Submission date: 17 of May 2026
Acceptance date: 7 of July 2026
Publication date: 17 of July 2026

RED FLAG INDICATORS FOR DETECTING CRIMINAL USE OF CRYPTOCURRENCY

INDICADORES DE ALERTA PARA DETECTAR EL USO DELICTIVO DE LAS CRIPTOMONEDAS

Elena Kirillova[1*]
E-mail: debryansk@mail.ru
ORCID: https://orcid.org/0000-0001-7137-901X
Oleg Blinkov[2,3]
E-mail: blinkov@inbox.ru
ORCID: https://orcid.org/0000-0002-3506-2194
Natalija Ogneva[3]
E-mail: ognevanatasha@mail.ru
ORCID: https://orcid.org/0000-0003-0852-5189
Tatyana Melnichenko[3]
E-mail: tmel23@yandex.ru
ORCID: https://orcid.org/0009-0006-0406-0782
Suliman Sabiev[4]
E-mail: sabiev-suliman@rambler.ru
ORCID: https://orcid.org/0000-0001-8651-6961
[1] Southwest State University, Kursk, Russia.
[2] Academy of the FPS of Russia, Ryazan, Russia.
[3] State University of Humanities and Social Studies, Moscow Region, Kolomna, Russia.
[4] Russian New University, Moscow, Russia.
*Corresponding author

Suggested citation (APA, seventh ed.)

Kirillova, E., Blinkov, O., Ogneva, N., Melnichenko, T., & Sabiev, S. (2026). Red flag indicators for detecting criminal use of cryptocurrency. *Universidad y Sociedad 18*(4). e6203.

ABSTRACT:

This article identifies and classifies key red flag indicators signaling the use of cryptocurrency in criminal activities, particularly money laundering and terrorist financing, and proposes mitigation measures relevant to legal and compliance frameworks. The study was based on a systematic literature review and bibliometric analysis conducted in accordance with PRISMA guidelines. More than 190 legal studies, analytical reports, and expert reviews published between 2007 and 2025 were screened in Scopus, Web of Science, and legal databases, with 52 works selected for detailed analysis. The identified indicators were grouped into five categories: transactional anomalies, anonymity-enhancing practices, suspicious behavior of senders and recipients, opaque or excessive sources of funds, and geographic risks related to poorly regulated jurisdictions. The findings show that these indicators can support early detection and compliance strategies for regulators, crypto exchanges, and financial monitoring units. The article emphasizes technological and legal countermeasures, including KYC integration, regulatory registration of crypto exchanges, and reporting obligations for suspicious transactions. By bridging criminological analysis with legal monitoring practice, the study contributes to AML/CTF compliance, digital law, financial security, and regulatory technology.

Keywords: Cryptocurrency, Money laundering, Terrorist financing, Red flags, Legal regulation, Transactions, Crypto exchange.

RESUMEN:

Este artículo identifica y clasifica indicadores clave de alerta que señalan el uso de criptomonedas en actividades delictivas, en particular el lavado de dinero y la financiación del terrorismo, y propone medidas de mitigación relevantes para los marcos legales y de cumplimiento normativo. El estudio se basó en una revisión sistemática de la literatura y un análisis bibliométrico realizado de acuerdo con las directrices PRISMA. Se examinaron más de 190 estudios legales, informes analíticos y revisiones de expertos publicados entre 2007 y 2025 en Scopus, Web of Science y bases de datos legales, seleccionándose 52 trabajos para un análisis detallado. Los indicadores

identificados se agruparon en cinco categorías: anomalías transaccionales, prácticas que mejoran el anonimato, comportamiento sospechoso de remitentes y destinatarios, fuentes de fondos opacas o excesivas y riesgos geográficos relacionados con jurisdicciones con escasa regulación. Los hallazgos muestran que estos indicadores pueden respaldar las estrategias de detección temprana y cumplimiento normativo para reguladores, plataformas de intercambio de criptomonedas y unidades de monitoreo financiero. El artículo destaca las contramedidas tecnológicas y legales, con la inclusión de la integración de KYC (Conozca a su Cliente), el registro regulatorio de las plataformas de intercambio de criptomonedas y las obligaciones de reporte para transacciones sospechosas. Al vincular el análisis criminológico con la práctica del monitoreo legal, este estudio contribuye al cumplimiento de las normas contra el lavado de dinero y el financiamiento del terrorismo (ALD/CTF), el derecho digital, la seguridad financiera y la tecnología regulatoria.

Palabras clave: Criptomoneda, Lavado de dinero, Financiamiento del terrorismo, Señales de alerta, Regulación legal, Transacciones, Intercambio de criptomonedas.

INTRODUCTION

The emergence and rapid expansion of cryptocurrencies have transformed the global financial landscape, creating new opportunities for innovation, investment, and digital economic development. Since the introduction of Bitcoin in 2009, cryptocurrencies have evolved from a niche technological experiment into a significant component of the international financial ecosystem. The growing adoption of digital assets by individuals, businesses, and institutional investors has been accompanied by the development of blockchain technology, decentralized finance platforms, and new forms of digital transactions that operate beyond the traditional banking system. These innovations have enhanced the efficiency, accessibility, and speed of financial transactions, particularly in cross-border contexts where conventional payment systems often face regulatory and operational limitations (Whyte, 2023).

Despite these benefits, the expansion of cryptocurrency markets has also generated substantial concerns among regulators, policymakers, and law enforcement agencies. The same characteristics that make cryptocurrencies attractive for legitimate economic activities may also facilitate their use in criminal operations. Features such as decentralization, pseudonymity, rapid international transfers, and the absence of traditional financial intermediaries can create opportunities for individuals and criminal organizations seeking to conceal illicit proceeds, evade regulatory oversight, or transfer funds across jurisdictions with limited transparency. Consequently, cryptocurrencies have increasingly become associated with a variety of criminal activities, including money laundering, terrorist financing, drug trafficking, corruption, cybercrime, tax evasion, human trafficking, and the financing of organized crime networks (Whyte, 2023).

The growing integration of cryptocurrencies into criminal schemes has attracted considerable academic and professional attention. Researchers and international organizations have emphasized that crimes involving digital assets often present unique challenges compared with conventional financial crimes. Cryptocurrency-related offenses frequently exhibit high levels of latency, making them difficult to detect, investigate, and prosecute. The global nature of blockchain networks, combined with the absence of centralized control and the use of sophisticated technological tools to obscure transaction trails, complicates the identification of perpetrators and the recovery of criminal assets. These challenges have intensified the need for effective monitoring mechanisms, regulatory frameworks, and risk assessment tools capable of identifying suspicious activities involving digital assets.

Among the various forms of cryptocurrency-related crime, money laundering and terrorist financing have emerged as particularly significant concerns. Criminal organizations increasingly exploit digital assets to move and conceal illicit funds while minimizing exposure to traditional anti-money laundering controls. The use of cryptocurrencies enables offenders to conduct transactions across multiple jurisdictions, convert assets into different digital currencies, and employ technological solutions designed to increase anonymity. As a result, the identification of indicators that may reveal the misuse of cryptocurrencies has become a critical priority for financial institutions, virtual asset service providers, regulators, and law enforcement agencies.

Scholars examining the criminal use of cryptocurrencies consistently emphasize several distinctive characteristics that contribute to their attractiveness for illegal purposes. These characteristics include the absence of a single issuing authority, the decentralized nature of blockchain transactions, the lack of traditional intermediaries, and the anonymity or pseudonymity of participants involved in transactions (Almaqableh et al., 2022; Bozorgi, 2024; Kapsis, 2023; Żyła-Kania, 2023). While these features provide legitimate users with greater autonomy and flexibility, they may also reduce transparency and facilitate the concealment of criminal activities. Consequently, understanding how these characteristics are exploited by offenders is essential for developing effective prevention and detection strategies.

One of the most important areas of contemporary research concerns the identification of red flags that may indicate the use of cryptocurrencies in criminal activities. Red flags represent observable indicators, behaviors, or transaction patterns that suggest an elevated risk of illicit activity and

warrant further investigation. The concept has become increasingly relevant in anti-money laundering and counter-terrorist financing frameworks because it enables institutions to adopt a risk-based approach to monitoring financial transactions. Rather than focusing exclusively on confirmed criminal conduct, red flag systems seek to identify suspicious behaviors at an early stage, thereby facilitating preventive intervention.

The existing literature identifies a wide range of cryptocurrency-related red flags. Among the most frequently reported indicators are transactions involving multiple service providers located in different countries, unusual or economically irrational transaction patterns, rapid movement or withdrawal of assets immediately after acquisition (Akcinaroglu & Shi, 2025; Wagman, 2022), deposits of large sums intended for cryptocurrency purchases, the use of multiple accounts to acquire digital assets, and coordinated transactions conducted from the same IP address by different individuals (Genccelep, 2022; Movchan et al., 2023; Teichmann, 2022;). Additional concerns arise from the use of privacy-enhancing technologies, including the conversion of Bitcoin into privacy-focused cryptocurrencies, the use of mixers and tumblers, and the presence of coded communications or encrypted symbols associated with illegal activities (Song et al., 2023).

Recent studies have also highlighted the growing sophistication of criminal methods involving cryptocurrencies. Criminal actors increasingly employ advanced technological tools to obscure transaction histories, fragment transfers across multiple wallets, and exploit regulatory differences between jurisdictions. These developments require continuous adaptation of monitoring systems and analytical methodologies capable of detecting emerging threats within rapidly evolving cryptocurrency ecosystems. Consequently, researchers and practitioners have emphasized the importance of developing comprehensive risk indicators that account for transactional, behavioral, technological, and geographical dimensions of cryptocurrency-related crime.

Although significant progress has been made in identifying suspicious indicators, important gaps remain in the existing body of knowledge. The rapid pace of technological innovation, the emergence of new digital assets, and the increasing complexity of decentralized financial systems create ongoing challenges for regulators and investigators. Furthermore, differences in legal frameworks across countries and the limited availability of empirical studies hinder the establishment of standardized approaches for identifying and assessing cryptocurrency-related risks. These limitations underscore the need for continued research aimed at strengthening the evidence base and supporting the development of effective countermeasures.

In response to these challenges, the present study seeks to contribute to the growing literature on cryptocurrency-related financial crime by identifying and classifying the principal red flags associated with criminal activity involving digital assets. Furthermore, the study aims to examine measures that may assist in reducing the risks of money laundering and terrorist financing through cryptocurrencies. By systematizing existing knowledge and highlighting key risk indicators, this research intends to provide a useful framework for policymakers, compliance professionals, financial institutions, and law enforcement agencies engaged in combating illicit activities within the rapidly expanding cryptocurrency environment.

MATERIALS AND METHODS

The red flag indicators of cryptocurrency use in criminal activity identified in this study are based on the analysis of more than 190 case studies conducted in various jurisdictions between 2007 and 2025, as well as the findings of the FATF report “Money Laundering and Terrorist Financing Red Flag Indicators Associated with Virtual Assets” (FATF, 2020).

In searching for documents, we adhered to the standards of the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA). PRISMA requires that all stages of the search and review process be thoroughly described and recorded by researchers. The PRISMA flow diagram consists of four stages: identification of articles, screening of articles, decision-making on the eligibility of studies, and the final compilation of the list of studies to be included in the systematic review (Figure 1).

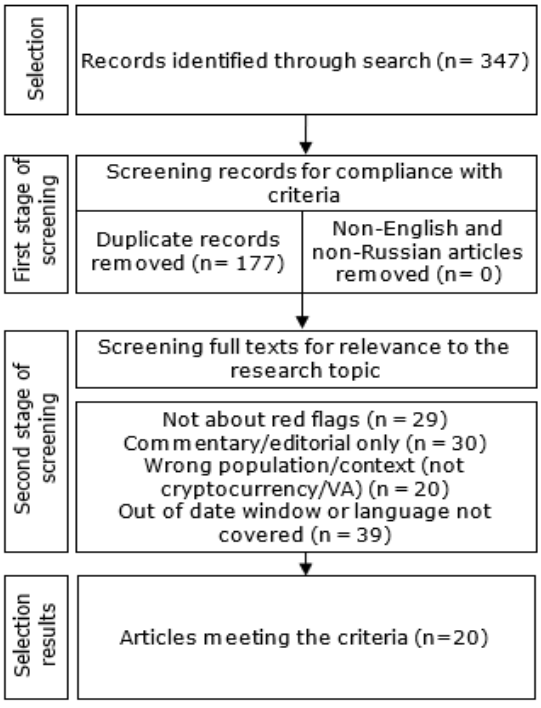

Fig 1. PRISMA diagram of the selection process of bibliographic sources for bibliometric analysis.

We selected studies written by experts on the following topics: "use of cryptocurrency in criminal activity," "crime and cryptocurrency," "money laundering through cryptocurrency," "suspicious cryptocurrency transactions." A bibliographic search was carried out in the Scopus and Web of Science databases, on the resource https://scholar.google.com.sv/scholar, and on official websites hosting key international legal acts. We reviewed reports, surveys, and analytical studies conducted by expert online resources. International legislative acts regulating the circulation of cryptocurrency were also included.

The studies were selected according to the following criteria:

1. Authors must have at least three publications on the topics "use of cryptocurrency in criminal activity," "crime and cryptocurrency," "money laundering through cryptocurrency," "suspicious cryptocurrency transactions" over the past 10 years;

2. A numerical predominance of more than 50% of studies on digital rights and digital assets with a legal focus in the total number of the authors' publications;

3. The author's profile must indicate that their publications are thematically related to legal sciences and digital law;

4. The work must have been written between 2007 and 2025.

Using this approach, more than 190 publications were initially selected. We read the full text of the articles, carefully studied legal acts regulating the cryptocurrency market, as well as reports, papers, and analytical reviews. In research articles, we paid attention to the abstracts and conclusions drawn by the authors. After careful selection, 52 works were chosen.

The use of this methodology allowed us to identify and classify the main red flag indicators of cryptocurrency use in criminal activity. The results of the article are of practical significance and can be applied in the monitoring activities of cryptocurrency exchanges.

RESULTS AND DISCUSSION

As the analysis of the selected studies shows, experts attribute the following characteristics of cryptocurrency to features that make it suitable for criminal use: the absence of a single issuing authority; the decentralized nature of cryptocurrency transactions (Almaqableh et al., 2022; Bozorgi, 2024; Żyła-Kania, 2023); the absence of intermediaries (Kapsis, 2023); and anonymity. It should also be noted that cryptocurrency transactions are characterized by speed and low fees, which serve as additional factors for the use of this asset in criminal activity (Tabla 1).

Table 1. Classification of cryptocurrency red flag indicators associated with money laundering and terrorist financing.

Category	Main Red Flag Indicators	Representative Sources
Transaction-related indicators	Large or frequent transactions, rapid deposits and withdrawals, transfers to unrelated jurisdictions, structured transactions, transfers from suspicious addresses	Genccelep (2022); Movchan et al. (2023); Teichmann (2022)
Enhanced anonymity indicators	Use of privacy-focused cryptocurrencies, mixing services, encrypted communications, peer-to-peer platforms, multiple wallets linked to the same IP address	Burgess et al. (2024); FATF (2020); Omeh (2024)
Payer and recipient indicators	Multiple accounts under different identities, suspicious IP addresses, false identification data, frequent changes in user information, unusual user behavior	Ma (2023); Melnyk (2023)
Source-of-funds indicators	Unexplained origin of funds, unusually large purchases, reliance on ICOs with limited transparency, income primarily derived from crypto activities	Jofre et al. (2024); Melnyk (2023)
Geographical risk indicators	Use of exchanges in poorly regulated jurisdictions, transfers to countries without crypto regulations, cross-border transactions lacking economic rationale	Kushelevitch (2024); Żyła-Kania (2023)

Table 1 summarizes the main categories of red flag indicators identified in the literature regarding the potential use of cryptocurrencies for money laundering and terrorist financing. The findings reveal that suspicious activities can be grouped into five broad dimensions: transaction patterns, anonymity-enhancing mechanisms, characteristics of payers and recipients, sources of funds, and geographical risks. Among these, transaction-related and anonymity-related indicators appear most frequently in the reviewed studies, highlighting the importance of monitoring unusual transaction behavior and technologies designed to conceal user identities.

The classification also demonstrates that cryptocurrency-related financial crime is a multidimensional phenomenon that extends beyond individual transactions. Factors such as user behavior, the origin of funds, and the regulatory environment of the jurisdictions involved play a significant role in assessing risk. Consequently, an effective anti-money

laundering and counter-terrorist financing framework should integrate indicators from all five categories to improve the detection and prevention of illicit activities within cryptocurrency ecosystems.

When cryptocurrency is used for criminal purposes, there is a set of indicators that may point to transactions connected to illicit activity. Such indicators are referred to as markers, red flags, or in this study, "red flag signals." Experts identify the following signals indicating the use of cryptocurrency for money laundering and terrorist financing: conducting transactions involving several providers located in different countries; performing cryptocurrency operations without logical explanation (Genccelep, 2022; Wagman, 2022); depositing large sums of money for cryptocurrency purchases (Movchan et al., 2023; Teichmann, 2022); maintaining multiple accounts for buying cryptocurrency (Akcinaroglu & Shi, 2025); transactions conducted by multiple individuals from a single IP address; the use of enhanced anonymity measures; and the use of symbols, codes, or encryption suggesting links to illegal activities (Song et al., 2023).

Other warning signs include interactions between cryptocurrency holders and individuals previously or currently involved in money laundering or terrorist financing, as well as transfers of cryptocurrency to countries with jurisdictions that allow operations without customer identification.

Some researchers rightly point out that suspicious behavior may also include knowingly loss-making operations with crypto-assets, the use of multiple accounts (Melnyk, 2023), and the use of numerous settlement tools (Jofre et al., 2024).

Agreeing with experts' opinions, it should be added that transaction-related red flag signals have long been widespread, and this set of indicators points to the use of cryptocurrency in illegal activity. Such signals must be highlighted as a separate group. In particular, suspicion should arise regarding the size and frequency of transactions. Such warning signals include: conducting several large transactions within a short period of time; transferring cryptocurrency to individuals in other jurisdictions where the owner has no business; depositing cryptocurrency on an exchange and instantly withdrawing it without making operations; transferring cryptocurrency from addresses suspected of fraudulent activity; and structuring transactions, for example, through repeated exchanges or transfers.

Experts have repeatedly noted that cryptocurrency transactions have become attractive to criminal communities due to certain advantages that make it highly probable to conceal traces of crime (Burgess et al., 2024). Such advantages include the anonymity of transactions, no one knows the owner of a cryptocurrency wallet, nor who carries out the transactions. There are also technological features that enhance the anonymity of cryptocurrency transactions, allowing the concealment of criminal activity. Thus, another group of red flag signals can be identified, connected with anonymity:

- transactions involving more than one type of cryptocurrency designed to provide enhanced anonymity;
- operations on unlicensed peer-to-peer platforms with a large number of virtual transfers, involving cryptocurrencies with enhanced anonymity and under high commission fees (Omeh, 2024);
- registration of domain names on the Internet through proxy services that conceal owners' names;
- transactions carried out using encrypted communication tools;
- large numbers of digital wallets registered to different users from the same IP address;
- receipt of funds from VASP providers lacking "Know Your Customer" (KYC) procedures;
- transfers of cryptocurrency to electronic wallets that provide mixing services during data exchange.

As an example, in 2017, the Alpha Bay marketplace was shut down, which had been used by criminals to purchase drugs, weapons, and malicious software for hacking computer equipment. The platform operated while concealing the data of its administrators and users and employed various types of VAS services used by more than 200,000 users and 40,000 vendors. The activities of the marketplace raised suspicions, and in 2017 the U.S. government shut down its servers and arrested the administrator, confiscating digital and physical assets. The arrest warrant was obtained after tracing cryptocurrency transactions to other accounts with enhanced anonymity (FATF, 2020).

The presence of one red flag indicator, or even several, is not always grounds for suspicion of unlawful activity, but this fact should prompt control and monitoring of clients who may be using cryptocurrency for money laundering or terrorist financing (Akartuna et al., 2023).

There are a number of red flag indicators related to unusual behavior of cryptocurrency senders and recipients, among which the following can be distinguished:

- creation of multiple accounts under different names to bypass trading restrictions;
- conducting transactions from suspicious IP addresses;
- registration of cryptocurrency sellers in jurisdictions different from their place of incorporation;
- provision of another person's identification data and false information regarding transactions and counterparties;

Vol 18 | No.4 | July-August | 2026
Continuous publication
e6203

- discrepancy between IP addresses associated with a client's profile and the IP addresses from which transactions are initiated;
- advanced age of a platform user combined with the execution of a large number of transactions, which may indicate that the person is a victim of financial exploitation (Ma, 2023);
- frequent changes of IP addresses, email addresses, or attempts to access a cryptocurrency wallet from different IP addresses within a short time, which may indicate attempts to hack the client's account.

Another group of red flag indicators can be distinguished based on the source of funds used to purchase cryptocurrency, with attention to the following factors:

- the amount of replenishment significantly exceeds the usual, and immediately after the purchase of cryptocurrency follows its conversion into fiat money;
- lack of information on the origin of funds used in Initial Coin Offerings (ICOs), where investors' personal data may be unavailable;
- the client's primary source of income consists of sums derived from cryptocurrency investments or fraudulent ICOs.

Criminals often use jurisdictions where cryptocurrency purchase/sale is poorly regulated at the legislative level for money laundering and terrorist financing; for example, where registration and licensing regimes for crypto exchanges are absent, which allows illegal funds to be moved and used in criminal activity. Given these trends, the following red flag indicators can be distinguished in connection with geographical risks:

- funds come from an exchange that is not located in the client's jurisdiction;
- the client uses an exchange to purchase cryptocurrency that is located in a jurisdiction where registration and licensing requirements for crypto exchanges are not enforced;
- the client transfers cryptocurrency funds to a jurisdiction where no legal acts regulating cryptocurrency transactions exist.

To minimize the risks of cryptocurrency use in criminal activity, many countries have introduced mandatory licensing and registration requirements for crypto exchanges. Such requirements are in force in the United Kingdom, France, the United States, and several other countries (Kushelevitch, 2024).

Additional measures may include requirements to report suspicious transactions and operations containing red flag indicators. In the future, it is advisable to introduce mandatory customer identification procedures on crypto exchanges. Clients should be required to provide personal identity information, address, and financial data, while being guaranteed protection of personal data and confidentiality.

CONCLUSIONS

The findings of this study allowed for the identification and systematization of the main red flag indicators associated with the potential use of cryptocurrencies in criminal activities, particularly money laundering and terrorist financing.

These indicators were grouped into five key categories: transaction-related indicators, indicators linked to enhanced anonymity measures, indicators associated with payers and recipients, indicators related to sources of financing, and indicators connected to geographical risk factors. This classification contributes to a better understanding of suspicious behaviors within cryptocurrency ecosystems and provides a practical framework for risk assessment and compliance monitoring.

The analysis highlights the growing complexity of detecting illicit financial activities in digital asset environments, where technological innovation and cross-border transactions often challenge traditional regulatory and supervisory mechanisms. The identified indicators may assist financial institutions, virtual asset service providers, regulatory authorities, and law enforcement agencies in strengthening preventive measures and improving the effectiveness of anti-money laundering and counter-terrorist financing efforts.

Despite its contributions, the study is subject to certain limitations. Although an initial sample of 185 sources was examined, only 52 publications met the inclusion criteria and specifically addressed red flag indicators related to cryptocurrency-based criminal activities.

Future research should expand the evidence base by incorporating additional empirical studies, comparative international analyses, and emerging regulatory developments. Furthermore, greater attention should be devoted to evaluating strategies and technological solutions capable of mitigating the risks associated with the misuse of cryptocurrencies for money laundering and terrorist financing in an increasingly digitalized financial environment.

REFERENCES

Akartuna, E. A., Johnson, S. D., & Thornton, A. E. (2023). The money laundering and terrorist financing risks of new and disruptive technologies: A futures-oriented scoping review. ***Security Journal, 36***(4), 615–650. http://dx.doi.org/10.1057/s41284-022-00356-z

Akcinaroglu, S., & Shi, M. (2025). Exploring the impact of cryptocurrency on terrorism. ***Terrorism and Political Violence, 37***(1), 111–135. http://dx.doi.org/10.1080/09546553.2023.2275057

Almaqableh, L., Reddy, K., Pereira, V., Ramiah, V., Wallace, D., & Veron, J. F. (2022). An investigative study of links between terrorist attacks and cryptocurrency markets. ***Journal of Business Research, 147***, 177–188. http://dx.doi.org/10.1016/j.jbusres.2022.04.019

Bozorgi, M. (2024). Exploring the role of fintech in terrorism financing: Legal frameworks and solutions. In N. Mansour & L. M. Bujosa Vadell (Eds.), ***Sustainability and financial services in the digital age*** (pp. 9–20). Springer. http://dx.doi.org/10.1007/978-3-031-67511-9_2

Burgess, A., Hamilton, R., & Leuprecht, C. (2024). Terror on the blockchain: The emergent crypto-crime-terror nexus. In D. Goldbarsht & L. de Koker (Eds.), ***Financial crime, law and governance: Navigating challenges in different contexts*** (pp. 203–227). Springer. http://dx.doi.org/10.1007/978-3-031-59547-9_9

Financial Action Task Force. (2020). ***Money laundering and terrorist financing red flag indicators associated with virtual assets***. FATF. https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Methodsandtrends/Virtual-assets-red-flag-indicators.html

Genccelep, R. (2022). Use of cryptocurrency for the crime of financing of terrorism. ***Bilişim Hukuku Dergisi, 4***(1), 33–80. http://dx.doi.org/10.55009/bilisimhukukudergisi.1132645

Jofre, M., Aziani, A., & Villa, E. (2024). Terrorist financing: Traditional vs. emerging financial technologies. ***Terrorism and Political Violence***, 1–14. http://dx.doi.org/10.1080/09546553.2024.2433635

Kapsis, I. (2023). Crypto-assets and criminality: A critical review focusing on money laundering and terrorism financing. In D. Jasinski, A. Phillips, & E. Johnston (Eds.), ***Organised crime, financial crime, and criminal justice*** (pp. 122–141). Routledge. http://dx.doi.org/10.4324/9781003020813-8

Kushelevitch, M. (2024). Unveiling the crypto-terror nexus: Law enforcement intelligence challenges against terrorist financing. ***Journal of Financial Crime, 32***(2), 403–415. https://doi.org/10.1108/JFC-12-2023-0330

Ma, W. (2023). Terrorist financing, war crimes, and crypto geopolitics. In K. Huang, D. Budorin, L. J. Tan, W. Ma, & Z. W. Zhang (Eds.), ***A comprehensive guide for Web3 security: From technology, economic and legal aspects*** (pp. 241–259). Springer. https://doi.org/10.1007/978-3-031-39288-7_12

Melnyk, D. S. (2023). Modern features of the cryptocurrency use for terrorist financing, money laundering and other unlawful activities: Prospective countermeasures. ***Bulletin of Kharkiv National University of Internal Affairs, 101***(2–1), 150–162. https://doi.org/10.32631/v.2023.2.14

Movchan, A., Shliakhovskyi, O., Kozii, V., & Fedchak, I. (2023). Investigating cryptocurrency financing crimes terrorism and armed aggression. ***Social & Legal Studios, 6***(4), 123–131. http://dx.doi.org/10.32518/sals4.2023.123

Omeh, J. E. (2024). ***Digital dangers of blockchain technology and cryptocurrency: How blockchain and cryptocurrency facilitate terrorism financing in North America***. SSRN. https://ssrn.com/abstract=4878432

Song, Y., Chen, B., & Wang, X. Y. (2023). Cryptocurrency technology revolution: Are Bitcoin prices and terrorist attacks related? ***Financial Innovation, 9***(1), Article 29. http://dx.doi.org/10.1186/s40854-022-00445-3

Teichmann, F. M. (2022). Current trends in terrorist financing. ***Journal of Financial Regulation and Compliance, 30***(1), 107–125. http://dx.doi.org/10.1108/JFRC-03-2021-0022

Wagman, S. (2022). Cryptocurrencies and national security: The case of money laundering and terrorism financing. ***Harvard National Security Journal, 14***, 87–126. https://journals.law.harvard.edu/nsj/2022/12/cryptocurrencies-and-national-security-the-case-of-money-laundering-and-terrorism-financing/

Whyte, C. (2023). Cryptoterrorism: Assessing the utility of blockchain technologies for terrorist enterprise. ***Studies in Conflict & Terrorism, 46***(7), 1126–1149. http://dx.doi.org/10.1080/1057610X.2018.1531565

Żyła-Kania, E. (2023). Use of virtual currencies for financing terrorism. ***Polish Journal of Political Science, 9***(1), 32–45. https://doi.org/10.58183/pjps.01032023