Iranian Journal of International and Comparative Law
Volume 2, Issue 1, 2024

The Feasibility of Addressing the Financing of Terrorist Crimes in the Realm of Cryptocurrencies: The Experiences of Iran and Other Countries

Peyman Namamian

Associate Professor of Criminal Law and Criminology, Faculty of Administrative Sciences and Economics, University of Arak, Arak, Iran. | p-namamian@araku.ac.ir

Article Info

Article type:
Research Article

Article history:
Received
13 June 2014

Received in revised form
28 June 2024

Accepted
28 June 2024

Published online
30 June 2024

https://ijicl.qom.ac.ir/article_2993.html

Keywords:
Cryptocurrencies,
Virtual Currency,
Blockchain Technology,
Digital Crimes,
Financing of Terrorist Crimes.

ABSTRACT

Cryptocurrencies, despite their ambiguous nature, represent one of the most significant new phenomena in the global economy. Since the introduction of the first cryptocurrency, Bitcoin, in 2009, terrorist groups have increasingly utilized these currencies to finance their activities. Consequently, states, organizations, and financial institutions have been compelled to adopt effective anti-terrorist financing strategies in response to this development. This research examines a range of issues related to cryptocurrencies, their utilization in terrorist financing, and the associated benefits and risks. Within the context of Iran's regulatory framework, existing policies and measures to combat the financing of terrorist crimes through cryptocurrencies have led to challenges characterized by conflicting and fragmented approaches to the regulation of cryptocurrency exchanges and mining, both theoretically and practically, which include the illegitimacy of exchange activities. Internally, the Central Bank has issued directives aimed at clarifying this phenomenon and has sought demands from higher authorities, particularly the Islamic Council. In contrast, other countries, such as China, have adopted a dual policy, prohibiting the use of cryptocurrencies in monetary and banking contexts. Notably, nations like Canada and the United States have established specific legal regulations and policies governing Bitcoin usage, while Japan has developed regulations for virtual currency exchange service providers, including mechanisms for identifying violators through guaranteed criminal enforcement.

Cite this article: Namamian, P. (2024). "The Feasibility of Addressing the Financing of Terrorist Crimes in the Realm of Cryptocurrencies: The Experiences of Iran and Other Countries", *Iranian Journal of International and Comparative Law*, 2(1), pp: 55-67.

10.22091/ijicl.2024.11013.1098
Publisher: University of Qom

Table of Contents

Introduction

Terrorist crimes, as a global phenomenon, have raised significant concerns for states as well as regional and international organizations, particularly as terrorist groups employ diverse methods to operate and finance their activities. In response to technological advancements, these groups have refined their operational techniques, especially in terms of financing.[1]

Cryptocurrencies and digital assets are increasingly scrutinized, not only by law enforcement and regulatory authorities but also by public opinion. While digital assets provide numerous benefits and opportunities for legitimate financial transactions, their emergence has simultaneously created new pathways for illicit activities.[2]

Cryptocurrencies[3] fall under the broader category of virtual currencies. The term "virtual currencies," when used independently, refers to any currency that exists solely in electronic form, lacking any official physical representation.[4] A virtual currency is defined as a digital representation of value that can be traded electronically and functions as a medium of exchange, a unit of account, or a store of value. However, it does not possess the legal status of traditional currency in any country; such operations can only occur with societal consent among users of virtual money.[5]

---

1 Dyntu & Dykyj, *Cryptocurrency as an Instrument of Terrorist Financing* (2021) 92-9; Terrorist groups have swiftly adopted cryptocurrencies to raise funds more efficiently than ever before. They have demonstrated the ability to collect substantial crypto donations in short periods, significantly reducing the time required for fundraising compared to traditional methods. While current cryptocurrencies may not entirely meet the specific requirements of terrorist groups, they can still be used for certain financial activities. However, the emergence of a widely adopted cryptocurrency that offers improved anonymity, security, and minimal regulation could increase its utility for terrorist organizations. Effective regulation, oversight, and international cooperation between law enforcement and intelligence agencies are crucial in preventing terrorists from exploiting cryptocurrencies to fund their operations.

2 Reuters, 'FTX Founder Sam Bankman-Fried Thought Rules Did Not Apply to Him, Prosecutor Says' (2 November 2023) https://www.reuters.com/legal/ftx-founder-sam-bankman-fried-thought-rules-did-not-apply-him-prosecutor-says-2023-11-02/.

3 It was first launched in late 2009, when a person or a group of persons known by the pseudonym "Satoshi Nakamoto," created a digital currency called "Bitcoin" The word "Bitcoin" is composed of two English words: "bit", which means information unit, and "coin", which means currency.6 Accordingly, the term "Bitcoin" refers to a currency taking the form of an "electronic information unit" that is issued and traded without oversight by any centralized authority or institutions. This coin preceded other types of cryptocurrencies, such as Ethereum, Tether, Solana, Zilliqa, and Dash,etc. Additionally, there are thousands of different cryptocurrencies.

4 Maddi, Ghaemi-Khargh, and Shafi'i, *Legal Jurisprudence Inquiry on the Issue of Legalization of Encrypted Currencies* (1400) 105/307-306.

5 Financial Action Task Force, 'Virtual Currencies – Key Definitions and Potential AML/CFT Risks' <http://www.fatf-gafi.

Cryptocurrencies have ushered in a transformative era within the financial landscape, enabling innovative opportunities while also presenting unique challenges. Amid these advancements, a troubling trend has emerged: the exploitation of cryptocurrencies by terrorist organizations to finance their illicit activities. The decentralized and anonymous nature of these digital assets provides fertile ground for covert fund transfers across borders, circumventing traditional regulatory frameworks and surveillance mechanisms. [1] Consequently, investigating and prosecuting cases of cryptocurrency-based terrorist financing has become a complex undertaking, necessitating novel approaches within the realm of international criminal law.[2]

The rapid convergence of virtual currencies and assets with the mainstream financial system has blurred the distinctions between physical and virtual assets/currencies. This merging has resulted in a marked increase in instances of money laundering, transnational organized crime, and terrorism financing facilitated by illicit cryptocurrencies, thereby raising concerns regarding the effectiveness of regulatory measures governing the "virtual currency/asset" domain. Furthermore, limited expertise in technology-based law enforcement and a growing sense of impunity exacerbate the challenges faced by criminal justice administration.[3]

The United States defines virtual currencies as "a digital representation of value that functions as an intermediary of exchange, measure of value, or store of value."[4] Similarly, the Central Bank of the European Union characterizes virtual currencies as "a digital representation of value that is not issued by a central bank or public institution and is not necessarily based on a credit currency; it is utilized by natural or legal persons as a means of exchange and can be transmitted, stored, or exchanged electronically."[5]

---

org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potentialaml-cft-risks.pdf>

1 Since the emergence of Bitcoin in 2009, cryptocurrencies have garnered significant attention as a form of internet-native money, promising to create financial systems that are more free, fair, and transparent. However, the use of cryptocurrencies by terrorist organizations has emerged as a pressing concern for regulators and policymakers globally. While visionaries see potential for positive change, terrorist groups have also recognized the opportunities offered by cryptocurrencies in their fundraising and financing operations, prompting the need for tighter oversight of these digital currencies that operate outside the control of any government.

2 Prosecuting terrorist financing poses significant challenges within the international criminal law framework, particularly under the jurisdiction of the International Criminal Court (ICC). The absence of a universally accepted definition of terrorism hampers the identification and prosecution of individuals involved in financing terrorist activities. Additionally, proving the specific intent and connection between the accused and the financed terrorist acts presents evidentiary difficulties. The ICC's limited resources and focus on other core crimes further constrain its capacity to effectively investigate and prosecute complex cases of terrorist financing. To overcome these challenges, exploring the concept of universal jurisdiction emerges as a potential solution. Embracing universal jurisdiction would allow states to collectively address the issue of prosecuting terrorist financing, regardless of an international consensus on the definition of terrorism. By adopting this approach, states can exercise their authority to investigate and prosecute cases with transnational dimensions, enhancing flexibility and responsiveness in combating these crimes. Furthermore, to address the gaps in the existing legal framework, alternatives for prosecuting terrorist financing under the ICC should be considered. This may involve amending the Rome Statute to include a provision explicitly addressing the crime of terrorist financing or interpreting existing crimes under the ICC's jurisdiction to encompass acts of terrorist financing (Kenny, 2019: 134-136).

3 Varun, *Prospects and Models of Combating Cryptocurrency Crimes' eucrim* (14 March 2024) https://eucrim.eu/articles/prospects-and-models-of-combating-cryptocurrency-crimes/.

4 Rajabi, *Virtual Currency: Legislation in Different Countries and Proposals for Iran* (2017) 3

5 European Central Bank, 'Opinion on Virtual Currencies' (2014) European Banking Authority 4. Europe has 31% of total cryptocurrency holders, followed by Asia and Oceania 28,7%, North and South America 28,3%, and finally Africa with the Middle East at 10,7%. These rates may go up and down from time to time; as per the most updated report for 2023, cryptocurrency adoption rates increased in certain region and declined in others; However, countries differ in their recognition of digital currencies. Some countries, including China, oppose them. While others have officially adopted them and even enacted specific laws to regulate cryptocurrencies, such as Ukraine, where the president of Ukraine legalized cryptocurrencies in March 2022, which helped strengthen the Ukrainian military supplies. Meanwhile, many other countries are still cautious about cryptocurrencies. The International Monetary Fund (IMF) warned against the total-legalization of cryptocurrencies, given their risks for financial stability; not only so, the IMF also urged El Salvador to ditch Bitcoin's legal tender status; Sénat No 820, Session Extraordinaire de 2021-2022, Proposition de Résolution : tendant à la création d'une commission d'enquête sur les crypto-actifs, présentée par Nathalie GOULET, p 6 -7. The top five countries in terms cryptocurrency holders in 2023 are: India, Nigeria, Vietnam, the United States, and Ukraine; Chainalysis Report, The 2023 Global Crypto Adoption Index: Central & Southern Asia Are Leading the Way in Grassroots Crypto Adoption, September 12, 2023.

In Iran, the central bank, as a specialized institution, classifies cryptocurrency as a type of financial asset. In Japan, the monetary law defines money as coins or paper currency issued by the Bank of Japan, with the authority for issuance and circulation granted to the government. However, since virtual currencies are issued by private entities, they do not conform to the definition established by Japanese currency law.[1] Consequently, the ambiguities surrounding the legal definitions of virtual currencies in Iran[2] and other jurisdictions can lead to criminal activities in the context of cryptocurrencies. It is imperative to adopt legislative measures that provide a precise definition of virtual currencies and address the criminalization of related offenses.

This research employs a comparative approach, utilizing descriptive and analytical methods to explore the feasibility of addressing the financing of terrorist crimes in the context of cryptocurrencies. The primary question guiding this inquiry is whether existing laws and regulations allow for the effective combat of terrorism financing within the realm of cryptocurrencies. The forthcoming sections will examine the regulatory frameworks of Iran and other countries, including China, Canada, the United States, and Japan, focusing on their respective approaches and policies regarding cryptocurrencies and the financing of terrorist crimes. Ultimately, this study aims to ascertain the possibility of effectively countering the financing of terrorist activities through cryptocurrencies in Iran and other nations within this ecosystem.

For the purposes of this study, methodologies employed include scientific abstraction, synthesis, observation, generalization, and the induction of literature and legal documents to elucidate the characteristics of Bitcoin, as well as strategies for promoting and preventing its use in financing terrorism.

1. Intrastate and International Legal Challenges

While traditional currencies, such as coins or banknotes, are issued by official financial authorities or institutions that regulate their circulation at both domestic and international levels, electronic cryptocurrencies operate outside such regulation and control. This lack of oversight pertains to their issuance, movement, and the identities of cryptocurrency users, a situation attributed to the encryption and anonymity that characterize this form of currency. The term "encryption" refers to the use of specific characters, digits, and codes that preserve message anonymity; thus, cryptocurrencies can be understood as concealed electronic representations of value, derived from the concept of “cryptography.”[3] Some researchers argue that the term “Crypto” has its origins in ancient Greek, specifically from "Kruptosgraphein": “Kruptos” meaning hidden, and “graphene” meaning writing. Therefore, virtual cryptocurrencies are not coins or banknotes; rather, they

1 Ishikawa, *Designing Virtual Currency Regulation in Japan: Lessons from the Mt Gox Case* (2017) 126.

2 Iran's legislature has yet to take meaningful action to regulate virtual currencies. The central bank has issued only brief and conflicting guidelines, leading to societal confusion and hindering the population's ability to benefit from cryptocurrencies. This lack of clear legislation and ongoing oversight has also contributed to an environment conducive to the spread of related crimes.

3 Cryptocurrencies have emerged as a novel method for criminals to finance a wide range of illicit activities, including terrorist fundraising beyond national boundaries. Evidence indicates that certain terrorist organizations are utilizing cryptocurrencies as a means to raise funds.

serve as digital money functioning similarly to traditional currencies for payment and exchange purposes, and they provide access to various services.

To comprehend the nature and functions of these currencies, one researcher has offered the following definition: they are virtual currencies detached from the socio-institutional environment, reliant on encryption (hidden writing: cryptography), and operate in a decentralized manner.[1, 2]

The exchange, extraction, and utilization of cryptocurrencies, like any other tool, can facilitate legitimate uses as well as criminal activities, thereby becoming a subject of criminological research. Notably, cryptocurrencies have been exploited to facilitate criminal activities that transcend domestic borders.

The advancements in this area, particularly concerning illegal actions, may exacerbate the threats associated with virtual currencies. Key factors contributing to this situation include: the high level of privacy and anonymity provided by virtual currencies; the widespread adoption by terrorists of encryption technology, social media, and other online platforms; the connections between terrorist actors and other criminal enterprises; and the rapid pace of innovation and adoption of virtual currencies.[3]

This article examines the feasibility of addressing and punishing criminals to ensure financial security and protect individuals' capital, utilizing both domestic and international laws. It appears that the absence of legislative policies and the lack of recognition of cryptocurrencies within domestic and international legal frameworks create a conducive environment for crimes against public safety, including the financing of terrorism and fraud. Consequently, the criminal justice system's capacity to prevent and address such crimes faces significant challenges and obstacles.[4]

In addition to the range of crimes that can be perpetrated domestically and internationally using cryptocurrencies, many cryptocurrencies are created without adequate financial and informational backing, and their trading on domestic and international exchanges is increasing daily.[5] Moreover, some of the largest historical frauds on an international scale have occurred within this space.[6]

However, effective criminal prevention measures can be implemented through the establishment of criminal and legislative policies that address the challenges posed by virtual currency technologies under domestic and international law. Given the dynamic nature of cyberspace, its political and security sensitivities, and the technical complexities involved, regulation in this area necessitates heightened attention. The criminal capacities of this domain have become a priority

1 Paul Pons, *Les Cryptomonnaies Impasse ou Révolution?* (2019) 71.

2 Of course, the features and technical criteria that can be raised regarding crypto currencies are as follows: 1. Cryptocurrencies set an example of rapid qualitative development, and constitute a significant shift in dealing with currencies as a medium of payment and exchange. 2. Compared to other currencies, cryptocurrencies are distinguished by a greater degree of secrecy and security in trading and exchange processes. 3. Cryptocurrencies are not subject to oversight by any centralized authority or institutions; therefore, they are not taxable, which makes them more attractive both to individuals and corporates. 4. The strength and risk of cryptocurrencies, as encrypted electronic information unit, lies in the fact that it would be almost impossible to remove or alter their encrypted information on the web, or prevent its circulation.

3 Keatinge, Carlisle, Keen, *Virtual Currencies and Terrorist Financing: Assessing the Risks and Evaluating Responses* (2018) 9.

4 It should be noted that "cryptocurrency-powered cybercrime has attracted some actors who intend to cause widespread disruption and need financing; "For example, North Korea is increasingly looking to cybercrime to raise funds in its efforts to escape impunity." (Collins, 2017: 54)

5 Stroukal and Nedvedova, 2016: 45

6 See: Marjan Sheikhi, 'The Biggest Cryptocurrency Scams in History' *Zoomit* (2 June 2021) https://www.zoomit.ir/economics/371412-biggest-cryptocurrency-scams.

for various criminal policy systems. Consequently, policymakers are developing legislative criminal policies to regulate the multifaceted aspects of delinquency, including technological offenses. This dimension of criminal policy plays a strategic role in formulating preventative and countermeasure programs against criminal phenomena, as it entails planning, modeling, and presenting actionable strategies for criminal justice system stakeholders.[1]

The challenges facing the criminal justice system in addressing and penalizing criminal actions related to cryptocurrencies, including the financing of terrorism, underscore the necessity for comprehensive legislative measures and broad criminalization. Thus, a comparative analysis of the challenges faced by Iran's criminal justice system in prosecuting virtual currency-related crimes, alongside an examination of the operational frameworks in countries such as Japan and the United States, will further illuminate these challenges. Key issues include ambiguities in the legal status and scope of criminal activities, the difficulty of adhering to existing laws, the need for cooperation with foreign nations and international institutions for information exchange regarding virtual currencies, the establishment of memoranda of understanding between private and public sectors, and the training of judges and judicial officers in this evolving field.[2]

2. Approaches and Policies

Some countries have enacted strict laws to ban Bitcoin, consequently limiting its use by consumers and merchants. This approach has been notably adopted by China, which views virtual currencies as unnecessary. China has implemented stringent regulations prohibiting Bitcoin as a currency or financial system. Specifically, "China[3] has prohibited the collection of financial aid through organized Internet crimes for all natural and private persons while banning the activity of cryptocurrency exchanges and blocking their use."[4,5]

In contrast, the United States and Canada have established specific regulations and legislative policies regarding Bitcoin. These countries have identified laws related to money laundering and reporting obligations to the Financial Crimes Enforcement Network (FinCEN) in the U.S. and the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) for users of virtual currencies. They have adapted existing laws to encompass Bitcoin. "America[6] and Canada,[7] through various laws and new regulations, have implemented controls on exchange systems (such as virtual currency exchanges) and businesses that buy, sell, or accept Bitcoin as a means of transaction."[8] These measures aim to mitigate illegal activities through virtual

1 Shamlou and Khalilipachi, *Criminal Risk-Based Policymaking Against Virtual Currency Technology* (2019) 247/103.
2 Nabavi and Saber, *Comparative Study of the Challenges of Iran's Criminal Justice System in the Proceedings of Crimes Related to Virtual Currencies* (1399) 179/1.
3 See: L. Rosini, 'Author Archive' *Virtual Currency Report* https://www.virtualcurrencyreport.com/author/lrosini/.
4 Suberg, *Bank Complete: China Blocks Foreign Crypto Exchanges to Counter Financial Risks* (2018) 12.
5 Bitcoin has a number of features that have attracted the attention of criminals as a way to evade responsibility for a crime.
6 The Financial Crimes Enforcement Network has the mission of protecting the financial system from illegal use and combating money laundering and promoting national security through the collection, analysis and dissemination of financial information and the strategic use of financial authorities. This network fulfills its mission by receiving and maintaining financial transaction data. The analysis and dissemination of that data is done for the purposes of law enforcement and establishing global cooperation with peer organizations of other countries and international institutions.
7 The Financial Crimes Enforcement Network has the mission of protecting the financial system from illegal use and combating money laundering and promoting national security through the collection, analysis and dissemination of financial information and the strategic use of financial authorities. This network fulfills its mission by receiving and maintaining financial transaction data. The analysis and dissemination of that data is done for the purposes of law enforcement and establishing global cooperation with peer organizations of other countries and international institutions.
8 Marini, *Regulation and Innovation: Public Authorities and the Development of Virtual Currencies* (2014) 21.

currencies, including money laundering. "Thus, the two countries exhibit differing perspectives on the use of virtual currencies in both legal and illegal contexts."[1,2]

Japan has also developed regulations for virtual currency exchange service providers. Under these rules, activities involving the buying and selling of virtual currencies, converting them into other virtual currencies, and managing users' virtual currencies require a license. Violations can lead to imprisonment, monetary fines, or cancellation and suspension of exchange activities.[3] However, none of these countries have officially recognized Bitcoin and other cryptocurrencies as legal tender.

"The regulation and implementation of laws regarding virtual currencies are promising, given their potential for illegal use and unique features such as anonymity and decentralization. Nevertheless, regulatory bodies in countries like the United States and Canada must ensure that the benefits of Bitcoin for merchants and users are not undermined by excessive regulation."[4]

3. The Legal and Technical Framework of Confrontation

The rise of cryptocurrencies has presented significant challenges for regulatory bodies, particularly as instances of their use for illegal purposes have emerged. To effectively address terrorist financing in the context of cryptocurrencies, it is essential to identify concrete examples.[5]

In Iran, anti-money laundering laws prohibit any criminal actions aimed at financing terrorist activities.[6] Terrorist groups are increasingly employing new tools and methods to secure their financial resources, with the Internet being one of the primary means at their disposal.[7] The cross-border nature and anonymity of virtual currencies, coupled with the lack of oversight over their transactions, facilitate the financing of terrorist organizations.[8]

---

1 Grinberg, *Bitcoin: An Innovative Alternative Digital Currency* (2011) 63.

2 On March 4, 2024, the Executive Office of the Counter-Terrorism Committee (CTED) of the United Nations Security Council hosted an important discussion on the latest trends and changes in the use of various types of virtual assets by ISIS-affiliated terrorist groups, al-Qaeda and their supporters, including for fundraising campaigns. The session provided member states with practical insight into how virtual assets are being used for terrorist financing purposes and how related technologies, including blockchain analytics, can help identify and suppress such abuses. Amidst ongoing work on drafting non-binding guidelines on measures to prevent and counter terrorist use of new payment technologies and fundraising methods based on the Delhi Declaration of the Counter-Terrorism Committee, this meeting It provided member states with practical insights on how to use virtual assets. for the purposes of terrorist financing, and how related technologies, including blockchain analytics, can help identify and suppress such abuses. Despite these trends, which indicate the increasing misuse of virtual assets by terrorist groups and their supporters, the majority of funds used for terrorist financing purposes are still collected and moved through cash, remittance services, and traditional financial institutions. Experts emphasized that digital currency transactions are traceable and immutable, meaning that blockchain intelligence can identify, track and trace the flow of funds transferred through such transactions in ways that are not possible with cash and other methods; https://www.un.org/securitycouncil/ctc/news/cted-hosts-insight-briefing-%E2%80%9Clatest-trends-use-cryptocurrency-terrorist-groups-and-their

3 Ishikawa, Op. Cit. (2017) 129.

4 Ly, *Coining Bitcoin's Legal Bits: Examining the Regulatory Framework for Bitcoin and Virtual Currencies* (2014) 608.

5 In October 2022, the UN Counter-Terrorism Committee Executive Directorate estimated that crypto was used to finance as many as twenty per cent of all terrorist attacks, up from approximately five per cent a few years ago; https://www.ifcreview.com/articles/2024/january/tackling-the-role-of-crypto-in-terrorist-financing/

6 "There are many terrorist groups that use cryptocurrencies for their massive fund-raising investments, such as ISIS, Mujahideen Council, Al-Qaeda, etc. "Due to external pressures such as loss of territory and limited financial regulation, diverse terrorist groups are building their financial portfolios through the dark web and cryptocurrencies to survive." (Zahirah and Ridwan, *The Utilization of Cryptocurrencies by the Terrorist Group as an Alternative Way of Hawala for Illicit Purposes* (2019) 10)

7 Entenmann and Van Den Berg, *Terrorist Financing and Virtual Currencies: Different Sides of the Same Bitcoin?* (2018).

8 A report by the Regional Office of the United Nations Office on Drugs and Crime for Southeast Asia and Oceania released on January 15, 2024 indicated that casinos are the main drivers of money laundering, underground banking and cyber fraud in East and Southeast Asia. Is. In fact, analysis by the United Nations Office on Drugs and Crime estimates that as of early 2022, more than 340 land-based casinos, both licensed and unlicensed, were operating in Southeast Asia, most of them in Online, they started live streaming and betting services. However, the formal online gambling market is expected to grow to more than $205 billion by 2030, with the Asia Pacific region expected to account for the largest share of market growth between 2022 and 2026, with a projected 37%. This study describes several policy developments and enforcement actions implemented by governments in the region to address the illicit casino-based capital flows, corruption, and money laundering that have partially fueled these trends;https://www.unodc.org/roseap/en/2024/casinos-casinos-cryptocurrency-underground-banking/story.html

As noted by Siahbidi-Kermanshahi and Tahal-Muayed (2016),[1] "If the fight against crimes in the context of cryptocurrencies develops to such an extent that the perpetrators are deprived of the possibility of laundering the proceeds of illegal acts, the commission of the crime will be practically useless." In essence, if criminals are unable to integrate illegal income into the legal financial system for legitimate or illegitimate purposes, such as financing terrorism, the incentive to commit these crimes diminishes.[2,3]

To understand how virtual currencies can be a primary means of financing terrorist crimes, two key aspects must be continuously examined. First, it is crucial to investigate how financial technologies, similar to virtual currencies, have successfully prevented illegal financial activities and, specifically, the financing of terrorism. Second, understanding the reasons behind the attraction of criminal groups to virtual currencies will help determine whether terrorists will continue to use them as other criminals do.

Adopting new strategies to better identify and disrupt terrorist financing through virtual currencies in the current digital financial landscape is imperative. Policy leaders must consider several fundamental principles that, if embraced, will significantly enhance the capacity to counter the terrorist use of virtual currencies. Governments should adopt three core principles at the highest levels and communicate these clearly to the private sector:

a. Prioritizing the financing of terrorist activities and other financial crimes, particularly via new virtual currencies;
b. Creating a policy and regulatory environment that fosters innovation;
c. Developing new strategies and legal tools for improved coordination, especially between public and private sectors.[4,5]

The use of virtual currencies in the United States has been reported as a method to evade government taxes by converting income into virtual currency and transferring it to foreign accounts. Concerns regarding the use of virtual currencies for financing terrorist activities, human trafficking, and sexual exploitation remain significant for governments and international institutions, especially in the United States and Canada.[6]

Global interest in combating the financing of terrorism surged after the events of September

1 Siahbidi-Kermanshahi and Tahal-Muayed, *Economic Criminal Law of Money Laundering* (2016).

2 "Given the key role of funding in supporting terrorist acts, counterterrorism efforts, particularly the financial sub-category of counterterrorism, often focus on tracking the flow of money through bank accounts and preventing financial transactions that may be used to support attacks. "However, the success of counterterrorism financial strategies in reducing terrorists' access to fiat currencies has raised concerns that terrorist groups may increasingly use digital cryptocurrencies such as Bitcoin to support their activities." (Dion-Schwarz, Manheim, B. Johnston, 2019: 3)

3 Goldman et al., *Terrorist Use of Virtual Currencies; Containing the Potential Threat* (2017).

4 Ibid, 33.

5 In the context of the Terrorist Financing Convention, the financing of terrorist crimes is explicitly considered a crime. The elements agreed upon in various definitions of terrorism include the use of unlawful violence or the threat thereof, terrorizing individuals, and surprising a target by harming, killing, or destroying it, whether it is a civilian or military target. As for the definition of the crime of terrorism financing, the Arab Convention on Combating Money-Laundering and the Financing of Terrorism stipulates that the following are criminalized acts of terrorism financing: 1. The provision of funds under any name in the knowledge that they will be used to finance terrorism; 2. The acquisition or collection of funds by any means with the intention that they should be used to finance terrorism; 3. The possession or holding of funds, or managing the investment thereof, in the knowledge that they are to be used to finance terrorism.15 Some have defined the crime of terrorism financing as "collecting, providing, or transferring funds by any means, directly or indirectly, in the knowledge that they are to be used, in full or in part, to finance terrorism according to the definitions of terrorism contained in the Arab convention."(Bahamaoui, *Mechanisms for Drying up Sources of Funding for Terrorist Groups* (2017) 71)

6 Kethineni and Dodge, *Use of Bitcoin in Darknet Markets: Examining Facilitative Factors on Bitcoin-Related Crimes* (2017) 90.

11, 2001, as the increasing activity of terrorist groups raised international concerns about their funding sources. The emergence of cryptocurrencies in 2009 introduced new challenges in the fight against terrorism financing, as these digital currencies operate through decentralized, encrypted protocols that allow for anonymity.

Addressing the financing of terrorism through cryptocurrencies involves several key aspects, notably legislative and procedural or technical measures. Given that cryptocurrencies lack a formal legal framework and central mechanisms for tracking transactions, countries and organizations have been compelled to enact legislation to mitigate the risks associated with their use in money laundering and terrorism financing.

The International Convention for the Suppression of the Financing of Terrorism highlights these challenges, noting that existing multilateral legal instruments do not explicitly address terrorism financing. The convention emphasizes the urgent need for enhanced international cooperation to devise effective measures for preventing and prosecuting terrorist financing.[1] Each State Party is mandated to take appropriate steps to identify, detect, freeze, or seize funds used for terrorist activities, including proceeds from such offenses, for potential forfeiture to compensate victims.[2]

The United Nations resolution on combating the financing of terrorism, adopted in 2001, further underscores the commitment to address all forms of terrorism financing. This resolution, issued under Chapter VII of the UN Charter following the September 11 attacks, emphasizes the need for international collaboration, particularly in Articles 1, 2, and 3. Organizations like the Financial Action Task Force (FATF), also known by the abbreviation GAFI "Le Groupe d'action financière",[3] play a crucial role in monitoring and preventing money laundering and terrorism financing, including through cryptocurrencies. Additionally, firms such as Chainalysis provide blockchain analysis to aid these efforts.[4]

National and international authorities are intensifying efforts to trace cryptocurrencies used for financing terrorism and to identify involved parties. Combating terrorism requires a holistic approach that extends beyond financial suppression to address the multifaceted dimensions of the phenomenon, including ideological, religious, economic, social, and political factors. A comprehensive strategy should include:

1. Reforming sources of terrorist ideology, such as educational institutions and associations.
2. Developing communities and regions that are breeding grounds for terrorism.
3. Cutting off funding sources.
4. Addressing political conditions and differences that foster extremism.
5. Utilizing force to confront armed terrorists.

In Iran, unauthorized electricity use for cryptocurrency mining has led to significant issues, prompting police seizures of Bitcoin mining farms. The unauthorized use of electricity, often

1 International Convention for the Suppression of the Financing of Terrorism, 1999.
2 Ibid., Article 8.
3 'Accueil' *Groupe d'action financière (GAFI)* https://www.fatf-gafi.org/fr/home.html.
4 For more information, visit https://www.chainalysis.com

linked to industrial operations, is criminalized under laws governing resource theft, ensuring stringent penalties.[1]

Strengthening international collaboration is essential for effectively addressing the challenges posed by cryptocurrencies in financing terrorism. Establishing robust asset confiscation and recovery systems at both national and international levels can act as a deterrent against organized crime and protect the integrity of financial markets. Additionally, capacity building for law enforcement is critical, necessitating specialized units equipped to investigate virtual currency-related crimes. Public awareness campaigns about the risks associated with cryptocurrencies can empower individuals to make informed decisions and contribute to crime prevention. [2]

Legislative efforts to combat terrorism financing, particularly concerning cryptocurrencies, align with relevant multilateral conventions and UN resolutions. Early initiatives to address cryptocurrencies' involvement in financing terrorism are also evident. Developed countries, such as the United States and those in Europe, have more resources and capabilities to combat this issue effectively, benefiting from centralized technology and advanced intelligence mechanisms.

Conclusion

The rise of cryptocurrencies has created new opportunities for terrorist organizations to exploit digital assets for financing their activities. The unique nature of cryptocurrencies, characterized by confidentiality and anonymity, poses significant challenges in combating terrorism financing. The complexity and global reach of these encrypted currencies complicate crime detection and enforcement efforts, particularly in Iran and other countries. Non-criminal prevention measures, such as technological and situational interventions, may offer greater efficiency and effectiveness than traditional criminal responses. This underscores the need for legislative policies that respect the principle of legality in defining crimes and punishments.

The challenges and opportunities presented by cryptocurrencies transcend national borders, reflecting the broader implications of globalization and technological advancement. Transnational crimes, including money laundering and terrorism financing, require countries to respond under their national laws, which often lack the necessary scope to address these cross-border issues. Thus, an international collaborative approach is essential for effectively combating transnational crimes.

In Iran, it is crucial to adopt robust legislative and criminalization policies to address these challenges. Establishing a clear legal framework for the use and exchange of cryptocurrencies is vital for combating internet fraud, money laundering, and terrorism financing. This framework will enhance the capabilities of law enforcement agencies to detect and pursue crimes within both domestic and international jurisdictions.

A comparative study of the legislative policies in developed countries reveals that risk-oriented approaches to anti-money laundering, in line with the requirements of the Financial Action Task Force (FATF), are essential. These approaches include monitoring, licensing,

1 Nabavi and Saber, Op. Cit. (1399) 1/189.

2 Varun VM, 'Prospects and Models of Combating Cryptocurrency Crimes: The India-EU Dialogue as a Perspective?' *eucrim* (2024) https://doi.org/10.30709/eucrim-2023-032.

record-keeping, and international cooperation to mitigate the criminal risks associated with virtual currencies. Iranian lawmakers should draw on the experiences and policies of leading countries, such as Canada, the United States, Japan, and China, while adapting these strategies to fit domestic legal principles.

While these countries have recognized the need to regulate cryptocurrency exchanges and mining, they have yet to establish comprehensive legislative frameworks that provide the necessary criminalization and enforcement measures. Addressing these gaps is critical to effectively countering the misuse of cryptocurrencies in financing terrorism and other illegal activities.

References

Books

Siahbidi Kermanshahi S and Tarhimmoyed AA, *Economic Criminal Law of Money Laundering* (1st edn, Mizan 2017) [In Persian].

Abbasi A, *Economic Criminal Law of Money Laundering; Combating Money Laundering in International Documents and Iran's Legal System* (1st edn, Mizan 2016) [In Persian].

Dion-Schwarz C, Manheim D and Johnston P B, *Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats* (RAND Corporation 2019).

Goldman Z K et al., *Terrorist Use of Virtual Currencies; Containing the Potential Threat* (Energy, Economics & Security 2017).

Keatinge T, Carlisle D and Keen F, *Virtual Currencies and Terrorist Financing: Assessing the Risks and Evaluating Responses* (European Union 2018) https://www.europarl.europa.eu/RegData/etudes/STUD/2018604970//IPOL_STU(2018)604970_EN.pdf.

Articles

Bahamaoui C, 'Mechanisms for Drying up Sources of Funding for Terrorist Groups' (2017) *Afak Ilmia Journal* 13: 5874-.

Shamlou B and Khalili Pachi A, 'Criminal Risk-Based Policymaking Against Virtual Currency Technology' (2019) *Majlis and Strategy* 27(103): 247278-. [In Persian]

Madadi M, Qaemi-Khargh M and Shafi'i Q, 'Legal Jurisprudence Inquiry on the Issue of Legalization of Encrypted Currencies' (2021) *Majlis and Strategy* 28(105): 334303-. [In Persian]

Nabavi M and Saber M, 'Comparative Study of the Challenges of Iran's Criminal Justice System in the Proceedings of Crimes Related to Virtual Currencies' (2019) *Comparative Law Research* 24(1): 183209-. [In Persian]

Bollen RA, 'The Legal Status of Online Currencies – Are Bitcoins the Future?' (2016) *Melbourne Business School, Financial Institutions, Regulation & Corporate Governance (FIRCG) Conference*.

Dyntu V and Dykyj O, 'Cryptocurrency as an Instrument of Terrorist Financing' (2021) *Baltic Journal of Economic Studies* 7(5): 89121-.

Grinberg R, 'Bitcoin: An Innovative Alternative Digital Currency' (2011) *Hastings Science and Technology Law Journal* 4.

Kenny C, 'Prosecuting Crimes of International Concern: Islamic State at the ICC?' (2019) *Utrecht Journal of International and European Law* 33(84): 120–145.

Kien-Meng Ly M, 'Coining Bitcoin's Legal Bits: Examining the Regulatory Framework for Bitcoin and Virtual Currencies' (2014) *Harvard Journal of Law and Technology* 27(2).

Irwin AS M and Milad G, 'The Use of Crypto-Currencies in Funding Violent Jihad' (2016) *Journal of Money Laundering Control* 19(4).

Silalahi Nuth M, 'Taking Advantage of New Technologies: For and Against Crime' (2008) *Computer Law & Security Review* 24(5).

Ishikawa M, 'Designing Virtual Currency Regulation in Japan: Lessons from the Mt Gox Case' (2017) *Journal of Financial Regulation* 3(1).

Kethineni S, Cao Y and Dodge C, 'Use of Bitcoin in Darknet Markets: Examining Facilitative Factors on Bitcoin-Related Crimes' (2017) *American Journal of Criminal Justice* 43(2).

Zahirah R and Ridwan M, 'The Utilization of Cryptocurrencies by the Terrorist Group as an Alternative Way of Hawala for Illicit Purposes' (2019) *Journal Kelompok Studi Mahasiswa Pengkaji Masalah Internasional (KSMPMI)* 2.

Reports and Strategic Documents

Rajabi A, 'Virtual Currency: Legislation in Different Countries and Proposals for Iran' (2017) *Strategic Report, Vice President of Infrastructure Research and Production Affairs Office, Communication Studies and New Technologies Research Center of the Islamic Council*: 1-24. [In Persian]

Doyle C, *Money Laundering: An Overview of 18 U.S.C. § 1956 and Related Federal Criminal Law*(Congressional Research Service 2017).

Marini P, 'Regulation and Innovation: Public Authorities and the Development of Virtual Currencies' (2014) *Senate, Commission Des Finances* http://www.senat.fr/rap/r-syn-en.pdf.

Online Articles and Blogs

Collins K, 'The Hackers Behind WannaCry Ransomware Attack Have Finally Cashed Out' *Quartz* (3 August 2017) https://qz.com/1045270/wannacry-update-the-hackers-behind-ransomware-attack-finally-cashed-out-about-140000-in-

bitcoin/.

Entenmann E and Van Den Berg W, 'Terrorist Financing and Virtual Currencies: Different Sides of the Same Bitcoin?' (1 November 2018) *International Centre for Counter-Terrorism – The Hague (ICCT)* https://icct.nl/publication/terrorist-financing-and-virtual-currencies-different-sides-of-the-same-bitcoin/#_ftnref3.

Suberg W, 'Bank Complete: China Blocks Foreign Crypto Exchanges to Counter Financial Risks' *Cointelegraph: The Future of Money* (5 February 2018) https://cointelegraph.com/news/ban-complete-china-blocks-foreign-crypto-exchanges-to-counter-financial-risks.

Sparshott J, 'Regulator on Bitcoin: Same Rules Apply' *The Wall Street Journalhttp://online.wsj.com/news/articles/SB*.

Conference Papers and Presentations

PONS JP, 'Les Cryptomonnaies Impasse ou Révolution?' (2019) *Thème de Recherché presented at the Université du Temps Libre du Bas Languedoc-UTL 34*, p 71.