



CRYPTOCURRENCIES AND TERRORIST FINANCING IN LEGAL REGULATORY AND SECURITY PERSPECTIVES

Salwan Jaber Hashim

College of Law, Al-Nahrain University, Iraq. E-mail: salwan.j.hashem@nahrainuniv.edu.iq

Elham Ibrahim Hussein

Laser Institute for Postgraduate Studies, University of Baghdad, Iraq.
Elham.I@ilps.uobaghdad.edu.iq

Mena Mahdi Abdallah

Laser Institute for Postgraduate Studies, University of Baghdad, Iraq. E-mail: mena.mahdi202a@colaw.uobaghdad.edu.iq

Magomed Tashtamirov

Head of the Department of Finance, Credit and Antitrust Regulation, Kadyrov Chechen State University, Russia. E-mail: magomed.tashtamirov@mymail.academy

Svetlana Bochkova

Department of Legal Regulation of Economic Activity, Russian State Agrarian University - Moscow Timiryazev Agricultural Academy, Russia. E-mail: svetlana.bochkova@mymail.academy

Yulia Frolovskaya

Department of Legal Regulation of Economic Activity, Financial University under the Government of the Russian Federation, Russia. E-mail: yulia.frolovskaya@mymail.academy

ABSTRACT

Objective: This study analyzes the concept, characteristics, and risks of cryptocurrencies, focusing on their potential role in financing terrorism. It clarifies the relationship between virtual currencies, electronic money, and cryptocurrencies, and examines how features such as decentralization, anonymity, and cross-border accessibility can facilitate illicit activities.

Methods: A comparative legal analysis was conducted, reviewing legislative and regulatory approaches toward cryptocurrencies in selected countries. Legal texts, central bank regulations, and policy statements were examined alongside academic literature to evaluate how jurisdictions address cryptocurrency misuse in terrorism financing and money laundering.

Results: Findings show that the anonymity, decentralization, and global nature of cryptocurrencies present significant challenges for regulators and law enforcement. While some jurisdictions impose strict prohibitions or licensing systems, others lack comprehensive legal frameworks, creating opportunities for exploitation. Terrorist organizations have used cryptocurrencies for fundraising and fund transfers, often via the dark web and encrypted platforms. However, the limited technological infrastructure in many conflict zones restricts large-scale reliance on cryptocurrencies for terrorism financing.

Conclusion: Cryptocurrencies combine technological benefits with substantial risks. Although their current role in terrorism financing is supplementary rather than primary,





advances in privacy-focused digital assets may increase future threats. Effective prevention requires stronger international cooperation, clear and enforceable regulations, and advanced monitoring tools to track suspicious transactions while supporting legitimate blockchain-based innovation.

Keywords: Cryptocurrencies; Terrorism; Money laundering; Finance.

INTRODUCTION

Digital currency is considered a form of money that falls under the broader monetary framework, encompassing all types of currencies, including traditional ones. Despite not having a physical or tangible form, it remains accessible in a digital manner. However, international organizations differ in their perspectives on its legal status and definition (Abdullayev et al., 2024).

Central banks and regulatory bodies attempt to define and restrict crypto currency concepts, but some prefer a broader and more inclusive definition that encompasses all digital transactions conducted via the internet, regardless of the underlying technology.

For instance, the World Bank (WB) classifies digital currency as a monetary unit that operates independently, having a predetermined daily value (Hilal et al., 2022). Meanwhile, the European Central Bank (ECB) defines it as an electronically stored monetary value, which can be used for transactions without the need for a bank account and is issued independently from central authorities.

Digital currency differs from electronic money, which serves as a legal tender and is commonly used for transactions. According to the Bank for International Settlements (BIS), digital currencies are considered "representations of value", while the Financial Action Task Force (FATF) categorizes them as either virtual currency or electronic legal tender, applying the term "virtual currency" as a broader classification.

The main issue explored in this research is the lack of clear legislative regulation for crypto currency use. This absence of government oversight leads to unregulated transactions in some countries, making crypto currencies a financial alternative that is beyond state control.

METHODOLOGY

This study adopts a comparative legal analysis methodology to examine and evaluate the regulatory approaches of different countries toward the use of





cryptocurrencies, with a particular focus on their potential role in financing terrorism and money laundering. Comparative legal analysis is a well-established method in legal scholarship that facilitates the identification of similarities, differences, and trends across jurisdictions.

The research used the selection of jurisdictions representing a diversity of legal systems, economic contexts, and policy approaches, including both countries with permissive regulatory environments and those with restrictive or prohibitive stances toward cryptocurrency use. Legislative texts, central bank regulations, governmental decrees, and relevant case law were collected from official legal databases, government websites, and credible secondary sources.

The analysis involved systematic coding and categorization of each jurisdiction's legal instruments according to key criteria: legal recognition or prohibition of cryptocurrencies, licensing requirements for trading platforms, anti-money laundering (AML) and counter-terrorism financing (CTF) obligations, enforcement mechanisms, and penalties for violations. Where available, official policy statements and international guidelines (such as those issued by the Financial Action Task Force) were also incorporated to provide broader context.

By comparing multiple jurisdictions, the methodology enables the identification of common challenges, best practices, and legal gaps, thereby informing recommendations for harmonizing regulatory responses at both national and international levels.

RESULTS AND DISCUSSION

First Requirement: Types and Characteristics of Digital Currency

Section One: Types of Digital Currencies

After clarifying the concept of digital currencies, they can be divided into three types: virtual currencies, electronic currencies, and legal digital currencies. The latter are issued by central banks or monetary institutions.

1. Virtual Currencies

Virtual currencies are recognized as those that do not have a physical existence but can be exchanged for value. They are traded over the internet and are currently used alongside official currencies such as the dollar and the euro. Their issuance does not require the presence of a central authority or a central bank.





According to the Bank for International Settlements (BIS), virtual currency is defined as:

"A type of unregulated digital money that operates outside the official monetary system and is not issued by central banks or regulated financial institutions but can be used for transactions and accepted by certain entities."

Virtual currencies are not legally binding as a means of payment, and there is no obligation for parties to accept them. They lack a centralized authority or regulatory framework, and their issuance is not controlled by central banks. Instead, they are created and managed within decentralized digital platforms, including blockchain-based systems, and are often used in online games and closed virtual communities. Their value and usage depend on the agreement and adoption by community members (Stokes, 2012).

There are differing views regarding the application of virtual currencies. Some argue that they contradict the principles of dealing with official currencies, while others believe they can function within a unified and regulated system. However, they lack a centralized regulatory authority that supervises their issuance, exchange, and trading. Moreover, virtual currencies do not have intrinsic value and do not represent legal tender in exchange for goods and services. Instead, their issuance and exchange occur electronically (Nagumanova et al., 2025).

2. Electronic Currencies

Electronic currencies represent digitally stored monetary value and are issued when financial transactions occur. They are used as a payment method and can be exchanged between individuals and entities.

Electronic currencies share characteristics with tangible money, particularly in their transferability. However, they are issued by central banks, regulated financial institutions, or legal entities as an official medium of exchange. Unlike virtual currencies, electronic money maintains a material aspect by converting physical cash into digital form.

Electronic currencies are primarily used for financial transfers and payments between financial institutions and traders through electronic payment systems (Sadegh Rajabi, 2023).

3. Stable and Pegged Digital Currencies

Stable digital currencies are a type of virtual currency, but they differ fundamentally in that they can be issued against collateralized assets. Some of these





currencies maintain a fixed exchange rate by being pegged to another currency at a 1:1 ratio, while others are backed by cryptocurrencies. Stable crypto currencies are specifically designed to maintain price stability (What are Stablecoins?, 2022).

4. Legal Digital Currency

Recently, central banks worldwide have been exploring the possibility of issuing a legal digital currency, despite the absence of a clear legal and regulatory framework (Mohammed Al-Adailah, 2020). This study does not imply direct engagement with virtual and encrypted currencies but rather examines the potential benefits of utilizing blockchain technology in digital payment systems. This includes applications beyond crypto currencies, such as cross-border financial transfers and remittances.

5. Crypto Currencies

Crypto currencies are a type of virtual currency that rely on blockchain technology for decentralization, transparency, and security. The most prominent examples are Bitcoin and Ethereum.

A report by the European Central Bank in 2012 categorized crypto currencies as a subset of virtual currencies, particularly mentioning Bitcoin. As a result, they are considered virtual rather than legally recognized monetary units and do not have an intrinsic value tied to a central bank or financial institution. However, crypto currencies can be exchanged for legal tender, and they are increasingly being used in commercial transactions.

In a later report from 2015, the European Central Bank further clarified that virtual currencies like Bitcoin are not issued by any central bank, government, or financial institution. While they can sometimes function as an alternative to money, they remain distinct from traditional currencies due to their decentralized nature. Bitcoin and similar cryptocurrencies are classified as centralized virtual currencies when pegged to legal assets such as the US dollar or the euro, or when backed by other forms of collateral.

Section Two: Characteristics of Crypto Currencies

Crypto currencies are distinguished from other types of virtual currencies by their unique cryptographic properties (Joebgies et al., 2025). These characteristics are based on modern technologies and automated systems, making crypto currencies fundamentally different from official currencies. Unlike traditional financial systems, crypto currencies operate on electronic devices and the internet, transcending





geographical boundaries. This adaptability has fueled their rapid adoption and growing popularity. The Bitcoin model is one of the most well-known examples of such a system.

Global Nature

Virtual currencies are not tied to any specific geographical location, financial institution, central bank, or governmental authority. Unlike local currencies, crypto currencies are not subject to state control or central bank regulations. No government can completely prohibit their use, nor can it monitor or control transactions involving them (Gawer, Bonina, 2024).

Privacy and Anonymity

Virtual currencies provide a high level of privacy. Transactions do not require personal identification, making it impossible to trace users through their names or institutions. Instead, crypto currency transactions are recorded on a public ledger called the blockchain, which maintains transparency while protecting users' identities. Transactions are identified by encrypted alphanumeric codes rather than personal names, ensuring anonymity and security.

1. Encryption:

Virtual currencies rely on encryption to transform sensitive transaction data into an unreadable format using mathematical algorithms or cryptographic keys. This process, known as cryptography, requires specific keys to decrypt the data, ensuring that only authorized individuals can access or process the information. As a result, encrypted data remains protected from unauthorized access.

Low Transaction Fees:

Unlike traditional currencies, virtual currencies generally have minimal or no transaction fees. In cases where fees do apply, they are significantly lower than those associated with conventional financial transactions (Vijayagopal et al., 2024).

2. High Security Levels:

The technology behind virtual currencies is one of their greatest strengths. They utilize highly secure and decentralized systems that provide advanced encryption and protection against fraud, hacking, and counterfeiting. Their blockchain-based ledger ensures the integrity and transparency of transactions.





3. Decentralization:

Virtual currencies operate without a central financial authority or regulatory body. They are issued by unknown entities and facilitate peer-to-peer transactions without the need for intermediaries. This allows users to send and receive funds without government oversight or central bank control. Payments and transfers occur directly between users, often through anonymous digital wallets, without requiring a centralized entity (Nouruldeen, 2018).

4. Transparency:

All transactions within the virtual currency network operate with full transparency. The transfer of funds between wallets is recorded on a public ledger, allowing all users to verify transactions while maintaining privacy regarding ownership and personal data (Zohry, Alsaied, 2021).

5. Avoidance of Infectious Diseases:

Unlike physical currency transactions, which involve direct contact and the exchange of cash, virtual currencies enable purchases and sales through the internet. This eliminates the risk of spreading infectious diseases linked to the handling of paper money. The COVID-19 pandemic highlighted the importance of digital transactions in minimizing the spread of viruses .

While these advantages make virtual currencies appealing, researchers debate whether they can function effectively as a widely accepted financial instrument. Issues such as encryption security, lack of legal recognition by governments, and the absence of central regulation pose challenges. Moreover, the anonymity of virtual currencies can create difficulties in verifying users' identities, which raises concerns about fraud, financial crimes, and disputes.

Second Requirement: Crypto Currency Use in Terrorist Financing and Its Legislative Response

Section One: Terrorist Financing

From a legal perspective, concerns have been raised regarding the use of crypto currencies in criminal activities. The dark web, an encrypted and anonymous section of the internet, has facilitated illicit transactions beyond legal oversight. Unlike the open web (surface web), where publicly accessible information can be analyzed, the dark web operates with anonymity, making it challenging to trace users. Crypto currencies play a fundamental role in facilitating these hidden transactions, allowing





individuals to buy and sell illegal goods and services anonymously, such as weapons, drugs, and counterfeit documents (Raman et al., 2023).

The European Union has acknowledged these risks, emphasizing that the dark web enables organized crime by providing encrypted payment methods and access to sensitive financial and personal data. Moreover, crypto currencies are widely used in cybercrimes such as fraud, money laundering, and ransom ware attacks (Europol, 2023).

Terrorist organizations have sought new methods to secure funding while evading law enforcement authorities. Given the growing international cooperation in countering terrorism financing and money laundering, these groups are continuously searching for innovative financial mechanisms. The differences in how public and private sectors address these challenges have further complicated regulatory oversight.

Terrorist organizations have increasingly relied on unconventional financial channels to secure funding, including trade in natural resources like oil and gas. While such transactions may appear legal, they often mask illicit financial activities. The decentralized nature of cryptocurrencies allows terrorist groups to conduct transactions outside the formal banking system, using encrypted networks to transfer funds without intermediaries.

Reports indicate that despite international regulations, criminal networks have successfully laundered millions of dollars through cryptocurrency transactions. For instance, in the United States, criminals have engaged in extortion, ransom schemes, and drug trafficking, accumulating illicit financial gains exceeding \$100 million.

While technological advancements have improved financial security, terrorist organizations have adapted to exploit these innovations for their benefit. Crypto currencies provide a modern tool for illicit financing due to their anonymity, fast transactions, low fees, and lack of centralized regulation. The dark web, encrypted messaging applications, and anonymous communication platforms have facilitated the global spread of terrorism financing.

Since 2014, crypto currencies have gained increasing attention as a means of funding terrorist activities, further complicating counterterrorism efforts. The widespread adoption of encrypted financial transactions and digital communication networks has made it easier for terrorist organizations to operate beyond the reach of law enforcement.





Following the publication of an article in 2015 titled "Bitcoin: A Viable Alternative to the Global Financial System," supporters of the so-called Islamic State encouraged the use of Bitcoin for fundraising. This was largely due to Bitcoin's intractability, making it an attractive alternative for financial transactions outside traditional banking oversight.

Extremist groups have leveraged social media platforms, including Twitter, to facilitate financial transactions. Several Twitter accounts affiliated with terrorist organizations have emerged, using cryptocurrency to solicit donations. One such account, named Al-Sadaqah, was linked to fundraising for groups supporting the conflict in Syria. Although this account was later suspended, it demonstrated the ability of extremist groups to use encrypted digital transactions for funding.

Transitioning from the Surface Web to the Dark Web

Terrorist networks have gradually shifted from public social media platforms to more concealed methods, such as encrypted online networks. This shift was partly driven by increased scrutiny from counterterrorism agencies. Consequently, extremist supporters began disseminating cryptocurrency wallet addresses to solicit funds, providing an added layer of anonymity for donors.

In a recent legal case in New York, U.S. authorities charged an individual with using Bitcoin to finance the Islamic State. Investigations revealed that substantial financial transactions had been successfully processed through crypto currency, bypassing traditional banking oversight. The case highlighted the use of Bitcoin for money laundering and fraudulent banking activities, raising significant legal and security concerns.

Bitcoin remains a controversial topic in counterterrorism discussions. While some experts argue that it is an unreliable and insignificant funding source for extremist groups, others highlight its risks, particularly in enabling anonymous financial transactions. Certain academics stress the growing threat of digital currencies in financing terrorism, warning against the potential consequences of unregulated cryptocurrency use.

The Financial Action Task Force (FATF) has issued warnings about the exploitation of cryptocurrencies in illicit financing, emphasizing the need for stricter regulatory oversight. However, some analysts believe that Bitcoin has not yet become the preferred or dominant financial tool for terrorist groups. Unlike traditional funding sources, cryptocurrencies still lack broad acceptance among extremist networks.





While Bitcoin is not currently the primary financial mechanism for extremist groups, its future role remains uncertain. The emergence of more advanced privacy-focused cryptocurrencies could make counterterrorism efforts more challenging. Enhanced encryption and anonymity features may provide new opportunities for terrorist organizations to evade financial monitoring systems.

In conclusion, despite its growing appeal among extremist supporters, Bitcoin has yet to replace traditional financing methods for terrorism. However, ongoing technological developments and increased privacy measures in digital currencies may reshape the landscape of terrorist financing in the future.

Crypto currencies and financial transactions are undeniably used by terrorist organizations as a means of securing and transferring funds. However, while digital currencies provide a degree of anonymity and the ability to bypass traditional financial restrictions, they are not the primary method of financing for extremist groups.

Crypto currencies serve as a tool that facilitates money transfers and fundraising, allowing terrorist organizations to partially evade regulatory scrutiny. However, the complete reliance of such groups on cryptocurrency remains unrealistic due to the limitations of the technology and the increasing global efforts to monitor illicit financial activities.

While terrorist organizations may attempt to utilize digital assets to exploit financial loopholes, crypto currencies remain a secondary rather than a primary financial instrument. Their role is supplementary, assisting in fundraising and money transfers, but they are not the dominant or irreplaceable component of extremist financing.

Crypto currencies remain merely a secondary and supplementary tool that certain individuals utilize. The lack of necessary infrastructure presents a significant challenge to their adoption, particularly as most terrorist organizations operate in impoverished regions such as the African coast, Yemen, Iraq, and Syria—areas that lack essential infrastructure, especially technological ones. This limitation significantly hinders the widespread adoption of crypto currencies, as without advanced infrastructure, large-scale usage remains unfeasible.

Moreover, crypto currency transactions are currently absent in these regions, further obstructing terrorists from leveraging them for financial transactions or acquiring essential resources. At present, terrorists primarily rely on circumventing global financial and legal systems to manage their funds, while crypto currencies remain in





their early stages as a secondary means of financing terrorism. However, could we eventually witness terrorist operations entirely funded by crypt currencies? And what stance do domestic and international legislators take on this issue?

Section Two: Legislation and Legal Framework

The stance of Arab legislators regarding digital currencies varies widely from one country to another, influenced by differences in economic policies, technological infrastructure, and approaches to regulating digital globalization. Some nations view cryptocurrencies as a financial tool that can be leveraged to boost economic growth and state revenues. In contrast, others have yet to legalize or properly regulate their use. Additionally, there are differences in the criminal classification of cryptocurrency-related activities, further highlighting the diverse regulatory landscape across the region.

However, a major concern for the governments of some countries is the use of crypt currencies in money laundering. Money laundering is a significant national and international issue due to its economic, political, and social consequences. This problem has intensified and become more complex with the rapid spread of crypt currencies and the limited ability to regulate them effectively (Sugeng Muntaha, Ade Saptomo, 2024).

Some define money laundering as the process of generating profits from illegal trade in a way that obscures the origins of the funds, while others view it as the act of concealing the sources of illicit money—such as proceeds from drug trafficking—by integrating them into legitimate investments.

Regarding the Egyptian legislation, Article 1, Paragraph (b) of Law No. 80 (2002) on money laundering defines it as:

(Any act involving the acquisition, possession, disposal, management, preservation, exchange, deposit, guarantee, investment, transfer, or manipulation of value if derived from a crime specified in Article (2) of this law, with knowledge of its illicit origin and with the intent to conceal the funds).

The Iraqi legislator stipulates that anyone who transfers, moves, or exchanges funds while knowing—or having reasonable grounds to know—that they are proceeds of a crime, with the intent of concealing or disguising their illicit origin, is guilty of money laundering. This also includes actions aimed at hiding or misrepresenting the truth regarding the source, location, condition, disposition, transfer, or ownership of these funds.





Money laundering has significant security, political, and economic repercussions. Economically, it contributes to a decline in national income levels due to capital flight from Iraq, leading to reduced domestic production and lower savings rates. One of its most critical consequences is the devaluation of the national currency and rising inflation rates, as capital outflows increase demand for foreign currencies, weakening the local economy.

Among the legislations that have imposed restrictions and penalties on such activities, the Egyptian legislator has explicitly criminalized dealings in digital currencies, including their issuance, trading, or promotion, due to the absence of a recognized legal framework for such transactions. Article (206) of the Central Bank and Banking Law prohibits the issuance, trade, or promotion of crypt currencies, as well as the establishment or operation of trading platforms or related activities, without prior authorization from the Central Bank's Board of Directors. This legal stance aims to mitigate the risks associated with individuals and institutions using digital currencies to bypass traditional financial regulations, which could facilitate financial crimes and illicit activities.

In the United Arab Emirates, during the early stages of digital currency adoption, the Governor of the Central Bank issued a warning in 2017 at the Islamic Financial Services Board Summit. He cautioned against the use of digital currencies due to the absence of operational licenses in the local market and the lack of government oversight, which could facilitate their use in illegal or illicit activities. At that time, there was no explicit legal provision prohibiting or criminalizing digital currencies; however, their use was discouraged due to financial and legal concerns (Qasim Farah, 2019).

Despite these initial warnings, the UAE pursued efforts to harness digital currency technology. The Ministry of Finance capitalized on this opportunity by collaborating with the Dubai Office for Smart Technology to launch a payment system based on Blockchain technology.

By 2022, the UAE took a more structured approach to digital currency regulation with the issuance of Law No. 4 (2022) concerning the regulation of virtual assets in Dubai. This law established the Dubai Virtual Assets Regulatory Authority (VARA)—an independent financial and administrative entity tasked with overseeing virtual asset transactions and ensuring compliance with regulatory frameworks.

The Algerian legislator has taken a clear stance on digital currencies, as outlined in Article (117) of the Algerian Finance Law, which completely rejects and





prohibits their use in all forms, including buying, selling, owning, and trading. However, enforcing this prohibition presents practical challenges due to the confidentiality, decentralization, and operational mechanisms of digital currencies, making it difficult to impose penalties and punitive measures effectively.

Similarly, the Hashemite Kingdom of Jordan has defined its position through a special circular issued by the Central Bank in 2021. This directive explicitly warned banks and financial institutions against engaging with cryptocurrencies in any capacity, including buying, selling, exchanging, futures trading, or investment. The prohibition was based on the need for caution to protect financial consumers, as these digital assets are not subject to any regulatory or legal oversight.

Many financial institutions and central banks worldwide have addressed the issue of digital currencies with caution, focusing on protecting consumers due to the risks and potential harm associated with these assets, which lack a legal and regulatory framework.

As for Iraq, a review of Central Bank Law No. (56) of 2004 and other applicable laws reveals that there is no explicit legal provision addressing or prohibiting digital currencies. However, the Central Bank of Iraq has previously issued warnings against dealing with them, citing the absence of legislation governing their use (Abood Al-Anzi, 2022). This suggests that while there is no formal prohibition, the Central Bank does not recognize digital currencies as legal tender. Nonetheless, this does not mean they are not considered assets, akin to gold or silver.

Therefore, the use of digital money is permissible as long as it is not employed for illegal purposes such as financing terrorism, money laundering, arms trafficking, extortion, or tax evasion. It appears that the Iraqi legislator has not overlooked this issue, as the Money Laundering Law explicitly states that its provisions apply to all illicit funds, including digital currencies.

Notably, the Money Laundering Law does not prohibit or restrict dealings in digital currencies outright. Instead, it focuses on regulating their use in illegal activities. Consequently, when digital money is utilized lawfully and legitimately, it falls outside the scope of this law's application.





CONCLUSION

The significance of this research lies in the necessity of defining crypto currency in societies. Governments may recognize it within a legal framework, but its misuse for criminal activities raises concerns about potential negative impacts.

Findings:

1. There is no universally accepted, comprehensive definition of crypto currencies. Instead, multiple definitions exist, each reflecting the entity's perspective defining them.

2. Crypto currencies are not a singular category; their types have evolved and continue to develop since their inception.

3. Crypto currencies possess various characteristics that have contributed to their widespread use and popularity, particularly among younger generations. Their global nature and lack of oversight make them easily tradable, yet this same feature presents risks, as they can be exploited for transnational criminal activities.

4. Countries have adopted differing stances on crypto currency trading. Some support it, others reject it outright, while some have yet to establish a clear position. As a result, several nations have not enacted legislation to regulate the mechanisms for adopting and using crypto currencies.

5. Crypto currencies contribute to an increase in high-risk crimes, including terrorism financing and money laundering, both of which can facilitate terrorist activities.

Recommendations:

1. Develop Comprehensive Laws and Regulations: Establish clear legal frameworks to regulate crypto currency usage and prevent their exploitation in terrorism financing and money laundering.

2. Enhance Criminal Investigation Capabilities: Provide specialized technical training for law enforcement and financial authorities to improve their ability to track and investigate crypto currency-related crimes.

3. Strengthen International Cooperation: Since terrorist financing and illicit cryptocurrency transactions often transcend borders, enhanced global collaboration among countries is essential for effective regulation and enforcement.





4. Leverage Advanced Technology: Utilize cutting-edge blockchain monitoring tools and data analytics to detect suspicious activities promptly and take swift action against illicit transactions.

5. Enact New Legislation: Some countries have introduced new laws to regulate and register crypto currency trading, ensuring better oversight and security in financial transactions.

REFERENCES

Abdullayev, R., Abdullayev, I., Kirillova, E., Plaksa, J., Shichiyakh, R., Stepanova, D. (2024). Cryptocurrency as a Socioeconomic Phenomenon. *Revista relações internacionais do Mundo Atual*, 2(44), 589-603.

Stokes, R. (2012). Virtual money laundering: the case of Bitcoin and the Linden dollar. *Information and Communications Technology Law*, 21(3), 221–236. <https://doi.org/10.1080/13600834.2012.744225>

Nagumanova, R., Plotnikova, L., Davletshina, A., Rubanov, V. (2025). Blockchain, Digital Assets and Currencies: Modern Aspects of Use and Accounting in the Russian Federation. *International Research Journal of Multidisciplinary Scope (IRJMS)*, 6(1), 579-593.

Sadegh Rajabi, M. (2023). The Legal Nature of Bitcoin and Its Compatibility with Different Natures. *Russian Law Journal*, XI(12), 559-570.

What are Stablecoins? (2022). CBINSIGHTS. Retrieved from: <https://www.cbinsights.com/research/report/what-are-stablecoins/>

Mohammed Al-Adailah, A.A. (2020). Virtual Digital Currencies: A Long Road to Terrorism Financing. *Journal of Al-Zaytoonah University for Legal Studies*, 1(1), 36.

Zohry, M., & Alsaied, M. (2021). The impact of Bitcoin Electronic Trust Factors on Hotel Transactions as a Mechanism for Digital Transformation in Egypt. *Journal of Association of Arab Universities for Tourism and Hospitality*, 0(0), 0–0. <https://doi.org/10.21608/jaauth.2021.75942.1177>.

Nouruldeen, S. (2018). The Impact of Bitcoin Mining and Virtual Currencies on the Stability of the Global Monetary System. *Afaq Ilmiya Journal*, 10(2), 221-222.

Abood Al-Anzi, H.W. (2022). Cryptocurrencies in the Balance of Iraqi and Comparative Law. *Al-Qurtas Journal for Economic and Commercial Sciences*, 2(3), 86.

Qasim Farah, A. (2019). Virtual Currencies in the United Arab Emirates: The Need for a Legal Framework to Address Their Risks—A Comparative Study. *University of Sharjah Journal*, 16(2), 712.

Article 1 of the Egyptian Anti-Money Laundering Law No. 80. (May 22, 2002). Retrieved from: <https://alp.unescwa.org/legislations/law-80-2002-promulgating-anti-money-laundering-law>





Sugeng Muntaha, & Ade Saptomo. (2024). Comparison Of Sanctions For The Crime Of Adultery In Toraja Customary Law And National Law In Indonesia. *Jurnal Hukum, Politik Dan Ilmu Sosial*, 3(1), 341–349. <https://doi.org/10.55606/jhps.v3i1.3385>

Europol. (2023). *Internet Organised Crime Threat Assessment (IOCTA)*. Publications Office of the European Union, Luxemburgo (pp. 1–63). Retrieved from <https://www.europol.europa.eu/sites/default/files/documents/iocta2018.pdf>

Raman, R., Kumar Nair, V., Nedungadi, P., Ray, I., & Achuthan, K. (2023, November 1). Darkweb research: Past, present, and future trends and mapping to sustainable development goals. *Heliyon*, 9. <https://doi.org/10.1016/j.heliyon.2023.e22269>

Vijayagopal, P., Jain, B., & Ayinippully Viswanathan, S. (2024). Regulations and Fintech: A Comparative Study of the Developed and Developing Countries. *Journal of Risk and Financial Management*, 17(8), 324. <https://doi.org/10.3390/jrfm17080324>

Gawer, A., Bonina, C. (2024). Digital platforms and development: Risks to competition and their regulatory implications in developing countries. *Information and Organization*, 34(3). <https://doi.org/10.1016/j.infoandorg.2024.100525>

Joebges, H., Herr, H. & Kellermann, C. (2025). Crypto assets as a threat to financial market stability. *Eurasian Economic Review*, 15, 473–502. <https://doi.org/10.1007/s40822-025-00311-4>

Law No. 4. (February 28, 2022). Regulating Virtual Assets in the Emirate of Dubai. Retrieved from: [https://dlp.dubai.gov.ae/Legislation%20Reference/2022/Law%20No.%20\(4\)%20of%202022%20Regulating%20Virtual%20Assets.html](https://dlp.dubai.gov.ae/Legislation%20Reference/2022/Law%20No.%20(4)%20of%202022%20Regulating%20Virtual%20Assets.html)

Hilal, W., Gadsden, S. A., & Yawney, J. (2022, May 1). Financial Fraud: A Review of Anomaly Detection Techniques and Recent Advances. *Expert Systems with Applications* 193. <https://doi.org/10.1016/j.eswa.2021.116429>

