



Faculty of Human and Social Sciences
Bachelor in International Relations

Bachelor Thesis

**Cryptocurrency as a tool of
financing the terrorist
organizations Hamas and
Palestinian Islamic Jihad by
the Islamic Republic of Iran**
Mechanisms and Means of
Counteraction

Student: Elena Carrillo Rubio

Supervisor: Dr. Galyna Solovei

Madrid, May 2025

*To my parents, Florian and Loli, for betting on my education and never ceasing to
believe in me.*

Abstract

Cryptocurrencies emerged in 2009 with the advent of Bitcoin. Since then, numerous digital currencies have arisen as a pervasive method of payment, fund transfer, or investment. Nonetheless, the nature of cryptocurrencies has enabled the creation of a parallel financial system that lacks legislative control. The objective of this study is to investigate how Iran is employing cryptocurrencies to finance non-state actors, particularly Hamas and the Palestinian Islamic Jihad.

Consequently, it will assess these groups' utilization of blockchain technology for fundraising, money laundering, and transferring funds. Additionally, it will examine the regulatory responses to these activities and their efficacy. Thus, this research seeks to answer the question of how Iran utilizes cryptocurrencies to finance the illicit operations of these two terrorist organizations.

By examining the nature of this phenomenon as a new form of proxy warfare, the study will use the theoretical framework of Structural Realism. Moreover, to determine whether there exists a real association between Hamas and the Palestinian Islamic Jihad's methods of finance and cryptocurrencies, the research will include qualitative research analyzing policy analysis and literature review. Furthermore, a comparative analysis will be carried out to assess the Iranian legislation regarding these cryptocurrency regulations, considering the European and American regulatory frameworks, given Iran's status as a key supporter of these groups.

Key Words: Cryptocurrency, Hamas, Palestinian Islamic Jihad, Iran, Virtual Assets.

Resumen

Las criptomonedas surgieron en 2009 con la llegada del Bitcoin. Desde entonces, han emergido numerosas monedas digitales como método general de pago, transferencia de fondos o inversión. No obstante, la naturaleza de las criptomonedas ha permitido la creación de un sistema financiero alternativo que carece de control legislativo. El objetivo de este estudio es investigar cómo Irán está empleando criptomonedas para financiar a actores no estatales, especialmente a Hamas y la Yihad Islámica de Palestina.

En consecuencia, se evaluará el uso de la tecnología blockchain por parte de estos grupos para la recaudación, el lavado y la transferencia de fondos. Además, se examinarán las respuestas regulatorias a estas actividades y su eficacia. Por lo tanto, esta investigación busca responder a la pregunta de cómo Irán utiliza las criptomonedas para financiar operaciones ilícitas de estas dos organizaciones terroristas.

Al examinar la naturaleza de este fenómeno como una nueva amenaza por delegación, el estudio empleará el marco teórico del realismo estructural. Asimismo, para determinar si existe una relación real entre los métodos financieros de Hamas y la Yihad Islámica Palestina y las criptomonedas, la investigación incluirá un análisis cualitativo que estudiará las políticas y una revisión de la literatura existente. Asimismo, se llevará a cabo un análisis comparativo para evaluar la legislación Iraní respecto a estas regulaciones de criptomonedas, considerando los marcos regulatorios europeos y americanos, dada la condición de Irán como apoyo clave de estos grupos.

Palabras clave: Criptomoneda, Hamas, Yihad Islámica de Palestina, Irán, Activos Virtuales.

Declaration of Use of Generative AI Tools in Bachelor Thesis

I, Elena Carrillo Rubio, student of International Relations at Universidad Pontificia Comillas, hereby present my bachelor's thesis " Cryptocurrency as a tool of financing the terrorist organizations Hamas and Palestinian Islamic Jihad by the Islamic Republic of Iran: Mechanisms and Means of Counteraction " declare that I have used the generative AI tool ChatGPT or other similar code IAG tools only in the context of the activities described below:

1. **Synthesizer and disseminator of complicated books:** To summarize and understand complex literature.
2. **Translator:** To translate texts from one language to another.

I affirm that all information and content presented in this thesis is the product of my individual research and effort, except where otherwise indicated and credit has been given (I have included appropriate references in the dissertation and have made explicit what ChatGPT or other similar tools have been used for). I am aware of the academic and ethical implications of submitting non-original work and accept the consequences of any violation of this statement.

Date: 1/05/2025

Signature: Elena Carrillo Rubio

A handwritten signature in black ink, consisting of a large, stylized capital 'R' followed by several loops and a long horizontal stroke.

List of Terms and Abbreviations

ACJ – American Jewish Committee

AML/CTF – Anti-Money Laundering / Counter Terrorism Financing

ARS – Alternative Remittance System

ATS – Alternative Trading System

BSA – Bank Secrecy Act

CASP – Crypto Asset Service Provider

CDD – Customer Due Diligence

CRS – Congressional Research Service

CFTC – Commodity Futures Trading Commission

DEX – Decentralized Exchange

DeFi – Decentralized Finance

EBA – European Banking Authority

EMTs – E-money Tokens

EU – European Union

FATF – Financial Action Task Force

FinCEN – Financial Criminal Enforcement Network

FTC – Federal Trade Commission

HAMAS – Harakat al-Muqawama al-Islamiya

HEZBOLLAH – Hizbullah (Party of God)

IRGC-QF – Islamic Revolutionary Guard Corps – Quds Force

IRS – Internal Revenue Service

ISKP – Islamic State of Khorasan Province

ISIS – Islamic State of Iraq and Syria

ISR – Intelligence, Surveillance, and Reconnaissance

KYC – Know Your Customer

MSB – Money Services Business

OFAC – Office of Foreign Assets Control

OSINT – Open-Source Intelligence

OTC – Over the Counter

PIJ – Palestinian Islamic Jihad

P2P – Peer-to-Peer

SDN – Specially Designated Nationals (List)

SEC – Securities and Exchanges Commissions

SIGINT- Signals Intelligence

US – United States

USDT – Tehther (Stablecoin)

Index

INTRODUCTION	9
CHAPTER 1: THEORETICAL AND METHODOLOGICAL FRAMEWORK OF THE STUDY	12
1.1. STATE OF THE ART	12
1.2. THEORETICAL FRAMEWORK	18
1.3. RESEARCH METHODS	22
CHAPTER 2: ANALYSIS ON THE EVOLUTION OF CRYPTOCURRENCY AS A TERRORIST FINANCING METHOD	25
2.1. TERRORIST FINANCING: TRADITIONAL METHODS AND EMERGING TRENDS	25
2.2. THE EMERGENCE AND RISKS OF CRYPTOCURRENCIES	28
2.3. THE ADOPTION OF CRYPTOCURRENCIES BY TERRORIST GROUPS	32
2.4. IMPLICATIONS FOR INTERNATIONAL SECURITY	37
CHAPTER 3: CASE STUDY AND STUDY ON LEGISLATIONS.....	39
3.1. CASE STUDY: HAMAS & THE PALESTINIAN ISLAMIC JIHAD AND THEIR USE OF CRYPTOCURRENCIES	39
3.2. STUDY ON THE CURRENT LEGISLATION ON CRYPTOCURRENCIES	44
3.3. COMPARATIVE ASSESSMENT	53
CONCLUSIONS.....	55
BIBLIOGRAPHY.....	61
ANNEXES.....	65
ANNEX I.....	65
ANNEX II	66

Introduction

The irruption of cryptocurrencies has precipitated a substantial transformation within the global financial landscape, offering benefits such as expediency, cost reduction and efficiency in international transactions. Nevertheless, these advantages are accompanied by significant risks, particularly with regard to illicit activities. The anonymity and lack of strict controls transform these digital assets into tools of specific interest to illicit actors for money laundering, the purchase of illegal goods and, of particular concern, the financing of terrorism.

This aspect poses a significant threat to international security and well-being, as terrorist organizations have exploited cryptocurrencies to evade traditional controls and regulations, impacting individuals by amplifying the global risk they represent. Thus, the analysis of this phenomenon is crucial to counter terrorist groups and stop the spread of such global risk.

To depict and highlight how terrorist organizations use digital assets to finance their activities, this investigation seeks to follow these specific objectives: to provide clarity on how terrorist groups employ cryptocurrencies to finance their operations; to investigate if and how Hamas and the Palestinian Islamic Jihad are getting financed through digital assets; and, to study American and European legislations on cryptocurrencies and terrorism financing and compare them to the Iranian legislations.

Ultimately, the objective of this investigation is to facilitate the development of more effective countermeasures against the financing of terrorism. This will be achieved by highlighting the vulnerabilities generated by insufficient regulation and the challenges of tracking illegal transactions in the digital age. The investigation will provide information to policy makers, financial regulators and security agencies so that they can address the evolving threats posed by the financing of terrorism through cryptocurrencies.

In order to comprehend how states respond to emergent threats, such as the use of cryptocurrencies to finance terrorist groups, this study will employ the theoretical framework of Neorealism. Neorealism, as formulated by Kenneth Waltz, is based on the notion that the international system is anarchic and devoid of a central authority capable of enforcing uniform rules. Consequently, states act rationally to ensure their survival, maximize their power and respond to threats to their stability and security.

This issue has been widely examined by researchers such as Ridwan (2029), Wagman (2022), Burgess, Hamilton, and Leuprecht (2024), and international institutions including the Financial Actions Task Force (FAFTF). These studies have yielded significant insights into cryptocurrency misuse's technical and legal characteristics, with a particular emphasis on aspects such as anonymity, decentralization, and the difficulty of tracking funds.

However, several gaps persist in the extant literature, concerning comparative analyses of regulatory responses to cryptocurrency misuse. Such a comparative study would assess the regulatory approach adopted by the United States, the European Union, and Iran, which has been providing financial and logistical support to these organizations. Moreover, while this issue has been widely recognized as a threat, research on the specific manner through which terrorist groups use cryptocurrency is mainly unexplored, and theoretical research on this area is relatively rare. Therefore, this research aims to address this lacuna offering an innovative analysis that highlights the vulnerabilities generated by insufficient regulation and the challenges of tracking illegal transactions in the digital age, and a clarification on how these groups employ digital assets through the lens of Structural Realism.

The methodology employed in this paper is a combination of a case study, which focuses on the evolution and use of cryptocurrency by terrorist groups from 2014 to the present, an exhaustive review of the relevant literature, to build a comprehensive and updated picture of the phenomenon, and a comparative study on three different cryptocurrency regulations: the American, the European, and the Iranian, in order to analyze the gaps, barriers and inconsistencies of each regulation and provide a framework for enhanced regulations.

As a result of the challenges associated with tracking and the anonymity and pseudonymity afforded by these systems, this study explores the technologies and mechanisms through which these groups exploit the digital financial system to fund their operations. Moreover, the existing regulatory gaps will be identified, to improve the legal response to this emerging risk.

A significant focal point would be the state of Iran, which has been providing financial and logistical support to these organizations. From a neorealist perspective, the aim is to

assess how state-sponsored networks can be interconnected with decentralized digital assets.

The structure of this paper is organized into four sections. The first section provides a contextualization of the evolution of terrorist financing, with a focus on cryptocurrency. Second, a case study on Hamas and the Palestinian Islamic Jihad is provided, to explore whether and how these groups employ cryptocurrency to fund their operations. Third, a comparative analysis on three different regulatory responses to this threat is developed, focusing on the European, American and Iranian legislations to further compare their efficacy and lacunas. Finally, a series of recommendations is proposed to enhance these regulatory responses to bolster counter terrorism policies.

This research is subject to certain limitations, mainly of pertaining to the clandestine nature of terrorist operations, which render it exceedingly challenging to access primary data and direct empirical evidence. Due to the confidential and secret nature of terrorist financial activities, many crucial details remain inaccessible, limiting analysis to secondary sources and publicly available data. Notwithstanding these restrictions, the findings will contribute significantly to facilitating the development of more effective countermeasures against the financing of terrorism.

Research Questions and Objectives:

This study aims to demonstrate that emergent digital assets, known as cryptocurrencies, are used to finance activities of terrorist groups, and analyze the specific mechanisms by which terrorist organizations use digital assets to mobilize funds in a decentralized and anonymous manner, evading traditional financial systems and international sanctions.

This investigation will thus provide a critical perspective on the challenges faced by states and international organizations in regulating and countering the financing of terrorism through digital assets. In addition, it will examine Iran's role in using alternative financial mechanisms to support these groups, considering their history of evading sanctions and clandestine financing. To this end, the study will seek to answer the following question: Does Iran finance these terrorist groups through cryptocurrencies, and if so, how?

Consequently, in accordance with this research question, the fundamental purpose of this study is to clarify how regulatory gaps in the cryptocurrency ecosystem can be used as a

mechanism to finance terrorist organizations and what implications this has on global security. Given the breadth of this objective, a series of secondary objectives have been identified to facilitate the realization of this goal:

- Study and examine pre-existing relevant data,
- Review the existing research and identify what aspects of cryptocurrency misuse remain underexplored,
- Establish a theoretical lens for the analysis that explains the phenomenon,
- Examine how terrorist groups employ cryptocurrencies to finance their operations,
- Investigate if and how Hamas and the PIJ are getting financed using cryptocurrency
- Study American and European legislations on cryptocurrencies and terrorism financing,
- Explore the concept of state sponsor of terrorism and its relation to cryptocurrencies,
- Study the lack of legislation on cryptocurrencies in Iran,
- Evaluate international responses to this threat.

Chapter 1: Theoretical and Methodological Framework of the Study

1.1. State of the Art

Illicit use of cryptocurrencies has been thoroughly documented in academic research. Initially, cryptocurrencies were perceived as an emerging threat within the context of organized crime and money laundering. However, as time has passed, their relevance in the realm of terrorist financing has been solidified. This phenomenon has generated an evolving interest among investigators and policy makers, as it poses unique threats in terms of economic security and state supervision.

Findings on illicit use of Cryptocurrencies

Preliminary research on the use of cryptocurrency in transnational crime indicated its involvement in various illicit activities. Durrant (2018) analyses how these virtual assets have facilitated money laundering and drug trafficking, emphasizing their capacity to conceal substantial quantities of wealth without the involvement of third parties. In a similar vein, CipherTrace (2021) observes an increase in the utilization of

cryptocurrencies for financial crimes, although the report specifies that up until 2021 money laundering was the prominent activity.

Leuprecht, Hamilton & Jenkins (2023) focus on the relation between cryptocurrencies and money laundering, with a particular focus on Canada. While this study does not address the issue of terrorism financing directly, its findings offer valuable insights into how criminal groups use these digital assets to transfer funds undetected.

Despite the fact that the initial studies on the potential for terrorist groups to utilize cryptocurrencies were purely theoretical in nature, subsequent empirical evidence has indicated an increase in their utilization. Brill & Keene (2014) identify that, during that period, terrorist groups continued to rely on traditional financing methods, although they anticipated the potential of cryptocurrencies as an alternative. Subsequent studies have shown an increase in the use of cryptocurrencies by these groups, although they still rely on traditional financing methods (see Goldman et al., 2017).

More recently, Dyntu & Dykyj, (2021) and Wardhana & Nugroho (2022) confirm that terrorist groups have started to use cryptocurrencies with increasing frequency due to their ease of transfer and the anonymity they offer. Arkatuna (2023) corroborates this, further highlighting that decentralized platforms and emerging digital tools facilitate the concealment of the involved actors' identities, rendering them more attractive to terrorist groups. Burgess, et al. (2024) provide a more in-depth analysis, examining the cases of Al-Qaeda and Hamas and emphasizing the lack of global compliance with FATF standards as a factor that has enabled the persistence of these methods.

Furthermore, Sterling et al. (2024) examine the role of Hamas in the implementation of cryptocurrencies. Zahirah & Ridwan (2019) establish a comparison between cryptocurrencies and the traditional system of Hawala, highlighting how the decentralization of virtual assets has erased the necessity of physical third parties, thus posing a new threat to financial surveillance.

Factors that ease the use of cryptocurrencies by illicit operators

A significant aspect of contemporary research has focused on the intersection of anonymity, decentralization, and transfer efficiency in the realm of cryptocurrency. This

nexus has prompted a transformation in cryptocurrencies, rendering them an attractive proposition for illicit actors.

Dion-Schwarz et al. (2019) and Ibrahim (2021) posit that, despite anonymity not being absolute, the absence of central regulation enables the utilization of cryptocurrencies for illicit purposes. Ajdini (2024) further reinforces this notion by highlighting the challenges posed by the absence of global harmonization regulatory frameworks, which hinders the identification and prevention of terrorist financing.

From a more technical perspective, Salami (2017) examines how the decentralized infrastructure of cryptocurrencies facilitates the financing of terrorism, particularly in countries with inadequate financial systems. Burgess et al. (2024) further expand upon this subject, documenting how terrorist groups have begun to use decentralized platforms, mixers and bridges to conceal the origin and destination of the funds. This phenomenon underscores the imperative for a comprehensive review of financial supervision mechanisms, as terrorist groups' strategies have evolved in tandem with technological advancements.

From a geopolitical perspective, Iran has emerged as a key actor in the terrorist financing spectrum. Malakoutikhah (2020) elucidates that Iran has emerged as both a sponsor and active perpetrator of terrorism. In addition, TRM Insights (2023) documents that Iran has facilitated the processing of up to 3 billion dollars in cryptocurrency, with the realm of evading sanctions. Lob (2022) highlights that these assets were employed in commercial transactions with other state and non-state actors. Skare (2023) examines the relationship between Iran, Hamas and the Palestinian Islamic Jihad discussing the state's role in financial and military support to these groups.

Regulatory responses

The international community has responded to the issue with a range of regulatory initiatives aimed at addressing the illicitness of cryptocurrencies. However, the effectiveness of these measures is subject to scrutiny. Wagman (2022) analyses how AML/CFT policies have been implemented to varying degrees of success, concluding that the unequal compliance of these regulations has enabled the utilization of cryptocurrencies in illegal activities. Rodrigues & Kurtz (2023) posit that, despite the FATF's emphasis on risk awareness, numerous countries have not yet implemented

comprehensive regulations, thereby enabling the perpetuation of these activities. Burgess et al. (2024) further highlight that the absence of regulatory oversight over emerging technologies such as DeFi, has been exploited by terrorist organizations.

Within the European context, Covolo (2020) evaluates the effectiveness of the 5th Anti Money Laundering Directive's, highlighting that despite its success in enhancing the detection of illicit transactions, there are still challenges related to crypto market surveillance. These limitations suggest that the current regulatory framework is inadequate in preventing the use of cryptocurrencies for terrorist financing.

The United States has been one of the most active countries in the fight against money laundering and the financing of terrorism (AML/CFT). Since the implementation of the Bank Secrecy Act (BSA) and the Financial Crimes Enforcement Network (FinCEN), the government has sought to regulate the flow of digital assets through the implementation of stringent Know Your Client (KYC) and Anti-Money Laundering regulations. However, reports such as Wagman (2022) and Rodrigues & Kurtz (2023) underline that despite the US having improved its surveillance of exchange and crypto wallets, there are some persistent gaps in the application of sanctions. Moreover, the Treasury Department and the OFAC have imposed sanctions on foreign exchanges that might be associated with terrorist financing. Furthermore, the U.S. Congress warns that terrorist groups such as Hamas and Al-Qaeda have utilized cryptocurrencies to circumvent banking restrictions.

In their study, Sadeghi & Naser (2023) compare the Iranian and American legal frameworks, positing that Iran has a poor regulatory framework that allows the financial exploitation of its infrastructure by illicit actors, while the United States has implemented more severe restrictions.

Turner (2020) further reinforces this preoccupation, highlighting that Iran has permitted crypto exchanges with minimal to no oversight, thereby facilitating the transfer of funds to illicit groups such as Hamas. Parvin & Allahyarifard (2024) add that Iran has recently implemented some control measures, but it lacks an effective supervision.

Gaps in the literature

Notwithstanding the number of studies on cryptocurrencies and the financing of terrorism, lacunae persist in the extant literature. For instance, Ridwan (2019) does not analyze regulatory responses, while Wardhana & Nugroho (2022) do not compare key differences between regulatory frameworks. Ibrahim (2021) focuses on Pakistan without conducting a global analysis, and Ajdini (2024) studies a regional case without addressing specific groups such as Hamas.

There is an absence of comparative analyses on the regulatory frameworks of the EU, the US and Iran, and their impact on the effectiveness of control measures. Moreover, this lacuna in the extant literature underscores the necessity for a study that examines if and how Hamas and other terrorist groups such as the Palestine Islamic Jihad utilize cryptocurrencies and the effectiveness of the regulatory frameworks of the US, the EU and Iran. This study will provide a detailed analysis of current challenges and potential regulatory solutions.

Key Concepts

To further understand how terrorist organizations might access cryptocurrencies, it is essential to define the term terrorism, bearing in mind that it is a contested concept. Bruce Hoffman describes terrorism as “*the threat of violence—used and directed in pursuit of, or in service of, a political aim.*” (Hoffman, 2017).

However, in 2011, Schmid proposed a revised academic definition of terrorism as a strategy of political violence aimed at generating fear and manipulating society. This definition focuses on civilians and non-combatants, using lethal attacks, kidnappings and prolonged tactics to coerce governments, intimidate populations and gain support. It can be used by state and non-state actors in contexts of repression, propaganda and irregular war. The repercussions of terrorism extend beyond the immediate victims, as the perpetrators endeavor to exert influence over a broader demographic through the instigation of fear and the utilization of media coverage. The underlying motivations that propel individuals to engage in terrorist activities are multifaceted, encompassing a spectrum of factors, including revenge, ideological and political convictions, and religious beliefs. Schmid also mentions that terrorist acts are seldom isolated events; rather, they are components of meticulously orchestrated campaigns designed to disrupt

the established balance of power and exert undue influence over the political landscape (Schmid, 2011).

The financing of terrorism has been a subject of extensive study within the domain of global security. Leuprecht, Crockfield and Simpson (2019) posit that terrorist financing constitutes the process through which terrorist groups obtain economic resources. Terrorist financing networks frequently operate in a discreet manner, mobilizing small amounts of money through legal mechanisms such as bank transfers, cash, or traditional banking systems. As Salami (2017) emphasizes, terrorist organizations frequently resort to different criminal activities such as kidnapping, drug trafficking, or bank robbery, in order to generate funds. Traditionally, such groups have resorted to the hawala system, however, these transactions can be time consuming and risky, especially when transferring large amounts. Therefore, they might opt for alternative trends.

Key Concepts

With the purpose of ensuring the study's comprehensibility, the key concepts will be defined:

Cryptocurrency: *“a digital representation of value that can be digitally traded and functions as a (1) medium of exchange; and/or (2) a unit of account; and/or (3) a store of value but does not have legal tender status. It is not issued nor guaranteed by any jurisdiction and fulfils the above functions only by agreement within the community of users of the virtual currency”* (FINANCIAL ACTION TASK FORCE, 2014).

Hamas: *“a militant Islamist group that emerged from the Palestinian branch of the Muslim Brotherhood in the late 1980s (...) Governments, including the United States and the European Union, have designated Hamas a terrorist organization because of its attacks against Israel, which include suicide bombing and rocket attacks”* (Robinson, 2024).

Palestinian Islamic Jihad: a small Sunni militant Islamic group that was founded in Egypt in the late 1970s, inspired by the Iranian Revolution. The group has focused mainly on attacking Israel through its military wing, the al-Quds Brigades. The group opposes a peaceful partition and seeks to establish an Islamic Palestinian state. It receives support from Iran and Syria (Pearson, 2012).

Iran: Iran, also known as the Islamic Republic of Iran or Persia, is a country in West Asia. Since the Islamic Revolution in 1979, Iran has had a close relationship with terrorism. It was designated as a state sponsor of terrorism in 1987. The country has been accused of training, funding, and arming and sheltering non-state actors such as Hezbollah and Palestinian terrorist groups sheltered in Gaza (Malakoutikhah, 2018), (U.S. Department of State, 2024).

Virtual Assets: *“a digital representation of value that can be digitally traded and function as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value, but does not have legal tender status (i.e., when tendered to a creditor, is a valid and legal offer of payment) in any jurisdiction. It is not issued nor guaranteed by any jurisdiction and fulfils the above functions only by agreement within the community of users of the virtual currency. Virtual currency is distinguished from fiat currency (a.k.a. “real currency,” “real money,” or “national currency”), which is the coin and paper money of a country that is designated as its legal tender; circulates; and is customarily used and accepted as a medium of exchange in the issuing country. It is distinct from e-money, which is a digital representation of fiat currency used to electronically transfer value denominated in fiat currency”.* (Financial Action Task Force, 2014)

1.2. Theoretical framework

In order to further comprehend this phenomenon from a theoretical perspective, this study will delve into the theories of international relations, especially the school of thought of Neorealism.

Neorealism offers an analytical framework that facilitates the explanation of how the international system’s anarchy allows the existence of non-state actors such as terrorist groups, the responses of states to these threats and the fight over the power equilibrium in cyberspace.

In this regard, Neorealism offers significant analytical advantages over classical realism, liberalism and constructivism.

Firstly, it is imperative to grasp the theory of Realism. In essence, Realism in the context of International Relations posits the primacy of power, the anarchy of the international system, and the dynamic interplay between states as the predominant actors in global

politics. According to Voinea (2013), Realism is predicated on an explanatory and pragmatic approach that prioritizes the analysis of international politics based on the search for power and security by states, ignoring the existence of non-state actors. Hence, analyzing a phenomenon driven by terrorist groups would require an extension of classical Realism principles.

Secondly, Liberalism posits that international cooperation, multilateral organizations and economic interdependence serve as a moderator in conflict and global challenges. Liberalism relies on the efficacy of international institutions, regulatory frameworks, and international legal instruments for addressing transnational challenges, nonetheless, the persistent existence and activity of terrorist groups underscores the failure of the application of such theory.

Liberalism generally favors transparency and accountability in international affairs, perceiving international institutions and laws as crucial for promoting cooperation and managing conflicts; however, terrorism violates international norms and laws, being a threat to democratic societies and a challenge to global stability (Rousseau & Walke, 2010).

For liberalists, addressing terrorism would require international cooperation but the transnational nature of these groups and their ability to exploit ungoverned spaces make state-led cooperation difficult to implement and enforce effectively. Moreover, the decentralized nature of cryptocurrency financing mirrors this challenge (Bakker, 2015).

Thirdly, Constructivism is a theoretical framework that emphasizes the role of norms, identities, shared ideas, and perceptions among international actors. While this framework has proven to be beneficial in elucidating certain ideological facets of terrorism, it encounters challenges in accurately delineating the structural emergence of terrorist entities and their methodologies for financial mobilization. In order to explain terrorism, Constructivism would focus on the social construction of terror as a threat, the identities and norms in shaping responses to it, and the significance of language and discourse in understanding and addressing terrorism. Furthermore, constructivists would focus on how the existing norms are being contested and reinterpreted, the success of international institutions in shaping the global agenda and their ability to socialize states into global norms. However, none of these explanations accurately enlightens the

phenomenon, rather Constructivism would merely focus on the social construction of this issue, offering less insight into tangible aspects in explaining the phenomenon (Reus-Smit, 2005).

Neorealism

Neorealism, also known as Structural Realism, as developed by Kenneth Waltz in 1979, focuses on the structural configuration of the international system as the primary determining factor in the behavior of states. In contradistinction to classical Realism, which accentuates human nature as a primary driving force in international politics, Neorealism posits that the anarchy of the international system and the distribution of capabilities amongst states serve as the fundamental factors that shape its decisions and actions (Lobell, 2010).

According to Waltz (1979), the international system is anarchic, thereby resulting in the absence of a central authority capable of regulating the conduct of international actors. Consequently, states are compelled to rely on their own capabilities to ensure their security (a.k.a. self-help system). This state of anarchy inevitably leads states to seek to maximize their security in an environment where uncertainty and distrust prevail. In such circumstances, states act in a rational manner, pursuing strategic interests and prioritizing survival and security over other objectives. States are regarded as homogeneous rational units, primarily seeking to ensure their own existence, despite significant variations in their capacities and relative power (Pashakhanlou, 2018). In this sense, the state follows the Westphalian order, establishing the principle of state sovereignty, internal and external) as a tenet, and defending its territoriality as a basis to guarantee power.

The pertinence of Neorealist theory in explaining the phenomenon of terrorism is predicated on its capacity to demonstrate how international anarchy engenders the optimal conditions for the proliferation and operation of non-state actors. The emergence of such actors is facilitated by the exploitation of institutional weakness, power vacuums, and internal conflicts within states characterized by fragile or failed institutions. This phenomenon can be attributed to the lack of a unifying global authority that can provide a sense of direction and stability, resulting in a state of perpetual uncertainty, insecurity, and constant competition for power and resources. This creates a landscape where non-state actors can directly intervene in these dynamics.

This condition enables these groups to establish autonomous operational bases, recruit followers, and develop alternative financing networks to the conventional financial system. Hence, regions exhibiting institutional fragility or the absence of effective governance, such as Somalia, Syria and Afghanistan, are conducive to the proliferation of these non-state actors, who seek to obtain power and influence in the absence of a robust state structure to control or neutralize them.

Furthermore, Waltz expounds on the notion that states find themselves in a security dilemma: if a state fortifies itself to an excessive degree, it engenders fear in others; if a state fails to act against a threat, it jeopardizes its own security. The implementation of sharp anti-terrorist measures by a state can engender further resentment and radicalization, thereby amplifying the terrorist threat rather than mitigating it.

Two approaches can be distinguished within Structural Realism: Mearsheimer's Offensive Realism and Waltz and Walt's Defensive Realism.

Defensive Neorealism

Defensive Neorealism, derived from Waltz's (1979) theory of Neorealism, and further elaborated by Walt in 1987, underscores the notion that states prioritize the maintenance of their security and the avoidance of superfluous conflicts that could potentially disrupt their power equilibrium. From this perspective, states perceive terrorism as a direct threat to their security and stability, which compels them to adopt preventive and regulatory measures to contain these threats (Walt, 1987).

In the face of the use of emergent technologies by terrorist organizations, such as artificial intelligence or cryptocurrencies, states have adopted stringent regulatory frameworks and international mechanisms to track and impede illicit activities and sources of financing. In the context of virtual assets, regulatory initiatives have been led by organizations such as the Financial Action Task Force (FATF), with transnational cooperation agencies such as Europol and Interpol playing a pivotal role in identifying and sanctioning terrorism-linked digital assets, thereby strengthening states' collective capacity against these unconventional threats.

Offensive realism

In contrast, offensive realism, led mainly by John Mearsheimer (2001), is also based on the anarchic nature of the international system. However, it diverges in its strategic response adopted by states. According to Mearsheimer, states pursue the continuous maximization of their power, capitalizing on strategic opportunities presented by the uncertainty of the international environment. The perceived possible intentions of other states push states to aggressively maximize their relative power until they achieve regional hegemony, if doable, as it is perceived as the most effective guarantee of survival (Pashakhanlou, 2018). Mearsheimer further theorizes that states might adopt expansionist and aggressive positions when the potential benefits outweigh the potential risks and costs. (Mearsheimer, 2001). Therefore, States may indirectly tolerate, support or even facilitate illicit activities such as terrorism, if these actions serve to strengthen their strategic position in relation to geopolitical rivals.

A pertinent example in this case is Iran. Reports have indicated that the country may be indirectly allowing or facilitating the use of cryptocurrencies by allied groups, such as Hamas, to circumvent international economic sanctions imposed primarily by the United States and its allies. This could be interpreted as a strategic move by Iran to exploit the existing regulatory gaps in the cryptocurrency sector, thus enhancing its geopolitical standing, weakening its regional rivals, and expanding its influence across regional and global domains.

1.3. Research Methods

In order to carry out this study, a comprehensive review of the extant literature was undertaken, encompassing both academic works and policy reports, with the aim of providing a complete overview of the current state of research in the following areas: terrorist financing methods, cryptocurrencies, and terrorist state-sponsorship.

To optimize the research, the question was broken down into the core themes

- Terrorist Groups: Hamas, Palestinian Islamic Jihad (PIJ)
- Financing Methods: Cryptocurrency, Virtual Assets, Bitcoin, Blockchain, Terrorist Financing

- Regulatory Aspects: Iran, State Sponsorship, Cryptocurrency Regulation, Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF).
- Legislative and Enforcement Terms: Financial Action Task Force (FATF), Sanctions, Compliance, Financial Intelligence Units.

This study employed academic, governmental, and industry sources. The academic databases were Google Scholar, JSTOR and SAGE Journals; reports from official bodies (e.g. FAFT, CRS, and Europol); grey literature and open-access reports (e.g. Chainalysis); and government-issued documents. The following Boolean Operators were used to search for relevant literature:

- *AND “cryptocurrency AND terrorism”; “Iran AND terrorism”; “Hamas AND financing”; “PIJ AND financing”; “Iran AND cryptocurrency” “cryptocurrency legislation”.*
- *OR: “Cryptocurrency OR Virtual Assets OR Blockchain AND Terrorism”*

The subsequent selection criteria were established for the selection of the documents:

- Inclusion: studies and reports published from 2014, academic papers, analysis of specific cases on cryptocurrencies and terrorist financing.
- Exclusion: studies before 2014, without relevance for the current matter, and unverified sources’ reports.

As the research is based on a literature review, one of the main limitations is the dependence on secondary sources, which implies that the information analyzed comes from pre-existing studies and official reports. In addition, the range of terrorist financing information is restricted to the data gathered and selected by the governments for disclosure. Moreover, the scope of information accessible is reduced due to the pseudonymity and highly adaptable nature of cryptocurrencies, and the heterogeneous array of regulatory frameworks and monitoring practices governing cryptocurrency on an international scale introduces a complex and multifaceted landscape.

The execution of this study will be accomplished through the utilization of qualitative methodology, encompassing the analysis of secondary sources, including open-source

intelligence reports, case studies and academic papers. More specifically, this study employs a Case-Study approach, a qualitative research methodology that allows for in-depth analysis of the phenomenon within its real context. This technique is based on the compilation of multiple sources of information, such as reports, previous analyses and academic papers. The present case study focuses on the evolution and use of cryptocurrencies as a method for terrorist financing. Therefore, it will concentrate on the following: first, how did terrorist groups finance their activities prior to the advent of cryptocurrencies; second, what cryptocurrencies are, and why they are of interest to illicit actors; and third, at what point and in what manner terrorist groups began to use them.

Moreover, this research combines the case-study approach with a comparative analysis. The investigation consists of studying whether these organizations have used cryptocurrencies to finance their activities; second, the strategies they have used to do so; and third, the threats they pose to global security. In addition, it analyses how differences in regulatory frameworks can influence the use of cryptocurrencies to finance illegal activities, and cases of terrorist financing prosecutions in countries that adhere to the rule of law, specifically the European Union and, in some cases, the United States, aiming to compare them to the Iranian legislation, which is regarded as insufficient.

In order to ascertain whether digital assets are utilized by terrorist organizations, such as Hamas, for the purpose of financing their illicit activities, and to examine the role of Iran in facilitating such activities, the study will be divided into four sections.

Firstly, an analysis will be conducted on how these groups have been employing traditional methods, such as hawala, for the purpose of financing their illicit activities, and why these might seem obsolete. Moreover, a further description on what cryptocurrencies are, how they emerged as an interesting source for illicit actors, and how they are employed by terrorist groups will also be carried out. Moreover, an examination will be conducted on how blockchain technology enables the smooth functioning of these groups, paying particular attention to the privacy features of cryptocurrencies and Decentralized Finance.

Secondly, a case study on the terrorist group Hamas, exploring its financing methods and its relation to Iran, will be carried out. This study will help exemplify the threat posed by

cryptocurrency as a method of terrorist financing and will be conducted under the theoretical framework of Neorealism.

Thirdly, a study of the European and American regulations on cryptocurrencies, as well as those of Iran, will be conducted, with a view to drawing parallels between them. Iran is a major supporter of these non-state groups, and the study will therefore provide a valuable insight into the relative strength of the respective regulatory frameworks.

Fourthly, the investigation would include an analysis of the global risks to society, a conclusion that summarizes the findings, and a series of recommendations for policy makers to implement improved measures to counter terrorism.

As a disclaimer, AI tools, such as Chat GPT and Notebook LM, were implemented in this study for complementary purposes. Specifically, these tools were employed to make summaries of academic pieces, institutional reports and legislative documents, and to translate documents. The use of these tools did not replace the analysis nor the original writing of the content but rather functioned as a support within the process of research and elaboration of the work.

Chapter 2: Analysis on the Evolution of Cryptocurrency as a Terrorist Financing Method

2.1.Terrorist financing: Traditional Methods and Emerging Trends

Terrorist organizations require sustained financial backing to function, acquire weaponry and materials to build explosives, obtain fraudulent documentation, and buy communication devices. Terrorist financing enables terrorists to obtain resources for the planning and execution of attacks. To facilitate these activities, such organizations require a financial support that can be provided from private donations as well as from illicit activities.

Originally, this transfer of funds was facilitated by a variety of traditional methods that include cash, informal value transfer systems such as Hawala, criminal activities, donations, and state sponsorship. The efficacy of such conventional methods underscores their flexibility, which lies in their capacity to adapt their tactics in response to rigorous regulations.

Hawala is an alternative remittance system (ARS), that functions outside the formal banking sector. It is a trust-based system of transferring funds or property of equivalent value between people in two or more locations without the actual physical movement of money (Norton & Chadderton, 2016). Operating outside the reach of formal financial institutions, hawala facilitates rapid, anonymous, and unregulated cross-border transfers, hindering detection and disruption by regularity and law enforcement authorities. Its cost efficiency, swiftness, and clandestine nature have made it a pivotal instrument for terrorist organizations, however this system necessitates face-to-face interaction, a component that introduces an unnecessary element of risk to transactions, as it eliminates secrecy and can engender potential for physical harm.

Terrorist organizations have also historically relied on a variety of illicit activities to generate resources. These encompass illicit drug trafficking, kidnapping for ransom, bank or commercial establishment robberies, financial fraud, extortion, human trafficking, and the illicit exploitation of natural resources in territories under their control. The trafficking of illegal substances has historically constituted a primary economic foundation, offering reliable and substantial revenue sources, however, this activity also fosters dependency on external criminal networks and exposes groups to risks associated with international law enforcement operations. Illicit natural resource exploitation, a practice particularly prevalent among ISIS, offers substantial revenue but is contingent on sustained territorial control, which is vulnerable to rapid loss in the context of military conflicts.

Concurrently, state sponsorship has been a significant traditional method for terrorist groups to get financed, especially when their activities are congruent with the specific strategic or ideological interests of some states. This sponsorship can take many forms, ranging from explicit financial support to indirect provision of logistical resources and training.

From a financial perspective, state sponsors often provide direct economic support to cover essential operations such as planning and executing attacks, maintaining organizational infrastructure, paying salaries, and providing financial support to family members of terrorists.

The facility of safe havens within the national territory of the sponsor enables terrorist groups to operate with greater security, facilitating strategic planning, training,

recruitment...Moreover, the provision of material resources, including weaponry, military equipment and forged documentation, constitutes a critical aspect of state sponsorship.

The underlying motivations for state sponsorship are complex and often motivated by weakening geopolitical adversaries, immobilizing strategic resources or expanding regional influence. Despite the diminishing of such practice since the Cold War (Norton & Chadderton, 2016), it persists as a pivotal resource for terrorist groups and a common custom for some states such as Iran which is subject of being a prominent state sponsor of terrorism since the 1980s, aiding Hamas, Hezbollah and Houthi rebels in Yemen (Malakoutikhah, 2018).

Nonetheless, it is essential to acknowledge the declining efficacy of these mechanisms as reliable sources. The initial critical dimension to be examined must be the impact of the global regulatory tightening that followed the 9/11 attacks. These attacks represented a critical juncture for regulatory compliance and intelligence agencies, forcing institutions to implement more stringent protocols regarding due diligence (KYC) and suspicious activity reporting (Norton & Chadderton, 2016). These regulations impose operational impediments on terrorist groups as financial transactions generate audit-trailable records that enable intelligence and law enforcement agencies' intervention.

What is more, this regulatory increase led to the parallel practice of “de-risking” among financial institutions, which have chosen to sever ties with clients or jurisdictions deemed to be high risk has led to the closure of avenues for actors that could be associated with terrorist financing (Goldman et al., 2017).

Concurrently, practices such as hawala have faced sustained pressure. While these systems have demonstrated flexibility, adaptability and effectiveness during the years, the success of law enforcement operations and the emergence of technologies such as signals intelligence (SIGINT), open-source intelligence (OSINT), or intelligence surveillance and reconnaissance (ISR), aimed at dismantling these networks, underscores the inherent fragility of a system that relies mainly on relationship trust.

As for cash and hawala, they present enormous logistical challenges due to their large-scale international mobilization. The enhanced border and customs security measures

elevate the risks associated with the physical conveyance of cash, endangering terrorist groups to the perpetual risk of seizure or loss.

From a strategic perspective, fiat methods imply reliance on regulatory gaps between jurisdictions or lax financial institutions. This reliance increases the risk of exposure and requires constant adaptability. Consequently, they may have become unreliable due to their increased vulnerability in the face of the strengthened response to counter terrorism.

2.2.The Emergence and Risks of Cryptocurrencies

Although the development of cryptocurrencies began in 1980 when the American cryptographer David Chaum, discovered an algorithm for secure information exchange called *blinded money*, the advent of modern cryptocurrency as a novel form of digital currency coincided with the global financial crisis of 2008. They became popular in 2009, with the arrival of Bitcoin, the best-known digital asset, which was created to offer a peer-to-peer payment system without intermediaries such as banks. Since then, the value and popularity of such asset has growth exponentially, reaching increments of 100,000 USD (Ajdini, 2024).

Cryptocurrencies are digital assets characterized by their uniqueness, and non-duplicability. They are secured by cryptography and involve sophisticated coding; thus, they are purely digital, and exist as encrypted strings of characters, therefore they cannot be taken out of the wallet to pay for everyday items such as a coffee.

To store, trade or use cryptocurrencies, people must have a digital wallet, which works like a program that receives, sends, and maintains codes that translate into this virtual currency. These digital wallets can take various forms, including online platforms and offline wallets stored on laptops, mobile phones or tablet devices. Moreover, contrary to conventional banking systems, cryptocurrencies are characterized by their intangible and stateless nature as digital assets (Brill and Keene, 2014).

These currencies do not have a legal status of official tender in any country, functioning rather as alternative means of exchange, units of account, and stores of value. Their underlying technology is the blockchain, a decentralized public ledger that records all transactions. The blockchain's architecture guarantees that the transactions are recorded publicly, while users remain untraceable, thereby facilitating the disguise of illegal transactions. These systems facilitate borderless transactions that are expeditious and cost

effective. Furthermore, technologies such as mixers and chain-hoppers bridges allow users to hide the origin and destination of funds, developing a complex web of untraceable transactions (Burgess, Hamilton & Leuprecht, 2024).

A key feature of the blockchain technology is its inherent decentralization, with an absence of a central regulator. This characteristic reduces operational costs and increases resilience to institutional failures, but it also introduces vulnerabilities from a security viewpoint. This decentralization imposes several limitations on the capacity of states and regulatory bodies to implement effective anti-money laundering (AML) and countering the financing of terrorism (CFT) mechanisms. The principal regulatory framework, based on the oversight and collaboration of centralized entities such as financial institutions and authorities, is inadequate when confronted with a technology whose very design is intended to evade such centralization (Rodrigues & Kurtz, 2019).

The pseudonymity provided by blockchain, wherein transactions are tied to cryptographic addresses rather than personal identities, is presented as another risk factor. While it is true that public records of transactions might ensure full transparency, this transparency becomes an illusion if cryptographic addresses cannot be easily linked to specific identities. Hence, this pseudonymity is biased, as sophisticated methods of digital forensics can trace transactions back to known identities under certain circumstances. Nonetheless, this technical complexity involved is such that it can allow criminals to operate with a considerable degree of impunity, especially when employing advanced techniques such as coin mixing or transactions chained across different exchanges.

The risks associated with blockchain are multifaceted. The ability of this technology to facilitate rapid, irreversible, and global transactions introduces a new dimension of risk. This technical advantage enables terrorist groups to make immediate cross-border movements, avoiding the slow bureaucracies of the traditional financial system. The irreversible nature of transactions holds appeal for illicit actors, as it virtually eliminates the risk of asset reversion or freezing by regulatory bodies once the transfer is executed.

The peer-to-peer nature of cryptocurrencies enables direct transactions between users, bypassing the involvement of regulated institutions. This characteristic poses an additional challenge for international financial supervision as the proliferation of unregistered P2P exchanges gives rise to a high-risk parallel economy. This is often

inaccessible to traditional regulatory tools, exacerbating the inherent challenges in combating illicit financial activities, thereby eroding the state's capacity to regulate monetary flows.

The recent introduction of smart contracts in DeFi, particularly on platforms like Ethereum, has further complicated this situation. These innovations have the potential to automate financial services without the need for intermediaries, exponentially multiplying the regulatory challenges and offering organizations a highly effective channel to move funds with minimal transparency and control. This evolution poses significant challenges to regulatory frameworks, underscoring the urgent need for adaptation by international organizations and intelligence agencies.

DeFi is the permissionless decentralized version of various traditional financial tools. It operates on peer-to-peer networks and relies on open-source interoperable digital-contracts that exist on the blockchain. This means that it functions without relying on intermediaries such as banks or brokerages. Moreover, DeFi protocols are generally permissionless by design, meaning anyone in any country can access them with little or no Know Your Customer (KYC) requirements.

In essence, virtual assets have transformed the landscape of financial systems and the digital realm. The original idea behind blockchain technology was to create a decentralized financial system without borders, central bank oversight or government regulation, yet its use has also attracted the attention of authorities and judicial agencies. Their unique qualities, such as anonymity and global reach, have generated a mixture of enthusiasm for their potential, and concern regarding their associated risks. Thus, despite their legitimate applications, these currencies have become a useful tool for criminals, terrorist organizations and entities seeking to evade international sanctions.

Plus, in 2014, the Financial Action Task Force (FATF), an international body dedicated to combating money laundering and terrorist financing, acknowledged the potential misuse of cryptocurrencies due to their anonymity, ease of use, and decentralized nature (Financial Action Task Force, 2014)

Cryptocurrencies provide an anonymous transfer of funds, hiding the identities of the transmitting parties and enabling users to engage in financial activities without disclosing their personal information (Ali, 2021). Despite the advantages of the decentralized nature

of cryptocurrencies, these characteristics generate vulnerabilities that can be exploited for fraudulent activities. The absence of Customer Due Diligence (CDD) and Know Your Customer (KYC) protocols enables users to conduct anonymous transactions, rendering cryptocurrencies appealing to money launderers, terrorist groups and other criminals (Ibrahim, 2021). This anonymity is further exploited on the dark web, where cryptocurrencies are the primary medium of exchange for illegal goods, weapons, and services.

2.2.1. Threats posed by Cryptocurrencies

Cryptocurrencies being inherently transnational and decentralized, operate outside the effective control of states, which poses a direct threat to the sovereign capacity of states to maintain and protect their territorial integrity and international security. Following Waltz's framework, the distribution of capacities determines a state's possibility for action. Consequently, the advent of cryptocurrencies is eroding a fundamental capacity of the modern state: the monopoly over legitimate financial instruments. This transformation undermines statal control over financial flows and weakens its ability to exercise economic authority in the international system. In light of this, if the structure of the international order is delineated by how material capabilities are distributed, the regulation of such capabilities is a form of structural power, and this power is being contested by technologies designed precisely to avoid it.

The transnational character of cryptocurrencies enables non-state actors, including terrorist groups, to conduct financial transactions free of geographic limitations or the oversight of government controlled financial intermediaries. This phenomenon represents a direct challenge to international AML/CTF regimes, whose structures are based on cooperation between formal financial entities and states. The increasing adoption of cryptocurrencies by illicit actors has exposed significant cracks in the regulatory frameworks, facilitating opacity of operations and limiting the capacity for early detection and coordinated responses by national or international agencies.

The connection between cryptocurrencies and other transnational criminal activities, including money laundering, illicit arms trafficking on the dark web, and cybercrime, aggravates the complexity of the threat. The concept of the crime-terror nexus assumes a novel dimension in the context of terrorist access to a parallel and less regulated financial system. This convergence of criminal and terrorist actors on decentralized digital

platforms reduces the state's capacity to monitor and disrupt transnational illicit networks, increasing their strategic vulnerability.

The adaptability and innovative capacity demonstrated by terrorist groups in the face of emerging technological developments reinforce the asymmetric nature of the challenge. The advent and rapid evolution of DEXs, and DeFi allow these actors to bypass intermediaries and operate with anonymity, speed and flexibility. This disparity between the rapid advancements made by terrorist groups in technology and the slower reaction of states to these threats further exacerbates the conditions of structural insecurity.

The inability to establish a coherent and effective global regulatory framework for cryptocurrencies further underscores the inherent fragmentation of power and competing interests within the international system. In accordance with the fundamental tenets of neorealism, states are unlikely to abandon their immediate national interests in favor of effective and enduring international cooperation, particularly when such cooperation demands concessions in terms of financial and technological sovereignty. This absence of political will creates a regulatory gap that terrorist organizations might exploit, benefiting from an anarchic environment where operational opportunities outweigh control and preventive mechanisms.

The irruption of cryptocurrencies represents a structural transformation with direct implications for the international order. While it was initially conceived as an instrument of decentralization, inclusion and financial privacy, the appropriation by illicit actors demonstrates its potential to undermine a much less idealistic aspect: the ability to destabilize the norms that support global economic governance and multilateral efforts against organized crime.

2.3.The Adoption of Cryptocurrencies by Terrorist Groups

Terrorism has evolved over time, adapting its methodology to the latest technological advances. These groups have leveraged social media sites such as Facebook, Instagram, or Twitter (now X), in addition to messaging applications like Telegram, in their efforts to solicit financial contributions and disseminate instructions on how to provide financial support. Crowdfunding platforms like GoFundMe have also been exploited, although increased awareness and subsequent bans have led to adaptations in their use (Fanusie, 2018).

States have intensified their pressure on traditional channels. Thereby, to face the enhanced vigilance of intelligence agencies and the increased presence of military forces in conflict zones, which challenged the success of the hawala and other traditional methods, terrorist groups adopted cryptocurrencies as a means of financial exchange (Ridwan, 2019). Hence, in light of coercive methods perpetrated by states, terrorists adopt reactive and innovative measures, taking advantage of the decentralized nature of digital assets. This can be perceived as an offensive tactic that enables these groups to avoid institutional encirclement and gain access to global markets of willing donors, fragmenting the containment capacities of states.

Cryptocurrencies have emerged as a significant medium for financing such activities as they offer anonymity, cross-border mobility, and a means to evade conventional financial regulations. These regulatory gaps enable terrorist organizations to operate with impunity, evading counter-terrorism efforts. While traditional methods are still the most used, cryptocurrencies present a unique set of features that appeal to these organizations.

Digital assets offer distinct advantages, particularly in terms of anonymity and pseudonymity. The early vision of blockchain technology envisioned a decentralized currency without governmental supervision or any identification required, aiming to preserve anonymity like cash. This aspect assumes even greater significance when considering that many currencies offer a high-opacity cryptographic protocol and that there exist services such as mixers or tumblers that obfuscate the origin and destination of funds, making identification more challenging.

Moreover, cryptocurrencies provide a means to collect donations and move funds globally, which allows an increase in their financial capabilities without the oversight of traditional financial institutions. For instance, ISIS and its supporters have increasingly used cryptocurrencies for fundraising campaigns, particularly for families in internment camps. What is more, Pro-ISIS groups in regions like Pakistan have raised significant amounts in cryptocurrency for propaganda and recruitment (TRM, 2023).

The quick and straightforward simplification of cross-border transactions by cryptocurrencies constitutes a notable strategic benefit. In contrast to the sluggishness, exorbitance and stringent oversight characteristics of traditional banking systems, cryptocurrencies facilitate expeditious, cost effective, and unmediated international

transfers. This interdependence reduces the risks associated with the movement of funds and improves logistical efficiency of transnational groups' activities.

The decentralized nature that characterized the operation of most cryptocurrencies constitutes a strategic benefit from the perspective of terrorist organizations. The absence of a central authority or any regulatory financial institution for cryptocurrencies provides terrorists with a financial safe haven that appears to be impervious to asset freezes, international sanctions, and other conventional coercive actions.

Furthermore, cryptocurrencies have been identified as a promising instrument for fundraising, given their capacity to be mobilized expeditiously through digital platforms and social networking sites. This attribute has the effect of expanding the potential donor base, thereby allowing terrorist groups to raise financial resources in a more expansive, agile and globalized manner, while concurrently evading the detection risks associated with traditional methods such as bank donations or physical cash movements.

Likewise, the ties between cryptocurrencies and the Dark Web offer a distinct tactical advantage, facilitating the direct procurement of weapons, explosive materials, and other goods needed for the planning and execution of terrorist operations. This integration of financial and technological systems results in the development of a sophisticated logistical infrastructure that is challenging to detect.

Moreover, their operational flexibility when confronted with evolving detection methods and international financial regulation. The analytical sophistication of government agencies has compelled terrorists to rapidly migrate between different cryptocurrencies or towards opaque ones, such as decentralized exchanges (DEX). This adaptability indicates the operational reality in which terrorist groups' innovations perpetually test the limits of international regulatory bodies.

To further understand how terrorist groups employ cryptocurrencies it is essential to consider the following four steps: recollection, storage, movement of funds, and use.

The collection phase is initiated when terrorist groups actively solicit funds through public and private campaigns. These groups often utilize encrypted messaging platforms, social networking sites, and their own websites to disseminate recruitment and demanding messages. The rhetoric employed in these campaigns often appeals to religious,

humanitarian or political causes, thus concealing the actual destination of the funds. Furthermore, they provide detailed instructions on how to donate in cryptocurrency to facilitate the process, minimizing technical hurdles.

Additionally, the implementation of rewards, such as the one offered by a pro-Al Qaeda outlet in the form of 1 Bitcoin for killing a Western police officer, demonstrates that this phase can extend beyond passive recruitment, incorporating material incentives to violent actions (COMMITTEE ON HOMELAND SECURITY, 2021).

Once raised, the funds must be stored in a secure manner until their prospective utilization is determined. In this regard, terrorist groups leverage the numerous digital wallets they might have established without undergoing verification procedures, preferring non-custodial solutions to optimize anonymity. A prevalent strategy involves the distribution of funds across multiple addresses, a maneuver designed to circumvent security protocols.

However, storing involves a latent risk: the partial traceability offered by public blockchains. While identities might be obscured, transaction patterns are not, necessitating the adoption of technical countermeasures such as mixers or the exchange of their cryptocurrencies to others to enhance privacy.

The third step, the movement of funds, represents one of the most exploited advantages of cryptocurrencies. The speed, low cost, and low friction offered by these currencies allow funds to be sent across borders without institutional intermediaries. This characteristic eliminates the need for traditional banking oversight, making it more difficult for financial authorities to detect. In an effort to conceal their activities, terrorist groups often employ DEXs, peer-to-peer marketplaces, or mixers to obscure their transactions, fragment their routes, and mitigate the risk of freezing or seizing their assets. The irreversibility of transactions further reinforces this operational protection, as once moved, the funds cannot be recovered (Brill & Keene, 2014).

The ultimate objective of these actors is to transform cryptocurrencies into goods, services or fiat currency, which can be used to sustain their illicit acts.

This phase presents practical challenges, especially in environments where cryptocurrencies are not widely accepted. Thus, numerous groups seek to reconvert funds through exchanges or Over the Counter (OTC) agents, DEXs, or P2P exchanges. Once

converted, this money is spent on logistic expenses such as salaries, weaponry, materials, and explosives, responding to instrumented rationality oriented towards surveillance and asymmetric power projection.

2.3.1. Evolution of Terrorists' use of Cryptocurrency

The utilization of cryptocurrency has undergone substantial evolution since at least 2014, when initial observations indicated the adoption of digital currencies for the purpose of concealing financial activities, acquiring materials, and soliciting donations. While the initial usage was limited, there has been a marked increase in the number of groups that expressed a growing interest in cryptocurrency. Around 2015, terrorist organizations such as ISIS started to solicit cryptocurrency donations (COMMITTEE ON HOMELAND SECURITY, 2021).

Whereas these early uses were documented, some assessments in 2017 indicated that the adoption of cryptocurrency by terrorist groups remained limited in comparison to its use by other criminal groups. Factors such as technical complexities and predilection for cash would be tied to the widespread adoption. Nevertheless, by 2020, there was an escalating discourse concerning the increased experimentation of jihadist networks with cryptocurrencies, and the US Department of Justice announced the largest seizure of cryptocurrency from terrorist organizations documented, involving millions of dollars across 300 accounts linked to Hamas' military wing, al-Qaeda and ISIS. Furthermore, TRM Labs (2023) identified numerous fundraising campaigns for ISIS families residing in internment camps, in the north of Syria, which aimed to receive cryptocurrency, resulting in the collection of sums ranging from a few dollars to almost ten thousand dollars.

Moreover, there was a substantial surge in the use of the TRON blockchain and a stablecoin called Tether (USDT) among terrorist organizations. The report published by TRM Labs highlights a 240% year-on-year surge in Tether among terror financing entities in 2022 compared to a 78% rise in Bitcoin use. This observation indicated a discernible predilection for stablecoins, presumably to mitigate price volatility.

According to the TRM's 2025 Crypto Crime Report, in the aftermath of October 7, 2023, attacks, the number of entities and individuals linked to the use of cryptocurrencies for terrorist purposes intensified, particularly in relation to Hamas and Hezbollah. The

sanctioned actors include GazaNow, a Gaza-based entity and its founder, Mustafa Ayash, who was accused of channeling financial resources to Hamas following attacks. Additionally, Tawiq Muhammad Sa'id al-Law, a Syrian hawala operator, was sanctioned for providing digital wallets to Hezbollah and facilitating the sale of raw materials from the IRGC-QF. Al-Law was also accused of transferring funds on behalf of sanctioned Syrian entities (TRM, 2025)

The case of the Islamic State of the Khorasan Province (ISKP) is also of particular concern, due to its recent activity. In 2024, ISKP was involved in a series of attacks in various countries including Turkey, Russia, or Austria, where cryptocurrencies played a significant role, such as the financing of the Moscow bombing in March 2024 as well as the transfer of funds to sympathizers involved in infiltration attempts at European sporting events (TRM, 2025). ISKP and other Islamic State affiliates have promoted the use of Monero in their official newsletters (ANNEX II).

2.4.Implications for International Security

Hence, it must be stated that terrorist groups do not seek to pursue an aggressive or hegemonic expansion, but the preservation of their existence. In a context of evolving economic isolation and international pressure, cryptocurrencies have become a functional resource that allows sustaining minimal logistical networks protecting operational infrastructure and maintaining the ability to act when feasible. This logic responds to a basic principle of strategic rationality: survival by evading traceability and dependence on state mechanisms.

This reality evidences a profound vulnerability in the international order: the growing disparity between the nature of contemporary threats and the capacity of states to respond. Consequently, the anarchic system engenders competition among states and within states themselves, resulting in a complex and dynamic back-and-forth dynamic, that might resemble to the nuclear proliferation.

While cryptocurrencies do not pose an immediate and devastating threat comparable to nuclear proliferation, they do constitute a structural disruption that operates on another level: the financial and technological, by destabilizing basic principles of traceability, oversight and monetary sovereignty.

In this sense, cryptocurrencies are reconfiguring the terrain of asymmetric warfare allowing non-state actors to finance themselves without any geographical restriction, evading sanctions and international financial monitoring. This can be characterized as entropic rather than catastrophic as it introduces opacity, decentralization, and chaos into a system that has historically relied on hierarchies and centralized power.

Thus, to speak about the relationship between cryptocurrencies and terrorist financing can no longer admit nuances. That risk is real, has been documented, and has begun to shape several concerns that go far beyond the current volume of illicit transactions.

The decentralized nature of cryptocurrency as well as its certain degree of anonymity, is disrupting the mechanisms on which global financial governance has been built. A system that was meant to be based on traceability and public-private cooperation, is now faced with a tool that allows for immediate transfer with no intermediaries and with active barriers to oversight.

Despite controlling attempts, regulatory agencies confront an extremely dynamic ecosystem. The emergence of new assets, the rise of DeFi, the proliferation of VASPs, and the intractability of applying standards such as the FATF's Travel Rule (Abrams & Andreeva, 2025) demonstrate that the issue is not merely regulatory but structural and operational. The state's capacity to respond is constrained by technical and institutional deficiencies, including a scarcity of tools, training, and interoperability capabilities: most agencies have neither the technical knowledge, nor legal tools necessary to deal with these threats. Thus, the gap between what technology allows and what regulation understands is, in many cases, abysmal.

Despite the public nature of blockchain, the use of mixers, uncustodied wallets and pseudonymous addresses fosters a remarkably robust environment for concealment.

Beyond the financial level, the use of crypto assets by terrorist groups is a direct risk to global stability. This is not an isolated phenomenon; it is part of an ecosystem in which different illegal activities are intertwined and feed off each other. The same infrastructure that is used to launder drug trafficking profits can be used to pay for weapons or send funds to a terrorist group. This multiplicity of uses complicates the investigation and disperses institutional resources, especially when there is no clear line connecting the warning signs to them.

In this line, reducing this phenomenon to a technical problem would be an oversimplification. Terrorist adoption of cryptocurrencies should not be interpreted as a technological accident or a current trend, but as a tactical and strategic adaptation to an increasingly hostile environment that hinders their chances of survival and expansion. The key is to understand that crypto adoption takes place in a historical context where traditional financial channels are increasingly restricted, driving terrorist groups towards this innovation. After 9/11, traditional financial channels – and even informal networks such as hawala – became more dangerous for terrorist groups. In this context, crypto assets offer a rational, decentralized, and unmediated solution suitable for evading controls without the need for large infrastructures or advanced technical expertise.

In this context, the use of cryptocurrencies is not only a rational course but also a predictable one. The attractiveness of a decentralized means of payment, without clear oversight, and which allows small contributions to be collected from a global base of supporters, becomes evident. This approach, far from being a mere innovation, stands as an act of survival in an increasingly digitalized and globalized environment. Terrorist organizations are no strangers to this transformation. In this sense, like any other actor, they seek to adapt to remain relevant.

Therefore, the challenge no longer lies solely in the volume of resources mobilized, but in the transformation of the rules of the game. Ultimately, cryptocurrencies have enabled these actors to evade traditional limits of state power, consolidating their presence in a decentralized and increasingly normalized digital space.

Chapter 3: Case Study and Study on Legislations

3.1. Case Study: Hamas & the Palestinian Islamic Jihad and their use of Cryptocurrencies

Hamas and its use of Cryptocurrencies

The Hamas organization, classified as a terrorist group by the United States, Israel, and the European Union, was established in 1988 during the First Intifada. Since their establishment, Hamas (also known as Harakat al Muqawama al Islamiyah, or Islamic Resistance Movement) has evolved into a multifaceted organization, displaying a dualistic role as both a political entity in Gaza and a terrorist group targeting Israel.

The organization has historically relied on financial support from Iran. For this state, Hamas represents a fundamental advantage in its regional rivalry with Israel and the US, allowing it to project power indirectly in a highly volatile region without entering open conflict. Therefore, the State has been providing military and economic assistance since the 90s, including an annual funding ranging from \$20 million to \$100 million (ACJ, 2025). This support also embraces intensive military training, particularly by the Islamic Revolutionary Guard Corps (IRGC) and Hezbollah, and technology transfer, especially in relation to the development of rockets and underground tunnels.

This dynamic has exhibited a notable degree of resilience, even in the face of temporary crises, such as the suspension of Iranian funding in 2012 due to political disagreements during the Syrian civil war (AJC, 2025).

The restoration of Iranian support in 2017 indicates the pragmatic and realistic nature of their alliance. Recognizing Hamas' strategic significance as means of exerting pressure on Israel and its Western allies, Iran has persistently reinforced its military and financial support to the group. This has contributed to their survival and relevance in the regional context.

This analysis reveals that their relationship is a component of a regional realpolitik logic in which both actors align in their opposition to Western hegemony in the Middle East and Israel. Despite the ideological differences between Iran, a Shiite state, and Hamas, a Sunni organization, the alliance between them is driven by shared objectives rather than ideological alignment. It serves as an illustration of how a state can leverage non-state actors to augment its geopolitical influence without assuming the direct costs associated with interstate confrontation.

Moreover, since at least 2019, the military wing of Hamas, the Izz al-Din al-Qassam Brigades, has engaged in cryptocurrency donation campaigns, primarily using Bitcoin, plus, the US Department of Justice found more than 150 cryptocurrency wallets associated with the Izz al-Din al-Qassam Brigades in 2020 (Congressional Research Service, 2024). These campaigns, launched on encrypted channels on Telegram, have incorporated software that generates unique addresses for each transaction, employing platforms like Binance, and using OTC exchanges for fund laundering (Burgess et al., 2024).

Recent reports indicate that cryptocurrency wallets linked to Hamas have received approximately \$41 million between 2020 and 2023 (Congressional Research Service, 2024). In addition, the US Treasury Department is investigating \$165 million in cryptocurrency linked transactions that could have facilitated the funding of Hamas prior to the October 2023 attacks. Nonetheless, the reliability of the \$41 figure remains a subject of debate.

In the aftermath of the October 7, 2023, attacks, US authorities have remained vigilant for any indicators that Hamas-affiliated entities might have continued their efforts to solicit cryptocurrency donations. In response, the Treasury Department expanded its sanctions to encompass additional Hamas financial agents and facilitators engaged in cryptocurrency-related activities. Moreover, it has issued a directive to financial institutions, urging heightened vigilance in the monitoring and reporting any related activities, and Israeli authorities have reportedly taken action by freezing any additional wallet associated with Hamas (Congressional Research Service, 2024).

Nonetheless, entities such as GazaNow and the Mujahideen Brigades persisted in receiving substantial contributions in crypto assets. The persistence of these practices suggests the limited effectiveness of the coercive measures applied to date by Israel and the US. In the case of GazaNow, the agency continued to solicit cryptocurrency even after being subject to sanctions by OFAC and other international agencies, accumulating thousands of dollars since October 2023 (TRM, 2025).

In March 2025, the Department of Justice unveiled the dismantling of a Hamas financing scheme, seizing approximately \$200,000 in cryptocurrency. These funds were traced from fundraising addresses related to Hamas, also used to launder more than \$1.5 million since October (Office of Public Affairs, 2025).

It is also estimated that Hamas has employed a shifting array of cryptocurrency wallets and addresses on encrypted platforms to receive donations, which have then been laundered through virtual currency exchanges and OTC brokers.

Hence, the case of Hamas illustrates how non-state actors exploit gaps in the international system to finance their operations, especially if they have the strategic backing of a state. The convergence between traditional state sponsorship and emerging technologies reveals a pattern of structural adaptation consistent with the postulates of offensive

neorealism. In an international environment, marked by constant competition and asymmetry of power, the use of cryptocurrencies is being consolidated as an emerging tool in the financial arsenal for terrorist groups.

The Palestinian Islamic Jihad

The Palestinian Islamic Jihad (PIJ) is a crucial actor in the geopolitical landscape of the Middle East, especially regarding the Israeli Palestinian conflict. Whereas not as extensively covered by media as Hamas, the PIJ has evolved into an armed group with significant operational capacity and firmly established within the Gaza Strip. The United States designated the PIJ as a terrorist organization, reflecting its role in perpetuating violence and its relevance for international security (Congressional Research Service, 2024).

The origins of the PIJ date back to the Muslim Brotherhood, which initially imparted a Sunni ideology to the organization and placed a significant emphasis on the Islamization of the Palestinian cause. Nevertheless, the group's strategy involved a shift in alignment to the Shiite revolutionary worldview, particularly under the influence of Ayatollah Khamenei (AJC, 2025). This shift meant a strategic move towards the establishment of a reliable sponsor: Iran. The PIJ's operational approach integrates Islamic rhetoric and a radical militaristic praxis, facilitated by the transnational sponsorship network led by Iran.

This strategic alliance between a Sunni militia and a Shiite theocratic state underscored a geopolitical instrumentalization logic. Iran perceives the PIJ as a means to harass Israel, while the PIJ employs Iran as a provider of funds, weapons, and legitimacy within an axis of resistance. This dependence was strengthened in episodes such as the Iranian funds cut-off in 2015, which was resumed once the PIJ adopted the Iranian narrative in Yemen (AJC, 2025).

Therefore, the funding of the PIJ functions as a way of proxy power projection, enabling Iran to operate at minimal costs and without assuming any political or military cost spent at a conventional war. For this reason, the PIJ is not a conventional ally, rather it merely assists Iran in preserving its position in the international arena.

To reinforce their alliance, the PIJ's military apparatus has undergone several improvements through training provided by the Islamic Revolutionary Guard Corps (IRGC) and Hezbollah. Moreover, the PIJ's active involvement in offensives, such as the

August 2022 and May 2023 ones, corroborates its capacity to function as an autonomous military entity. Plus, the documented participation of PIJ members in the October 2023 attacks, alongside Hamas, reinforces the notion of the tactical coordination between Iranian-backed Palestinian armed factions (AJC, 2025).

In relation to whether the PIJ is engaged with virtual currencies, according to data collected by the Wall Street Journal, it is estimated that the PIJ received approximately \$93 million between 2020 and 2023. This transition to the digital currency realm coincides with periods of heightened tensions, such as the Israeli counter-offensive in 2023 (Akartuna, 2023).

Conclusions

Thus, it can be deduced that Iran is acting as a rational actor employing Hamas and the PIJ as an indirect strategy to maximize its power against regional rivals such as Israel and Saudi Arabia. This logic aligns closely with Mearsheimer's theory, exemplifying how states seek to become regional hegemons because the anarchic system imposes incentives to accumulate as much power as possible. In the case of Iran, its support responds to a strategy to project its influence in territories where its direct involvement would be costly or have a high political implication. This denotes the use of a form of soft balancing through proxies, a tactic that aligns with the Mearsheimerian idea of weakening adversaries (Israel) without engaging in direct confrontation.

The duality between offensive and defensive approaches is key to understanding Tehran's behavior. On one hand, the support to these groups is a tactic for regime preservation and dissuasion against its rivals (Israel or the US). This logic is reinforced if Iran is perceived as a state acting to maintain its regional balance and ensure its survival under constant international encirclement. Nonetheless, it could also be reasoned that Iran is going beyond mere defense, and it is actively seeking to increase its sphere of influence in the Levant and the Gulf through proxies, ideological alliances, and financial networks.

Furthermore, the relationship between Iran and these groups is not unidirectional but characterized by a noticeable reciprocity, as Iran acquires the capacity to control the region, and the organizations receive substantial benefits, including training, resources, and a great degree of symbolic legitimacy.

3.2. Study on the Current Legislation on Cryptocurrencies

At the core of this phenomenon, the effectiveness of regulatory frameworks, particularly AML/CFT mechanisms is being called into question, leading to a reconsideration of state oversight and response capacities in a context characterized by evolving decentralization and technological sophistication.

While some jurisdictions impose strict rules, others maintain permissive or ambiguous standards. This inconsistency creates safe havens for criminal actors, who route funds through low-regulation environments to avoid detection. This absence of a unified international regulatory framework undermines deterrence and enforcement.

The existence of anomalous regulatory frameworks, characterized by divergent approaches and an absence of uniformity further underscores the complexity of the issue. Despite the existence of various entities, such as the FATF, that aim to control this threat, not all states have adopted their recommendations. Moreover, while some jurisdictions impose strict rules, others maintain permissive or ambiguous standards. This inconsistency creates safe havens for criminal actors, who route funds through low-regulation environments to avoid detection. This absence of a unified international regulatory framework undermines deterrence and enforcement.

Therefore, it is essential to examine the diverse regulatory frameworks, to explain the observed discrepancy and ascertain the underlying causes of these shortcomings. In addition, the legitimacy of states such as Iran is being called into question. As previously observed, Iran has been exposed to have connections with terrorist groups and might be using crypto assets to facilitate the financing of these organizations.

Hence, this study will focus on three key actors in the field: the United States, the European Union and Iran. Each of these countries employs a distinct approach to cryptocurrency regulation, supervision, and the implementation of control measures in the context of combating illicit uses.

3.2.1. The United States

The American legislation is divided into federal and state governments' regulations. At the federal level, most of the focus has been at the administrative and agency level, including the Securities and Exchange Commission (SEC), the Federal Trade

Commission (FTC), the Commodity Futures Trading Commission (CFTC), and the Department of the Treasury through the Internal Revenue Service (IRS), the Financial Crimes Enforcement Network (FinCEN), and the Office of the Comptroller of the Currency (OCC) (Dewey and Patel, 2025).

The Public Law 116-283 of January 1st, 2021, which contains the Anti-Money Laundering Act (AML Act 2020), serves to reinforce the role of the FinCEN as the primary entity involved in the fight against money laundering (Thornberry, 2021). According to the FinCEN, any entity that accepts and transmits cryptocurrencies is designated a “Money Service Business” (MSB) and is obligated to comply with Anti-Money Laundering (AML) regulations. The Treasury Department and the Office of Foreign Assets Control (OFAC) have intensified oversight over exchanges that facilitate transactions with sanctioned jurisdictions. All citizens and entities within the country are prohibited from conducting commercial activities with individuals or companies listed on the OFAC’s “Specially Designated National List” (SDN list). This proscription extends to cryptocurrency transactions involving sanctioned countries, such as Iran, North Korea and Russia (Dewey and Patel, 2025).

Several bills have been introduced in the Congress since 2022. These include the Responsible Financial Innovation Act (RFIA), a bill designed to provide regulatory clarity to the agencies supervising digital assets markets, establish a regulatory framework for digital assets, integrate these into banking law and existing tax, and spur innovation. As well as the Toomey Stablecoin Bill, which will create a regulatory framework for stablecoins and their issuers, outlining options for issuance and distinguishing stablecoins that do not offer interests from securities (Dewey and Patel, 2025).

Moreover, the House of Financial Services Committee aims to develop a regulatory framework for cryptocurrencies to protect investors and consumers. Now, the sale of cryptocurrency is regulated if it constitutes the sale of a security under state or federal law or is considered money transmission under federal or state law. Entities that facilitate the sale of securities or act as a market maker in crypto securities have to be registered as broker dealers with the SEC and members of the Financial Industry Regulatory Authority (FINRA), and these can only be traded on licensed security exchanges or at ATS approved by the SEC.

The IRS taxes cryptocurrency as property, not currency per se. This affects the record-keeping, the payment of taxes on gains from sales or the use of crypto for the purchase of goods and services. Specific forms (Schedule D of IRS Form 1040 and IRS Form 8949) are used to report capital gains and losses. (Dewey and Patel, 2025).

At the State level, many governments have also proposed laws. Some states like Wyoming or Utah, have tried to promote these assets by favorable regulations, exempting cryptocurrencies from state securities laws or money transmission statutes, and creating crypto-friendly banking regulations. Arizona, Hawaii, Kentucky, Nevada, Utah, Vermont, and West Virginia have adopted a regulatory sandbox program that allows innovators in fintech, blockchain or cryptocurrencies to test products with regulatory relief for a limited time (Dewey and Patel, 2025).

Conversely, a growing number of states are making it harder for blockchain companies to operate by requiring money transmitter licenses and strict adherence to securities laws.

3.2.2. European Union

In contrast to the United States, where the regulatory framework for cryptocurrencies is characterized by fragmentation and the involvement of multiple agencies, the European Union has adopted a more consolidated approach, evidenced by the enactment of Regulation (EU) 2023/1114, also known as MiCA, and the recent AML/CFT Directive (2023/1113).

MiCA regulates the issuance, marketing, and trading of cryptocurrencies and other services that are not yet covered by pre-existing financial services legislation. The primary goal of this regulation is to protect investors and preserve financial stability, while fostering innovation and promoting the attractiveness of cryptocurrencies. MiCA dictates transparency requirements, ensuring all crypto businesses disclose risks associated with investments and keep consumers informed.

The 2024 EBA report emphasizes that EU regulatory policy is based on three fundamental pillars: risk-based supervision, mandatory traceability of transactions and greater cooperation between national and European supervisors (EBA, 2024). In order to operate within the EU, all Crypto-Asset Service Providers (CASPs), issuers of asset referenced tokens (ARTs), and e-money tokens (EMTs) must be authorized and demonstrate that they comply with the AML/CFT standards (European Banking Authority, 2024).

The EU has expanded its AML/CFT framework to encompass cryptocurrency via the Fifth Directive against Money Laundering, thereby imposing monitoring and reporting requirements on VASPs (Rodrigues & Kurtz, 2019). MiCA works in conjunction with this directive as well as the Transfer of Funds Regulation (TRF) to combat illicit activities. This includes the implementation of a risk-based approach with Customer Due Diligence, reporting requirements for crypto transactions, and the implementation of the crypto Travel Rule, a regulatory provision that obligates Virtual Asset Service Providers (VASPs) and other financial institutions to obtain, hold, and transmit information about the origin and beneficiary of virtual assets transfers (Abrams & Andreeva, 2025).

The TFR (Regulation EU 2023/113) extends information requirements for transfer of cryptocurrencies to ensure financial transparency in line with international standards (European Union, 2023).

3.2.3. Study on the European and American Legislation

The responses adopted in each jurisdiction exhibit notable disparities in terms of coherence, effectiveness, and strategic vision. These discrepancies are not merely technical or administrative in nature; rather, they reflect profoundly divergent political and regulatory perspectives on the integration of this disruptive tool into the prevailing international financial order.

The European Union adopted a prominently preventive stance, which has embarked on a comprehensive and harmonized regulatory framework through its proposal for MiCA. This initiative aims to address the details inherent in cryptocurrencies through a centralized structure that circumvents the internal regulatory fragmentation of the bloc.

It must be said that the MiCA proposal is ambitious and has the potential to ensure regulatory consistency, especially given its explicit attempt to subject decentralized exchanges (DEXs) to strict legal domicile requirements within the EU. Nonetheless, this strategy gives rise to significant concerns regarding the viability of constraining European citizens' access to cross-border and technologically decentralized platforms, whose appeal precisely stems from their capacity to evade national judicial controls.

Additionally, the incorporation of cryptocurrency service providers into traditional AML/CFT regulations, as outlined in the EU's Fifth Anti-Money Laundering Directive,

represents a critical acknowledgment of the criminal potential associated with these assets. Nevertheless, the successful execution of this directive demands solid regulatory and operational endeavors by member states, particularly regarding technical resources and analytical capabilities to monitor the intricate digital financial transactions, domains in which deficiencies may be noted. This proactive European approach, while well-intentioned, inevitably faces limitations, especially in the face of the dynamism and speed of innovation in the crypto sector.

The American regulation is characterized by notable institutional and jurisdictional fragmentation. Federal agencies such as the SEC, CFTC, FinCEN, IRS and OCC have each adopted distinct regulatory perspectives, producing considerable operational uncertainty for businesses and individuals. This fragmentation gives rise to a multitude of concurrent interpretations regarding the legal nature of these assets, particularly in the pivotal discourse surrounding the question of whether cryptocurrencies fall under the scope of the Howey Test¹ when deemed securities or commodities. This legal uncertainty has the potential to suppress legitimate innovation and create regulatory ambiguities that could be exploited by terrorists.

At the State level, the US exhibits even greater regulatory diversity. While some states actively promote favorable environments for blockchain innovation, others have taken more restrictive stances. This heterogeneity may create an environment conducive to innovation by allowing for the concurrent implementation of multiple experimental regulatory approaches, but there is also the potential increase in vulnerabilities, particularly regarding regulatory arbitrage, where companies and illicit actors seek jurisdictions with lax regulations or limited capacity.

A particularly salient point in both jurisdictions pertains to the regulation of DeFi. The EU has taken steps to impose bans or restrictions on specific decentralized platforms unless they adopt regulated corporate structures. By contrast, the US is still deliberating on the application of traditional legal frameworks such as the Commodity Exchange Act to novel Decentralized Autonomous Organizations (DAOs). This discrepancy highlights a fundamental threat in the realm of international crypto regulation: the inherent difficulty

¹ American legal framework used to determine if a transaction can be qualified as an investment contract and has to be regulated.

in extending legal frameworks designed for centralized entities to financial organizations that seek to circumvent conventional regulatory oversight.

3.2.4. Iran

The Iranian government's position on cryptocurrencies has been characterized by its inconsistency. While the Iranian government has formally acknowledged the legitimacy of cryptocurrency mining since 2018 (Turner, 2020), it has concurrently prohibited the utilization of cryptocurrencies as a medium of exchange within the country.

As US sanctions began to have adverse effects on the economy, the government started to reconsider its stance on digital assets (Freeman Law, 2022). In 2019 regulations were introduced to legalize cryptocurrency mining as a legal economic sector but not as a means of payment.

Iran has been exploring the creation of its own digital currency since 2018, in order to enhance the government's control over the national currency and its users.

Sadeghi and Nasser assert that in Iran, the primary issue is that the government has sought to exploit cryptocurrency mining as a source of revenue, yet without sanctioning its utilization as a medium of exchange (Sadeghi & Nasser, 2021).

Nonetheless, in the late 2024, the Central Bank of Iran (CBI) restricted the conversion of Iranian Rials into crypto conversions on the primary electronic payment network (Smart & Ahlawat, 2025), moreover it has recently approved a "Policy and Regulatory Framework for Cryptocurrencies" alongside other governmental bodies.

In January 2025. The government issued a directive formalizing cryptocurrency market regulation (Boltuc, 2025) and crypto platforms can now obtain direct payment gateways within a regulatory framework, and brokers must conduct Iranian rial transactions transparently through designated accounts approved by the CBI.

3.2.5. Study on the Iranian Legislation

Iran's cryptocurrency regime is a dense, contradictory, and evolving regulatory framework characterized by a structural tension between state control, the need for technological innovation, and geoeconomic survival under conditions of external

pressure. Iran has adopted a regulatory framework that is deeply instrumental in nature, reflecting its logic of containment rather than a coherent digital strategy.

The country's initial approach was prohibitionist; in 2018, the trading and holding of cryptocurrencies were banned due to concerns regarding money laundering. However, this decision was reversed in 2019, when the intensification of international sanctions compelled the regime to reconsider the functional potential of crypto assets to avoid financial isolation. This shift did not signify a fundamental legal redefinition, rather, it was a sensible response to a pressing need: reduce the reliance on the US dollar in the face of an economic blockade (Freeman Law, 2022). This motivation was reflected in the conditional legalization of mining, recognized as a legal economic activity, but restricted by asymmetric energy policies and subject to centralized control through the Iranian Central Bank (Turner, 2020).

In practice, miners must sell their digital assets to the state in exchange for energy. This dynamic of economic subjugation curtails the autonomy of the sector and also engenders an atmosphere of legal ambiguity, execrated by intermittent prohibitions and opaque oversight. Concurrently, the regime explicitly prohibits the use of cryptocurrencies as a medium of exchange within the national jurisdiction and the possession of substantial global crypto assets. This regulatory paradox reflects a double-edged policy: the state seeks to benefit from the potential of cryptocurrencies, while it maintains strict control over their monetary function.

The introduction of the crypto-rial, a Central Bank Digital Currency (CBDC) currently in the testing phase (TRM , 2023), serves to further bolster this authoritarian centralization logic. Contrary to its portrayal as a decentralized solution, the digital rial is a mechanism for financial surveillance and the reinforcement of the state's monopoly on monetary issuance. It is not envisioned as a means of evading sanction but as a domestic instrument of fiscal and monetary control.

The regulatory framework governing exchanges underscores the constraining nature of the model. Iran has implemented a licensing system that imposes stringent requirements, compelling the distribution of sensitive user data and impeding the functionality of these platforms. These regulatory demands, rather than fostering a balance between security and technology, engender discord with local operators and have compelled numerous

users to adopt a state of digital informality. This difficulty is further intensified by the absence of a designated tax regime, which hinders the ability to trace sanctions and fosters an environment conducive to illicit activities.

Internationally, Iran is listed alongside North Korea or Myanmar on the FATF blacklist, due to its persistent structural deficiencies in AML/CFT. The FATF has identified two key areas of concern: the absence of criminalization for certain financial crimes and the Iranian inability to freeze terrorist assets (Malakoutikhah, 2018). This, alongside the opacity of Iranian institutions, hinders the evaluation of the country's genuine commitment to AML/CFT standards.

The Iranian geostrategy is another pivotal factor. The use of digital assets to circumvent sanctions has included bilateral initiatives with Russia, such as the joint development of gold-backed stablecoin, and the alleged involvement of IRGC-linked entities in financial avoidance schemes. Moreover, in 2021 annual electricity employed for mining activities in Iran amounted to approximately 10 million barrels of crude oil, representing 4% of the country's total oil exports and indicating that Iran may be avoiding conventional financial channels by mining to monetize its energy output and circumventing formal export sanctions.

In this context, the Iranian population has adopted cryptocurrencies as means to safeguard their capital against inflation, facilitate international transfers and access digital goods (Smart & Ahlawat, 2025). These strategies have been employed through the use of virtual private networks (VPNs) and fake IDs. This parallel digital economy has exposed the limitations of the official financial system and challenged the regulatory capacity of the State.

In January 2025 the central authorities adapted a formal cryptocurrency market regulation. Hence, cryptocurrencies now obtain direct payment gateways within a regulatory framework and brokers are obligated to conduct Rial's transactions transparently through certain accounts designated by the CBI. This means that the CBI is the sole authority to regulate the cryptocurrency market, including the licensing, marketing, oversight, and the issue of directives – all traders require a license issued by the bank. Moreover, all transactions from fiat to crypto must be overseen by a government-controlled API (Bourton, 2025).

However, it must be stated that there is no evidence on effective implementation of this regulation. What is more, the concentration of control in a government entity with no effective accountability mechanisms or independent oversight casts doubt on the veracity of the tools, as they can facilitate an opaque and politicized management of digital financial flows.

This regulatory system could allow for selectivity in the granting of licenses, in addition to enabling channels under state control for operations that escape international scrutiny. This assessment represents a reaffirmation of the State's logic of survival, in the face of external pressures through internal mechanisms of containment and control.

Moreover, this has given rise to apprehension regarding the potential for statal or parastatal actors to exploit the crypto space in the Iranian context to clandestinely finance non-state armed groups. For several decades, Iran has regarded organizations such as Hamas or Hezbollah as national liberation movements, a narrative that has been employed to justify its financial military, and logistical support. The IRGC's Quds Force, a pivotal entity in Iran's regional power projection, has historically served as the conduit through which this sponsorship is articulated (Congressional Research Service, 2024).

While there is no conclusive evidence that Iran directly used cryptocurrencies to fund these groups, the convergence between three factors – Hamas and PIJ's documented use of crypto, Iran's weak AML/CFT architecture and the state's willingness to evade sanctions is alarming. This suggests a highly exploitative environment. Hence, rather than a punctual accusation, this analysis implies that Iran configures a structural risk infrastructure that could have been instrumentalized directly or through third parties to sustain the funding of these actors.

The anonymity and transnationality that Iran explores to maintain its international trade could be co-opted by networks linked to terrorist financing. The absence of detailed public strategies from Iran to mitigate these risks, coupled with its reluctance to reform its institutional controls substantively, and Iran's cheap electricity, further fuels these suspicions.

Thus, a positive evaluation of the Iranian regulatory framework on cryptocurrency according to the parameters of coherence, openness and predictability is not possible. Despite sporadic advancements, the regulatory structure is characterized by its restrictive

nature, reactive approach, and orientation towards state control rather than technological advancement or financial inclusion.

3.3. Comparative Assessment

In the European Union and the United States, attempts at regulation seek to integrate cryptocurrencies without destabilizing their systems. In the EU, this integration is proposed through the MiCA regulation, which aims to standardize the standards on crypto service providers and reduce fragmentation. In the US, although this fragmentation is greater, there is an active legal infrastructure, as different agencies compete for jurisdiction, but all of them operate under the logic of preserving the dynamism of the market without compromising the security of the financial system.

Furthermore, both portray the tension on how to adapt the legal framework to the rapid pace of technological innovations. The EU wants cryptocurrencies to enter the system, but it wants to avoid a weaker institutional control at all costs. While the US hesitates between allowing experimentation and shutting it down when it threatens its sectoral regulatory model. Despite the challenges, both frameworks point to a regulatory modernization that is based on principles such as transparency, accountability, and consumer protection.

Iran, on the other hand, operates under a different logic. There, cryptocurrencies are a resource in the face of geopolitical isolation, hence, regulation does not seek to integrate but to instrumentalize: Plus, it does not attempt to stabilize the market but to take control of it; and it is not designed to protect the user, but to protect the state and its interests.

While the EU and the US regulate from a logic of predictability and market order, Iran regulates from uncertainty: it prohibits, then partially permits, then restricts again, then legalizes...accordingly to the needs of the moment. This reactive and contradictory logic generates an environment of legal ambiguity, which favors both informality and repression.

The difference is also clear at the institutional level. While in the EU and the US regulatory agencies are constrained by legal and democratic frameworks, in Iran monetary and financial authority is subordinated to political and national security

objectives – one can deduce it is a result of the desire for total fiscal surveillance and control.

At the international level, this divergence is even more evident, the US and the EU actively participate in the development of global standards for AML/CTF while Iran, remains on the FATF blacklist. Nevertheless, it must be stated that despite their differences, none are fully effective in curbing this type of terrorist financing.

The lack of international coordination is a great threat as the anarchic system implies the employment of gray zones, such as Iran, in areas like cryptocurrencies, where legal ambiguities allow circumvention of sanctions, illicit financing and transfer of power to non-state actors. Moreover, the absence of a coordinated regime is fragmenting the international order and producing a system susceptible to conflict. Hence, the lack of coordination between powers only reinforces the logic of survival and encourages offensive behavior, reducing the effectiveness of multilateralism.

Besides, the absence of a coercive capacity in international financial organizations results in significant fragmentation. If a state, for instance, Iran, elects to abstain from cooperation or to engage in actions that are not subject to oversight, there is an absence of an effective supranational mechanism to impede such activities.

International cooperation, being non-binding, is inherently fragile. Non-state actors, including terrorist groups, have been known to exploit these gaps. They use cryptocurrencies as they offer decentralized, pseudonymous, cross-border transactions that are difficult to trace without active state collaboration. The absence of a robust regulatory framework in states or the lack of enforcement of such a framework, grants these actors a degree of freedom in their use of these technologies without rigorous scrutiny. Conversely, the absence of global coordination hinders the effective tracking of digital assets. Pseudonymous transactions, unregulated platforms and lax jurisdictions allow funds to move easily. This absence of harmonization is a vulnerability exploited by these groups, as the legality of digital assets can vary significantly across different states, and that gap is precisely what allows terrorist groups to stay under the radar.

Before conclusions, it is important to assert that it has been observed that financial power is experiencing a structural reconfiguration, driven by three paths. The technological decentralization of capital has begun to erode the historical monopoly of states over

monetary and financial control, as evidenced by the emergence of cryptocurrencies, DeFi, or P2P exchanges. This decentralization does not eliminate power, rather, it redistributes it among non-state actors, private infrastructures, and jurisdictions.

Plus, some actors are taking advantage of opacity to build alternative financial corridors, thereby enabling the flow of funds that is not subject to Western oversight.

Consequently, the financial landscape is suffering a transformation, moving from a competition between currencies to a competition between divergent legal systems. This dynamic could potentially indicate the decline of the Westphalian system of states: the principle of a state's sovereignty over financial systems is showing signs of weakening, as besides volume of reserves and value of the currency, it now encompasses surveillance capacity, technological mastery and ability to control.

Conclusions

The advent of cryptocurrencies can be constructed as a functional process of disintermediation of violence, insofar as it enables non-state actors to finance their activities without resorting to formal financial channels, which are dominated by states. Following a Hobbesian logic, the capacity to obtain economic resources without the intermediation of the State represents a substantial shift in the distribution of power. Then, cryptocurrencies do not emerge as a fully autonomous alternative to traditional financing methods, but rather as a hybrid financial structure whose capacity for evasion functions in response to the inherent fragmentation of the international system. The traditional Westphalian conception of state power is being challenged by a network of decentralized nodes capable of mobilizing resources and influence beyond the confines of traditional state-centric logics.

Although one can deduce that cryptocurrency still accounts for a relatively small fraction of total terrorist financing, focusing solely on such a proportion would be a simplistic prospect. The relevance of this transformation lies less in its current magnitude and more in its innovative capacity. Evidence found suggests that this threat is not speculative. The risk is present in the capacity for escalation, which could manifest itself quickly if measures are not implemented with vision and anticipation.

This phenomenon should be understood as an indicator of a deeper transformation in the relationship between the state, technology, and security. Cryptocurrencies, in and of themselves are not the fundamental problem. They are the reflection of a system in transformation, where non-state actors learn to navigate in the gray areas of global governance. To neglect this convergence between technological innovation and structural pressure would imply a denial of a threat that has the necessary elements to consolidate in the coming years.

Tracing cryptocurrency requires more than traditional forensic skills. It involves understanding blockchain architecture, cryptographic protocols, and constantly evolving technologies and most law enforcement agencies lack the technical infrastructure and skilled personnel required to keep up.

This analysis has shown that cryptocurrencies represent a disruptive financial tool used by both state and non-state actors to redefine the balances of power in the international system. Through the case study of Hamas and PIJ and their relationship with cryptocurrency and the Iranian state sponsor, it has become evident how the structural logic of offensive realism is manifested in the instrumental use of cryptocurrencies to circumvent sanctions, maintain networks of allies, and project indirect influence in conflicting zones.

One of the most significant findings is the comprehension that, although there is no conclusive evidence that Iran has funded terrorist groups through cryptocurrencies, the convergence between the fragility of Iran's regulatory framework, its history of sponsoring armed groups, and the functional opacity of its financial system poses a considerable structural threat. This threat is neither conjunctural nor accidental, but arises from a strategic system designed to operate outside international norms, undermining multilateral mechanisms for oversight and containment of terrorism.

Likewise, the comparative analysis of the EU, the US and Iran has revealed profound divergences in both their conception and their execution. While the former seeks to integrate cryptocurrencies within the traditional financial system under a logic of transparency and accountability, Iran adopts a strategy of instrumentalization, where opacity and centralized control serve as tools of state survival. Nevertheless, despite their

structural and philosophical differences, neither of these regulatory models has been able to effectively curb terrorist financing through digital assets.

The transnational and pseudonymous nature of cryptocurrencies has eroded a central tenant of modern state sovereignty: control over financial instruments. By facilitating transactions outside the reach of regulated institutions, these assets have generated an environment in which actors such as Hamas can obtain funding without relying on traditional networks. This transformation not only implies an operational change, but a structural reconfiguration of the foundations on which global financial governance is based.

In this context, cryptocurrencies should not be analyzed only as one more tool in the arsenal of terrorist groups but as a symptom of a deeper transformation: the decentralization of financial power in an international system that has failed to adapt quickly enough. The threat lies in the growing trend towards an environment where state surveillance and international cooperation are overwhelmed by technologies designed precisely to resist external intervention.

Ultimately, this paper demonstrates that cryptocurrencies are not a neutral technological threat but a strategic issue of the first order. Their use by terrorist groups represents a growing fissure in the international system. In the face of this threat, fragmentary regulations and diplomatic declarations are not enough. What is required is coordinated, structural and technologically competent approaches, that recognize that state sovereignty in the 21st century is increasingly being played out on the digital plane.

Limitations

This study has approached the financing of terrorism through cryptocurrencies from a neorealist perspective, placing special emphasis on the case of Iran and its relationship with Hamas and the PIJ. Nevertheless, as with any analysis focused on a dynamic and rapidly evolving phenomenon, it presents certain limitations that have to be acknowledged.

First, the lack of access to classified sources or confidential operational data limits the possibility of establishing a direct empirical connection between the Iranian state and the use of cryptocurrencies for terrorism financing. While the use of digital assets by Hamas and the PIJ has been documented, and the existence of conducive structural conditions

within the Iranian financial system has been demonstrated, it has not been possible to confirm with conclusive evidence the existence of a direct and verifiable transfer line of crypto assets between them.

Secondly, the speed of technological innovation poses a methodological challenge. Many of the mechanisms used in the crypto ecosystem are in continuous transformation, which means that any technical tool runs the risk of becoming obsolete. Despite including recent developments (such as DeFi platforms), the pace of evolution of the industry requires constant updating of the conceptual and regulatory apparatus.

Another limitation stems from the fragmentation of the international regulatory framework, which makes a logical and uniform comparison extremely difficult. Even though the paper has contrasted the regulatory frameworks of the EU, the US and Iran, it has not delved into the regulatory responses of other relevant powers such as Russia, Turkey or the United Arab Emirates.

This paper has also opted for an approach focused on the structural analysis of the international system and the conditions of possibility of allowing the financing of terrorism through digital assets, but it has not explored the ideological, sociological, or psychological dimensions of recruitment and radicalization that could intersect with the use of these digital tools.

As for future lines of research, several lines worth exploring have been identified.

- Exploration of the crime-terrorism-crypto nexus on the dark web markets, with attention to how these hybrid spaces can configure decentralized networks of military financing, trafficking or logistics.
- Assessing the impact of new emerging technologies, such as CBDCs, Web3, and asset tokenization, on global governance and security policies.
- Analysis on the specific use of crypto assets by different terrorist groups, using blockchain forensic analysis and collaboration with specialized cyberintelligence agencies.

These lines would enrich the analysis begun in this paper and offer new perspectives to understand the phenomenon, which, far from being marginal, is redefining the operational conditions of power in the 21st century.

Recommendations

A series of recommendations ought to be implemented in order to enhance both financial and international security policies and control the phenomenon of terrorist financing.

States have the authority to consolidate control over digital finance channels, preventing illicit actors from exploiting regulatory lacunas. Then it would be essential to:

- Strengthen state monitoring exchanges, especially P2P and DeFi.
- Force exchanges to share transaction data with international (or national) financial intelligence agencies, including on pseudonymous blockchain systems.
- Develop a national blockchain analysis tool with advanced attribution capabilities.

Coordination among different nations would be necessary to further implement surveillance mechanisms:

- Establish a multilateral coalition specific to cryptofinance and CFT, based on shared intelligence.
- Create a joint EU-US-G7's allies task force under the coordination of bodies such as the FATF to harmonize sanctions and illicit wallets' identifiers.

Reform the current regulatory frameworks: closing the loopholes.

- The EU has to push for third countries to adopt similar rules as MiCA and Travel Rule, as a prerequisite for economic cooperation.
- In the US the fragmentation must be resolved by unifying the federal framework with clear authority to create a lead crypto regulatory agency.
- Push for mandatory identity verification (KYC) mechanisms using signature systems.

Deterrence through economic power and targeted sanctions

- Apply direct sanctions against exchanges operating in lax jurisdictions if they do not cooperate actively against terrorist financing.
- Imposing trade or technological restrictions on state actors that leave the door open for evasion.

The international system will only be able to preserve the integrity of its structures against terrorism financing if it achieves regulatory harmonization and interstate deterrence.

Bibliography

- Abrams, A., & Andreeva, J. (2025). *EU Crypto Regulations 2025*. London: The SUMSUBER.
- AJC. (2025). Hezbollah, Hamas, and More: Iran's Terror Network Around the Globe. *AJC*.
- AJDINI, V. (2024). ABUSE OF CRYPTOCURRENCIES AS A MODERN FORM OF MONEY LAUNDERING AND FINANCING OF TERRORISM. *Visions*, 42.
- Akartuna, D. A. (2023). *Israel orders seizure of crypto wallets worth \$94 million linked to Palestinian Islamic Jihad*. Hong Kong: Elliptic.
- Bakker, E. (2015). *Terrorism and Counterterrorism Studies*. Leiden: Leiden University Press.
- Boltuc, S. (2025). *Crypto Under Control: The Geopolitical Drivers of Iran's New Regulation*. Special EurAsia.
- Brill, A., & Keene, L. (2014). Cryptocurrencies: The Next Generation of Terrorist Financing? *Defence Against Terrorism Review*, 7- 30.
- Burgess, A., Hamilton, R., & Leuprecht, C. (2024). Terror on the Blockchain: The Emergent Crypto-Crime-Terror Nexus. In *Financial Crime, Law and Governance* (pp. 203–227).
- CipherTrace. (2021). *Cryptocurrency Crime and Anti-Money Laundering Report*. CipherTrace, Cryptocurrency Intelligence.
- COMMITTEE ON HOMELAND SECURITY. (2021). *TERRORISM AND DIGITAL FINANCING: HOW TECHNOLOGY IS CHANGING THE THREAT*. Washington DC: U.S. GOVERNMENT PUBLISHING OFFICE.
- Congressional Research Service. (2024). *Terrorist Financing: Hamas and Cryptocurrency Fundraising*. Washington DC: CRS.
- Covolo, V. (2020). The EU Response to Criminal Misuse of Cryptocurrencies: The Young, already Outdated 5th Anti-Money Laundering Directive. *European journal of crime, criminal law and criminal justice*, 217-251.
- Dewey, J. N., & Patel, S. (2025). *BLOCKCHAIN & CRYPTOCURRENCY LAWS AND REGULATIONS 2025 USA*. HOLLAND & KNIGHT LLP. Miami: Global Legal Insights.
- Dion-Schwarz, C., Manheim, D., & Johnson, P. B. (2019). *Terrorist Use of Cryptocurrencies Technical and Organizational Barriers and Future Threats*. California: RAND Corporation.
- Durrant, S. (2018). *Understanding the Nexus between Cryptocurrencies and Transnational Crime Operations*. New York: CUNY: City University of New York .
- Dyntu, V., & Dykyj, O. (2021). CRYPTOCURRENCY AS AN INSTRUMENT OF TERRORIST FINANCING. *Baltic Journal on Economic Studies*, pp. 67-72.

- European Banking Authority. (2024). *Preventing money laundering and terrorism financing in the EU's crypto- assets sector*. Paris : European Union.
- European Union. (2023). Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849.
- Financial Action Task Force. (2014). *Annual report 2014-2015*. Paris: FATF.
- Financial Action Task Force. (2014). *Virtual Currencies Key Definitions and Potential AML/CFT Risks*. Paris: FATF.
- FINANCIAL ACTION TASK FORCE. (2014). *Virtual Currencies Key Definitions and Potential AML/CFT Risks*. Paris: FATF/OECD.
- Freeman Law. (2022). *Iran - Cryptocurrency Laws and Regulation*. Retrieved from Freeman Law.
- Goldman, Z. K., Maruyama, E., & Roserberg, E. (2017). *TERRORIST USE OF VIRTUAL CURRENCIES Containing the Potential Threat*. Washington, DC: Center for a New American Security.
- Hoffman, B. (2017). *Inside Terrorism* (Vol. 3). New York: Columbia University Press.
- Ibrahim, S. A. (2021). Decrypting the Risks of Cryptocurrency: Money Laundering, Terrorism Financing, and Proliferation Financing. *PAKISTAN HORIZON*, pp. 73-89.
- Leuprecht, C., Hamilton, R., & Jenkins, C. (2023). Virtual money laundering: policy implications of the proliferation in the illicit use of cryptocurrency. *Journal of Financial Crime*, 1036-1054.
- Leuprecht, C., Cockfield, A., & Simpson, P. (2019). *Tracking Transnational Terrorist Resourcing Nodes and Networks*. Florida State University Law Review.
- Lob, E. (2022, December 27). Iran and cryptocurrency: Opportunities and obstacles for the regime. *Middle East Institute*.
- Lobell, S. E. (2017). *Structural Realism/O!ensive and Defensive Realism*. Oxford Research Encyclopedia of International Studies.
- Malakoutikhah, Z. (2020). Iran: Sponsoring or Combating Terrorism? *STUDIES IN CONFLICT & TERRORISM*, 43(10), 913-939.
- Mearsheimer, J. (2001). *The Tragedy of Great Power Politics*. New York: WW Norton and Company.
- Norton, S., & Chadderton, P. (2016). *Detect, disrupt and deny*. Australian Strategic Policy Institute.
- Office of Public Affairs. (2025, March). Justice Department Disrupts Hamas Terrorist Financing Scheme Through Seizure of Cryptocurrency. *U.S. Department of Justice*.
- Parvin, K., & Allahyarifard, A. (2024). Government Regulation in Combating Money Laundering Through Cryptocurrency: a Comparative Study of the

- Legal Systems of the Islamic Republic of Iran and Italy. *University of Tehran press*, 54(3).
- Pashakhanlou, A. H. (2018). The Past, Present and Future of Realism. In *Realism in Practice: An Appraisal*. E-IR.
- Pearson, E. (2012). Palestine Islamic Jihad . In G. Martin, *The SAGE Encyclopedia of Terrorism* (pp. 1765-1771). California: SAGE.
- Reus-Smit, C. (2005). Constructivism. In A. L.-S. Scott Burchill, *Theories of International Relations* (3 ed.). New York: Palgrave Macmillan.
- Ridwan, R. Z. (2019). The Utilization of Cryptocurrencies by the Terrorist Group as an Alternative Way of Hawala for Illicit Purposes. *Jurnal Sentris KSMPMI*, 2.
- Robinson, K. (2024, October 17). What is Hamas. *Council on Foreign Relations*.
- Rodrigues, G., & Kurtz, L. (2019). *Cryptocurrencies and anti-money laundering regulation in the G20*. Belo Horizonte: Institute for Research on Internet and Society.
- Rousseau, D. L., & Walke, T. C. (2010). Liberalism. In V. M. Myriam Dunn Cavelty, *The Routledge Handbook of Security Studies*. London.
- Sadeghi, M., & Naser, M. (2021). *A Comparative Study of Challenges and Solutions for the Use of Digital CryptoCurrencies in the Iranian and American Legal System*. Law Quarterly.
- Salami, I. (2017). Terrorism Financing with Virtual Currencies: Can Regulatory Technology Solutions Combat This? *Studies in Conflict and Terrorism*(41), pp. 968-989.
- Schmid, A. P. (2011). *THE ROUTLEDGE HANDBOOK OF TERRORISM RESEARCH*. (A. P. Schmid, Ed.) Oxon, London: Routledge.
- Skare, E. (2023, December 18). Iran, Hamas, and Islamic Jihad: A marriage of convenience. *European Council on Foreign Relations*.
- Smart, N., & Ahlawat, R. (2025). *Beyond the headlines of Iran's crypto usage*. Investigations. Amsterdam: Crystal.
- Sterling, A., Ostroff, E. G., Lowe, M. S., & Orso, M. (2024). *The Cryptocurrency Conundrum: Balancing Innovation with Terrorism Financing Risks*. Troutman Pepper Locke. Consumer Financial Services Law Monitor.
- Terner, S. (2020). Iran's muddled relationship with cryptocurrency is self-inflicted. *Atlantic Council*.
- Thornberry, W. M. (2021). *National Defense Authorization Act for Fiscal Year 2021*. Washington DC, United States: U.S. Government.
- TRM . (2023). *Iran's Crypto Economy*. TRM Insights.
- TRM. (2023). *Illicit Crypto Ecosystem Report* .
- TRM. (2025). *2025 Crypto Crime Report*. San Francisco, CA: TRM Labs.
- U.S. Department of State. (2024). *Country Reports on Terrorism: 2023*. Washington DC: U.S. Department of State.
- Voinea, E. (2013). *Oxford Research Encyclopedia of International Studies*. University of Birmingham. E-International Relations.

- Wagman, S. (2022). CRYPTOCURRENCIES AND NATIONAL SECURITY: THE CASE OF MONEY LAUNDERING AND TERRORISM FINANCING. *HARVARD NATIONAL SECURITY JOURNAL*.
- Walt, S. (1987). *Origins of Alliances*. Ithaca: Cornell University Press.
- Waltz, K. N. (1979). *Theory of international politics* (Vol. 44). Addison-Wesley.
- Wardhana, A. T., & Nugroho, B. W. (2022). *Abuse of Cryptocurrency to Funding International Terrorism Activities*. Yogyakarta: Dept. of International Relations, Faculty of Social and Political Sciences, UMY.
- Zahirah, R., & Ridwan, M. (2019). The Utilization of Cryptocurrencies by the Terrorist Group as an Alternative Way of Hawala for Illicit Purposes. *Sentris Kelompok Studi Mahasiswa Pengkaji Masalah Internasional*, 2.

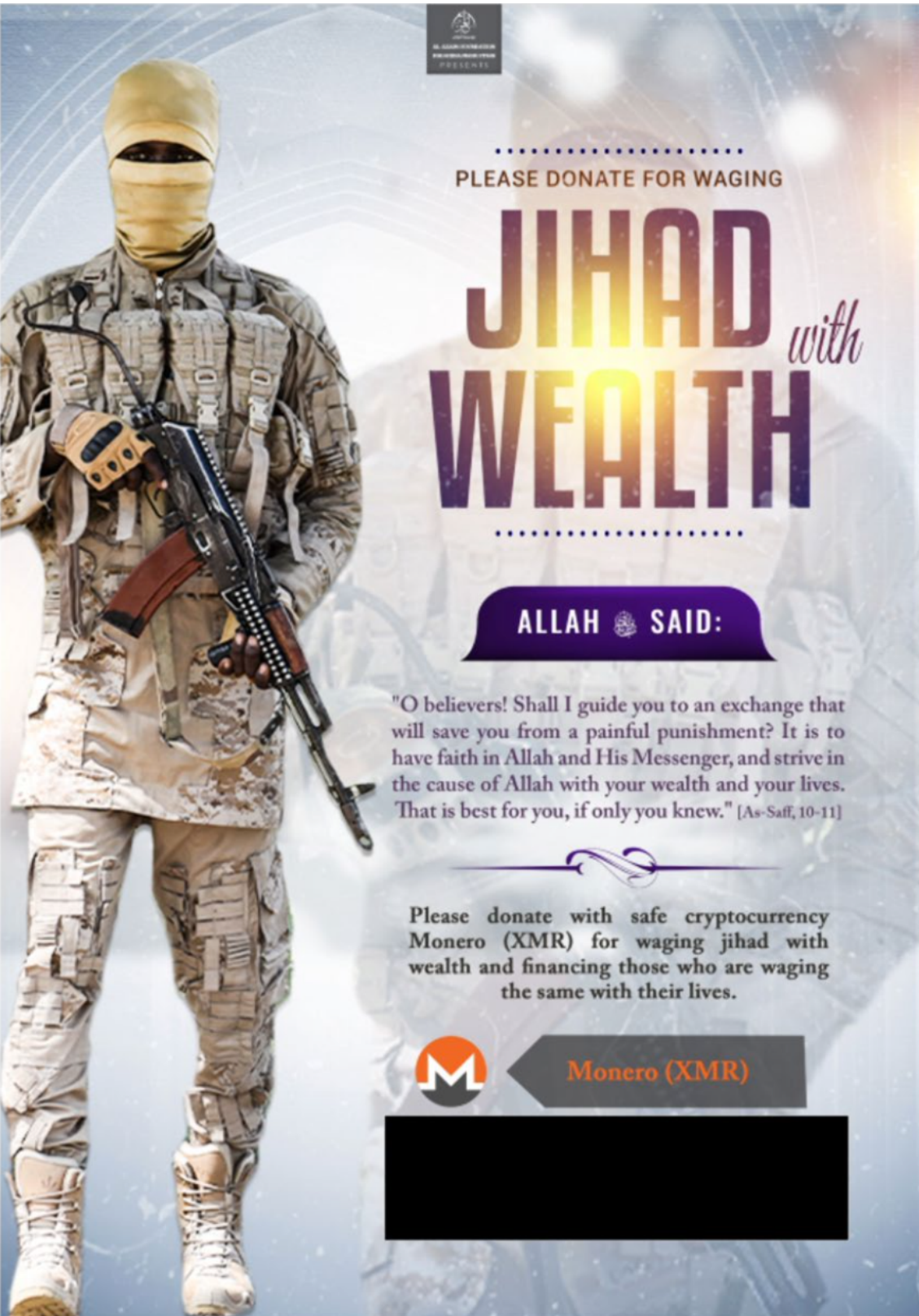
ANNEXES

ANNEX I

YEAR	Key Event	Group	Technology/Platform
2014	First evidence of Bitcoin being used for donations	Unspecified / early adopters	Bitcoin (BTC)
2015	ISIS begins soliciting donations in BTC.	ISIS	Bitcoin, own websites
2017	Assessments point to limited use due to technical complexity and preference for cash.	Various	BTC, but low volume
2018–2020	Escalating use: encrypted campaigns on Telegram, 150 wallets identified by the DOJ (US)	Hamas (al-Qassam Brigades), ISIS, al-Qaeda	Binance, Telegram, and OTC exchanges
2020	Record DOJ seizure: millions of USD in 300 wallets linked to terrorist groups	Hamas, al-Qaeda, ISIS	BTC, single-address systems
2021	Diversification: growing adoption of stablecoins and alternative platforms	Hamas, ISIS	Tether (USDT), TRON, mixers, DEX
2022	240% increase in Tether use by terrorist entities.	Various Jihadist groups	Stablecoins (USDT), TRON
2023	Activation of military-offensive and internment camps-linked campaigns	Pro-ISIS, Hamas	Exchanges P2P, non-custodial wallets
Oct. 2023	Attacks on Israel. Investigation opened for \$165M in Hamas-associated transactions	Hamas	BTC, stablecoins, OTC
March 2025	Dismantling of Hamas' financing network	Hamas (al-Qassam)	BTC, encrypted platforms

Table 1: Summary of cryptocurrency use by terrorist groups. Own production.

ANNEX II



ISKP FOUNDATION
FOR AN ISLAMIC STATE PRESENTS

.....
PLEASE DONATE FOR WAGING


JIHAD *with* WEALTH

.....

ALLAH ﷻ SAID:

"O believers! Shall I guide you to an exchange that will save you from a painful punishment? It is to have faith in Allah and His Messenger, and strive in the cause of Allah with your wealth and your lives. That is best for you, if only you knew." [As-Saff, 10-11]

Please donate with safe cryptocurrency Monero (XMR) for waging jihad with wealth and financing those who are waging the same with their lives.

 **Monero (XMR)**




Figure 1: ISKP soliciting cryptocurrency via newsletter