertise of law enforcement agencies in detecting and countering crypto-related criminal schemes.

Much attention in the methodological approach was given to analysing the effects of legal regulation on the scale of crypto-crime. Various models of legislative control were considered, including the presence of mandatory Know Your Customer (KYC) (2025) and Anti-Money Laundering (AML) (2025) procedures, the degree of transparency of transactions on crypto-platforms, as well as the level of interaction between state and international structures in terms of suppressing illegal transactions. In this context, special attention was also given to the implementation of the FATF's Travel Rule (Financial Action Task Force, 2021), which requires Virtual Asset Service Providers (VASPs) to collect and share sender and recipient information during transactions. Additionally, the EU's Fifth Anti-Money Laundering Directive (AMLD5) (2025) was considered, as it introduced regulatory obligations for platforms facilitating exchange between virtual and fiat currencies.

RESULTS

Regulatory and legal frameworks for crypto-crime: Classification, challenges, and transnational enforcement

The application of regulatory and legal terminology significantly affects the categorisation and tracking of illicit activity in the crypto ecosystem. The term crypto-crime aligns with the broader concept of crypto-asset crime, encompassing all types of offenses involving virtual assets – not only crypto (virtual) currencies like Bitcoin or stablecoins, but also other digital financial instruments such as utility tokens and tokenised securities. In contrast, the narrower term crypto (virtual) currency crime relates only to offenses involving currencies used primarily as a medium of exchange (Furneaux, 2018). This distinction determines the regulatory approach and scope of enforcement action across different jurisdictions. The author understand "crypto-crime" as any illicit activity in which virtual (crypto) assets (cryptocurrencies, tokens) are instrumental to the offense, either as the target, means, or proceeds of crime.

Regulation (EU) 2023/1114 of the European Parliament and of the Council "On Markets in Crypto-Assets" (2023), known as the Markets in Crypto-Assets Regulation (MiCA), provides the first comprehensive, official classification of crypto-assets within the European Union. Under MiCA, crypto-assets are categorized into three primary types:

1.Asset-referenced tokens (ARTs): These tokens aim to stabilize their value by referencing multiple assets, such as a basket of currencies or commodities. They are designed to maintain a stable value over time and are subject to stringent regulatory requirements, including authorization and supervision by competent authorities.

2.Electronic money tokens (EMTs): EMTs are crypto-assets that seek to stabilize their value by referencing a single official currency. They function as a digital representation of fiat money and are primarily used for payment purposes.

3.Other crypto-assets: This category encompasses all crypto-assets that do not qualify as ARTs or EMTs. It includes utility tokens, payment tokens, and other digital representations of value or rights that are not classified under the previous two categories.

MiCA also establishes a regulatory framework for crypto-asset service providers, including requirements for authorization, governance, and operational conduct. The regulation aims to ensure consumer protection, market integrity, and financial stability within the crypto-asset markets.

A divergence in legal frameworks can be observed between international and regional authorities. The Financial Action Task Force (FATF) (2021) employs the broad term virtual assets and regulates actors through the category of

Virtual Asset Service Providers, which includes exchanges, brokers, and wallet providers. FATF standards mandate comprehensive compliance procedures, including KYC and AML requirements, and recommend the implementation of the Travel Rule to track cross-border transactions. In contrast, the AMLD5 (2025) relies on the more limited term "virtual currencies" and regulates only exchange and wallet services directly tied to fiat conversion or custody. This narrower scope initially excluded a wide range of actors present in the illicit crypto market.

A gradual harmonisation has been observed, particularly through the EU's adoption of the MiCA framework and AMLR proposals, which expand the regulatory perimeter to align with FATF recommendations. These legislative updates redefine virtual assets to include a broader array of instruments, integrate licensing for VASPs, and incorporate enforcement tools such as cross-border transaction monitoring and enhanced transparency obligations. The shift from AMLD5 to MiCA and AMLR reflects the evolution of risk understanding and signals stronger institutional capacity to address complex and decentralised forms of crypto asset crime. The alignment of legal taxonomies with FATF standards enhances cross-border cooperation, improves traceability of illicit flows, and contributes to a more comprehensive picture of crypto-crime dynamics across jurisdictions.

The global discussion around crypto regulation has increasingly emphasized the principle of the supremacy of law, ensuring that digital asset markets operate within enforceable legal frameworks. Numerous jurisdictions have referenced this principle when integrating crypto-assets into existing financial regulations, reinforcing the idea that technological innovation must remain subject to the rule of law – as reflected in key rulings and policy frameworks from the EU, the U.S., and international bodies such as the FATF (Florea & Pustelnik, 2021).

Crypto-crime, as a relatively new form of illegal activity, has emerged at the intersection of digital technology and the criminal world, gaining increasing significance in the modern economy and society. This term is widely understood as a set of offences committed using crypto-assets and related blockchain technologies, which have unique characteristics that distinguish them from conventional types of crime. Crypto-crime is based on the use of digital assets that provide high transaction speed, decentralization, and a form of pseudonymity. While blockchain technology allows transactions to be visible to all participants, it is complex to directly link these transactions to a specific individual. This level of anonymity is more accurately described as pseudonymity, where transactions are associated with wallet addresses rather than personal identities. However, certain blockchain instruments, such as anonymity-enhanced coins, crypto-mixers, and crypto-tumblers, are designed to further obscure the link between

transactions and the individuals involved. These properties make crypto-assets an attractive tool for criminals, allowing them to conceal the origin and destination of funds and to circumvent controls by State authorities and conventional financial institutions (Collins, 2022). Thus, the key essential feature of crypto crime is the ability to exploit the technological features of crypto-systems for the implementation of illegal purposes.

Another prominent feature is the transnational nature of these crimes. Crypto transactions take place in a global digital space where jurisdictional boundaries are blurred, and law enforcement faces serious limitations. This raises complex issues of law enforcement coordination and regulation of crypto-asset activities at the international level (Cunjak, 2022). A significant aspect is the diversity of forms and methods of committing crypto-crime – from fraud, theft, and money laundering to the financing of terrorist and extremist activities. They are united by high technological complexity, requiring criminals to constantly update their knowledge and use innovative digital tools, which complicates the detection and suppression of such crimes (McCord et al., 2022).

The legal definition of crypto-crime continues to be one of the most complex and debatable problems in modern legal science. The lack of a universal and generally accepted definition of this phenomenon is conditioned by the fact that crypto-assets, despite their widespread use, have not yet received a stable and unambiguous status in the legal systems of most states. Some jurisdictions consider crypto- as property, others – as a means of payment or a digital asset, and others prohibit its circulation altogether. This creates heterogeneity in approaches and creates a legal vacuum in which crypto-assets are difficult to qualify and systematise.

Further difficulties arise when attempting to incorporate crypto into existing criminal law frameworks. Conventional categories such as fraud, embezzlement, terrorist financing, or money laundering do not always adequately cover the specificities of crypto-asset schemes (Nursaliyeva et al., 2023). For example, hacking a smart contract or using a decentralised autonomous organisation (DAO) to commit a crime do not fit into the usual legal constructs (Trozze et al., 2022). Moreover, many actions with crypto-assets, despite their evident criminality, may not fall under the current legislation due to gaps in terminology and legal regulation tools.

Classification challenges are also related to the multi-level and hybrid nature of crypto offences. One offence may combine elements of economic, informational, cross-border, and even terrorist nature. This requires a comprehensive approach to qualification, which is particularly difficult in the absence of unified methodologies and judicial practice. As a result, there are

differences in the interpretation of analogous acts in different countries, which hinders international cooperation and legal harmonisation.

Furthermore, the legal assessment of crypto-assets is complicated by the rapid development of technology, which outpaces the updating of the regulatory framework. Legislation often does not have time to adapt to new forms of criminal activity, which makes law enforcement reactive rather than proactive (Fathi et al., 2025). Under such conditions, the fight against crypto-crime requires not only the improvement of legal mechanisms, but also the development of innovative approaches to the qualification of digital offences, including elements of technical and behavioural analysis.

Rise of crypto-crime: Trends, case studies, and regulatory challenges in the digital era

In the context of digital transformation, the rise of crypto-crime has been a notable by-product of the increasing use of blockchain technology and digital assets. The decentralised nature of cryptocurrencies and the high level of transaction anonymity have created an environment where illicit activities, such as investment fraud, extortion, and money laundering, have proliferated at an alarming rate. Anonymity means complete untraceability, where no identifier links activities to a user. Pseudonymity uses a consistent alias, like a wallet address, allowing transactions to be publicly tracked under that alias without revealing real-world identity. Bitcoin exemplifies pseudonymity, not anonymity, on its blockchain.

This transformation has reshaped the landscape of criminal activity, making it difficult for traditional legal frameworks and authorities to effectively monitor and control. The digital revolution, while enabling greater innovation, has also exposed vulnerabilities, particularly in terms of users' digital literacy and the lack of preparedness among law enforcement (Kumisbekova et al., 2019; Temirzhanova et al., 2019). As the crypto-crime ecosystem evolves, new technological tools and sophisticated schemes emerge, further complicating regulation and enforcement efforts. Thus, digital transformation in this context not only highlights the risks associated with crypto-assets but also underscores the necessity of an integrated approach combining regulatory oversight, user education, and technological advancement.

The initial stage of development of blockchain technologies, especially in the period from 2011 to 2014, coincided with the emergence of the first large-scale crimes committed using them. The Silk Road (2025) darknet market, which operated on the Tor network from February 2011 to October 2013, occupies a special place among them. This site became not just a marketplace for illegal goods, but also a kind of demonstration of how anonymous crypto technologies

can be integrated into a sustainable criminal infrastructure. Silk Road offered a wide range of illicit goods, including drugs, malware, forged documents, and accounts of hacked services. In September 2013, the site had approximately 13,000 active adverts under relevant headings. Other categories reflecting the scale of criminal activity included 159 offerings under "Services" (including hacked accounts), 801 offerings under "Digital Goods", and 169 under "Counterfeits".

Silk Road recorded 1,229,465 transactions during its period of operation – from 6 February 2011 to 23 July 2013. The total revenue reached 9,519,664 BTC (Bitcoin), of which 614,305 BTC was the site's commission fees. Considering the Bitcoin exchange rate at the time, the total amount of goods and services sold was about USD 183 million. The transactions involved 146,946 buyers and 3,877 sellers from various countries. According to the registration data, the most users were from the US (about 30%), followed by residents of the UK, Australia, Germany, Canada, France, Sweden, Russia, Italy, and the Netherlands. At the same time, 27% of customers chose not to indicate their location at all, which complicated the analysis of the geography of criminal activity.

The Silk Road case is also unique in that it was the first case to receive a trial and conviction for a crypto offence. The platform's founder, Ross Ulbricht, was sentenced to a double life sentence on charges including money laundering, drug trafficking, running a criminal organisation, and complicity in other crimes. This was a prominent precedent in both legal and criminological terms, although U.S. President Donald Trump granted him a partial clemency by commuting his sentence.

In parallel with Silk Road, other models of crypto-crime developed, the most notable of which was an extortion scheme using encryption software. The CryptoLocker (Kelion, 2013) is a virus, which operated between September 2013 and June 2014, infected between 200,000 and 250,000 computers, mostly in the US and UK. The malware blocked access to user data, demanding a ransom of 0.3 to 2 BTC (approximately USD 600-700 at that time) to decrypt it. If the ransom was not paid within 72 hours, the encryption key was irretrievably destroyed. In the first three months of CryptoLocker's operation alone, the attackers made 41,928 BTC – the equivalent of about USD 27.78 million at the then-current exchange rate. On some days, their daily profits reached up to USD 1 million. Even one of the district police departments in Massachusetts was among the victims. Considering the disruption of businesses, authorities, and other organisations, the total damage caused by the attacks was estimated at hundreds of millions of dollars.

These two cases – Silk Road and CryptoLocker – set the vector for further development of crypto-crime. They demonstrated that crypto can be not only a

means of anonymous payment, but also a tool for building complex and sustainable criminal systems. Their successful operation in an environment of weak regulation, technological opacity and cross-border jurisdiction has become a challenge for the international community. Both cases are key to understanding the quantitative and qualitative attributes of crypto and are essential to developing mechanisms for their prevention, legal response, and statistical recording.

Particular attention should be paid to the increase in the number of victim complaints and the amount of damages suffered (Table 1). The increase in complaints about crypto crime is not accidental and shows that this type of criminal activity has reached a new level of development, which is confirmed by the data for 2024.

Year	Number of complaints	Damage amount in millions of USD
2024	149,686	9,322.9
2023	69,469	5,587.5
2022	53,124	2,570.1
2021	34,202	1,607.7
2020	35,229	246.2
2019	29,313	159.3
2018	36,477	182.1
2017	4,139	58.4
2016	1,904	28.3
2015	1,920	2

Table 1 – Number of reported cryptocurrency-related offences and amount of damage caused

Source: compiled by the author based on Internet Crime Complaint Center (2024).

The data shows an exponential increase in both the number of reported crypto-related offences and the amount of damage caused by them over the period from 2015 to 2024. While in 2015 there were less than 2 thousand complaints with a total damage of USD 2 million, in 2024, the number of appeals approached 150 thousand and the damage amounted to more than USD 9.3 billion. Such dynamics indicates two interrelated trends: firstly, the rapid spread of crypto technologies in everyday life, and secondly, the growing vulnerability of users and law enforcement institutions to increasingly sophisticated crypto crime schemes. Table 2 shows the types of crypto-related offences by complaints and losses.

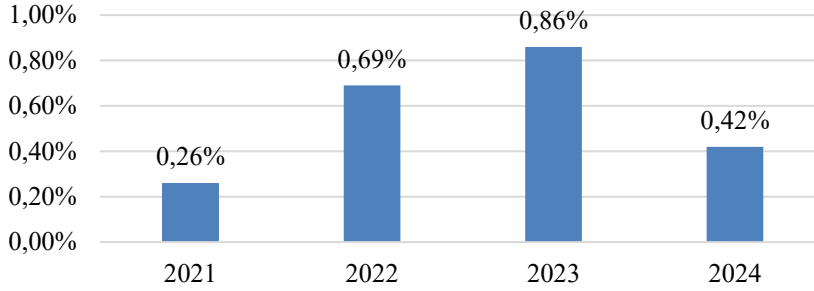
Type of crime	Number of complaints	Damage amount in millions of USD
Extortion	47,054	96.1
Investments	41,557	5,819.5
Personal data leakage	11,644	1,120.8
Technical support	11,129	962
Employment	6,533	197.2
Phishing/Spoofing	3,938	28.5
Trust/Romantic relationships	3,811	237.2
Imitation of government agencies	3,585	146.1
Non-payment/Non-delivery	2,492	55.1
Advance payments	1,537	36.4
Other	1,315	63.5
Data leakage	846	167.9
Identity theft	527	20.2
Credit card/cheque fraud	389	24.9
Ransomware	389	1.1
Lottery/Raffles/Inheritance	329	6.3
Business email compromise	256	63.9
Real estate	256	5.9
SIM card replacement	215	28.5
Stalking/Harassment	211	0.2
Overpayment	186	0.3
Malware	53	0.2
Botnet	44	0.7
Crime against children	42	0.02

Table 2 – Types of crypto offences by complaints and losses, 2024

Source: compiled by the author based on Internet Crime Complaint Center (2024).

The analysis shows that the most significant financial losses in crypto crime are related to investment schemes – with 41,557 complaints, losses reached USD 5.8 billion, substantially higher than losses in all other categories. Extensive losses are also observed in cases of identity leakage (USD 1.12 billion) and fraud under the guise of tech support (USD 962 million), despite fewer complaints. Therewith, extortion leads in the number of incidents recorded (47,054 cases), but the damage caused is much less – USD 96.1 million, which may suggest the "smaller" nature of such crimes. Romantic fraud – a form of Internet crime in which perpetrators establish a relationship of trust with victims via social networking or dating sites to lure them out of money – (USD 237.2 million with 3,811 complaints) and business email compromise (USD 63.9 million with 256 complaints) deserve special attention, as both have a high average amount of

damage per incident. Categories such as stalking, botnets, and offences against children are recorded rarely and are associated with minimal financial losses but have high social significance. Figure 1 shows the proportion of crypto transactions



related to illegal activity in the total volume of transactions.

Figure 1 – Percentage of total crypto volume associated with illicit activity
Source: compiled by the author based on Transaction Monitoring Labs (2025).

After a minimum value in 2021 (0.26%), there was an increase in 2022-2023, which may reflect increased cybercriminal activity and growth in crypto fraud schemes. In 2024, the rate dropped again to 0.42%, which may reflect both improved monitoring and compliance and a shift by criminals to more covert methods of laundering funds.

Exploring the dual nature of crypto-assets

While the risks associated with crypto-assets – including their misuse for illicit purposes – deserve critical attention, it is equally important to highlight the transformative potential of blockchain and distributed ledger technologies (DLT) in modern finance. Crypto assets offer enhanced transparency, decentralization, and efficiency in cross-border transactions, often at lower costs and with faster settlement times compared to traditional systems. Moreover, DLT facilitates innovative financial instruments such as smart contracts, decentralized finance (DeFi), and tokenized assets, which have the potential to increase financial inclusion and stimulate economic development. Recognizing these advantages is essential for developing balanced regulatory approaches that mitigate risks without stifling technological innovation.

Crypto-crime has become increasingly diverse and widespread, reflecting both the growth of the digital asset market and its vulnerabilities. One example is also the darknet platform Hydra, founded in 2015. Hydra quickly became the largest Russian-language illegal marketplace, serving over 17 million users and 19,000 sellers. It was used to sell drugs, forged documents, stolen data, and launder funds using Bitcoin (Tidy, 2022). The total turnover of the platform was

about USD 5 billion. Hydra was characterised by a high level of organisation, including a 'bookmarking' system, internal wallets, and even technical and legal support for its customers. In April 2022, Hydra was shut down as a result of an international law enforcement operation in Germany and the United States, during which servers were confiscated, and EUR 23 million worth of Bitcoins were seized. In December 2024, one of its operators, Dmitry Pavlov, was sentenced to life imprisonment for criminal association and money laundering.

Another example of large-scale crypto crime was Monopoly Market (Europol, 2023), a darknet marketplace that operated from 2019 to 2021. Unlike other marketplaces, it exclusively accepted the anonymous cryptocurrency Monero, making it virtually impossible to track transactions. The platform's turnover was estimated at EUR 1.23 billion. In 2023, SpecTor's international police operation arrested 288 sellers, seized USD 51 million in cryptocurrency and cash, 850 kg of drugs and 117 firearms. The platform's founder, Serbian Milomir Desnica, was detained, extradited to the United States, and pleaded guilty to money laundering and trafficking in illegal substances.

Another widespread scheme was the exploitation of crypto cash machines. In 2023, there were more than 5,500 complaints related to the use of such devices, and the cumulative losses from these frauds totalled more than USD 189 million (Internet Crime Complaint Center, 2023). Criminals often contacted victims disguised as tech support, tax, or police officers, convincing them to deposit bitcoin funds through the ATM. Due to the high anonymity of the transactions, the victims were deprived of their money without the possibility of a refund. These schemes were widespread in the U.S. and mainly involved extortion, fake tech support, and imitation of government agencies.

The phenomenon of romantic crypto frauds, known as Pig Butchering, also deserves special attention. In these schemes, criminals build emotional relationships with victims, most often through social media or messengers, and convince them to invest in fictitious crypto-investment platforms. Victims see the fake 'profits', continue investing, and then the site disappears and communication with the scammer is cut off. According to Chainalysis (2025), revenues from such schemes grew 85% in 2024 compared to 2020, reaching hundreds of millions of dollars. In the US alone, the damage from "romantic" crypto-scams totalled USD 237 million for 2024.

Some of the most significant forms of crypto crime have been pyramid schemes, extortion programmes, and criminal schemes using Virtual Private Network (VPN) services and models-as-a-service. One of the largest fraudulent projects in the history of crypto was PlusToken, a pyramid scheme that operated from mid-2018 and targeted mainly users from China and Southeast Asia. The organisers promised investors high returns from investing in their own token, with

funds coming in Bitcoin, Ethereum (ETH), and EOS crypto-assets. Cumulatively, over USD 2 billion was raised from around 3 million users. In 2019, the project suddenly ceased operations, and its leaders went into hiding. It was later found that over BTC 180,000, ETH 6.4 million, and USDT 111,000 (a token that is pegged to the value of the US dollar) were laundered through PlusToken (PlusToken scammers didn't…, 2019), leading to dramatic market fluctuations. In 2020, Chinese law enforcement arrested 109 people involved in the scheme, and eight key organisers were sentenced to terms of up to 11 years in prison.

One of the most persistent and evolving threats in the field of crypto-crime is the laundering of illicit funds through digital assets. As traditional financial systems adopt increasingly robust compliance frameworks, criminal networks are turning to crypto-assets to obscure the origins of their proceeds and to facilitate the movement of value across borders. The relative anonymity, high transaction speeds, and global accessibility of crypto platforms have made them an attractive channel for concealing funds obtained through fraud, ransomware attacks, darknet market activity, and other illicit means. Chainalysis (2025a) reports that roughly over 50% of illicit crypto-asset proceeds are channelled through centralized exchanges, either directly or after obfuscation via intermediary services. These platforms are favoured for laundering due to their liquidity and integration with traditional banking systems, which allow criminals to convert virtual assets into fiat currency.

Criminal actors frequently exploit intermediary "hops" – personal wallets or nested services – to obscure transaction history, accounting for more than 80% of total value during the layering phase of laundering schemes. Meanwhile, decentralized finance protocols and mixers are also used for laundering, though their traceability and forensic transparency generally make them less attractive to organized networks. DeFi platforms, cross-chain bridges, and mixers captured an increasing share of illicit flows – especially in 2023, bridge protocols received nearly USD 744 million from stolen-wallet addresses, and mixer tools continued to process significant volumes, including funds linked to state-sponsored thefts and darknet activities. Chainalysis (2025b) emphasizes that while mixers remain technically challenging for law enforcement, stablecoins now dominate illicit transaction volumes, representing as much as 63% of illicit activity in 2024, up from prior years. From 2019 to 2022, criminals moved an estimated USD 100 billion worth of illicit funds into conversion services – centralized exchanges, DeFi platforms, mixers, and bridges – with 2022 alone accounting for around USD 30 billion. Notably, by 2025, total illicit crypto flows potentially exceeded USD 51 billion, with stolen funds emerging as the most significant category of criminal proceeds – underscoring the evolution of money laundering methods in the crypto space.

Pump-and-dump schemes represent a form of market manipulation commonly associated with low-liquidity or obscure crypto assets, particularly those traded on decentralized or lightly regulated platforms. The term originates from traditional financial markets but has found renewed relevance in the context of crypto trading, where regulatory oversight is often limited, and new tokens appear with high frequency. In a typical pump-and-dump operation, perpetrators artificially inflate the price of a low-value cryptocurrency (the "pump") by disseminating misleading, exaggerated, or outright false information about the token's potential, often using coordinated social media campaigns, messaging platforms (such as Telegram or Discord), or even fake endorsements. Once a significant number of retail investors are lured into buying the token – thereby driving up demand and price – the orchestrators of the scheme sell off their previously acquired holdings at the peak price (the "dump"), realizing a substantial profit. This sudden liquidation usually causes the token's value to collapse sharply, leaving unsuspecting investors with significant financial losses. The process typically occurs over a very short period – sometimes hours or even minutes – which makes post-factum intervention by regulators or platforms nearly impossible.

In late 2017 and early 2018, cybersecurity entrepreneur John McAfee and his associate Jimmy Watson orchestrated a classic pump-and-dump campaign. They secretly accumulated various lesser-known altcoins – such as Verge (XVG), and Reddcoin (RDD) – then publicly promoted them via McAfee's Twitter account, misleading investors about their value. After inflating prices, they sold their holdings, netting over USD 2 million in illicit profits. This led to charges from the Commodity Futures Trading Commission (2021) for manipulative conduct. SafeMoon (Joshi, 2025), a highly speculative token launched in 2021, saw a meteoric rise in price after going viral on platforms like TikTok, YouTube, and Reddit. Influencers and aggressive online promotion led to massive public investment, resulting in a significant price pump. However, investigations later revealed that insiders, including developers, may have sold large amounts of their holdings during the peak. This contributed to a dramatic price collapse, leading to multimillion-dollar investor losses.

The wave of ransomware attacks has been no less destructive. Among the most famous are WannaCry, Ryuk, DarkSide, LockBit, Conti, and others. These malware programmes encrypt data on victims' computers while demanding a ransom in crypto, most commonly Bitcoin or Monero. In 2023 alone, according to Chainalysis, notorious ransomware groups received over USD 1.1 billion in crypto, a record amount for ransomware. Victims ranged from individuals to large organisations such as hospitals, municipalities, schools, and businesses. A well-known case is the attack on Colonial Pipeline in the United States in May 2021,

which caused fuel supply disruptions on the East Coast. The company paid a USD 4.4 million ransom to the hackers, part of which was later recovered by law enforcement after tracking the transactions (2021 colonial pipeline…, 2022).

The spread of ransomware is also fuelled by the Ransomware-as-a-Service (RaaS) model, where malware developers rent malware to other criminals through darknet channels, including encrypted messaging platforms such as Telegram, which facilitate anonymous communication and distribution. Thus, even those without technical skills can launch a cyberattack. For the "favour", the developers receive a percentage of the ransom. This has democratised access to digital ransomware and enabled a dramatic increase in attacks. The average ransom in 2023 was USD 365,000 and the number of attacks increased by 47% compared to 2022 (Waldman, 2023).

The involvement of VPN services in crypto-crime schemes is also of interest. For example, a 2024 report by Zscaler ThreatLabz reports that 56% of organisations have experienced one or more cyberattacks related to VPN vulnerabilities, highlighting the increasing frequency and sophistication of attacks targeting VPN services (Seaton, 2024). VPNs allow attackers to anonymise their activity when accessing the darknet, conducting transactions, and managing malicious botnets. While VPN services themselves are not illegal, their widespread use in cybercrime raises the question of the need to regulate and monitor anonymous network solutions.

Swiss and German authorities, supported by Europol and Eurojust, shut down the cryptocurrency mixing service Cryptomixer.io in late November 2025. This operation targeted a platform launched in 2016 that allegedly laundered over €1.3-1.51 billion in bitcoin linked to ransomware, darknet markets, drug trafficking, and other cybercrimes. Authorities seized three servers in Switzerland, the cryptomixer.io domain, over 12 terabytes of data, and more than €25 million ($29 million) in bitcoin during the action from November 24-28. The takedown disrupts a key tool for obscuring illicit crypto transactions through pooling and redistributing funds, following similar actions like the 2023 ChipMixer shutdown (Reuters, 2025).

Geography and evolution of illicit crypto transactions

The geography of crypto addresses receiving funds associated with illicit activity has undergone significant changes. According to a Chainalysis (2025a; 2025b), as of 2024, approximately 39% of all illegal crypto transactions were linked to jurisdictions under US sanctions, including Iran and Venezuela. In Iran, centralised crypto exchanges play a key role in circumventing international financial sanctions imposed on the country. These platforms enable companies and individuals to transfer significant amounts of digital assets across national

borders, avoiding traditional banking systems that are strictly monitored by sanctions authorities. This practice is driven by serious international pressure to curb Iran's economic activities, as well as a desire to keep the internal economy resilient in the face of currency instability and inflation. The use of centralised exchanges allows accelerating the movement of capital, simplifying currency exchange, and minimising the risks of blocking transactions, which helps to maintain liquidity and the functioning of legal and shadow economic sectors within the country (Bayena, 2025). In Venezuela, especially among users of P2P platforms, the use of crypto to circumvent currency controls, to store savings in hyperinflation and to launder illegal proceeds is widespread. Among Latin American countries, Venezuela leads in the volume of P2P transactions, indicating the widespread use of digital assets for capital preservation (Erazo, 2020).

Terrorist financing using crypto-assets continues to be a serious threat despite the relatively small volume of such transactions. An example is the Israeli operation in 2023 that froze more than 190 crypto wallets linked to the Hamas group; one of them received over USD 7.7 million in bitcoin (Reuters, 2023). Terrorist organisations are actively using anonymous crypto-assets, mixers, and platforms in poorly regulated jurisdictions to conceal the sources of funds. In response, international regulators have increased measures to combat such schemes, including sanctions, publication of blacklists of addresses and stricter KYC/AML requirements for crypto platforms.

Moldova has also recorded several high-profile cases of crypto fraud, reflecting the growing activity of criminal groups in this area. One of the most significant episodes occurred in February 2025, when law enforcement authorities uncovered a large-scale scheme of fictitious crypto-asset investments. Fraudsters, operating through call centres in Chisinau, attracted victims with online advertisements promising quick and guaranteed income. After filling in forms with personal data, the victims received calls from "financial advisers" convincing them to invest (Fraudulent cryptocurrency investment…, 2025). One notable incident was a joint operation by Romanian and Moldovan law enforcement agencies in March 2023 aimed at dismantling a crypto fraud scheme. The criminal group, active since 2020, used fake social media accounts and fake recommendations from Romanian influencers to convince victims to invest in non-existent crypto platforms, promising guaranteed returns of up to 100%. As a result, at least 32 people lost around EUR 320,000. The proceeds were transferred to accounts in Moldova and laundered through an organised criminal group. During the operation, 21 people were identified and charged and assets were frozen to compensate for the losses (European Union Agency for Criminal Justice Cooperation, 2023).

The role of digital literacy in the spread of criminal practices, especially those related to the use of crypto-assets, is becoming increasingly relevant in the context of the rapid development of digital technologies and increased access to online financial services (Tinmaz et al., 2022). It acts as a two-way factor: on the one hand, as an amplifier of criminal opportunities, and on the other hand, as a shield that can protect users from cyber threats. Digital literacy has emerged as a multifaceted concept requiring comprehensive assessment frameworks, with systematic reviews revealing a growing prevalence of digital literacy research that examines various dimensions of technological competence. United Nations Educational, Scientific and Cultural Organization (UNESCO) (Antoninis, 2019) global framework identifies seven core competence areas for digital literacy: fundamentals of hardware and software, information and data literacy, communication and collaboration, digital content creation, safety, problem solving, and career-related competences, providing a structured approach to understanding and measuring these skills. Recent research has focused on developing psychometrically sound measurement instruments, such as the Digital Literacy Scale (DLS) validated using the Rasch model for secondary school students, while other studies have demonstrated that digital literacy measures can achieve high reliability and construct validity across different demographic groups (Avinç & Doğan, 2024). The measurement of digital literacy typically employs both self-assessment scales and performance-based assessments, with comprehensive models incorporating digital literacy frameworks, measuring tools, and intervention programs to address the digital skills gap. However, systematic reviews highlight the need for age-appropriate instruments, particularly for older populations, as few existing measurements have been validated for diverse demographic groups, indicating ongoing challenges in creating universally applicable digital literacy assessments (Oh et al., 2023).

From the perspective of criminals, high levels of digital competence enable the development of sophisticated fraud and evasion schemes (Temirzhanova et al., 2018). Today's attackers confidently use anonymous crypto wallets, transaction mixing systems, VPNs Telegram and Tor networks, infiltrate darknet forums, and apply sophisticated social engineering techniques. They can spoof the interfaces of popular crypto services, use malicious scripts, and manipulate users to create plausible phishing attacks (Baltezarević, 2022). This technically weaponised approach makes criminals increasingly challenging for law enforcement agencies to reach, especially in the context of cross-border and poor international coordination of investigations.

On the other hand, the massive vulnerability of users is often precisely due to a lack of knowledge about digital security and the specific features of crypto-asset infrastructure functioning. Ordinary users do not always understand how to

distinguish genuine resources from fraudulent ones, how the blockchain system is organised, and what risks accompany each transaction (Sorban, 2020). This opens opportunities for targeted deception, ranging from conventional "tech support letter" schemes to more sophisticated forms, including crypto-based investment pyramid schemes or "pig butchering" – long-term manipulative schemes that use trust and psychological pressure.

Organisations, including small and medium-sized businesses, are also vulnerable: lack of trained staff, poorly protected corporate systems, and careless handling of digital assets lead to data compromise and losses in case of ransomware or phishing attacks (Yesimov & Borovikova, 2022). Often such attacks result in business disruption, leakage of confidential information, and financial losses. Notably, digital literacy performs not only the role of individual protection but also contributes to the formation of collective security. A society with a strong level of digital culture is less susceptible to mass deception schemes, recognises potential threats more quickly, and can take an active part in the creation of digital countermeasures, including through civic initiatives and educational programmes (Iskakova et al., 2016).

Thus, improving digital literacy is merely a matter of individual survival in the digital environment, but also an element of strategic defence at the state level. Investments in systemic cybersecurity education and digital hygiene, regular awareness campaigns, and the inclusion of crypto-asset security topics in educational courses can markedly reduce the number of potential victims and increase society's resilience to cyber threats. Without this, any technological or legal measures will stay insufficiently effective.

Public awareness campaigns and accessible educational initiatives should be developed to improve users' ability to assess the credibility of platforms and protect their assets in the digital environment. However, a more holistic approach must also address the role of professionals within the ecosystem. Regular specialized training should be mandatory for Virtual Asset Service Providers (VASPs) to ensure they are equipped to identify and prevent the misuse of their platforms. These training programs should include topics such as compliance with AML/CFT regulations, detection of suspicious transaction patterns, and collaboration with authorities.

In parallel, law enforcement agencies and the judiciary require continuous capacity building. Without a clear understanding of the structure and operation of crypto-related crimes, legal proceedings may be delayed, misdirected, or ineffective. Therefore, specialized professional training is necessary to improve the investigation, prosecution, and adjudication of offenses involving crypto assets. Cross-border cooperation and knowledge exchange between jurisdictions should also be encouraged to address the global nature of such crimes effectively.

Ultimately, only through coordinated efforts – combining user education, industry accountability, and institutional readiness – can the risks associated with crypto assets be minimized while preserving their innovative potential.

Legal regulation of the crypto-asset sphere plays a key role in shaping the security and stability of digital financial markets, which directly affects the dynamics of crypto-related crime and damage. There is a trend towards stricter legislative measures and active implementation of regulations aimed at preventing fraud, money laundering and terrorist financing through digital assets. These changes are naturally reflected in the transformation of indicators of the number of offences and the scale of financial losses (Goyal & Yadav, 2024). For example, the European Union adopted the Regulation (EU) 2023/1114 of the European Parliament and of the Council "On Markets in Crypto-Assets" (2023). It provides for a mandatory licence for crypto exchanges, full-fledged requirements for customer identification, investor protection and combating money laundering and terrorist financing. In early 2025, the first exchangers – Gemini, OKX and Crypto.com – received licences in the EU (in Malta and Luxembourg), which confirms the transition to effective supervision (Howcroft & O'Donnell, 2025). In Moldova, as of 1 July 2023, Law of the Republic of Moldova No. 66 (2023) was adopted, prohibiting individuals and legal entities from conducting transactions with cryptocurrencies (payments, transfers, etc.), leaving only the possibility of ownership for investment; at the same time, income from crypto-investments is taxed at the rate of 12%.

The introduction of mandatory KYC and AML procedures, including Travel Rule on crypto exchanges and platforms makes it much more complicated for attackers to commit criminal acts anonymously. For example, heavily regulated countries (US, UK, and South Korea) have seen a decrease in major hacks and fraudulent schemes as transparency and control over the flow of funds has improved. Following increased legal measures, many platforms have become more security responsible, which entails a reduction in vulnerabilities and overall damage (Sater, 2020). According to Chainalysis (2025a), the number of hacks on major exchanges has decreased from 35 incidents in 2021 to 12 in 2024, and the overall damage has decreased by about 40%. Analogously, in the EU, after the MiCA regulation came into force in 2024, the proportion of anonymous transactions fell by 30%, which increased the transparency of transactions and strengthened control over the flow of funds.

The development of international cooperation between law enforcement agencies of different states contributes to the effective detection and dismantling of criminal networks involved in crypto-crime. Joint operations, information exchange, and coordination of actions allow blocking large money laundering channels and apprehending key players, which also affects the positive dynamics

of reducing criminal manifestations. However, overly rigid or uncertain regulation can stunt innovation and reduce investor confidence, with its own risks and side effects. As a result, the optimal regulatory policy should balance between protecting users and supporting technological development.

DISCUSSION

The dynamics of the spread of crypto-related offences demonstrate the gradual but steady transformation of crypto crime into a systemic phenomenon. At first, such crimes were sporadic, but with the development of the technological base and the growing popularity of digital assets, a qualitative shift took place: crimes became more structured and criminal networks became professionalised. New opportunities for anonymity, transaction speed, and decentralisation have made this new financial instrument an attractive tool for both small-scale fraudsters and transnational groups. This trend requires a constant review of government and business response strategies. Kethineni and Cao (2019) conducted a study focusing on the stages of development of crypto-assets and their involvement in criminal activities. The researchers described how the emergence of darknet marketplaces influenced the formation of large-scale criminal schemes and emphasised the role of platforms for anonymous trade in illegal goods and services. The current study agrees with the Kethineni and Cao conclusions regarding the significance of analysing these activities. Additionally, new trends in patterns of criminal activity were identified, including the emergence of social engineering attacks and more sophisticated forms of blockchain technology exploitation.

An examination of the geographical distribution of crypto-crime demonstrated that the problem is not strictly territorial. This is because cryptocurrencies were originally designed as global mediums of exchange, independent of national borders (Lavrukhina et al., 2025; Matkarimov et al., 2024). Therefore, digital criminals move freely between jurisdictions, exploiting differences in legislation, cybersecurity levels, and access to VPNs and other anonymisers. The geographical mosaic of incidents complicates investigations and highlights the need for closer international cooperation between law enforcement agencies, as well as the harmonisation of legal norms. Giommoni et al. (2023) also paid attention to the geographical distribution and legal aspects of combating crypto-crime. The researchers analysed how differences in national laws and international incompatibility hinder the effective countering of criminals. Opitek et al. (2023) emphasised the poor coordination between countries and insufficient information sharing. These findings largely coincide with the current results on the geography of crime and significance of international cooperation. In contrast to the Opitek et al. study, the present study

added a social dimension – the impact of digital literacy of the population, which helps to understand the reasons for the vulnerability of certain groups of users, thus broadening the scope of understanding of the problem.

The analysis of the types of criminal activity in the crypto-asset environment revealed a high degree of diversity in methods, ranging from classic schemes to defraud users to complex forms of malicious influences, including exploits and the use of ransomware. Some of these offences are technically sophisticated, making them difficult to prevent at the planning stage. In addition, the criminal arsenal is constantly evolving, with new schemes and tools emerging, such as bait-and-switch platforms, blockchain-to-blockchain migrations, and phishing platforms, which help criminals effectively mask transaction traces by exchanging one crypto asset for another to create "layers" that distance actual funds from criminal ones (Barlybayev & Turginbayeva, 2025; Mukhamediyarova et al., 2025). This points to the need for constant monitoring and rapid adaptation of defence mechanisms. Agarwal et al. (2023) focused on the technical characteristics of modern crypto-assets, especially focusing on ransomware and its exposure mechanisms. The researchers described vulnerability exploitation modules and malware propagation schemes. Fylaktou and Savvides (2025) also confirmed the significance of ransomware as one of the principal tools of crypto-criminals, which is in line with current observations. However, unlike their technical analysis, the current study covers a wider range of offences, including social engineering attacks and fraud, which gives a more holistic view of the state of crypto-crime.

Analysing the temporal dynamics of crypto-crime not only allows tracing the evolution of threats but also capturing periods of highest activity. Such spikes are often associated with technological innovations or global events that affect user behaviour. A retrospective helps us understand what events served as catalysts for criminal activity and highlight key moments that influenced increased controls or the introduction of new countermeasure tools. Thus, studying the history of crypto-crime becomes a valuable resource for predicting future risks. Christensen (2025) conducted a study aimed at identifying time trends of crypto-criminal activity depending on technological changes and criminals' adaptation to new conditions. The researcher identified cycles of attack spikes associated with the introduction of new blockchain technologies and changes in user behaviour. These findings are broadly consistent with the current retrospective analysis, but Christensen did not focus on the socio-economic and cultural factors that influence the spread of crime, which is a major part of the current study.

Digital illiteracy and poor cyber hygiene are a major contributing factor to the success of crypto-criminals (Iskakova & Mukhamedjanov, 2022). Users with

a low level of technical proficiency become easy targets for social engineering attacks, especially with the complex or confusing terminology of crypto services. Their lack of understanding of how wallets function, encryption technics, or transaction validation makes them vulnerable even when using basic defence mechanisms. This points to the need for large-scale educational campaigns covering not only young people, but also elderly users, who are often out of the information field. Li et al. (2024) investigated the relationship between the level of digital literacy of the population and the risks associated with crypto jacking. The researchers' findings showed that a low level of digital competence directly correlates with increased vulnerability to fraudulent schemes and social engineering attacks. İli (2025) pointed out the need for large-scale educational campaigns, reaching not only young people, but also elderly users, who are often out of the information field. This aspect fully coincides with the current findings and emphasises the need for educational programmes to improve user security.

The legal response to crypto-crime lags significantly behind technological changes. Despite individual successful cases, the overall regulation of crypto-assets is still fragmented and ambiguous. Legislative gaps allow criminals to exploit legal loopholes, while the lack of unified international practices makes it challenging to stop crimes. The emergence of digital assets requires the development of flexible and adaptive regulatory mechanisms that can not only respond to current challenges but also work proactively (Blikhar et al., 2023). Recognizing these risks, the Financial Action Task Force (FATF) introduced international standards for virtual assets (Vas) and Virtual Asset Service Providers (VASPs), including the Travel Rule, aiming to establish a more unified compliance approach. Similarly, the EU's Fifth Anti-Money Laundering Directive (AMLD5) marked an important step by extending AML requirements to virtual currency exchange platforms and custodian wallet providers. Courtois et al. (2021) also focused on analysing the legal regulation of crypto-assets and enforcement problems in the international context. The researchers noted many gaps and imperfections in the legislation of different countries, as well as the complexity of law enforcement coordination. These findings coincide with the current understanding of the value of strengthening international mechanisms to combat crypto-asset crime. However, unlike Courtois et al. study, the aspect of digital literacy and the role of the information space was added to the analysis, which allows considering the problem not only from a legal but also from a socio-cultural standpoint.

Media and social networks play a dual role in the context of digital assets (Laktionova et al., 2024). On the one hand, they serve as a platform for educational and preventive materials, while on the other hand, they become a channel for disseminating fake information, investment frauds, and advertising

campaigns masking fraudulent projects. The popularisation of crypto through influencers without proper regulation contributes to the formation of inflated expectations and trust among unprepared users, which makes them vulnerable to manipulation (Gulaliyev et al., 2023). This emphasises the need for information responsibility and the implementation of digital ethics standards at a mass level. Anser et al. (2020) also studied the influence of media and social networks in shaping public perception of crypto-assets and related crimes. The researcher revealed that the media often creates either an overly panicked or romanticised image of crypto criminals, which distorts the perception of the problem. The current findings confirm the significance of this aspect and emphasise the need to promote digital ethics and responsible reporting.

Overall, crypto-crime is a multifaceted phenomenon that combines technological, social, legal, and educational aspects. Comparison with the results of previous studies confirmed the value of a comprehensive approach to analysing the problem, including both technical methods of combating it, as well as digital literacy and international cooperation. Such a multifaceted understanding enables a more effective development of strategies to prevent and counter crypto related illegal manifestations.

CONCLUSION

The results of the study confirmed that crypto-crime has become a significant and rapidly growing phenomenon in the modern digital society due to the unique technological characteristics of crypto assets and related blockchain systems. The key feature of crypto-crime is the use of digital assets that provide a high level of anonymity and decentralisation of transactions, making it challenging for government and financial authorities to control. The study highlights a correlation between users' low digital competence and their increased vulnerability to fraudulent activities, such as phishing, fake investment platforms, and romance fraud. This issue is further exacerbated by the limited expertise of law enforcement agencies in detecting and addressing crypto-related crimes. Between 2015 and 2024, the number of registered complaints about crypto-related offences rose from less than 2,000 to almost 150,000, and the total amount of damage increased from USD 2 million to more than USD 9.3 billion. The increase is particularly steep after 2020, indicating the massive proliferation of blockchain-technology and the increasing vulnerability of users and law enforcement.

An analysis of crime types shows that the largest financial losses are associated with investment fraud – 41,557 complaints with damages of around USD 5.82 billion, significantly greater than damages in other categories. Meanwhile, identity leakage and fraud under the guise of tech support caused USD 1.12 billion and USD 962 million in damages, respectively, despite fewer

complaints. Extortion offences are the most numerous, with 47,054 cases, but the total damages in this category are much lower (USD 96.1 million), indicating the more "small-scale" nature of such crimes. By mid-2025, approximately 80% of illicit crypto assets had been laundered through centralized exchanges, while the use of DeFi protocols, mixers, and NFT marketplaces for obfuscation also increased significantly. This underscores the urgent need for enhanced regulatory oversight across both traditional and emerging crypto platforms to combat the evolving laundering techniques.

Examples of large cases, such as Silk Road and CryptoLocker, as well as Hydra and Monopoly Market platforms, demonstrate the evolution of crypto-crime from individual fraudulent schemes to complex international structures with a turnover in the billions of dollars. Importantly, these cases have become legal and criminological precedents, exposing the challenges of regulating and coordinating international efforts to combat crypto-crime. At the same time, the continuous improvement of technologies such as Ransomware-as-a-Service and the active use of VPN and other anonymising services complicate law enforcement activities and require new integrated approaches.

Another valuable finding is the role of digital literacy: a high level of knowledge among criminals contributes to the sophistication of schemes, while a lack of digital awareness among the general public increases vulnerability, making users easy targets for fraudsters. Therefore, a holistic approach, which includes not only improving digital literacy and hygiene for consumers, but also providing in-depth professional training for businesses involved with virtual assets and government actors responsible for protecting customers from abuse, becomes a key strategy for reducing crypto-crime.

Finally, the study emphasised the need for balanced and internationally harmonised regulation of the crypto-asset sphere. The introduction of KYC and AML procedures, including Travel Rule, makes anonymous criminal transactions much more difficult and contributes to the reduction of major attacks and frauds, as evidenced by the reduction of vulnerabilities and damage in countries with strict controls. To foster technological innovation and market entry, it is crucial to initially allow the technology to be available, gather practical insights on its use or misuse, and then adopt the most effective and appropriate regulations that protect users while supporting development.

A limitation of the study is its focus on the main known cases and data, which may not cover all new and hidden forms of crypto-crime. Another limitation is related to the dark figure of crypto-crime, encompassing crimes that were not reported for various reasons. In-depth analyses of rapidly changing technological and legal aspects, as well as the development of more accurate

methods to detect and classify crypto-assets, are recommended for further research.

REFERENCES

2021 colonial pipeline ransomware attack. (2022). https://www.hsdl.org/c/timeline/2021-colonial-pipeline-ransomware-attack/

Agarwal, U., Rishiwal, V., Tanwar, S., & Yadav, M. (2023). Blockchain and crypto forensics: Investigating crypto frauds. *International Journal of Network Management*, *34*(2), e2255. https://doi.org/10.1002/nem.2255

Anser, M.K., Zaigham, G.H.K., Imran Rasheed, M., Pitafi, A.H., Iqbal, J., & Luqman, A. (2020). Social media usage and individuals' intentions toward adopting Bitcoin: The role of the theory of planned behavior and perceived risk. International journal of communication systems, *33*(17), e4590. https://doi.org/10.1002/dac.4590

Anti-money laundering (AML). (2025). https://www.swift.com/risk-and-compliance/anti-money-laundering

Anti-money laundering directives. (2025). https://www.lseg.com/en/risk-intelligence/financial-crime-risk-management/eu-anti-money-laundering-directive

Antoninis, M. (2019). Digital literacy skills: From a framework to a measure. https://uis.unesco.org/en/blog/digital-literacy-skills-framework-measure

Avinç, E., & Doğan, F. (2024). Digital literacy scale: Validity and reliability study with the rasch model. *Education and Information Technologies*, *29*(17), 22895-22941. https://doi.org/10.1007/s10639-024-12662-7

Baltezarević, R. (2022). Digital literacy as a means of preventing cybercrime. *Bastina*, *57*, 131-139. https://doi.org/10.5937/bastina32-38103

Barlybayev, A., & Turginbayeva, A. (2025). Development and Implementation of an Advanced Fuzzy Expert System for the Assessment of Information Security Risks. *Journal of Computational and Cognitive Engineering, 4*(4), 570–580. https://doi.org/10.47852/bonviewJCCE52024683

Bayena, M. (2025). $15.8B in crypto linked to sanctioned entities in 2024. https://grafa.com/news/cryptocurrencies--15-8b-in-crypto-linked-to-sanctioned-entities-in-2024-378472

Blikhar, M., Vinichuk, M., Kashchuk, M., Gapchich, V., & Babii, S. (2023). Economic and legal aspects of ensuring the effectiveness of counteracting corruption in the system of anti-corruption measures of state authorities. *Financial and Credit Activity: Problems of Theory and*

Practice, *4*(51), 398–407. https://doi.org/10.55643/fcaptp.4.51.2023.4138

Carletti, R., Luo, X., & Adelopo, I. (2024). Understanding criminogenic features: Case studies of cryptocurrencies-based financial crimes. *Journal of Financial Crime*, *32*(3), 681-705. https://doi.org/10.1108/jfc-06-2024-0176

Chainalysis. (2025a). 2025 Crypto crime mid-year update: Stolen funds surge as DPRK sets new records. https://www.chainalysis.com/blog/2025-crypto-crime-mid-year-update/

Chainalysis. (2025b). The Chainalysis 2025 Crypto Crime Report. https://go.chainalysis.com/2025-Crypto-Crime-Report.html

Christensen, L.D. (2025). Preventing fraud in crypto payments. *Journal of Economic Criminology*, *7*, 100124. https://doi.org/10.1016/j.jeconc.2024.100124

Cohen, L.E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, *44*(4), 588-608.

Collins, J. (2022). *Crypto, crime and control: Cryptocurrencies as an enabler of organized crime*. Geneva: Global Initiative Against Transnational Organized Crime.

Commodity Futures Trading Commission. (2021). CFTC charges two individuals with multi-million dollar digital asset pump-and-dump scheme. https://www.cftc.gov/PressRoom/PressReleases/8366-21

Cong, W., Harvey, C., Rabetti, D., & Wu, Z. (2025). An anatomy of crypto-enabled cybercrimes. *Management Science*, *71*(4), 3622-3633. https://doi.org/10.1287/mnsc.2023.03691

Costea, A.-M., Putină, N., & Brie, M. (2024). Cybersecurity in the Republic of Moldova in the context of European integration. *Romanian Journal of European Affairs*, *24*(2), 97-113.

Courtois, N.T., Gradon, K.T., & Schmeh, K. (2021). Crypto currency regulation and law enforcement perspectives. *arXiv preprint arXiv:2109.01047.* http://dx.doi.org/10.48550/arXiv.2109.01047

Cunjak, I.M. (2022). Crypto-assets illicit activities: Theoretical approach with empirical review. *International e-Journal of Criminal Sciences*, *5*(17), 1-29.

Erazo, F. (2020). Venezuelans are running out of crypto P2P trading options. https://cointelegraph.com/news/venezuelans-are-running-out-of-crypto-p2p-trading-options.

European Union Agency for Criminal Justice Cooperation. (2023). Support to operation against cryptocurrency fraud in Romania and the Republic of

Moldova. https://www.eurojust.europa.eu/news/support-operation-against-cryptocurrency-fraud-romania-and-republic-moldova

Europol. (2023). 288 dark web vendors arrested in major marketplace seizure. https://www.europol.europa.eu/media-press/newsroom/news/288-dark-web-vendors-arrested-in-major-marketplace-seizure

Fathi, M., bin Saud Al-Shammar, M., & Khalifa Mohamed, G.S. (2025). Cryptocurrency and criminal liability: investigating legal challenges in addressing financial crimes in decentralized systems. *Journal of Money Laundering Control*, *28*(3), 504-517. https://doi.org/10.1108/JMLC-07-2024-0110

Financial Action Task Force. (2021). Updated guidance for a risk-based approach to virtual assets and virtual asset service providers. www.fatf-gafi.org/publications/fatfrecommendations/documents/Updated-Guidance-RBA-VA-VASP.html

Florea, E., & Pustelnik, E.S. (2021). On regulation of cryptocurrency: international experience. Supremacy of Law, *1*, 69-83. https://doi.org/10.52388/2345-1971.2021.1.06

Fraudulent cryptocurrency investment scheme thwarted in Chisinau. (2025). https://ordinesilege.md/ru/2025/02/18/v-kishineve-presechena-moshennicheskaya-shema-s-investicziyami-v-kriptovalyutu/

Furneaux, N. (2018). *Investigating cryptocurrencies: Understanding, extracting, and analyzing blockchain evidence*. Hoboken: John Wiley & Sons.

Fylaktou, G., & Savvides, C. (2025). Fraud, crime prevention and financial crime investigation in blockchain. In M. Themistocleous (Ed.), *Handbook of Blockchain Technology* (pp. 311-328). Cheltenham: Edward Elgar Publishing. https://doi.org/10.4337/9781803922805.00032

Giommoni, L., Décary-Hétu, D., Berlusconi, G., & Bergeron, A. (2023). Online and offline determinants of drug trafficking across countries via cryptomarkets. *Crime Law and Social Change*, *81*(1), 1-25. https://doi.org/10.1007/s10611-023-10106-w

Gottschalk, P. (2018). Convenience triangle in white-collar crime: Case studies of relationships between motive, opportunity, and willingness. *International Journal of Law, Crime and Justice*, *55*, 80-87. https://doi.org/10.1016/j.ijlcj.2018.10.001

Gottschalk, P. (2019). Convenience triangle in white-collar crime: An empirical study of prison sentences. *Deviant Behavior*, *42*(7), 886-902. https://doi.org/10.1080/01639625.2019.1705679

Goyal, A., & Yadav, A. (2024). Regulatory approaches to cryptocurrency: Balancing investor protection, market stability, and innovation. In *Proceedings of the 2nd International Conference on Emerging*

Technologies and Sustainable Business Practices-2024 (ICETSBP 2024) (pp. 635-648). Dordrecht: Atlantis Press. https://doi.org/10.2991/978-94-6463-544-7_42

Gulaliyev, M., Abasova, S., Guliyeva, S., Samedova, E., & Orucova, M. (2023). The Main Problems of Building the Digital Economy of Azerbaijan. *WSEAS Transactions on Business and Economics, 20*, 1383–1395. https://doi.org/10.37394/23207.2023.20.123

How much did CryptoLocker make? (2023). https://darwinsdata.com/how-much-did-cryptolocker-make/.

Howcroft, E., & O'Donnell, J. (2025). Exclusive: Crypto giants set for EU green light amid growing regulatory rift, sources say. https://www.reuters.com/sustainability/boards-policy-regulation/crypto-giants-set-eu-green-light-amid-growing-regulatory-rift-sources-say-2025-06-13/

İli, B. (2025). Analysis of complaints regarding cryptocurrency investment fraud: An evaluation from the perspective of new media literacy. *Iğdır University Journal of Social Sciences*, *38*, 214-229. https://doi.org/10.54600/igdirsosbilder.1580718

Internet Crime Complaint Center. (2023). Cryptocurrency Fraud Report. https://www.ic3.gov/annualreport/reports/2023_ic3cryptocurrencyreport.pdf

Internet Crime Complaint Center. (2024). Internet Crime Report 2024. https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf

Iordachi, V. (2023). Strategic directions for the development of the capital market in the era of globalization: A legislative-normative analysis in the context of the Republic of Moldova. *Journal of Research on Trade, Management and Economic Development*, *20*(2), 67-80.

Iskakova, Z., & Mukhamedjanov, A. (2022). SCO transport and logistic assistance to the states of the Central Asia region. In *The Shanghai Cooperation Organization: Exploring New Horizons* (pp. 180–196). Taylor and Francis. https://doi.org/10.4324/9781003170617-16

Iskakova, Z.T., Bimbetov, A.B., & Sarsenova, S.N. (2016). Institution building of the eurasian economic union: Challenges and opportunities. *Journal of Advanced Research in Law and Economics, 7*(4), 817–827. https://doi.org/10.14505/jarle.v7.4(18).13

Joshi, A. (2025). Is SafeMoon dead? A deep dive into the rise, fall, and the final chapter of a cryptocurrency dream. https://zenledger.io/blog/is-safemoon-dead/

Kelion, L. (2013). Cryptolocker ransomware has "infected about 250,000 PCs". https://www.bbc.com/news/technology-25506020

Kethineni, S., & Cao, Y. (2019). The rise in popularity of cryptocurrency and associated criminal activity. *International Criminal Justice Review*, 30(3), 325-344. https://doi.org/10.1177/1057567719827051

Know Your Customer (KYC). (2025). https://www.swift.com/risk-and-compliance/know-your-customer-kyc

Krishnan, L.P., Vakilinia, I., Reddivari, S., & Ahuja, S. (2023). Scams and solutions in cryptocurrencies – A survey analyzing existing machine learning models. *Information*, *14*(3), 171. https://doi.org/10.3390/info14030171

Kumisbekova, Z.T., Moroz, S.P., Abilova, M.N., Seitova, A.N., & Ten, V.V. (2019). Agreement on share participation in housing construction: Historical aspect and legal nature. *Journal of Legal Ethical and Regulatory Issues, 22*(1).

Laktionova, O., Ismailov, T., Kalinin, O., Gonchar, V., & Onofriichuk, O. (2024). Digitalization and management of crypto assets as a source of investment for green projects. *E3S Web of Conferences, 558*, 01028. https://doi.org/10.1051/e3sconf/202455801028

Lavrukhina, K., Tytok, V., Biloshchytskyi, A., Tormosov, R., Kalinin, O., & Mostovenko, O. (2025). Research on the prospects and risks of digital economic transformation: Positive impact, key threats, and the role of clusters in the transformation of Ukraine's national economy. In *SIST 2025 - 2025 IEEE 5th International Conference on Smart Information Systems and Technologies, Conference Proceedings*. Astana: Institute of Electrical and Electronics Engineers. https://doi.org/10.1109/SIST61657.2025.11139283

Law of the Republic of Moldova No. 66. (2023). https://www.legis.md/cautare/getResults?doc_id=136851&lang=ru.

Li, P., Li, Q., & Du, S. (2024). Does digital literacy help residents avoid becoming victims of frauds? Empirical evidence based on a survey of residents in six provinces of east China. *International Review of Economics & Finance*, *91*, 364-377. https://doi.org/10.1016/j.iref.2024.01.056

Maimon, D., Louderback, & E.R. (2018). Cyber-dependent crimes: An interdisciplinary review. *Annual Review of Criminology*, *2*(1), 191-216. https://doi.org/10.1146/annurev-criminol-032317-092057

Matkarimov, B., Barlybayev, A., & Karimov, D. (2024). Enhancing Analytical Precision in Company Earnings Reports through Neurofuzzy System Development: A Comprehensive Investigation. *Journal of Electrical and Computer Engineering, 2024*, 8515203. https://doi.org/10.1155/2024/8515203

McCord, A., Birch, P., & Davison, A. (2022). Technology enabled crime: Examining the role of cryptocurrency. *DOAJ: Directory of Open Access Journals*, *4*(4), 428-451. https://doi.org/10.18716/ojs/krimoj/2022.4.4

Mukhamediyarova, O., Moroz, S., & Akimbekova, S. (2025). Current issues of agricultural land transfer in the Republic of Kazakhstan. *Acta Scientiarum Polonorum Administratio Locorum, 24*(1), 115–127. https://doi.org/10.31648/aspal.9812

Nursaliyeva, G., Baikenzhina, K., Kalmaganbetova, D., Balgimbekova, G., Seitzhanova, N., & Kussainova, L. (2023). Methodology for the legislative application of evaluative categories in criminal law. *Journal of Law and Sustainable Development, 11*(5), e0725. https://doi.org/10.55908/sdgs.v11i5.725

Nuridin, S., Ongarbayev, Y., Muratkhanova, M., Kalmaganbetova, D., & Yessentemirova, A. (2025). Analysis of the institution of parole in the context of criminal law theory and practice. *Rivista Di Studi Sulla Sostenibilita, 1*, 105–123. https://doi.org/10.3280/riss2025oa19392

Ogele, E.P. (2024). Terrorist financing in the digital age: An analysis of crypto currencies and online crowd funding. *Journal of Terrorism Studies*, *6*(2), 4. https://doi.org/10.7454/jts.v6i2.1080

Oh, S.S., Kim, K., Kim, M., Oh, J., Chu, S.H., & Choi, J. (2021). Measurement of digital literacy among older adults: Systematic review. *Journal of Medical Internet Research*, *23*(2), e26145. https://doi.org/10.2196/26145

Opitek, P., Butor-Keler, A., & Kanclerz, K. (2023). Selected aspects of crime involving virtual currencies. *Terroryzm*, *4*(4), 325-376. https://doi.org/10.4467/27204383ter.23.030.18332

Otero, R.G., & Diaz, R.M. (2025). Crypto crime: Approaches from transnational crime and money laundering in Colombia. *Procedia Computer Science*, *257*, 1166-1171. https://doi.org/10.1016/j.procs.2025.03.155

PlusToken scammers didn't just steal $2+ billion worth of cryptocurrency. They may also be driving down the price of bitcoin. (2019). https://www.chainalysis.com/blog/plustoken-scam-bitcoin-price/

Rahman, A., Debnath, P., Ahmed, A., Dalim, H.M., Karmakar, M., Sumon, M.F.I., & Khan, M.A. (2024). Machine learning and network analysis for financial crime detection: Mapping and identifying illicit transaction patterns in global black money transactions. *Gulf Journal of Advance Business Research*, *2*(6), 250-272. https://doi.org/10.51594/gjabr.v2i6.49

Regulation (EU) 2023/1114 of the European Parliament and of the Council "On Markets in Crypto-Assets". (2023). https://eur-lex.europa.eu/eli/reg/2023/1114/oj/eng

Reuters. (2023). Israel freezes crypto accounts seeking Hamas donations, police say. https://www.reuters.com/technology/israel-freezes-crypto-accounts-seeking-hamas-donations-police-say-2023-10-10/

Reuters. (2025). Swiss, German authorities shut down cryptomixer.io in money laundering crackdown. https://www.reuters.com/business/finance/swiss-german-authorities-shut-down-cryptomixerio-money-laundering-crackdown-2025-12-01/

Rustamaji, M., & Faisal, F. (2024). Law enforcement strategies against money laundering through cryptocurrency: Comparative studies in several countries. In *Proceedings of the International Conference on Cultural Policy and Sustainable Development (ICPSD 2024)* (pp. 560-572). Dordrecht: Atlantis Press. https://doi.org/10.2991/978-2-38476-315-3_76

Sater, S. (2020). Do we need KYC/AML: The Bank Secrecy Act and virtual currency exchanges. *Arkansas Law Review*, *73*(2), 397-423.

Seaton, W. (2024). New VPN risk report: 56% of enterprises attacked via VPN vulnerabilities. https://securityboulevard.com/2024/05/new-vpn-risk-report-56-of-enterprises-attacked-via-vpn-vulnerabilities/?utm

Silk Road. (2025). https://www.britannica.com/topic/Silk-Road-marketplace

Sorban, K. (2020). The role of digital literacy and online intermediaries in tackling cybercrime. *Just Fair and Healthy*, *16*(3), 179-192.

Spagnuolo, M., Maggi, F., & Zanero, S. (2014). Bitiodine: Extracting intelligence from the bitcoin network. In N. Christin, R. Safavi-Naini (Eds.), *Revised Selected Papers of the 18th International Conference "Financial Cryptography and Data Security"* (pp. 457-468). Berlin, Heidelberg: Springer. https://doi.org/10.1007/978-3-662-45472-5_29

Temirzhanova, L.A., Imangaliev, N.K., Syzdykov, A.Z., Eshnazarov, A.A., & Sagymbekov, B.Z. (2018). Improving the mechanism of countering certain types of fraud in the Republic of Kazakhstan. *Journal of Advanced Research in Law and Economics, 9*(5), 1776–1788. https://doi.org/10.14505//jarle.v9.5(35).33

Temirzhanova, L.A., Imangaliev, N.K., Sagymbekov, B.Z., Eshnazarov, A.A., & Syzdykov, A.Z. (2019). Countering fraud committed using information technology in Kazakhstan. *Journal of Advanced Research in Law and Economics, 10*(7), 2122–2132. https://doi.org/10.14505/jarle.v10.7(45).25

Tidy, J. (2022). Hydra: How German police dismantled Russian darknet site. https://www.bbc.com/news/technology-61002904

Tinmaz, H., Lee, Y., Fanea-Ivanovici, M., & Baber, H. (2022). A systematic review on digital literacy. *Smart Learning Environments*, *9*, 21. https://doi.org/10.1186/s40561-022-00204-y

Transaction Monitoring Labs. (2025). Crypto Crime Report. https://www.trmlabs.com/reports-and-whitepapers/2025-crypto-crime-report

Trozze, A., Kamps, J., Akartuna, E.A., Hetzel, F.J., Kleinberg, B., Davies, T., & Johnson, S.D. (2022). Cryptocurrencies and future financial crime. *Crime Science*, *11*, 1. https://doi.org/10.1186/s40163-021-00163-8

Waldman, A. (2023). Cyber insurance report shows surge in ransomware claims. https://www.techtarget.com/searchsecurity/news/366552773/Cyber-insurance-report-shows-surge-in-ransomware-claims

Yesimov, S.S., & Borovikova, V.S. (2022). Administrative and Legal Implementation of the Rights of Business Entities. *Social and Legal Studios, 5*(3), 16–22. https://doi.org/10.32518/2617-4162-2022-5-3-16-22

Zhao, K., Dong, G., & Bian, D. (2023). Detection of illegal transactions of cryptocurrency based on mutual information. *Electronics*, *12*(7), 1542. https://doi.org/10.3390/electronics12071542

The Law, State and Telecommunications Review / Revista de Direito, Estado e Telecomunicações

Contact:
Universidade de Brasília - Faculdade de Direito - Núcleo de Direito Setorial e Regulatório
Campus Universitário de Brasília
Brasília, DF, CEP 70919-970
Caixa Postal 04413

Phone: +55(61)3107-2683/2688

E-mail: getel@unb.br

Submissions are welcome at: https://periodicos.unb.br/index.php/RDET