LUISS

Department of Political Sciences

Master's Degree in International Relations
Major in **Security**

Chair of **International Economics**

# *HAWALA AND CRYPTOCURRENCIES: A NEW AVENUE FOR TERRORIST FINANCING*

Prof. Marco Simoni
SUPERVISOR

Prof. Marco Magnani
CO-SUPERVISOR

Anna Miccoli
CANDIDATE
ID No. 648852

Academic Year 2022/2023

*This Page Intentionally Left Blank*

*To Pitti and the great Economist Riccardo Miccoli*

# ACKNOWLEDGEMENTS

First and foremost, I extend my sincerest gratitude to my supervisor, Professor Marco Simoni, who believed in and supported my idea from the very beginning. Having him as a guide has indeed been an honour. I would also like to thank my co-supervisor, Professor Marco Magnani, for his precious recommendations and advice concerning my Thesis.

A sincere note of appreciation goes to Professors Eitan Azani, Tal Shaanan and Andrea Sestino for their valuable time granted during our interviews as experts in the present research field. Their insights enriched my knowledge and further ignited my passion for a topic that often remains underexplored.

This Thesis would not have been possible without the sincere contributions of both Dr. Chris Leigh and Dr. Ram Willner. Over time, they have been steadfast guides on this academic journey, evolving into my trusted mentors. Additionally, a special acknowledgement goes to Dr. Riccardo Miccoli with whom I developed the core idea of this Thesis.

Lastly, my deep gratitude extends to LUISS Guido Carli University and Reichman University for their unwavering support over these two pivotal and formative years, which have laid my forthcoming career. A heartfelt thanks to the professors and colleagues I have had the privilege to meet and learn from during this remarkable journey.

# TABLE OF CONTENT

# LIST OF FIGURES

# LIST OF TABLES

# LIST OF ABBREVIATIONS

| | |
|---|---|
| **AML** | Anti-Money Laundering Law |
| **ATM** | Automatic Teller Machine |
| **APG** | The Asia/Pacific Group on Money Laundering |
| **AQB** | Al-Qassam Brigades |
| **AQAP** | Al-Qaeda in the Arabian Peninsula |
| **ATA** | Anti-Terrorism Act |
| **BaFin** | Federal Financial Services Authority |
| **BNB** | Binance Coin |
| **BTC** | Bitcoin |
| **CBUAE** | Central Bank of the U.A.E. |
| **CFTC** | Commission for Future Trade in Goods |
| **CTC** | Counter-Terrorism Committee |
| **DOJ** | Department of Justice |
| **EAG** | The Eurasian Group |
| **ERC20** | Ethereum Request for Comment |
| **ETH** | Ethereum |
| **EUROJUST** | European Union Agency for Criminal Justice Cooperation |
| **FATF** | Financial Action Task Force |
| **FEMA** | Financial Exchange Management Act |
| **FERA** | Foreign Exchange Regulation Act |
| **FFI** | Norwegian Defence Research Establishment |
| **FBI** | Federal Bureau of Investigation |
| **HSI** | Homeland Security Investigations |
| **IRS-CI** | Internal Revenue Service – Criminal Investigation |
| **GDP** | Gross Domestic Product |
| **FIU** | Financial Intelligence Unit |
| **FSRBs** | FATF-style Regional Bodies |
| **GAFILAT** | The Financial Action Task Force of Latin America |
| **GCC** | Gulf Cooperation Council |
| **GIABA** | The Intergovernmental Action Group against Money Laundering in West Africa |

| | |
|---|---|
| **GwG** | Geldwäschegesetz |
| **ICT** | Information and communication technologies |
| **IFT** | Informal Fund Transfer |
| **IMF** | International Monetary Fund |
| **IOM** | International Organisation for Migration |
| **IVTM** | Informal Value Transfer Methods |
| **IVTS** | Informal Value Transfer System |
| **LC** | Local Currency |
| **KNOMAD** | Global Knowledge Partnership on Migration and Development |
| **KWG** | Kreditwesengesetz |
| **KYC** | Know Your Costumer |
| **ISWAP** | Islamic State West Africa Province |
| **MENAFATF** | The Middle East and North Africa Financial Action Task Force |
| **MSBs** | Money Service Business |
| **NAP** | National Action Plan |
| **SBP** | State Bank of Pakistan |
| **SECP** | Securities and Exchange Commission of Pakistan |
| **StGB** | Strafgesetzbuch |
| **U.A.E.** | United Arab Emirates |
| **UK** | United Kingdom |
| **UN** | United Nations |
| **UNDCP** | United Nations Drug Control Programme |
| **UNODC** | United Nations Office on Drugs and Crime |
| **UNSC** | United Nations Security Council |
| **USA** | United States of America |
| **USDT** | Tether |
| **WMD** | Weapons of Mass Destruction |
| **XRP** | Ripple |
| **ISIS** | Islamic State of Iraq and Syria |

# GLOSSARY OF ARABIC TERMS

| | |
|---|---|
| **Al-Qāʿida** | The base |
| **Gharar** | Uncertainty/Risk |
| **Ḥaraka al-muqāwama al-islāmiyya** | Islamic resistence movement |
| **Hawāla** | Transfer |
| **Hizb Allāh** | Party of God |
| **Maysir** | Gambling |
| **Riba** | Interest / Usury |
| **Shari'a** | Islamic Law |
| **Tālibān** | Students |

# CHAPTER I.

# INTRODUCTION

## 1.1 Background and Research Question

In today's globalised world, marked by rapid technological advancements and enhanced connectivity, the traditional barriers of time and space have significantly diminished, transforming the world into a closely interconnected global village.[1] These developments have undoubtedly brought numerous positive outcomes, revolutionising transportation and communication and fostering international cooperation.[2] However, alongside these remarkable advancements, the world continues to grapple with persisting challenges by criminal organisations.[3]

Modern technologies such as artificial intelligence, robotics, and blockchains have provided terrorist organisations with more straightforward means to exploit the global financial system. Among the significant abuses of this system, money laundering stands out as a grave concern. Money laundering has become a prominent tool for criminal organisations seeking to disguise the origins of their funds and legitimise their activities.

Traditionally, terrorist groups have employed various methods to move their funds and support their illicit activities. Before modern technologies, they relied on traditional means such as physical cash smuggling, informal value transfer systems like the *hawāla* system, and exploiting charitable organisations to funnel money.[4] While cash has traditionally been the chosen medium, these groups increasingly favour cryptocurrencies, particularly Bitcoin (BTC), to raise and transfer funds. Specifically, cryptocurrencies are digital or virtual currencies that which operate without a central bank and employ encryption for protection. They are decentralised systems built on blockchain technology, a distributed ledger that records transactions across multiple computers or nodes. Blockchain-based technologies enable

[1]Jean-Guillaume Poulain and Julien Reynald, "IMF Working Paper: IMF Lending in an Interconnected World," *International Monetary Fund* 17, no. 155 (2017): 8-15, https://doi.org/10.5089/9781484305867.001.
[2] Mesut Savrul and Ahmet Incekara, "The Effect of Globalisation on International Trade: The Black Sea Economic Cooperation Case" paper presented to the *International Conference on Eurasian Economies*, (9-11 Sept. 2015): 88-94.
[3] Serhii S. Cherniavskyi et al., "International Cooperation in the Field of Fighting Crime: Directions, Levels and Forms of Realisation," Journal of Legal, Ethical and Regulatory Issues 22, no. 2 (2019): 8, https://www.abacademies.org/articles/international-cooperation-in-the-field-of-fighting-crime-directions-levels-and-forms-of-realization-8346.html.
[4] Bruce Hoffman, "Change and Continuity in Terrorism," *Studies in Conflict & Terrorism* 24, no. 5 (2001): 425-426, https://dx.doi.org./10.1080/105761001750434268.

cryptocurrencies to function by ensuring transparency, security, and immutability of transactions.[5] Each transaction is verified and added to a block, then linked to the previous blocks, creating a chain of information.[6] Due to its decentralised nature, it does not require intermediaries, such as banks, and allows for peer-to-peer transactions, faster settlement times, and reduced transaction costs. The blockchain's cryptographic algorithms ensure the integrity and privacy of the transactions, making cryptocurrencies a secure and efficient means of digital exchange.

Terrorists gained a new route to exploit modern technology for their financial activities as cryptocurrencies gained popularity between 2009 and 2010. Terrorists can take advantage of the qualities of cryptocurrencies that make tracing transactions difficult by seeking BTC instead of cash. For instance, because of such technologies, they can now escape discovery using pseudonymity, encrypted wallets, and decentralised platforms. Cryptocurrencies also have a global reach and quick transfer capabilities, making them an appealing alternative for international criminal financial activity.[7] Indeed, technically, cryptocurrencies possess global reach and rapid transfer capabilities, rendering them an enticing option for international criminal financial activity. With cryptocurrencies, transactions can be conducted across borders swiftly and without intermediaries or regulatory oversight. The anonymity offered by specific cryptocurrencies further obscures the identities of individuals involved, making it challenging to trace illicit transactions: These factors, combined with the decentralised nature of cryptocurrencies, which hinders centralised control and monitoring, make them an appealing choice for criminals seeking to engage in cross-border financial activities discreetly and efficiently.

This tendency has presented substantial challenges for law enforcement authorities and international organisations in their continuous attempts to combat terrorist financing and money laundering effectively. The U.S. government launched initiatives to combat *hawāla* and prevent terrorist financing, such as the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism" (USA PATRIOT Act) of 2001.[8] The USA PATRIOT Act empowers law enforcement agencies to investigate and prosecute terrorist financing.[9] Furthermore, the Financial Action Task Force (FATF), an intergovernmental body

[5] Antoine Bouveret, and Vikram Haksar, "What are cryptocurrencies," *Finance and Development* 55 no. 2 (2018): 26-29.
[6] Andrea Sestino et al. "The Business Opportunity of Blockchain Value Creation among the Internet of Value," *Global Business Review*, (2022), https://doi.org/10.1177/09721509221115012.
[7] Arianna Trozze et al., "Cryptocurrencies and Future Financial Crime," *Crime Science* 11, no. 1 (2022): 20-22, https://doi.org/10.1186/s40163-021-00163-8.
[8] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. no. 107–56, 115 Stat. 272 (2001), https://www.govinfo.gov/content/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf.
[9] *Ibid*.

that establishes standards and encourages the implementation of anti-money laundering and terrorist financing measures, has produced many studies and organised conferences on *hawāla* and terrorist funding.

The *First International Conference on Hawāla* was pivotal in the fight against *hawāla* and terrorist financing.[10] The conference, hosted by the United Arab Emirates (U.A.E) government and the United Arab Emirates Central Bank, brought together experts and stakeholders worldwide to examine the problems and prospects of regulating *hawāla*. The *First International Conference on Hawāla* produced the "Abu Dhabi Declaration on Hawāla".[11] This Declaration underscored the significance of strengthening global cooperation and collaboration to fight terrorist financing and establishing a framework for the regulation and control of *hawāla*. The Declaration recognised *hawāla's* cultural and societal relevance while emphasising the importance of preventing misuse for illicit purposes. Moreover, it called for measures that would strike a balance between preserving *hawāla*'s cultural relevance and ensuring it is not exploited for illegal activities.

Furthermore, in 2002, the International Monetary Fund (IMF) and the World Bank (WB) initiated a study effort to increase understanding of informal funds transfer (IFT) systems, including *hawāla*. The project aimed to grasp the structure and operation of IFT systems and the potential hazards and benefits that come with them. In early 2003, a report titled "Informal Funds Transfer Systems: An Analysis of the Informal *Hawāla* System" was published due to research effort.[12] The report thoroughly examines *hawāla* and other IFT systems, including their history, characteristics, financial legislation, and oversight implications. Several critical challenges associated with IFT systems were identified in the report, including their potential use in money laundering and terrorism financing and the difficulty of regulating and supervising these systems to balance financial inclusion with the need to prevent illicit activities. The research also emphasised the significance of handling IFT systems using a risk-based approach based on understanding each system's risks and vulnerabilities.

Following the success of the *First International Conference*, the U.A.E government hosted the *Second International Conference on Hawāla* in April 2004 under the direction of the

[10] R. Barry Johnston, "Regulatory Frameworks for Hawala and Other Remittance System", paper presented to the First International Conference on Hawala (Abu Dhabi, 15-16 May 2002), https://www.imf.org/external/pubs/nft/2005/hawala/hawala.pdf.

[11] International Monetary Fund, "Abu Dhabi Declaration on Hawala" (declaration presented to the First International Conference on Hawala, Abu Dhabi, 16 May 2002), https://digitallibrary.un.org/nanna/record/467698/files/A_56_993-EN.pdf?withWatermark=0&withMetadata=0&version=1&registerDownload=1.

[12] Mohammed El Qorchi et al., "Informal Funds Transfer Systems: An Analysis of the Informal Hawala System", IMF-World Bank Paper, no. 222 (August 2003): 30-64.

U.A.E Central Bank.[13] The *Second International Conference on Hawāla* expanded on the first conference's conclusions and allowed further debate and collaboration. The conference included issues such as the role of *hawāla* in the global economy, the difficulty of regulating *hawāla* in different jurisdictions, and the rising use of technology in informal payment systems, such as cryptocurrency.[14] Furthermore, in 2005, it was held the *Third International Conference on Hawāla*, the conclusion of the series of International Conferences on *hawāla* **was** also announced at this meeting. The significance of *hawāla* and other informal transfer techniques in supporting economic movements, particularly those connected to workers abroad, was emphasised throughout the session. One of the conference's significant accomplishments was raising awareness of these practices and their effects. The last request was for states to assess and control the risks of such systems, particularly concerning touchy subjects like money laundering and terrorism financing.[15]

These international agencies' combined efforts with national governments and regulatory bodies have resulted in a more detailed legislative framework, awareness, and improved coordination in combating terrorist financing and money laundering. However, it is an ongoing struggle, and constant adaptation and collaboration are required to keep abreast of terrorist groups' increasing techniques in manipulating the global financial system.
Based on the above, this Thesis is aimed to answer the following research question:

***RQ.*** *What is the role of cryptocurrencies and hawāla in financing transnational crimes, specifically concerning money laundering and terrorism financing? Moreover, what are current issues and actions useful to prevent such a challenge?*

Thus, this Thesis aims to investigate the role of cryptocurrencies and *hawāla* in facilitating transnational crimes, explicitly focusing on money laundering and terrorism financing. It will explore the risk of this new approach to supporting and facilitating terrorist organisations and the potential of cryptocurrencies to exceed the *hawāla*. Furthermore, the Thesis examines the efforts undertaken by international institutions, notably the IMF, WB, FATF and the UN, to mitigate and address these challenges, emphasising their role in limiting the misuse of such financial systems.

[13] Raul Hernandez-Coss, "Regulatory Frameworks for Hawala and Other Remittance System" (paper presented to the Second International Conference on Hawala, Abu Dhabi 3-5 April 2004), https://www.imf.org/external/pubs/nft/2005/hawala/hawala.pdf.
[14] *Ibid.*
[15] *Ibid.*

## 1.2 Literature Review

The following work begins by reviewing the extensive literature on the subject matter to give appropriate answers and insights to the research questions at hand. The literature on terrorism covers a wide range of subjects, including the evolution of terrorist organisations, the challenges and risks they pose, and the overall effects on society.

The origins of terrorism may be found in different historical contexts and movements. From ancient times to today, acts of violence aimed at instilling fear and achieving political, ideological, or religious goals have occurred in various forms. Examples include the activities of groups such as the Sicarii in ancient Judea, the Assassins in the mediaeval period, and anarchist movements in the 19th and early 20th centuries.[16] Maximilien Robespierre, a French philosopher and politician of the late 18th century, was one significant historical figure who explored the idea of terrorism.[17] The influential work "Virtue and Terror (Revolutions)",[18] written by Robespierre, was and is a considerable contribution to terrorism literature. Robespierre investigates the use of violence during the French Revolution and the concept of state-sanctioned terrorism in this essay. The analysis of Robespierre reveals the connections between terrorism, revolutions, and government. He broadens our knowledge of terrorism beyond the actions of organisations by discussing the role of terror in the framework of a revolutionary government. The essay examines how terrorism might be used as a tactical tool to seize and hang upon power during times of instability.

It is important to note that since these early works, there has been a tremendous evolution in both contemporary thinking and the academic study of terrorism. The study of terrorism as an academic discipline is relatively recent, starting between 1960 and 1970. David Rapoport, a prominent political science professor at the University of California-Los Angeles, contributed to the field significantly. In 1969, Rapoport recognised the lack of available material on terrorism as he prepared a series of lectures. He played a crucial role in stimulating scholarly interest in terrorism with his work. One of Rapoport's landmark studies is "The Four Waves of Modern Terrorism," published in 2004.[19] In this influential work, Rapoport presents

[16] The Sicarii were a radical Jewish faction during the First Jewish-Roman War in ancient Judea. They used concealed daggers to assassinate their enemies and opposed Roman rule. The Assassins were a secretive Muslim sect during the medieval period. They conducted political assassinations and covert operations, primarily targeting political and military figures. Anarchic movements emerged in the 19th and early 20th centuries as a response to social and economic inequalities.

[17] Maximilien Robespierre (1758–1794) was a French politician and lawyer who rose to prominence during the French Revolution. He was a significant player in the radical Jacobin movement and promoted the Republic of Virtue, which strongly emphasised values like justice and equality. But in July 1794, he was detained, found guilty of treason, and put to death by guillotine.

[18] Maximilien de Robespierre, *Virtue and Terror,* rev. Slavoj Zizek, ed. Jean Ducange, trans. John Howe (Brooklyn: Verso Books, 2017).

[19] David C. Rapoport, "The Four Waves of Modern Terrorism," in *Attacking Terrorism: Elements of a Grand Strategy*, ed. Audrey Kurth Cronin and James M. Ludes (Washington, DC: Georgetown University Press, 2004), 47.

a framework that classifies several historical waves of terrorism based on their ideological underpinnings, objectives, and strategies. He traces the historical development of terrorist movements, identifying important traits and trends within each wave. Rapoport's analysis (2004) provides valuable insights into how terrorism has evolved.[20]

Since the 1970s, there has been a notable expansion in the literature on terrorism. Scholarly interest in the subject has grown, with researchers, academics, and professionals dedicating their efforts to examining various aspects of terrorism. Martha Crenshaw and Brian Jenkins made contributions, two scholars widely recognised for insights into the psychology of terrorism, hostage-taking dynamics, and the strategies employed by state and non-state actors in countering terrorism.

There are several reasons why there is more interest in terrorism today. The devastating effects of significant terrorist strikes, particularly the assaults on the World Trade Centre and Pentagon on September 11, 2001, which increased demand for information and analysis on terrorism and its perpetrators, was one crucial motivator. This, together with the evolving nature of terrorists, sparked the development of an industry of terrorism specialists, and authors have made significant contributions to the literature from various perspectives.

The transition from fighting terrorism within national borders to a "global war on terror" beyond any established boundaries has resulted in the involvement of Geography experts and ample literature on the geographical aspects of terrorism.[21] There is considerable literature on the confluence of terrorism studies and Geography. For instance, Professor Steven M. Radil has conducted extended investigations on the global patterns of terrorism between 1998 and 2005, analysing causes and consequences from a geographical point of view.[22] Today, academics and experts consider Geography and other areas of study as a fundamental part of their work for more comprehensive research.

Moreover, Jurgen Brauer, a German American economist and expert on the economic aspects of peace and security, presents an entirely fresh analytical viewpoint.[23] According to Brauer, the phenomenon of terrorism can be visualised in the context of an economic scenario known as the "terror market", wherein on the one hand, there are terror organisations which pose as rational players in a business or enterprise that "produces terrorism", and on the other

[20] David C. Rapoport, "The Four Waves of Rebel Terror and September 11," in *Anthropoetics* 8, no.1 (Spring/Summer 2002): 14.
[21] Bush, *A Joint Session of Congress and the American People*, *op. cit*.
[22] Steven M. Radil, "Global Patterns of Terrorism, 1998-2005: A Geographic Overview and Root Cause Analysis," Dissertation, (University of Colorado at Colorado Springs, 2006).
[23] Jurgen Brauer, "The Terrorist Firm: Innovation, Substitution and Productivity," in *Fighting Terrorism: Financial and Economic Aspects*, *Occasional Paper NATO Defence College* (2004).

hand counter-terrorism organisations and nation-states.[24] Because of their unstable financial situation, terrorist organisations cannot produce due to their precarious financial circumstances.[25] In this regard, the German American economist distinguishes between two categories of restrictions on the terrorist organisation: interventions by the state that reduce revenue and measures that raise the costs of terrorist activities.[26] The latter approach has just been adopted after years of relying mostly on defensive measures and anti-terrorist laws, which are no longer enough. Nowadays, international organisations and states tend to combat everything related to terrorist financing as the means of financing terrorism advances. Given the above, Brauer argues that while governmenal focus on terrorism financing is crucial, there are still some critical obstacles. When trying to impose a "tax" on any attempt to finance terrorism, "terrorists can be expected to take a number of tax evasion measures in the sense of finding new sources of revenue and new ways of moving funds."[27]

The sudden change in the world landscape with new technologies has led scholars and experts to delve further into this complex issue, examining how technological advancements have facilitated and challenged terrorist financing and money laundering activities. Several notable works shed light on this subject. Many authors have contributed to this field, highlighting the intricate connections between illicit financial networks, terrorism, and the global financial system. Notable works include "Treasury's War: The Unleashing of a New Era of Financial Warfare" by Juan Zarate, the former Assistant Secretary of the Treasury for Terrorist Financing under the George W. Bush administration.[28]

An extensive literature review reveals that non-state players, hostile to states, are increasingly using terrorism, which has evolved from being primarily used as a tool by state actors. A rising emphasis on religious grounds for participating in terrorist violence coincides with this transition. Scholars have given the literature on regulatory and policy perspectives much attention. Academics such as Dirk Ryman and Benjamin Trump provide a thorough examination of the regulatory environment involving cryptocurrencies, including initiatives to address their potential abuse for illegal activity. Furthermore, Yaya J. Fanusie and Tom Robinson analyse policy proposals and tactics to counter the hazards of money laundering and

[24] *Ibid*.
[25] *Ibid*.
[26] *Ibid*.
[27] *Ivi,* p. 22.
[28] Juan C. Zarate, *Treasury's War: The Unleashing of a New Era of Financial Warfare* (New York: PublicAffairs Book, 2013), 115-120.

terrorist financing using cryptocurrencies in their book "Cryptocurrencies, Anti-Money Laundering and Counter-Terrorist Financing."[29]

Overall, the expanding literature on terrorism has helped deepen our understanding of this complex phenomenon, guiding practice and policy and developing a more nuanced and all-encompassing strategy for confronting its problems. As academics and researchers work to expand their knowledge and support ongoing efforts to stop and lessen the effects of terrorism worldwide, it continues to change the discipline.

### 1.3 Methodology and Research Design

The idea behind this thesis was driven by my internship at the International Institute for Counter-Terrorism (ICT) in Herzliya, Israel, allowing for a unique opportunity to undertake on-site research on the crucial issues of money laundering and terrorist funding in the Middle East.[30] The experience at the institute allows to learn firsthand the difficulties and complications of preventing illicit money activity in the region. Furthermore, attending seminars by ICT's executive director, Dr Boaz Ganor, provided insight into how terrorist organisations have evolved their methods and strategies. My attention was drawn to the discussions concerning using cryptocurrencies for terrorist financing.

Recognising this topic's potential significance, the methodology combines qualitative and quantitative research methods to provide a holistic understanding of the subject matter. Through an explorative research design, this thesis implements a qualitative study approach emphasising using in-depth interviews to gain deeper insights and understandings.[31] The sample consisted in three experts: Two Professors from Reichman University in Herzliya, Tel Aviv District (IDC), because both recognised experts in the research field related to *hawāla* and cryptocurrencies, and a Researcher expert in the field of blockchain-based technologies and crypto. Specifically, the involved participants were Professor Eitan Azani, aged 65, several years experienced as a researcher and professional in the field of the study related to the financial instruments used in terror financing, particularly emphasising the *hawāla* system. Then, Professor Tal Shaanan, aged 40, since its expertise in the field of *hawāla* and cryptocurrencies as well: He emerged as a leading voice in the field of the relationship among *hawāla* and cryptocurrencies, bringing a unique perspective to the study. Finally, Professor

[29] Yaya J. Fanusie and Tom Robinson, "Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services," *Foundation for Defense of Democracies and Elliptic,* (12 Jan. 2018): 7, https://doi.org/10.1080/00431672.2019.1538758.
[30] ICT is an independent think tank founded in 1996 in Herzliya, Israel. It is specialized in terrorism, counter-terrorism strategies, homeland security measures, intelligence interpretation and policies related to national defense and security.
[31] Russell Belk at al., *Qualitative Consumer and Marketing Research*, (Los Angeles: SAGE, 2012), 31-39.

Andrea Sestino, aged 30, experienced in new technological integrations both as a researcher and professional, specifically on blockchain-based technologies and cryptocurrencies at a general level. Furthermore, the qualitative component considers the theoretical consultation of the classic and modern literature on money laundering and terror financing.

Moreover, examining a real-life case study will show the precise methods by which cryptocurrencies are used for terrorism financing within the *hawāla* system. A full awareness of the current level of knowledge and available countermeasures will also be attained through an assessment of the literature, reports, and regulatory frameworks specifically by the UN, FATF since its initial contribution to *hawāla*'s conferences until today's new effort to combat terrorists. The quantitative analysis will permit the evaluation of enormous datasets, allowing for the discovery of significant indicators, risk factors, and trends connected to the above cryptocurrencies inside the *hawāla* system. Graphs and illustrations from reputable sources, including financial institutions and international organisations, are also included. This study also concentrates on assessing the efficacy of current defences and locating potential holes or weak points in security systems. The approach used is particularly suited for this investigation since it enables a thorough analysis of the research issue, identifies unique flaws, and suggests potential remedies to stop the unauthorised use of financial systems.

The Thesis will consist of five chapters, of which the first is the introductory one. Chapter II will explore the concept of terror financing and money laundering, including the definitions and the various sources and channels used in terrorist activities. This chapter will also examine the connection between terror financing and money laundering, highlighting the interplay between illicit activities. Chapter III will concentrate on the *hawāla* informal value transfer system, its networks, and the distinction between lawful and criminal uses such as terror financing. Additionally, we will vet the various views on whether or not it should be made legal. Cryptocurrencies will be discussed in Chapter IV, along with their history and distinctive traits. This chapter will examine the mechanism of cryptolaundering and the most popular cryptocurrencies among terrorists. Moreover, we will look at specific case studies that provide a real-world example of using cryptocurrencies to finance terrorism. Considering the international and regional cooperation efforts made up to that point, Chapter V will draw conclusions and provide recommendations while discussing upcoming difficulties and opportunities in combating terrorism's illicit commerce.

# CHAPTER II.

# TERROR FINANCING AND MONEY LAUNDERING: DEFINITIONS AND OVERVIEW

## 2.1 Exploring Terror Financing

The movement of money is a crucial intermediary step in terrorism financing, and it plays a significant role in enabling terrorist organisations to carry out their activities.[32] While the sources of terrorist funding and the use of finances are frequently examined and targeted, the methods by which terrorists move money are sometimes disregarded. To limit the danger of detection and action by authorities, terrorist organisations raise funds in locations far from their bases or intended attack sites.[33]

This finding became more evident in the aftermath of the September 11th, 2001, attacks. Terrorist organisations need money to carry out their operations, which include planning and carrying out attacks, recruiting and training members, procuring weapons and equipment, and maintaining their organisational infrastructure.[34] Adequate funding allows them to build their networks, increase their capacities, and sustain their operations over time. According to Interpol, the international police organisation, "the frequency and seriousness of international acts are often proportionate to the financing that terrorist groups might get."[35]

Furthermore, it is crucial to acknowledge that the money flow will persist for individuals conducting *Informal Value Transfer Systems* (IVTS) transactions, such as *hawāla*, behind the scenes. The covert nature of these operations makes it challenging to eliminate such informal systems.[36] However, combating terrorist financing must focus on enhancing cooperation among countries and effectively implementing international conventions.

### 2.1.1 Definition of Terror Financing

Following the awful events of 9/11, the UN increased its efforts to combat terrorism, e.g. by introducing the Security Council Resolution 1373 in 2001, calling upon states to implement

[32] Michael Freeman and Moyara Ruehsen, "Terrorism Financing Methods: An Overview," *Perspectives on Terrorism* 7, no. 4 (2013): 5, http://www.terrorismanalysts.com/pt/index.php/pot/article/view/279/html.
[33] *Ibid*.
[34] *Ibid*.
[35] International Criminal Police Organisation, *Counter-Terrorism Global Strategy 2022-2025*, (Lyon: November 2022): 3-4.
[36] Shivangi Seth and Gatra Priyandita, "Combating the Cyber Heists that are Costing the Global Economy," *Australian Strategic Policy Institute* (June 2023), https://www.aspistrategist.org.au/combating-the-cyber-heists-that-are-costing-the-global-economy/.

measures, including collaboration and the repression of terrorist finance, in the battle against terrorism.[37] However, even before the Twin Towers attacks, the UN had been actively engaged in fighting terrorism and its financing through numerous measures, principally through the development of international treaties. The UN General Assembly adopted the *United Nations International Convention for the Suppression of Terrorist Financing* on December 9, 1999, an important international convention that strives to combat terrorist financing. Article 2 of the Convention defines terrorism as follows:

> "Any person commits an offence within the meaning of this Convention if that person by any means, directly or indirectly, unlawfully, and willingly, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, to carry out:
>
> *(a)* An act which constitutes an offence within the scope of and as defined in one of the treaties listed in the annexe; or
>
> *(b)* Any other act intended to cause death or serious bodily injury to a civilian or to any other person not taking any active part in the hostilities in a situation of armed conflict when the purpose of such act, by its nature or context, is to intimidate a population or to compel a government or an international organisation to do or to abstain from doing an act."[38]

In addition, the International Convention for the Suppression of Terrorist Financing defines funds for terrorism to mean:

> "Assets of every kind, whether tangible or intangible, movable, or immovable, however acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such assets, including, but not limited to, bank credits, travellers' checks, money orders, shares, securities, bonds, drafts, letters of credit."[39]

Importantly, not all countries that signed the Convention have agreed on what actions constitute terrorism. Different countries' legal and political frameworks, historical circumstances, and security concerns contribute to differing perceptions and definitions of terrorism. This sparked an ongoing discussion about the definition of terrorism. Scholars, professionals, and

[37] UNSC Res 1373 (28 September 2001) UN Doc S/RES/1373.

[38] *International Convention for the Suppression of the Financing of Terrorism*, G.A. Res. 54/109, U.N. GAOR, 54th Sess., 76th mtg., Supp. no. 49, U.N. Doc. A/Res/53/108 (1999), https://treaties.un.org/doc/db/terrorism/english-18-11.pdf.

[39] *Ibid.*

international organisations have all proposed various definitions of terrorism, each reflecting their unique perspectives and areas of expertise.

In 2005, Alex P. Schmid and Albert J. Jongman published their primary work, "Political Terrorism: A New Guide to Actors, Authors, Concepts, Data Bases, Theories, and Literature."[40] Their research looked at 209 different definitions of terrorism. Schmid and Jongman's work attempts to provide a complete guide to understanding and analysing terrorism for researchers, policymakers, and practitioners by delving into the numerous players in political terrorism, such as state-sponsored terrorism, extremist groups, and individual terrorists. The study also examines these actors' historical backdrop, ideological objectives, and methods.[41]

Moreover, the European Union created Directive 2017/541 (Art. 3) on fighting terrorism. It describes terrorism as an organised and systematic attempt to instill fear, a crucial element in terrorism that distinguishes it from other types of political violence.[42]

It is important to note that Directive 2017/541 replaced the previous Council Framework Decision 2002/475/JHA, which aimed to provide a framework for cooperation and coordination among EU countries in combating terrorism and amended the Council Decision 2005/671/JHA on terrorism. The IMF and the WB, as international financial institutions, are more concerned with the economic consequences of terrorism than with defining specific definitions of terrorism. Instead, they often rely on internationally accepted legal frameworks, such as the *United Nations International Convention for the Suppression of the Financing of Terrorism* (1999), to guide their efforts in combating terrorism-related issues.[43]

Overall, the continuous controversy surrounding the need to find a universal definition for terrorism has raised another debate, among experts in the field, regarding whether or not a definition of terrorism is necessary. According to Martha Crenshaw, a renowned terrorism scholar, having a clear and widely agreed concept is critical for effective counter-terrorism measures.[44] She claims that defining terrorist acts provides a shared framework for understanding and responding to them. Furthermore, legal expert Kent Roach emphasises the relevance of a definition in the legal world, stating that it clarifies judicial procedures and assures uniformity in prosecuting terrorists.[45]

---

[40] Albert J. Jongman and Alex P. Schmid, *Political Terrorism: A New Guide to Actors, Authors, Concepts, Data Bases, Theories, and Literature* (1st ed, New York: Taylor & Francis Group, 2005), 130-140.
[41] *Ibid*.
[42] Council Directive 2017/541/EC of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA (OJ L 88/6), 31 March 2017, 12.
[43] International Convention for the Suppression of the Financing of Terrorism, *cit*.
[44] Martha Crenshaw, *Explaning Terrorism: Causes, Process and Consequences* (1st ed, Oxford: Routledge, 2011), 20.
[45] Kent Roach, *Due Process and Victims' Rights: The New Law and Politics of Criminal Justice* (1st ed, Toronto: University of Toronto Press, 1999), 310-320.

However, human rights lawyer Anthony Dworkin expresses concern about the potential misuse of a broad definition of terrorism, which could infringe on civil liberties and be used to crush dissent.[46] These experts' perspectives emphasise the complexities of the discussion and the importance of exercising caution when addressing whether a definition of terrorism is required.

### 2.1.2 Sources and Channels of Terror Financing

Terror financing hides a complicated and meticulous framework designed to assure the continuation and expansion of terrorist activities. The terror finance chain consists of three steps: raising, moving, and using funds.

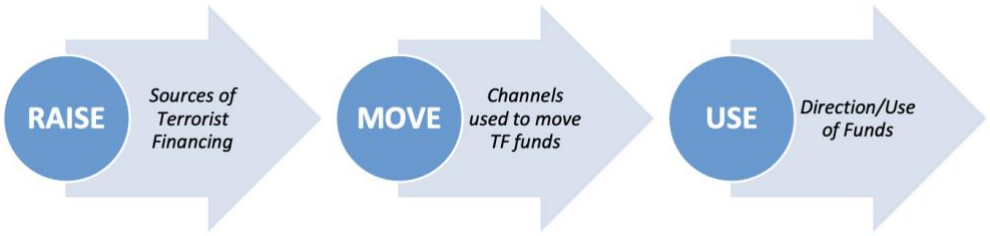



**Figure 1**: The three stages of terror financing; Source: Central Bank of Bahrain (2020).

The first stage entails acquiring or collecting financial resources, which are essential in ensuring terror activities' sustainability and growth. Fundraising methods can vary and may include both legal and illegal means.[47] To illustrate this, in 2015, the Norwegian Defence Research Establishment (FFI), through the important study of terrorist organisations and the presence of jihadi cells in Europe, reported the main types of terrorist financing.[48] **Figure 2** shows a bar graph illustrating the four main types of financing: legal activities, criminal activities, popular support and terrorist support.

[46] Anthony Dworkin, "Individual, Not Collective: Justifying the Resort to Force against Members of Non-State Armed Groups," *Stockton Center for the Study of International Law*, 93/1, (2017), 16.
[47] FATF (2019), *Terrorist Financing Risk Assessment Guidance,* FATF, Paris, https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Terrorist-Financing-Risk-Assessment-Guidance.pdf.coredownload.pdf.
[48] The Norwegian Defence Research Establishment (FFI) is an institution established in 1946, that holds the primary responsibility for conducting defense-related research and development in Norway.

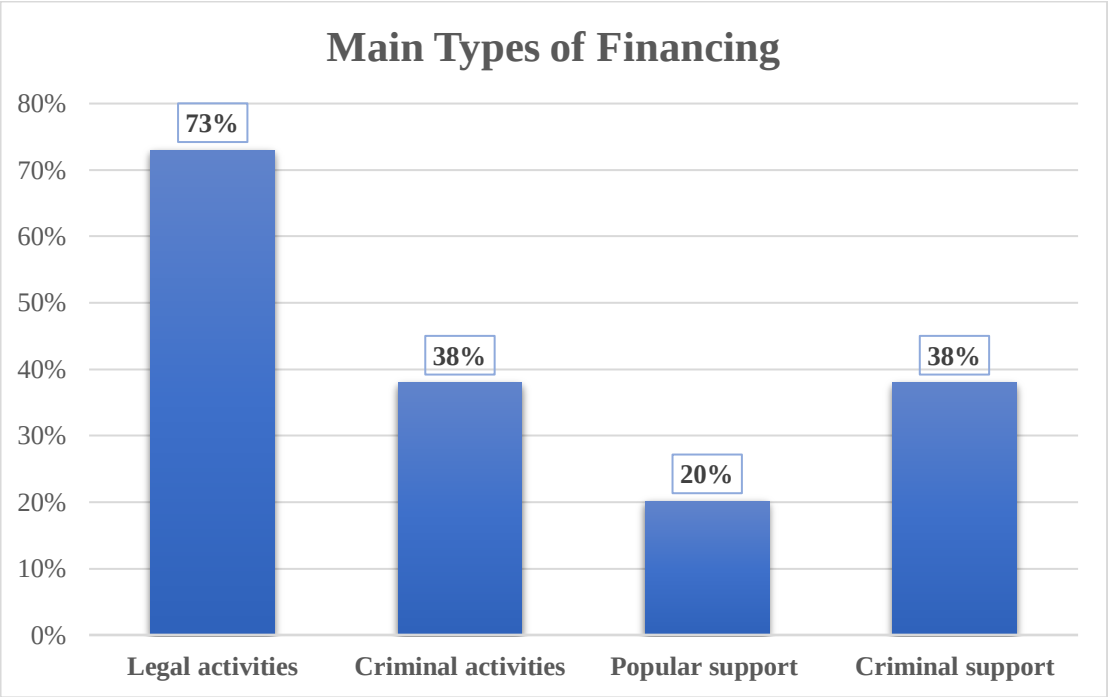



**Figure 2**: Percentage distribution of the four main types of terror financing; Source: FFI (2015).

To begin with, legal activities are the most common type of funding, with 73% involved in some actions that fall within the boundaries of the law but may indirectly contribute to the financing or support of terrorist organisations.[49] Legitimate businesses, investments, or financial transactions that do not mandate formal qualifications or have low entry barriers pose a higher risk when diverting funds for terrorist activities. Similarly, non-profit organisations and legitimate charities are susceptible to misuse by terrorists because they are subject to less stringent regulatory requirements and benefit from public trust.[50]

Moreover, criminal activities and terrorist support are the second most common financial sources, with 38% of cells using both. Criminal activities involve criminal actions carried out by individuals or organised criminal networks to generate funds for terrorist purposes, which play a crucial role in terrorist financing. These include various unlawful activities, including drug trafficking, credit card and cheque fraud, arms smuggling, and human trafficking. For example, *Al-Qāʿida* and the *Tālibān* have been known to engage in narcotics trafficking and kidnapping for ransom to gain significant financial resources. Terrorist support is defined as providing direct help to terrorist organisations, such as financial aid, weapons, and

[49] Emilie Oftedal, "The Financing of Jihadi terrorist cells in Europe," *Norwegian Defence Research Establishment FFI-rapport 2014/02234* (16 January 2015): 16-20, https://www.ffi.no/en/publications-archive/the-financing-of-jihadi-terrorist-cells-in-europe.
[50] FATF, *Terrorist Financing Risk Assessment Guidance, cit.*, p. 8-10.

training, by state sponsors, sympathisers, families or foreign entities. This form of funding boosts extremist groups' operational capacities, allowing them to carry out assaults, build their networks, and sustain their infrastructure.[51] Governments or organisations providing financial resources or military help to accomplish their political or strategic goals are examples of state sponsorship. Terrorist support may be seen in Iran's support for *Hizb Allāh*, commonly known as *Hezbollah*, in Lebanon and Pakistan's previous support for militant groups such as the Haqqani Network.[52]

Popular support is the least common type of funding sources. Individuals or communities who sympathise with or lend ideological and financial support to terrorist groups are examples of popular support.[53] This assistance can take many forms, including monetary gifts, recruitment efforts, safe havens, and the propagation of extreme ideology. Certain population elements may be attracted to the cause and provide resources willingly. The *Islamic State of Iraq and Syria* (ISIS) has received widespread public support from sympathisers worldwide, attracting financial contributions and recruits to sustain its activities.[54]

The second stage involves the movement of funds from one location or entity to another to transfer or distribute large amounts of money for their operations. The choice of a specific channel for moving funds by terrorists depends on their particular needs and the evolving landscape of financial systems and technologies. There are various indicators to consider, but usually, terrorists refer to only a few of the most important ones to carry out the movement of funds without any difficulties regarding *volume, risk, convenience, simplicity, costs and speed*.[55]

As for *volume*, terrorists prefer methods permitting the volume and the capacity to transfer large sums of money in a single transaction. It is essential to underline that different approaches differ in their ability to handle significant amounts of money. For instance, moving bulk cash is much more challenging than transferring through formal banking institutions because it allows only a limited quantity and weight of currency.

Another relevant indicator is the presence of *risks* connected with illegally moving money. In general, terror organisations are well aware of the possibility of being discovered by authorities, so they may utilise strategies to avoid law enforcement agencies tracking down their

[51] Oftedal, *op. cit*., p. 19-20.
[52] U.S. Department of State, *Country Reports on Terrorism*, DC: Bureau of Counterterrorism, 2019, 258, https://www.state.gov/reports/country-reports-on-terrorism-2019/.
[53] Oftedal, *op. cit*., p. 19.
[54] FATF, Terrorist Financing Risk Assessment Guidance., *cit*., p. 11.
[55] Freeman and Ruehsen, *op. cit.*, p. 6-7.

funds. For instance, cash smuggling is less dangerous than other methods, such as electronic transfers or traditional banking systems.[56]

Furthermore, *convenience* is a crucial element in transporting illicit finances for terrorists. Geographical, cultural and linguistic factors determine convenience. Terror organisations may choose ways that provide convenience and accessibility, allowing them to rapidly shift funds between places without attracting undue notice.[57] To be specific, the Lebanese terror organisation *Hezbollah* earns millions of dollars each year from the trafficking of diamonds from the Ivory Coast to Asia. The distance between the two continents is immense, but it is possible since the movement is of diamonds, which are relatively easy to conceal.[58]

Moreover, terrorist financiers frequently choose the most straightforward methods of moving monies. Complex procedures increase the likelihood of errors or detection, thus jeopardising their operations. They seek to speed up the whole process and limit the possibility of exposure by using simple techniques, like wire transfers through many bank accounts.[59]

Furthermore, terrorists also consider the issue related to *cost-effectiveness* while moving funds. The choice is based on ways involving the fewest expenses, thus maximising the revenue for illegal activity. Typically, high fees are associated with specific transactions for bank transfer costs through international banks, which range between 12% and 15%, while *hawāla* charges between 0.2% and 0.5% as an informal value system.[60]

Last in order, terrorist operations frequently require *quick access to finances*, especially when the purchase or immediate action is required. As a result, they may prioritise approaches that allow for the speedy transfer of funds and the prompt implementation of results. In illegal fund transfers, the *hawāla* system will be favoured over the standard banking system, because it only requires that deposits have to be held for a day before they are cleared.

All these indicators are present in formal and informal channels used to transfer funds.[61] In the case of informal channels, they reflect an unofficial type of communication which is not based on any hierarchy or organisation but relies on interpersonal and social ties. The so-called cash couriers are among the most well-known and oldest informal methods. Terror organisations or criminal groups hire couriers to transport cash from one country to another. This is possible by concealing huge sums of money in luggage, packages or hidden vehicle parts and transporting

[56] *Ibid*.
[57] *Ibid*.
[58] James J. F. Forest, "Crime-Terror Interactions in Sub-Saharan Africa," *Studies in Conflict & Terrorism* 45, no. 5-6 (2019): 372-375, https://doi.org/10.1080/1057610X.2019.1678881.
[59] Freeman and Ruehsen, *op. cit.,* p. 8.
[60] *Ivi*, p. 7.
[61] Dr. Eitan Azani interview by Anna Miccoli, February 8, 2023, audio, 34:12.

it across borders without drawing attention to themselves. According to the U.S. Department of the Treasury, cash couriers are still highly used by the terror organisation *ISIS* to move and smuggle cash between Iraq and Syria.[62] *Hezbollah* still mainly uses couriers to move cash, diamonds, and art. The main routes involve Beirut, Dubai, Johannesburg and Hong Kong.[63] Even if today, there are more controls and inspections to limit this illicit transfer, the system of cash couriers is still used because "cash is anonymous and leaves no audit trail."[64]

*Informal value transfer systems* are another example of informal channels. These systems transfer funds through a network of trusted individuals that build a hidden financial system.[65] Nikos Passas defines IVTS as "any system or network of people facilitating, on a full-time or part-time basis, the transfer of value domestically or internationally outside the conventional, regulated financial institutional systems."[66] IVTS can be classified into informal funds transfer (IFT) system and informal value transfer methods (IVTM).[67] The former are alternative financial systems that use informal channels to transmit funds. The *hawāla* is an example of an IFT system. The latter are still informal economic systems, but unlike IFT systems, they cover a broader range of procedures than merely the transmission of monies. While IFT systems are limited to transferring monies, IVTM can include a broader spectrum of value exchange, such as goods, commodities, or services. IVTM can consist of barter systems, commodity-based transfers, and other non-monetary transactions.

A traditional IVTS operation has four actors: sender, recipient and two IVTS operators. **Figure 3** below shows how funds are transferred through IVTS: The sender in country A entrust the funds to the IVTS operator in country A, who, in turn, contacts the IVTS operator in country B to give him instructions. Simultaneously, the sender in country A gets in touch with the recipient in country B to give instructions on collecting the funds sent.[68]

---

[62] The Department of Treasury, Office of Inspector General, *Operation Inherent Resolve – Summary of Work Performed by the Department of the Treasury Related to Terrorist Financing, ISIS, and Anti-Money Laundering for First Quarter Fiscal Year 2021,* January 4, 2021, https://oig.treasury.gov/sites/oig/files/2021-01/OIG-CA-21-012.pdf.
[63] The Department of Treasury, *Treasury Disrupts International Money Laundering and Sanctions Evasion Network Supporting Hezbollah Financier*, April 18, 2023, https://home.treasury.gov/news/press-releases/jy1422.
[64] FATF and MENAFATF (2015), *Money Laundering through the Physical Transportation of Cash* , FATF, Paris, France and MENAFATF, Manama, Bahrain, 26, https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/money-laundering-through-transportation-cash.pdf.coredownload.pdf.
[65] Matteo Vaccani, "Alternative Remittance Systems and Terrorism Financing," *World Bank Working Paper*, no. 180, 2010: 7, https://doi.org/10.1596/978-0-8213-8178-6.
[66]Nikos Passas, "Informal Value Transfer Systems and Criminal Organizations; A Study into So-Called Underground Banking Networks," *SSRN Electronic Journal* (1999), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1327756.
[67] *Ibid*.
[68] U.S. States Department of the Treasury Financial Crimes Enforcement Network, *Informal Value Transfer Systems*, March 2003, 5, https://www.fincen.gov/sites/default/files/advisory/advis33.pdf.

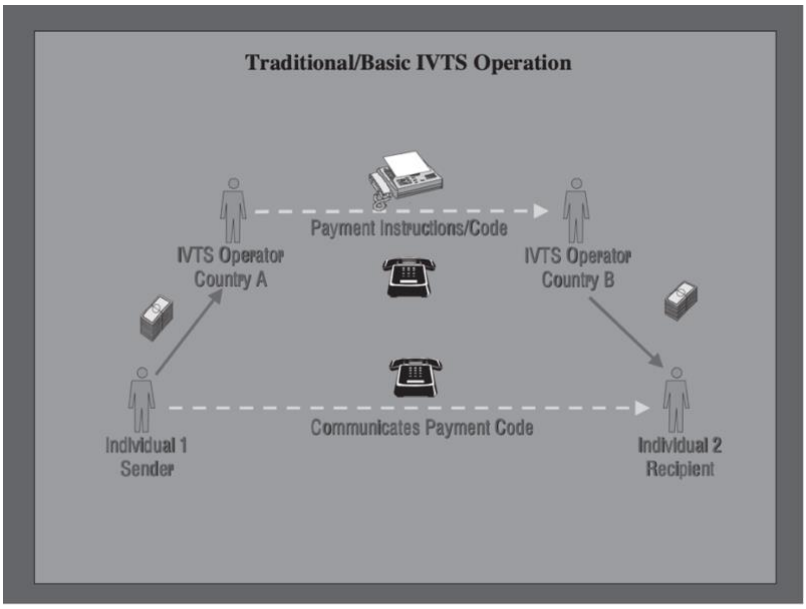



**Figure 3**: IVTS traditional mechanism; Source: FinCEN (2003).

Initially, IVTS were adopted mainly by immigrants or people living in areas where banking systems did not exist, while terrorist groups also employ them today. In 2003 Passas published a report which describes the different types of informal value transfer systems and their geographical origins, for instance, "*hundi*" (to collect) in Pakistan and Bangladesh; "*Black Market Peso Exchange*" in South America; "*hawāla*" (transfer) in India, Middle East, and UAE, "*fei ch'ien*" (flying money) in China *inter alia*.[69] Depending on their origins, these systems can differ in their names and mechanisms, but the goal is unique.

Initially, IVTS referred to *hawāla* and *fei ch'ien* but was later used to identify other informal transfer systems.

On the other hand, formal channels refer to official and prescribed methods of communication within an organisation or institution with precise hierarchy, structure and communication methods.[70] Formal channels rely on instructions, rules and procedures to ensure business purposes stay within legal and ethical boundaries.[71]

Funds transfer through banks is the most successful channel that can easily manage large sums of money globally and be controlled for terrorism financing. The formal banking sector comprises investment and commercial banks, credit unions, and saving banks. These

[69] Passas, *Informal Value Transfer Systems and Criminal Organizations; A Study into So-Called Underground Banking Networks*, *cit*., p. 13-20.
[70] Gjermund Haslerud and Bent Sofus Tranoy, *Fighting Terrorist Finance – Issues, Impacts and Challenges*, Kjeller: Norwegian Defence Research Establishment, (2005), https://ffi-publikasjoner.archive.knowledgearc.net/bitstream/handle/20.500.12242/1874/05-02100.pdf.
[71] *Ibid*.

institutions offer services like loans, credit lines, and international money transfers. The banking system is frequently believed to be a formal conduit away from illicit activities. Instead, it emerges as a potential method for funding crime and terrorism. Terrorists often choose banks with insufficient or weak anti-money laundering systems because it is easier to move money without control. The 1970 Bank Secrecy Act of the United States and more recent amendments in Title III of the USA Patriot Act are clear examples of the measures adopted by governments, in this case, the U.S. one, to prevent financial institutions from being used as tools by criminals to hide or launder their illicit gains. [72] The Bank Secrecy Act states that banks and other financial organisations are required by law to supply authorities with documentation, such as currency transaction reports. Banks may request such documentation when customers deal with suspicious cash transactions exceeding $10,000.[73] Despite numerous efforts by banks and governments, there are still some instances where terrorists can use the banking system for their ends.

Another possible scenario may be related to those terrorist groups that could include corrupt employees or recruit an affiliate to be employed within the banks. The reasons why an employee accepts to collaborating with a criminal organisation can vary from monetary rewards to ideological affiliation or even extortion. First, the infiltrator or corrupt employee detects weaknesses in the bank's internal controls, procedures or systems between banks. This might include identifying areas of inadequate supervision, monitoring or controls. By taking advantage of its position within the bank, the affiliated individual gains access to systems, data or confidential information to facilitate illegal or unauthorised activities or divulge confidential information. This entails falsifying records, creating misleading documentation or other techniques to hide communications or transactions.

Nevertheless, formal banks maintain with mechanisms to thwart attempts to compromise customer data from corrupt employees. Terrorists are therefore far more probable to gain access to banks undetected by authorities. *Al-Qāʿida*, however, avoided some of these restrictions by using bank branches in Pakistan and the United Arab Emirates, "which at the time lacked good regulatory oversight and by allowing mostly low-level (…) operatives to use banks for the 9/11 plot."[74]

[72] Bank Secrecy Act, 31 U.S.C. § 5311 et seq. (1970); USA PATRIOT Act §§ 301-377, 115 Stat. at 296-342.
[73] Freeman and Ruehsen, *op. cit*., p. 17.
[74] John Roth, Douglas Greenburg and Serena Wille, *Monograph on Terrorist Financing*, (National Commission on Terrorist Attacks Upon the United States, 2004), 26, https://govinfo.library.unt.edu/911/staff_statements/911_TerrFin_Monograph.pdf.

Money Service Businesses (MSBs) are an additional channel for transferring funds by terrorists along with formal banking institutions. The MSBs can be defined as "currency dealers or exchangers; check cashers; issuers (or redeemers) of traveller's checks, money orders, or stored value cards; and money transmitters" and they offer a variety of financial services to both consumers as well as companies, including wire transfers, electronic cross-border money transfers, currency exchange and domestic and international money transfer services.[75] Like banks, MSBs are subject to regulatory audits and are required to follow anti-money laundering laws depending on the country where the business is registered. However, MSBs are exempt from severe "know your consumers" (KYC) procedures that banks usually have to respect, and they do not require customers to provide all of the private information needed to open an account, only an identity document.[76]

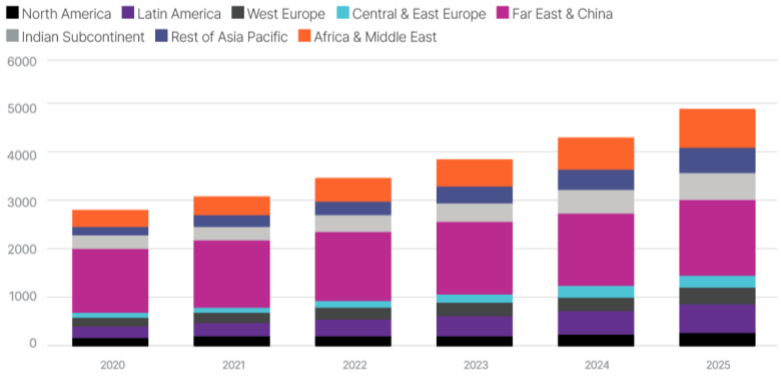
Due to the rapidity and simplicity of operations, MSBs stand out as potential conduits for terror organisations by transferring money between countries and individuals. There are different ways through which MSBs can be used by terrorists. For instance, terrorists may use MSBs to transmit cash to individuals associated with terrorist groups or actively fund terrorist actions through alternative payment methods like internet payment systems and prepaid cards without drawing the attention of authorities. In addition, to avoid sanctions, this system must conform to anti-money laundering regulations. For example, the Western Union Company, a multinational money services company headquartered in Englewood, Colorado, was fined $600 million by the USA in 2017 for inadequate compliance with anti-money laundering regulations as stated, "Western Union's blatant disregard of their anti-money laundering compliance responsibilities was criminal and significant" [77] and "as a major player in the money transmittal business, Western Union had an obligation to its customers to ensure they offered honest services, which include upholding the Bank Secrecy Act, as well as other U.S. laws."[78]

The methods discussed previously are the most widely used by terrorists to transfer funds, although they are not the only ones. Terrorist groups have recently begun to take advantage of the Internet and telecommunications services, including virtual currencies such as Bitcoin, electronic payment systems such as PayPal or Satispay, mobile payment services and BLIK, a sex/digit code shown by the programme that can be used to accept transactions or

[75] Bank Secrecy Act, *cit*.
[76] Freeman and Ruehsen, *op. cit*., p. 12.
[77] Office of Public Affairs, "Western Union Admits Anti Money Laundering and Consumer Fraud Violations, Forfeits $586 Million In Settlement With Justice Department and Federal Trade Commission," U.S. Department of Justice, accessed July 11, 2023, https://www.justice.gov/opa/pr/western-union-admits-anti-money-laundering-and-consumer-fraud-violations-forfeits-586-million.
[78] *Ibid*.

withdrawals from an automatic teller machine (ATM), just as if customers were paying with a card.[79] Compared to the traditional forms of payments, the new payment methods (NPMs) benefits include increased anonymity in transactions, less regulation, and, most importantly, difficulties in detecting suspicious activities due to decentralisation and complexity in tracking the cash flow.

Based on 2021 Mobile Wallets Reports by Boku, a fintech pioneering the first global mobile payments network, in collaboration with the digital technology analyst house Juniper Research, the number of mobile digital wallets was 2.8 billion in 2020 and is expected to increase to 4.8 billion in 2025, representing about 60% of the world's population.[80] Therefore, with the increasing use of electronic payment systems, some countries such as Saudi Arabia and India, are endeavouring to limit cash usage. The report contains statistics from 19 nations in Asia Pacific, Latin America, Eastern Europe, Africa and the Middle East.[81]




| | 2020 | 2021 | 2022 | 2023 | 2024 | 2025 |
|---|---|---|---|---|---|---|
| North America | 184.7 | 201.0 | 219.9 | 233.2 | 247.6 | 275.4 |
| Latin America | 227.3 | 277.5 | 336.6 | 406.9 | 494.9 | 605.7 |
| West Europe | 200.1 | 216.3 | 245.1 | 257.0 | 285.3 | 331.9 |
| Central & East Europe | 76.3 | 103.2 | 143.0 | 187.5 | 215.0 | 248.9 |
| Far East & China | 1,343.4 | 1,386.9 | 1,429.8 | 1,466.5 | 1,501.8 | 1,541.4 |
| Indian Subcontinent | 269.2 | 287.4 | 333.2 | 393.7 | 465.6 | 550.4 |
| Rest of Asia Pacific | 179.7 | 223.1 | 281.7 | 349.9 | 426.5 | 520.7 |
| Africa & Middle East | 322.9 | 390.0 | 471.4 | 561.5 | 669.6 | 798.2 |
| Global | 2,803.7 | 3,085.5 | 3,460.6 | 3,856.5 | 4,306.3 | 4,872.7 |

**Figure 4**: Mobile wallets in use by region (2020-2025); Source: Juniper Research (2023).

Between 2020 and 2025, Southeast Asia is expected to see the largest rise in the use of digital wallets, specifically mobile wallets, whereas China and the Far East are nowadays responsible

[79] Michael Jacobson, "Terrorist Financing and the Internet," *Studies in Conflict & Terrorism* 33, no. 4 (2010): 353–63.
[80] Boku and Juniper Research, *2021 Mobile Wallets Report*, San Francisco (2021): 9, https://www.paymentscardsandmobile.com/wp-content/uploads/2022/02/Mobile-Wallets-Report-2021.pdf.
[81] *Ibid*.

for the majority of mobile wallets worldwide. With a predicted rise of 147% between 2020 and 2025, Africa and the Middle East are expected to have the second-largest mobile wallet industries. By 2025, North America and Western Europe will have the weakest growth rates, at 65% and 50%, respectively.[82] What is more, South Asia, Africa and the Middle East are also the main places where terrorists live, as demonstrated by **Figure 5**, reported by the Institute for Economics and Peace, which shows the presence of terrorist groups worldwide on a scale from having a very high impact to having no impact in the areas.[83]

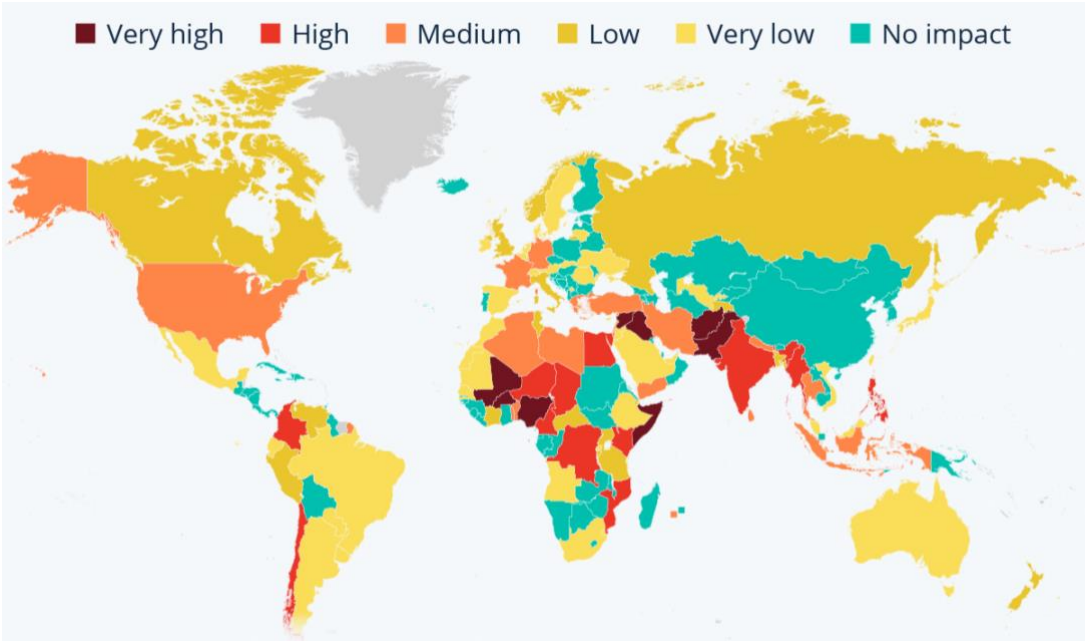



**Figure 5**: Evaluating the global impact of terrorism; Source: Institute for Economics and Peace (2023).

The Institute for Economics and Peace depicts the impact of terrorism globally in 2023 through the Global Terrorism Index (GTI), which considers four factors–the number of attacks, victims, people wounded, and hostages–used to determine this categorisation and concludes that "terrorism is dynamic, and, although the overall change in the last three years has been minimal, there have been sharp rises and falls in terrorism in many countries during this period, notably Niger, Myanmar and Iraq."[84] The quick expansion of digital wallets and subsequent use of e-payments in these regions has undoubtedly enhanced the use of these new payment systems by terrorist groups.

[82] *Ibid*.
[83] Institute for Economics & Peace, *Global Terrorism Index 2023: Measuring the Impact of Terrorism*, (Sydney: March 2023): 8-9, http://visionofhumanity.org/resources.
[84] *Ivi*, p. 2.

The third and last stage is the use of funds collected. Terrorists do not manage and use funds for one specific purpose because this may vary according to the organisation's needs, capabilities, motivation and structure. In this regard, terrorists use the funds they collect for two main purposes: operational expenditure and organisational expenditure.[85] The former refers to all the expenses for terror attacks and pre-operational surveillance. Funds are also required to pay the expenses of weapons, explosives and transportation to the target location. In addition, the funds are used to build safe heavens, as Osama bin Laden did, by paying the *Tālibān* $10 and $20 million yearly between 1996 and 2001, as a reward for safe shelter in Afghanistan.[86]

Moreover, money can be used to obtain fake identity documents to avoid arousing suspicious at checkpoints. The cost of organising terrorist attacks varies depending on the organisation itself; the finances required for attacks carried out by minor organisations or lone actors are less than those needed for an attack planned by a major and structured organisation. To give an instance, the 2004 terrorist attack in Madrid, where approximately 190 people were involved in the killing, cost €150,000.[87]

Conversely, the second purpose refers to the expenses required for the organisation's growth and maintenance. Some funds are used to recruit new members and establish training camps. The cost of recruitment and propaganda has decreased with the growth of the internet and social media. While previously, most recruiting announcements and propaganda relied mainly on printed advertisements or word-of-mouth, today, terrorist groups may spread their propaganda through online magazines like *Al-Qāʿida'*s inspire and recruit new members by using platforms such as Twitter or Tik Tok and television outlets. For example, "*Hezbollah*'s purchase of the Al Manar satellite TV operation and Al-Nour Radio has been used to support its fundraising efforts and to publicise calls for volunteers to do *Hezbollah* military training."[88]

Furthermore, part of the organisational expenditures is used to pay the salaries of the organisation's leader and of some members but also to assist the families of the imprisoned or killed members, such as *Hamās*, which pays between $12,000 and $15,000 for suicide bomber families.[89] Medical, social and educational services are provided, too, where governments only

[85] Simon Norton and Paula Chadderton, "*Special Report: Detect, Disrupt and Deny: Optimising Australia's Counterterrorism Financing System*, Australian Strategic Policy Institute (2016): 36-42, https://www.jstor.org/stable/resrep04244.9.
[86] FATF, *Emerging Terrorist Financing Risks*, *cit*., p. 9-10,
[87] Wilson Center, The 3/11 Madrid bombings: an assessment after 5 years, 10 April 2009, https://www.wilsoncenter.org/article/the-311-madrid-bombings-assessment-after-5-years.
[88] FATF, *Emerging Terrorist Financing Risks*, *cit*., p. 11.
[89] Colin P. Clarke, *Terrorism, Inc.: the financing of terrorism, insurgency, and irregular warfare*, Praeger Security International, 2015, 109; Adam Dolnik, Anjali Bhattacharjee, 'Hamas: suicide bombings, rockets, or WMD?' *Terrorism and Political Violence*, 2002, 14:3:13.

offer inadequate social services, allowing terror organisations to maintain power locally and internationally.[90]

The more money a terrorist group has, the greater threat it poses.[91] The availability of financial resources is a key factor in the strength and reach of terrorist organisations. Larger fundings provide more opportunities, but even modest sums can be used effectively, giving terrorists the opportunity to expand their network and carry out terror attacks.

### 2.2 Understanding the Concept of Money Laundering

Terrorists generate significant profits from their illicit operations. However, the use of such gains is constrained by the fact that the money was obtained illegally; therefore, it is advisable to keep it hidden to avoid raising suspicion from the authorities. This process is better defined as money laundering, through which the proceeds of unlawful activities are dissimulated to conceal their illegal sources. Money laundering is a phenomenon that impacts the global scene and is not just a technique employed by terrorists. The aim is to be able to launder the money and then use it for additional purposes.[92]

Globalisation has made it possible for more investments and transfers across borders in both the legal and illicit economies, including terrorism. In this regard, financial markets have recently become extremely dangerous due to money launderers, whose easier access to information has slowed down the rate at which the economy is growing.[93]

#### 2.2.1 Definition of Money Laundering

As with the word "terrorism", there are several ways in which the term "money laundering" is defined. In the 1980s, governments and international organisations started to become more interested in the subject. The expression is relatively new and first featured in the United States case US v $4,255,625.39 1982.[94]

Money laundering was explicitly defined for the first time by the *United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances* in Vienna, Austria, 1988.[95] The convention, also called the Vienna Convention, states in Article 3(b):

---

[90] *Ibid*.
[91] Norton and Chadderton, *op. cit*., p. 12.
[92] Paul A. Schott, *Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism* (Washington D.C.: The World Bank, 2003).
[93] Bonnie Buchanan, "Money Laundering – a Global Obstacle," *Research in International Business and Finance*, 18, no. 1 (2004): 115.
[94] See United States v. $4,255,625.39, 551 F. Supp. 314 (S.D. Fla. 1982).
[95] *United Nation Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances*, New York, 20 December 1988, United Nations Doc. E/CONF.82/14, https://www.unodc.org/pdf/convention_1988_en.pdf.

*i.* The conversion or transfer of property, knowing that such property is derived from any (drug trafficking) offense or offenses or from an act of participation in such offense or offenses, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an offense or offenses to evade the legal consequences of his actions;

*ii.* The concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of property, knowing that such property is derived from an offence or offences or from an act of participation in such an offence or offences.[96]

However, the Vienna Convention only recognises as a crime the unlawful funds obtained through the laundering of drug trafficking profits. It was agreed henceforward to widen the scope of money laundering under the Vienna Convention as new risks and offences emerged over time. In 2000, in Palermo, Italy, the United Nations General Assembly adopted the *Convention against Transnational Organised Crimes* through resolution 55/25 of 15 November 2000.[97] The Convention represent a milestone in the fight against transnational organised crime because it not only punishes money laundering from drug trafficking but "requires all participant countries to apply that convention's money laundering offences to "the widest range of predicate offences."[98] Article (6) defines the criminalisation of money laundering process as follows:

> *(a) (i)* The conversion or transfer of property, knowing that such property is the proceeds of crime, for the purpose of concealing or disguising the illicit origin of the property or of helping any person who is involved in the commission of the predicate offense to evade the legal consequences of his or her action;
>
> *(ii)* The concealment or disguise of the true nature, source, location, disposition, movement or ownership of or rights with respect to property, knowing that such property is the proceeds of crime;
>
> *(b)* Subject to the basic concepts of its legal system:
> *(i)* The acquisition, possession or use of property, knowing, at the time of receipt, that such property is the proceeds of crime;
>
> *(ii)* Participation in, association with or conspiracy to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the offences established in accordance with this article.[99]

[96] *The Vienna Convention*, Article 3(b).
[97] *United Nations Convention against Transnational Organised Crimes*, New York, 12 December 2000, United Nations A/RES/55/25, https://treaties.un.org/doc/source/docs/A_RES_55_25-E.pdf.
[98] *The Palermo Convention*, Article 2 (2).
[99] *The Palermo Convention*, Article 6.

The FATF is an organisation that has been consistently fighting money laundering since its creation in July 1989 by the G7 through the *Economic Declaration* held in Paris.[100] The FATF defines money laundering as "processing criminal proceeds to disguise their illegal origin."[101]

In 1990, the FAFT released all the countermeasures against money laundering in a compilation of *Forty Recommendations*.[102] In October 2004, the FAFT published a *Ninth Special Recommendation* on terrorist financing that was later added to the existing recommendations.[103] Nevertheless, as money laundering and terror financing dangers have evolved over time, the FATF has continued to update the Recommendations. In 2012, for instance, the *Forty Recommendations* and the *Ninth Recommendation* were revised to address new threats like weapons of mass destruction.[104] Furthermore, a new revision was put into effect in 2019 to add new, legally binding measures for the regulation and oversight of activities and services providers related to virtual assets or crypto assets.

To prevent criminals from hiding their illicit operations and dirty money behind covert business structures, restrictions were further tightened in 2022.[105] The World Bank and the International Monetary Fund recognised all the recommendations as the global standards for preventing money laundering and terror financing.

### 2.2.2 The Process of Money Laundering

According to the United Nations Office on Drugs and Crime (UNODC), approximately between 715 billion and 1.87 trillion euros are laundered annually, representing between 2 to 5% of the global GDP.[106] In this regard, the European Union Agency for Criminal Justice Cooperation (EUROJUST) released a report on money laundering in October 2022, which indicates that from 2016 to 2021, money laundering crimes made up about 15% of all instances reported to the agency.[107]

---

[100] *The Economic Declaration*, Paris, 16 July 1989, G7 Research Group, http://www.g8.utoronto.ca/summit/1989paris/communique/index.html.

[101] FATF and GAFI (2006), *Trade Based Money Laundering*, FATF, Paris, https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Trade%20Based%20Money%20Laundering.pdf.coredownload.pdf.

[102] FATF (2003-2004), *FATF 40 Recommendations*, FATF, Paris, https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Standards%20-%2040%20Recommendations%20rc.pdf.coredownload.pdf.

[103] FATF (2012-2023), *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation*, FATF, Paris, https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf.

[104] *Ibid*.

[105] *Ibid*.

[106] "Money Laundering," United Nations Office on Drugs and Crime, accessed July 21, 2023, https://www.unodc.org/unodc/en/money-laundering/overview.html.

[107] European Union Agency for Criminal Justice Cooperation, *Eurojust Report on Money Laundering*, (Luxembourg, Publication Office of the European Union, 2022), 7, https://www.eurojust.europa.eu/sites/default/files/assets/eurojust-report-money-laundering-2022.pdf.

To date, **Figure 6** displays a pie chart with the overall number of cases (21.377) and the number of instances involving money laundering (2.870).[108] Moreover, next to the pie chart, there is a bar graph that displays the amount of money laundering cases concerning all the cases for each year between 2016 and 2021.[109] The graph shows a remarkable increase in money laundering cases over the years. Thus, importantly, the graph displays a striking surge in money laundering cases over the years, particularly concerning instances involving this illicit activity. The upward trend is evident from the steep rise in the number of reported incidents over the depicted period. The data highlights a concerning reality, indicating that money laundering has become a prevalent and growing issue within the financial system. The graph's clear upward trajectory underscores the need for stronger regulatory measures, international cooperation, and increased awareness to combat this criminal behavior effectively: As financial systems become more interconnected and sophisticated, it is crucial to address the root causes of money laundering and enhance the efforts to detect and prevent such activities to safeguard the integrity and stability of the global financial landscape.

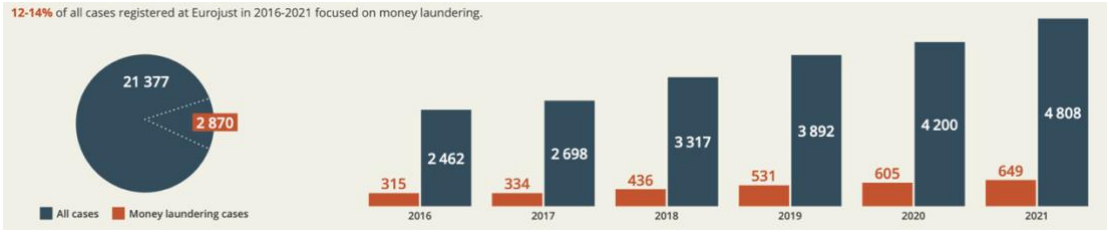



**Figure 6**: Number of money laundering cases as a proportion of all cases; Source: Eurojust (2022).

Money laundering stems from various criminal activities, such as illegal arms sales or human trafficking. The process of money laundering does not vary depending on the type of criminal activity but instead follows a single cycle that enables illicit funds to enter the legal financial system, conceal their trustworthy source, and then transform into legitimate money.[110] This process has three significant steps: placement, layering and integration as described by **Figure 7** below.

[108] *Ibid*.
[109] *Ibid*.
[110] Schott, *op. cit*., p. 23.

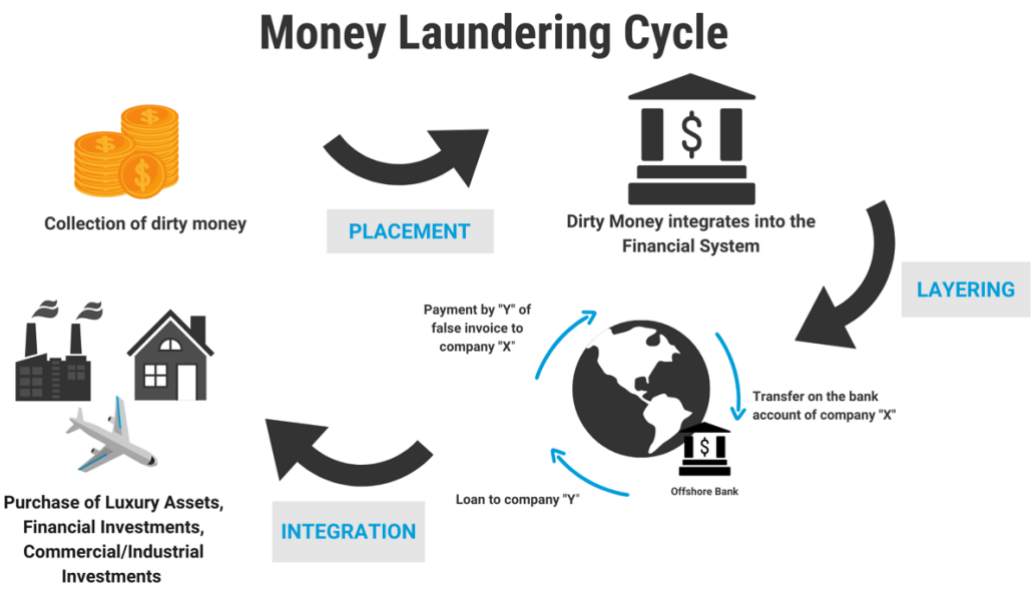



**Figure 7**: The three stages of money laundering; Source: UNODC (2022).

The first stage begins with transferring illegal funds into the legitimate financial system from a criminal source. As long as it is legitimate, the financial system can be any financial instrument, including banks and legal assets. Criminals may construct offshore corporations, split up large sums of money into smaller ones, or falsify invoices to make the source of funds appear legitimate to raise as little suspicion as possible throughout the transit of illicit monies.

*Layering*, which comes after placement, breaks down significant amounts of illegal cash into smaller sums to stay below the legal limit set by anti-money laundering legislation. This is conceivable because layering occurs across legal lines, making it more challenging for law enforcement to find signs of money laundering. The most popular methods employed by money launderers are buying foreign money orders, buying and selling luxury goods abroad, and trading in foreign currencies.[111] The third and last stage is *integration* which entails, as the term suggests, integrating illegal funds into the financial system's accounts. Standard integration strategies involve, for instance, making unrepayable loans to shareholders.[112]

All the cases of money laundering may not involve all three stages together but may combine or repeat the same stages several times.

[111] *Ibid*.
[112] *Ibid*.

## 2.3 The Connection between Terror Financing and Money Laundering

Money laundering and terror financing are two crimes that are often associated with or thought to be the same type of crime. Although the steps of money laundering and of terrorism financing are very similar (e.g., as for placement, layering and integration), there are some key distinctions between the two processes).[113]

As the diagram below shows, unlike the money laundering process, terrorists may raise funds from both illegal and legal sources during the placement phase. Furthermore, in the final stage, the integration, the funding process in terror financing is usually linear, with the funds collected being utilised for terrorist acts and other services, such as supporting dislocated cells. Still, the money laundering process is generally circular, with the money returning to the person who generated it.[114]

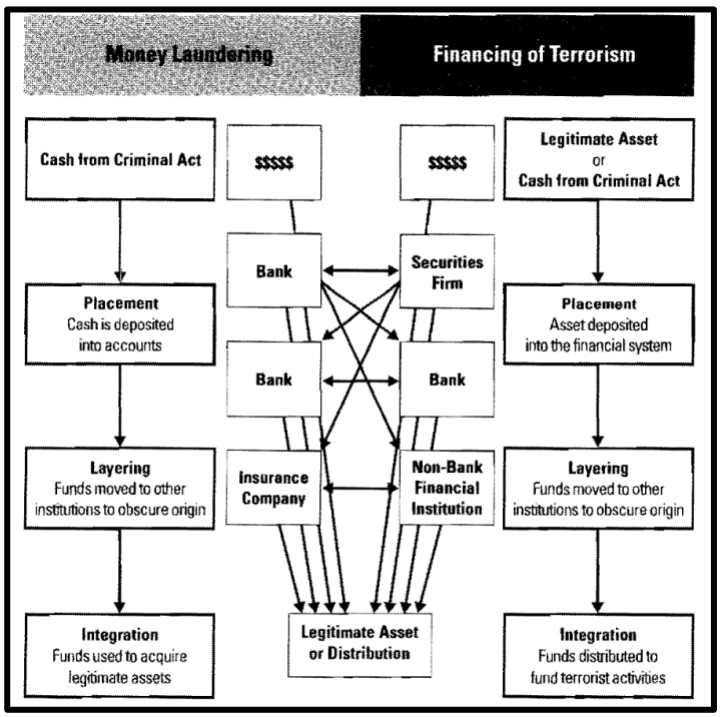



**Figure 8**: The process of money laundering and financing of terrorism; Source: Word Bank (2004).

Addressing the differences between money laundering and terror financing is crucial for financial institutions and authorities to limit these illicit processes successfully. Johnson, in 2008 argued how important it is to pay attention to money laundering and terrorism not as two totally distinct processes but because the former is an indispensable component in "fighting the war against terrorism" after the September 11th terrorist attacks.[115] Moreover, it is important

[113] *Ivi*, p. 22.
[114] *Ibid*.
[115] Jackie Johnson, "Is the Global Financial System AML/CFT Prepared?" *Journal of Financial Crimes* 15, no. 1 (2008): 7-14, http://dx.doi.org/10.1108/13590790810841662.

to pay attention to new methods as terrorists and launders are always looking for alternative methods to avoid control.

# CHAPTER III.
# HAWĀLA:
# UNVEILING THE INFORMAL VALUE TRANSFER SYSTEM

## 3.1 Introduction to Hawāla

The international community became aware of the growing issue of terrorism after the terrorist attacks of 11, 2001, which had previously only affected specific regions of the world. Methods of financing terrorism received much attention. Moreover, after the attacks of September 11, public interest in the IVTS[116] grew, particularly that of *hawāla*, mainly practiced in South Asia and the Middle East.[117] The term *hawāla* comes from Arabic and means "transfer" or "wire", and it can be defined as an "alternative or parallel remittance system that exists and operates outside the traditional banking system."[118] *Hawāla* is known by several names worldwide, including *Hundi* in India, *Padala* in the Philippines, and *Hui Kuan* in Hong Kong. This informal transfer method demonstrates that, regardless of its name or location of origin, it is adaptable to suit cultural and linguistic situations everywhere. Even if the terminology varies, the essential premise of informal money transfers based on trust remains intact across all denominations.[119]

Even if the origins of *hawāla* remain somewhat uncertain it is believed to have originated between the 8th and 9th century in South Asia, and its expansion was aided by the intense trade that linked Asia, the Middle East and Europe along the Silk Road. Before the invention of paper money, traders used to pay with gold and other valuable metals.[120] The adoption of *hawāla* enabled traders to transmit their funds over long distances reliably, involving a network of intermediaries and family members to facilitate the transfer of payments between parties without physically moving the goods across borders.[121]

Because of its linkages with the Islamic moral traditions of *Shari'a*,[122] *hawāla* has spread considerably throughout the Middle East, particularly in the setting of mediaeval Islamic business.[123] According to Ali et al. in the Islamic religion, every economic activity has a

[116] Passas, *Informal Value Transfer Systems, Terrorism and Money Laundering*, cit.
[117] Mohammed El Qorchi, "Hawala: How does this Informal Funds Transfer System Work, and Should it be Regulated?" *Finance & Development* 39, no. 4 (2002), https://www.imf.org/external/pubs/ft/fandd/2002/12/elqorchi.htm.
[118] *Ibid*.
[119] Dr. Tal Shaanan interview by Anna Miccoli, February 10, 2023, audio, 25:13.
[120] El Qorchi et al., *Informal Funds Transfer Systems: An Analysis of the Informal Hawala System*, *cit*., p. 10.
[121] *Ibid*.
[122] Shari'a refers to the Islamic legal and moral code that governs every aspect of Muslim life, derived from the Qur'an and the Sunna, the customs and practises of the Prophet Muhammad, the founder of Islam (610 AD).
[123] Dulce M. Redin et al., "Exploring the Ethical Dimension of "Hawala," *Journal of Business Ethics* 124, no. 2 (2014): 328, https://www.jstor.org/stable/24033272.

spiritual dimension;[124] in fact, *Shari'a* discourages excessive uncertainty in contracts (*gharar*), interest from money (*maysir*) and prohibits charging or payment (*riba*), or interest resonance as found in *hawāla*, where interest is conspicuously absent. Islamic law aims to foster justice, obedience to *Allah*, the Arabic word to indicate God, moral rectitude, trust, and the well-being of the ummah or community, which are all compatible with *hawāla*. Although some Islamic legal ideas are consistent with the informal *hawāla* transfer mechanism, it is not exclusive to Islam and can also be employed for other cultures.[125]

Originally used to facilitate long-distance trade, *hawāla* was later utilised and still used by immigrants in Europe, North America or the Persian Gulf region, or North America to enable them to send a portion of their earnings to their families who live abroad by paying low commissions or even no interest.[126] Despite the spread of banks and other Western institutions created to regulate the global and regional economic system better, it never entirely disappeared, adapting to new technologies.[127] Today, phone, internet, and fax ensure *hawāla*'s continued and efficient use. The popularity of this informal fund transfer system lies in its speed, inexpensiveness, and, most importantly, less bureaucratic way of transferring money.[128] Terror organisations have started using *hawāla*, too, since it provides anonymity, unlike banks or any other formal payment method where everything is regulated and subject to the law.

### 3.1.1 Hawāla Network

Although *hawāla* operates informally, finances are transmitted through well-defined schemes and actors "outside of or parallel to traditional banking or financial channels"[129] with no physical or electronic movement. The *hawāla* transfer can occur within the borders of a single country (*domestic hawāla*) or entail the cross-border movement of funds between countries (*international hawāla*).[130]

Typically a *hawāla* transaction involves four main actors: two customers, identified as CA and CB, who are the sender and receiver of funds placed in two different countries,

---

[124] Abbas J. Ali et al., "Islamic Perspectives on Profit Maximasation," *Journal of Business Ethics* 117, (November 2012): 467-475, https://doi.org/10.1007/s10551-012-1530-0.
[125] Redin et al., *op. cit*., p. 331-332.
[126] El Qorchi, *Hawala: How does this Informal Funds Transfer System Work, and Should it be Regulated, cit*.
[127] Redin et al., *op. cit*., p. 328-329.
[128] Interview with Eitan Azani, Director of Research of the Institute for Counter-Terrorism and Head of the BA and MA Specialisation in Counter-Terrorism, Reichman University. February 8, 2023, audio, 34:20.
[129] Adil Anwar Daudi, "The Invisible Bank: Regulating the Hawala System in India, Pakistan and the United Arab Emirates," *Indiana International & Comparative Law Review* 15, no. 3 (2005): 622, https://research.amanote.com/publication/EZFX1XMBKQvf0Bhi4Jlk/the-invisible-bank-regulating-the-hawala-system-in-india-pakistan-and-the-united-arab.
[130] Interview with Eitan Azani, Director of Research of the Institute for Counter-Terrorism and Head of the BA and MA Specialisation in Counter-Terrorism, Reichman University. February 8, 2023, audio, 34:22.

respectively country A and country B; and two hawaladars, called HA, for the "initiating intermediary" and HB, the "receiving intermediary," who act as intermediaries to facilitate funds transfer between the two clients CA and CB.[131] Furthermore, because HA often obtains funds from CA, it is acceptable for HB to advance the amounts to CB in the local currency correspondent.[132]

A possible scenario of a *hawāla* transaction is extensively described in **Figure 9** below, representing an expatriate worker in a foreign country who wants to send funds to his/her family living in another country. First of all, the expatriate worker is a customer (CA) living in country A, contacts HA to transmit a remittance from country A to another customer (CB), his/her family in country B. The HA receives the funds in one currency from CA and provides the latter with an authentication code to prove the transaction. Then, HA contacts the receiving country's hawaladar counterparty HB through email, phone or fax, transforming the payment into local currency for the customer receiver (CB) in country B.[133] The receiver must provide the code to collect the sum previously sent by CA.

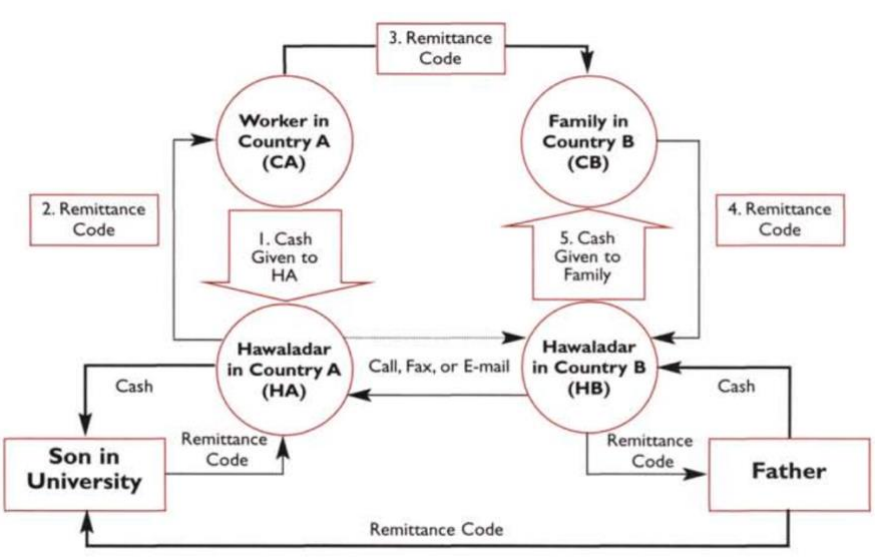



**Figure 9**: Sample transaction of the informal *hawāla* system; Source: IMF (2003).

**Table 1** below illustrates how the budget sheet changes after a *hawāla* remittance for the sender, recipient, and intermediaries. The top of the table indicates the balance changes between the two customers, while the bottom shows the balance changes between the two hawaladars. In

[131] El Qorchi et al., *Informal Funds Transfer Systems: An Analysis of the Informal Hawala System*, *cit*., 38-39.
[132] *Ibid*.
[133] *Id.*

the above section of the table, the remittance sender in country A pays the hawaladar in his or her own country in dollars, requesting that the same value in his or her local currency (LC) be sent to someone in country B, such as his or her family. The sender pays in dollars, which reduces his or her assets, while the recipients receive a net worth in local currency. The two hawaladars subsequently take over the transaction, and the hawaladar in country A comes into contact with the hawaladar in country B, stating "to whom the payment is to be made along with an agreed method by which the recipient can be identified."[134] To correctly complete this *hawāla* transaction, the hawaladar in country B must have funds available to make payments. The financial involvement of the two hawaladars is reflected at the bottom of the table as follows:

> "As for the intermediaries, however, the hawaladar in country A (HA) has received funds in trust without making a payment, and the one in country B has made a payment without receiving its countervalue. Both these hawaladars have taken a financial position in the deal […]. In effect, HB has made a loan to HA, and the transaction needs to be cleared and settled between the intermediaries. After the *hawāla* remittance is completed, HA has a liability to HB, and HB a claim on HA. The principals in the initial transaction do not play any role in the subsequent clearing and balancing of this position. HA and HB can settle their positions in various ways, including simple or complex reverse informal *hawāla* transactions."[135]

[134] *Ivi*, p. 40.
[135] *Ivi*, p. 42.

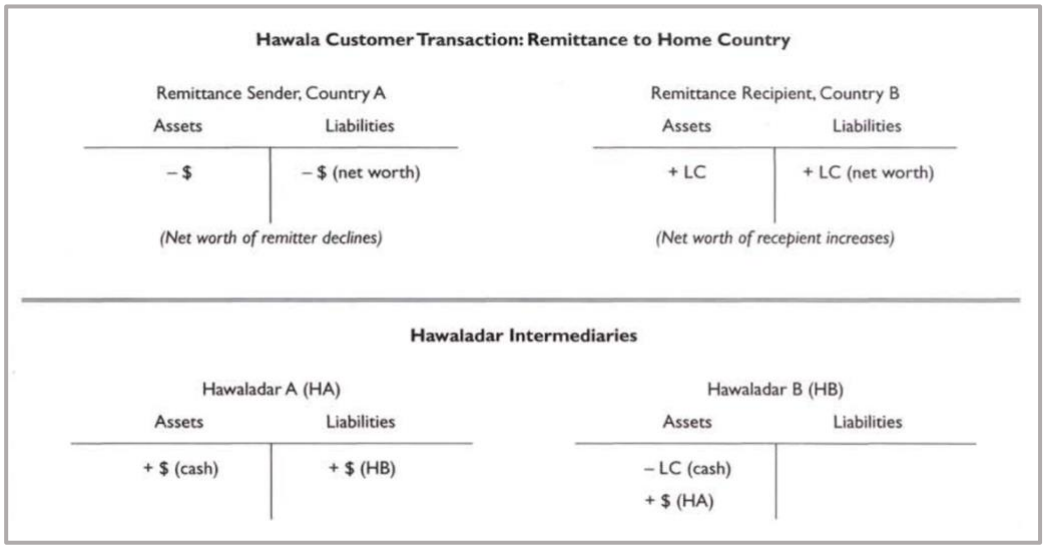



**Table 1**. Model of the informal *hawāla* remittance transaction; Source: IMF (2003).

Reverse *hawāla* is undoubtedly the most well-known method of settling scores among hawaladars.[136] As the name implies, it is a transaction that goes in the opposite direction and can be simple or complex based on the transactions. To begin, despite being the simplest to implement, the simple *hawāla* reverse is rarely used for two reasons: the likelihood that *hawāla* remittances from country B to country A will pass through the same hawaladar, or the aggregated remittance flows between the two countries are highly asymmetric. In this instance, completing the *hawāla* transaction merely through simple or complex transactions involving only two hawaladars is difficult. The volume of remittances from countries like South Asia, sources of emigration and recipient countries like the USA is significant, necessitating a more extensive network of connections than two hawaladars.[137] The reverse simple *hawāla* transaction is less linear because the transaction is built on trust and a network of contacts. An example of a reverse *hawāla* transaction is reported in **Figure 9** above. In a country where foreign currencies and capital flows are restricted, a client in country B, a father (CB), wants to send funds abroad to country A to pay his son's (CA) tuition fees. However, eventual currency controls may limit the amount of money the father wishes to purchase abroad. Consequently, he decides to send the amount through the *hawāla* system contacting the hawaladar in his (HB) and giving him a specified sum of local currency. The customer in country B may be unaware that he is initiating a *hawāla* or *reverse hawāla* transaction. This is determined by how HB handles the transaction: it is a *reverse hawāla* transaction if HB decides to involve in the

[136] *Ivi*, p. 76.
[137] *Id*.

transaction another hawaladar HA in country A to deliver the funds to the student; otherwise, a *hawāla* transaction occurs when HB directly manages the delivery of funds to the customer in country A.[138]

The complex reverse *hawāla*, on the other hand, is usually used when capital transfers are strictly controlled.[139] In a country where foreign exchange or capital movements are restricted, HB may receive local currency from a customer in country C who wishes to send a portion of his funds abroad. If the transaction is not completed, HB may seek assistance from HA. HA can resolve the situation in one of two ways: either by recommending a hawaladar in country C, HC because they are correspondents or because an open position between them remained unstable from a previous transaction, or HA directly instructs HC to make the funds available to any beneficiary C.[140] Alternatively, HB could contact HC directly and demand HA to complete the transaction.

In addition to the simple and complex reverse *hawāla*, there are other ways to balance the outstanding positions of hawaladars. Bilateral financial settlement is one of the most straightforward techniques for settling a *hawāla* transaction. HA can pay HB immediately or place the payment into HB's bank account. It should be highlighted that the deposit is made to a report in a nation other than HB's home country, as this could raise suspicions or subject the promise to local limitations. Instead, multilateral financial settlements are more likely due to settlements through third country accounts. HA will generally manage its debt to HB by depositing funds into an account owned by HB but in country C. This third country should permit transactions with convertible currencies or currencies that can be easily converted into other currencies. Multilateral financial settlement is frequently utilised when a third country is available that accepts convertible currencies and does not impose constraints or restrictions, as in country B.

Another way to settle *hawāla* transactions is for HA to provide international services to HB or the inhabitants of country B.[141] In the case of the latter, if they want to travel or purchase services in another country, such as a medical service, they are limited by the possibility of foreign currency rationing enforced by their country B. The solution for inhabitants of country B is to purchase services from HB in their local currency. Furthermore, "HB itself is a potential

[138] *Ibid*.
[139] *Ivi*, p. 77.
[140] *Ibid*.
[141] *Ivi*, p. 83.

consumer of international services, and this transaction is paid for by HA, which clears both accounts."[142]

In addition, the control of informal remittances occasionally extends beyond direct bilateral agreements to higher-level intermediaries, potentially including more than two hawaladars. Higher levels of financial consolidation within the *hawāla* chain are predicted, with fewer operators holding more prominent roles than the initial intermediates HA and HB. Hawaladar can fill this function with vast networks, significant transactions, and entities unrelated to the *hawāla* system. El Qorchi et al. point out that "neither on-site discussions nor the literature revealed any specific instances where individuals or groups admitted to being consolidators."[143]

### 3.1.2 Legitimate and Illegitimate Uses: White and Black Hawāla

Initially, *hawāla* was exclusively employed for legitimate transactions, such as business. Due to its informality, anonymity, and lack of regulations, the system has become a new route for illicit and criminal objectives to conduct illegal trafficking, money laundering, and terrorist financing without leaving any detectable traces.

According to Interpol, it is critical to distinguish between *hawāla* transactions where "the source of the money is genuine (white *hawāla*) and those where the source and aim of the transactions are illegitimate (black *hawāla*)."[144]

The term "*white hawāla*" is evocative, referring to legal funds sent through *hawāla* methods.[145] This category comprises all transactions often linked with personal investments and expenditures, migrant worker remittances and humanitarian assistance aid. Considering its speed, efficiency, and minimal transportation costs, the *hawāla* system is commonly employed for investment and personal expenditures. People living in remote areas or with limited access to banking services might also use the *hawāla* system to transfer payments for other purposes.[146] The *hawāla* system often covers medical expenses for a family member living in areas with a limited or non-existent healthcare system and is used to pay for university fees or other legitimate demands.[147]

According to the International Organisation for Migration (IOM), between 2020 and 2021, there were approximately 281 million international immigrants worldwide, accounting

---

[142] *Id*.
[143] *Ivi*, p. 85.
[144] Patrick M. Jost and Harjit Singh Sandhu, *The Hawala Alternative Remittance System and its Role in Money Laundering*, (Lyon: Interpol General Secretariat, 2000), 12-13, https://www.assetsearchblog.com/wp-content/uploads/sites/197/2013/06/FinCEN-Hawala.pdf.
[145] *Ibid.*
[146] El Qorchi et al., *Informal Funds Transfer Systems: An Analysis of the Informal Hawala System*, *cit*., p. 61.
[147] *Ibid.*

for two-thirds of migrant workers.[148] By 2022, migrant workers reached 169 million, accounting for roughly 5% of the worldwide workforce.[149] These employees emigrate from their home nation to a foreign country in search of better career opportunities that will enable them to support their relatives abroad. Migrant workers join the global labour force and earn a living in host countries, with a portion of their earnings being transferred back to family in their home country.[150] *Hawāla* is unquestionably the cheapest, most accessible, and fastest transmitting remittances.

Remittances not only help migrant families but also strengthen local commerce and the country's economy. Humanitarian organisations working in war or post-conflict reconstruction areas where conventional financial institutions are limited or inaccessible rely heavily on the *hawāla* system.[151] The transfer of tangible currency is one of the most dangerous aspects of these trades. In this scenario, the *hawāla* system exchanges payments rapidly and reliably without physically moving the amount. International organisations use *hawāla* too since it has lower expenses and more affordable currency rates than typical formal banking methods.[152] These humanitarian organisations have limited resources and cash, which are insufficient to cover standard banking systems' exorbitant fees and transaction expenses.[153] The *hawāla* system's informal and decentralised structure allows for greater flexibility and agility in coping with complicated and uncertain situations.

On the other hand, "black *hawāla*" transactions entail unlawful activity or major crimes like smuggling, money laundering, and terrorist financing.[154] Indeed, early in the 1960s and 1970s, the *hawāla* network became an ideal conduit for smuggling and trading activities, notably in South Asia.[155] This was due to gold import limitations, which led smugglers to exploit the *hawāla* system to carry gold from locations such as the Gulf Cooperation Council (GCC) countries to South Asia.[156] To move the earnings back to the countries of origin and buy more gold, the traffickers and smugglers used people initially from South Asia but living in GCC countries to transfer the funds, thereby becoming hawaladars. For instance, in Dubai, "hawaladars would finance gold exports to their counterparts and clients in South Asia. The

[148] Marie McAuliffe and Anna Triandafyllidou, *World Migration Report 2022*, (Geneva: International Organization for Migration, eds., 2021), 10-25, https://publications.iom.int/books/world-migration-report-2022.
[149] *Ibid*.
[150] *Ibid*.
[151] El Qorchi et al*., Informal Funds Transfer Systems: An Analysis of the Informal Hawala System*, *cit*., p. 62-63.
[152] *Ibid*.
[153] *Ibid*.
[154] *Ivi*, p. 64.
[155] *Ivi*, p. 65-66.
[156] *Ibid*.

remitting workers received better rates because hawaladars charged higher fees from smugglers "who made substantial profits from the gold trade."[157]

Moreover, because of its confidentiality and absence of a paper trail, *hawāla* became an appealing source of financing for terrorists.[158] The focus on this informal value transfer method arose after law enforcement traced an anonymous cash transfer related to *Al-Qāʿida* operatives that were suspected to be involved in the 9/11 terrorist attacks.[159] The money is supposed to be sent from a Boston transfer facility to an *Al-Qāʿida* suspect in an exchange house in the U.A.E.[160] The lack of means to identify or examine the origin of the funding is of particular concern to authorities and international bodies. Indeed, the *hawāla* system conceals the source of payments via a considerable network of intermediaries in several jurisdictions.

Aside from being a mechanism used by terrorist groups to carry out attacks, the *hawāla* is a system that is very vulnerable to money laundering in all three stages, including placement, layering, and integration.[161] In the initial phase, hawaladars operate independently of the *hawāla* network. This is because if any suspicious bank deposits are made regularly; they can be explained as the source of those economic activities. Furthermore, because *hawāla* leaves little or no paper trail, it enables layering in the money laundering process.[162] Unlike traditional banking systems, which may leave traces, *hawāla* systems limit detectability because transactions are based on trust.[163]

Furthermore, hawaladars preserve certain records containing the entire details of transactions, although retrieving these is frequently challenging for authorities. *Hawāla* procedures are also subject to exploitation in the last stage of money laundering, integration.[164] At this point, the *hawāla* system helps transform the money and make its origin as authentic as possible.

### 3.2 Hawāla *a*s a Tool for Terror Financing

*Hawāla* is an ancient way of transferring money built on relationships with family, friends, and the community. Despite developing contemporary technologies and expanding traditional banking infrastructure, it keeps up its presence in many businesses. Both cultural and economic

[157] *Ibid*.
[158] Daudi, *op. cit*., p. 633.
[159] Michael Freeman, "The Sources of Terrorist Financing: Theory and Typology," Journal Studies in Conflict & Terrorism 34, no. 6 (2011): 461.
[160] *Ibid.*
[161] Jost and Sandhu, *op. cit*., p. 12-13.
[162] *Ibid*.
[163] *Ibid.*
[164] *Ibid.*

reasons support *hawala*'s undeniable attractiveness.[165] However, when people must choose a method of money transmission, the system's discretion, efficiency, and dependability frequently balance their power.

Although many people use *hawāla* for legal reasons, by nature of its very structure, it can also be used for illegal activity. The system can circumvent the more stringent regulatory authorities thanks to its capacity to function outside the regular banking environment. This has inevitably drawn the attention of numerous criminal organisations, which saw it as a way to transfer money anonymously.[166] Criminal organisations and terrorist groups have quite diverse financial tactics. Contrary to popular belief, these organisations do not slavishly follow a single fund transmission method. Depending on the circumstances and their particular difficulties, they may switch between formal channels, such as banks, and informal ones, such as *hawāla*.[167] Moreover, terrorists can still favour conventional financial institutions in areas with poor banking infrastructure.

However, the *hawāla* system's clandestine character ensures that it remains the preferred option to channel resources to locations with stringent oversight and laws.

### 3.2.1 Reasons for Terrorists' Preference for *Hawala*

Several factors influence people's decisions to choose *hawāla* instead of other transfer techniques. Mr. El Qorchi outlines *hawāla*'s main attributes: *speed, cost, cultural convenience, adaptability, and anonymity*.[168]

First of all, *hawāla* and other informal transfer mechanisms are preferred because they take only a short time, on average, between 6 and 12 hours, to transfer between people in large international cities.[169] The *speed* is dictated by the fact that there is no physical movement of currency between countries because the amount received by the recipient is settled locally. Additionally, in some circumstances, receivers get their funds quickly. In others, they can get them immediately at home by giving a password to the *hawāla* agent who referred them.[170] *Hawāla* transactions used to be conducted over the phone and relied solely upon human confidence, but today's hawaladars have access to technology tools like email and the

[165] Genesis J. Martis, "A Guidance to Understand Hawala and to Establish the Nexus with Terrorist Financing," *Association of Certifed Anti-money Laundering Specialists,* March 18, 2018, https://www.acams.org/en/media/document/9406.
[166] *Ibid*.
[167] M. Freeman and M. Ruehsen, *op. cit*., p. 5-11.
[168] El Qorchi et al*., Informal Funds Transfer Systems: An Analysis of the Informal Hawala System, cit*., p. 44-45.
[169] *Ibid*.
[170] Central Bank of Sri Lanka, Annual Report 2021, p. 163.

telephone.[171] It is important to note that any *hawāla* money transfer will take roughly 24 hours to complete in more remote areas or communities with limited communications.[172]

The transaction *cost*, which is less than the high fees of financial transfers through traditional banking channels, is another aspect that makes *hawāla* appealing to consumers.[173] *Hawāla* transfers can be carried out directly from the hawaladars' residences or from their businesses, such as travel agencies or phone stores, which have few or no operating costs related to the transaction.[174] The ultimate share in a transaction is not fixed because it is affected by the interaction of numerous circumstances, and it is believed that the cost of a *hawāla* transaction between large international centres ranges on average between 2% and 5%.[175] The transaction amount, the parties' financial condition, the exchange rate, the distribution of funds, their ability to negotiate a fair deal, and their familiarity with the *hawāla* system's market dynamics can all affect the actual cost.[176] Hawaladars are incentivised to offer competitive pricing to attract consumers because the *hawāla* industry is also quite competitive.

*Cultural convenience* is what makes *hawāla* unique.[177] It spread was made possible by the demand for community members or migrants abroad who, due to language barriers or a lack of educational resources, did not feel confident handling their bank accounts and sending money to their families abroad.[178] *Hawāla* does not have linguistic barriers; it has a system built on mutual trust that encourages privacy and confidentiality during a transfer.[179] Usually, the reference hawaladar handles the transaction in these circumstances and releases the funds to the recipient families, frequently outside the banking or postal organisations.

What is more, *hawāla*'s exceptional *adaptability*, which ensures its operation even in challenging situations like war, economic crises, or the absence of banking services, enables it to adapt to changes in different places and periods.[180] *Hawāla* is the most reliable and advantageous practical solution in dangerous nations with high levels of governmental instability, such as Iraq or Afghanistan, as it makes it possible to get around regulations and economic constraints that would otherwise make it challenging to go onward.[181] These nations are typically characterised by a local currency depreciating against other currencies, which

[171] El Qorchi et al*., Informal Funds Transfer Systems: An Analysis of the Informal Hawala System, cit*., 44-45.
[172] *Ibid*.
[173] Central Bank of Sri Lanka, *op. cit*., p. 163.
[174] M. El-Qorchi et al*., Informal Funds Transfer Systems: An Analysis of the Informal Hawala System, cit*., 45-46.
[175] *Ibid*.
[176] *Ibid*.
[177] *Ibid.*
[178] Central Bank of Sri Lanka, *op. cit*., p. 163-164.
[179] M. El Qorchi et al*., Informal Funds Transfer Systems: An Analysis of the Informal Hawala System, cit*., 45-46
[180] *Ibid*.
[181] *Ivi*, p. 48-49.

could cause the exchange rate to vary from the currency's actual market value. This can lead to a difference between the official exchange rate and what we refer to as "parallel," which can offer better terms and influence customers to select informal systems like *hawāla*.[182]

Another distinguishing feature of the *hawāla* system is *anonymity*.[183] The hawaladar, who maintains anonymity, personally records the details of the operation and there is no official documentation or record. There is no accounting standard or paperwork that all hawaladars must complete after a transaction; each hawaladar records transitions as it sees fit. Because it is uncommon for a hawaladar to request proof of identification from the recipient, this system enables users to remain utterly untraceable by the police. Any codes or messages are typically removed after the procedure to allay any potential suspicion.[184]

While *hawāla* has valid uses in helping underserved communities, the above characteristics can also be used for illegal purposes, including by terrorist organisations.[185] Remarkably, the *hawāla* system's speed allows transactions to be completed relatively quickly. This *speed* may be crucial for criminal organisations requiring money immediately without bureaucratic approval. Additionally, *hawāla* transactions are less expensive than those conducted through conventional banking channels. To preserve money that can be used to purchase weapons or carry out terrorist activities, terrorist organisations will find the cheapest solution. Because *hawāla* has its roots in local communities, some terrorist organisations from Asia and the Middle East consider it acceptable to employ.[186] *Hawāla* may be employed in challenging or changing environments, which are typically the bases of terrorist organisations, thanks to its *adaptability* and flexibility. The *anonymity* that *hawāla* ensures is what terrorist organisations are drawn to the most. It is very challenging for authorities to trace the flow of *hawāla* funds due to a lack of documentation and traceability. This enables terrorists to avoid having their money operations intercepted.

The best example of a country where multiple terrorist organisations use *hawāla* to transfer funds is Afghanistan, which has an antiquated and virtually nonexistent banking infrastructure. The Afghan drug industry accounts for almost 60% of all money transfers.[187] One of the largest terrorist organisations in the nation, the *Tālibān*, has successfully transferred money from the sale of drugs and opium using the unofficial *hawāla* system. The *Tālibān* earn around $150

[182] *Ibid*.
[183] *Ibid*.
[184] *Ibid*.
[185] *Ibid*
[186] *Ibid*.
[187] Doris Buddenberg and William A. Byrd (editors), *Afghani stan's Drug Industry: Structure, Functioning, Dynamics, and Implications for Counter-Narcotics Policy*, UNODC and the World Bank, 2006, p.161.

million a year from this trade, according to the United Nations Office on Drugs and Crime.[188] Moreover, before the 9/11 attacks, *hawāla* relocated the *Al-Qāʿida* headquarters within the Afghan environment.[189] Following the bombings in East Africa in August 1998, which increased global scrutiny of established financial systems, the *hawāla* system's significance increased dramatically. Bin Ladin effectively transferred money through a *hawāla* network that is well-established and active in Pakistan, Dubai, and the rest of the Middle East.[190] *Al-Qāʿida* found the *hawāla* system to be incredibly alluring since, in contrast to regular banking institutions, it was not subject to prospective governmental regulations and did not maintain extensive records in a standardised form. *Hawāla* operators kept records, which were frequently written in their shorthand and only preserved for a short time. The terror organisation relied on a dozen reliable hawaladars who almost definitely knew where the money came from and what it was used for.[191] *Al-Qāʿida* also employed hawaladars who were uninformed of their activities and others who were prepared to cooperate despite being suspected of dealing with *Al-Qāʿida*.

### 3.3 The Legalisation of Hawāla: Divergent Opinions and Future Trends

The legalisation of *hawāla* is still a contentious issue in several countries. In moving funds across borders, two categories of countries are identified: receiving and sending remittance countries.[192] The former is the starting point of cross-border transactions, while the latter is the transaction's destination and, consequently, the recipient's homeland. Understanding the role of remitting and receiving countries is critical to a precise awareness of the cultural and economic dimensions and, most crucially, governments' policies towards the informal *hawāla* system.[193]

Examining a remittances' geographical distribution is crucial in order to analyse the costs related to them thoroughly. This research is important due to the wide disparity in costs among different geographic regions and the fact that economies of scale cause the volume of remittances to significantly affect costs. Additionally, it stands to reason that more remittance operators will choose to operate on routes with bigger remittance volumes because they are more competitive.

---

[188] *Ibid*.
[189] John Roth, Douglas Greenburg and Serena Wille, *Monograph on Terrorist Financing*, (National Commission on Terrorist Attacks Upon the United States, 2004), 25, https://govinfo.library.unt.edu/911/staff_statements/911_TerrFin_Monograph.pdf.
[190] Ibid.
[191] *Ibid*.
[192] *Ivi*, p. 106-107.
[193] *Ibid.*

**Figure 10** illustrates the top ten remittance-sending and receiving countries. On the left-hand side of the figure, is the top ten remittance-sending countries' bar graph, and on the right side is the top ten remittance-receiving countries' bar graph.

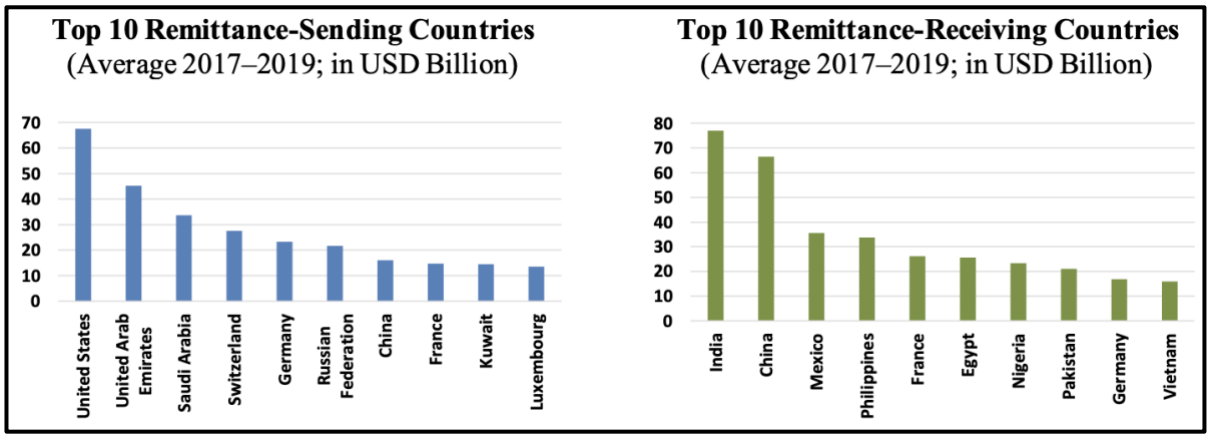



**Figure 10**. Global remittance leaders: Ten top sending and receiving countries; Source: KNOMAD (2019).

According to the Global Knowledge Partnership on Migration and Development (KNOMAD)[194], the top ten receiving countries account for over 50% of remittances, and the top ten sending countries account for almost 60% of all worldwide remittances.[195] The USA was and remains the top sender of remittances among the top ten countries, while India and China are the top receivers. Germany, instead, is in a fascinating situation because each nation plays multiple roles, serving as both senders and recipients of sizable flows.[196] Germany naturally has high outgoing remittances due to its strong economy and a large community of international workers. Nevertheless, the country receives much foreign aid due to the generations of immigrants living there. This occurrence highlights the complex remittance patterns of two of Europe's largest economies.

Historically, *hawāla*-receiving countries had no countermeasures to regulate or counteract the informal *hawāla* system.[197] Due to the rising use of *hawāla* by criminal groups, terrorists, and money launderers, receiving nations have decided to implement regulations prohibiting the *hawāla* system and, more broadly, any IVTS whilst favouring transparency and financial inclusion measures.

[194] KNOMAD is a global initiative created by the World Bank to assist governments, civil society, international organisations, and other stakeholders maximise the interaction between migration and development.
[195] Tito Nicias Teixeira da Silva Filho, "IMF Working Paper: No Easy Solution A Smorgasbord of Factors Drive Remittance Costs," *International Monetary Fund* 21, 199 (July 2021): 8-9, https://doi.org/10.5089/9781513592954.001.A000.
[196] *Ibid*.
[197] *Ibid.*

One receiving country, India, has decided to ban the informal *hawāla* transaction.[198] Initially, India did not implement any restrictions on *hawāla* transactions, but this type of IVTS was later declared unlawful, threatening the country's ongoing criminal activities. To address the issue, the Indian government has implemented various policies to combat *hawāla* and its associated risks. These measures include increased monitoring and data collection, stricter sanctions against currency fraud, and collaboration with international agencies to monitor cross-border transactions. In 1973, India adopted the Foreign Exchange Regulation Act (FERA) to implement restrictions governing the flow of foreign capital into the country's economy.[199] The eighth and ninth articles establish the limitations of the *hawāla* system. For example, Article Eight prohibited the conversion of foreign money and the transmission of funds through unauthorised channels.[200] Article nine granted the government the authority to establish controls on foreign exchange transactions, including the power to authorise, restrict, or ban such transactions.[201] Following India's liberation in those years, there were various terrorist attacks financed through *hawāla*, such as the 1993 Mumbai serial blasts carried out by the Dawood Ibrahim crime gang.[202] The FERA's constant modifications in 1999 prompted the Indian government to resolve to replace and integrate the FERA with the Financial Exchange Management Act (FEMA).[203] This act continued prohibiting *hawāla* style transactions and included new rules to govern foreign exchange and foreign exchange issues in the country.
Therefore, India was always committed to opposing any form of *hawāla*, such as when it established the Financial Intelligence Unit (FIU) in 2004 to combat money laundering. The FIU is in charge of receiving, processing, analysing, and disseminating financial information relating to suspicious transactions, which might aid in identifying suspected money laundering activities.

India sought to improve its formal financial system by lowering remittance fees and providing better service. The *United Nations Sustainable Development Goals*, adopted in September 2015, put this problem to the forefront for the first time by agreeing to lower transaction costs of migrant remittances to less than 3% and eliminating remittance corridors with costs greater than 5%.[204] As a result, customers would be more inclined to use the regular

[198] *Ivi*, p. 108-109.
[199] Foreign Exchange Regulation Act, § 46 (1973).
[200] Foreign Exchange Regulation Ac, art. 8.
[201] Foreign Exchange Regulation Ac, art. 9.
[202] John F. Burns, " Riot Scars Are Gone, but Bombay Is Still Healing," *New York Times*, April 17, 1994, https://www.nytimes.com/1994/04/17/world/riot-scars-are-gone-but-bombay-is-still-healing.html.
[203] Foreign Exchange Management Act, § 42 (1999).
[204] The United Nations approved the Sustainable Development Goals (SDGs) in 2015 as a worldwide call to action to end poverty, safeguard the planet, and ensure that by 2030, all people will enjoy peace and prosperity. See https://www.undp.org/sustainable-development-goals.

financial system rather than *hawāla*. The Indian government has also recently implemented several measures to regulate *hawāla* transactions better. For example, the Black Money (Undisclosed Foreign Income and Assets) and Imposition of Tax Act of 2015 seek to combat the issue of black money and build a more transparent economy.[205] The Black Money Act focuses on undeclared abroad income and assets, including houses, financial accounts, and other non-declared assets outside of India.[206] On October 8, 2016, the government declared a restriction on using 500 and 1000 rupee notes, the national currency, lowering cash settlement and, as a result, the ability to move dirty money through *hawāla*.[207]

Like India, Pakistan is also dedicated to combating the exploitation of the *hawāla* system.[208] To combat the country's endemic money laundering and corruption, the Foreign Exchange Regulation Act (FERA) was enacted in 1947, making all informal transfer mechanisms illegal, including *hawāla*.[209] Besides that, Pakistan has two key financial regulators the State Bank of Pakistan (SBP) and the Securities and Exchange Commission of Pakistan (SECP).[210] In 2002, these two institutions established an Anti-Money Laundering (AML) section to boost financial sector supervision. Pakistan also fights against IVTS to combat terrorist financing. As a result, in 2004, Pakistan modified the Anti-Terrorism Act (ATA) of 1997to give law enforcement authorities additional powers to combat terrorist financing and money laundering under FATF Special Recommendation VI, which suggests the need for hawaladar licences. [211] The State Bank of Pakistan required all hawaladars to register as licenced foreign exchange dealers and set minimum capital requirements in June 2004.[212] The SBP programme established exchange companies and an integrated system for delivering domestic remittances. This mechanism gives law enforcement agencies the ability to control and govern it. As a result, genuine remittances from Pakistanis residing abroad, formerly sent through the *hawāla* system before 2001, now mostly flow through the formal banking sector.

---

[205] Black Money (Undisclosed Foreign Income and Assets) and Imposition of Tax Act, § 22 (2015).
[206] *Ibid*.
[207] Vidhi Doshi, "India Withdraws 500 and 1000 Rupee Notes in Effort to Fight Corruption," *The Guardian*, November 8 2016, https://www.theguardian.com/world/2016/nov/08/india-withdraws-500-1000-rupee-notes-fight-corruption.
[208] El Qorchi et al*., Informal Funds Transfer Systems: An Analysis of the Informal Hawala System, cit.,* p. 109-110.
[209] Foreign Exchange Regulation Act, § 7 (1947).
[210] The United Nations approved the Sustainable Development Goals (SDGs) in 2015 as a worldwide call to action to end poverty, safeguard the planet, and ensure that by 2030, all people will enjoy peace and prosperity. See https://www.undp.org/sustainable-development-goals; The Exchange Commission of Pakistan was established under The Securities and Exchange Commission Pakistan Act, § 42 (1997).
[211] The Anti-Terrorism Act, § 27 (1997); See FATF Special Recommendations IX, sec. 6, October 2001, https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Ixspecialrecommendations.html.
[212] Muhammad Subtain Raza, Muhammad Fayyaz and Haseeb Ijaz, "The Hawala System in Pakistan: A Catalyst for Money Laundering & Terrorist Financing," *Forensic Research and Criminology International Journal* 5 no.4 (2017): 368-369, 10.15406/frcij.2017.05.00167.

One of Pakistan's most notable achievements in countering terrorist financing and other unlawful activities is the National Action Plan (NAP) of January 2015.[213] Following the 16 December 2014 attack on the Army Public School in Peshawar by the Pakistani terrorist group *Tehrik-i-Taliban Pakistan*, this strategy was enacted.[214] The NAP established the National Apex Committee to organise and coordinate all required responses to the battle against terrorism.[215] The central strategy of the PAN was to freeze and block the terrorists' financial assets. Although the NAP has been implemented successfully, the Pakistani government still requires time and resources to address financing terrorism and money laundering effectively.[216]

On the other hand, the *hawāla -remitting* countries have more permissive foreign currency regulations and more sophisticated financial systems, which may indicate opportunities for illegal activity. Therefore, the remitting nations implement measures to restrict such actions. For instance, Germany's involvement in AML dates back to 1993, when the first anti-money laundering act, the *Geldwäschegesetz* (GwG), was passed under section 261 of the German Criminal Code (*Strafgesetzbuch - StGB)*.[217] According to this law, financial institutions and other businesses covered by the GwG Act must identify the actual beneficiaries of their customers and look into money laundering to confirm the identity of their clients.[218] These institutions are required to notify the authorities of any questionable transactions. Later, updates were made in 2017 to implement the most recent EU AML directives, then again in 2018 and 2020.[219] The Bundesanstalt für Finanzdienstleistungsaufsicht, also known as the Federal Financial Services Authority (BaFin) have regulated these financial institutions since May 1, 2002 and can prosecute them under Section 54 of the German Banking Act (Kreditwesengesetz – KWG).[220] The BaFin is a federally independent organisation in Germany that reports to the Federal Ministry of Finance and is involved in implementing German

[213] The National Counter Terrorism Authority, Ministry of Interior together with the Parliament approved the National Action Plan on December 24, 2014, to counter terrorism, https://nacta.gov.pk/nap-2014/.
[214] Shamaimaa Khalil, "Pakistan Taliban: Peshawar School Attack Leaves 141 Dead," *BBC News,* December 16, 2014, https://www.bbc.com/news/world-asia-30491435.
[215] National Action Plan, *cit*.
[216] MS Raza et al., *op. cit*., p. 340.
[217] GwG (1993) https://www.bafin.de/SharedDocs/Downloads/EN/Aufsichtsrecht/dl_gwg_en.pdf?__blob=publicationFile&v=1; StGB (1998) https://www.iuscomp.org/gla/statutes/StGB.htm#86a.
[218] FATF (2022), Anti-money laundering and counter-terrorist financing measures –Germany, Fourth Round Mutual Evaluation Report, FATF, Paris, 26, https://www.fatf-gafi.org/content/dam/fatf-gafi/mer/Mutual-Evaluation-Report-Germany-2022.pdf.coredownload.inline.pdf.
[219] Directive (EU) 2015/849 of the European Parliament and of the Council of May 20, 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC—Official Journal of the European Union (L 141/73).
[220] BaFin checklist "Authorisation as a credit institution" of 20.08.2017, amended on 14.11.2017, available at: https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/2017/rs_1709_marisk_ba.html; KWG § 54 (1998).

AML/CFT rules and financial institution monitoring.[221] As a result, Germany is highly cautious in its fight against the *hawāla* system, as transferring money for business without a permit from the Federal Office of Banking Supervision is prohibited. In recent years, attempts have been made to establish official forms of *hawala*, but these efforts have yet to progress as there is no specific authority for the use of *hawāla* as a sole agent. One of these forms is Kaah Express, which has branches in Düsseldorf, Cologne, Munich, Stuttgart, and Frankfurt and reinvests its profits and differences in the traditional financial system.[222] Except for a few attempts, Germany remains committed to preserving banking stability outside of the *hawāla* system, which protects the integrity and safety of its system.

The U.A.E is among the main remittance countries too. The nation was constantly fighting *hawāla* traders and non-bank money transfer companies. The U.A.E has since chosen to ratify many anti-money laundering resolutions since the 1980s. The regulation of money exchange activities in the U.A.E is covered by the 1980 Banking Law and further resolutions, such as Resolutions No. 31/2/1986 and No. 123/7/92. [223] These rules allowed money changers to legally obtain money transfer operator licences. To register U.A.E. hawaladars, the U.A.E. Central Bank (CBUAE) started issuing certificates in 2002 and ensuring their data was secure at the bank.[224] All customer information must be provided by hawaladars, who must report any unusual transfers. The supervisory authorities must "provide financial institutions with guidelines and feedback to improve the effectiveness of the implementation of law enforcement measures" according to Council of Ministers Decision No. 10 of 2019 on the Regulation implementing Decree-Law No. 20 of 2018 on the fight against money laundering and financing terrorism and illegal organisations.[225] As a result, the CBUAE now approves lawful *hawāla* transactions and governs them by the Registered *Hawāla* Providers Regulation Circular No. 24/2019, which issues a legal *hawāla* provider certificate to every *hawāla* provider.[226] To obtain the certificate:

> "Applicants must apply to the CBUAE for registration. They must be non-U.A.E nationals, officially residing in the U.A.E, and legally competent. The CBUAE will then notify the

[221] Fabian Teichmann and Chiara Wittmann, "The Abuse of Hawala Banking for Terrorist Financing in German-speaking Countries," *Journal of Money Laundering Control* Vol. ahead-of-print No. ahead-of-print, 10.1108/JMLC-01-2022-0013.
[222] *Ivi*, p. 7.
[223] Federal Law No. 10 (1980) concerning the Central Bank, monetary system, and organisation of banking; Resolution No. 31/2/1986 regarding the regulation of money changing business in the U.A.E.; Resolution No. 123/7/92 regarding the regulation of the money changing business in the U.A.E.
[224] El Qorchi et al*., Informal Funds Transfer Systems: An Analysis of the Informal Hawala System,* cit., p. 120-123.
[225] Federal Decretal-Law No. 20 (2018) on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations.
[226] CBUAE, *Registered Hawala Providers Regulation*, Circular No. 24/2019.

application whether the application was approved or rejected, with reasons for the decision. The *hawāla* providers must apply to renew their Certificate no less than two months before the current Certificates expires. *Hawāla* providers must add *hawāla* activity to their trade license, install required security systems, and register with CBUAE. They must open an account with a U.A.E bank."[227]

There may still be instances of money laundering or terrorist financing despite efforts to control the *hawāla* system. In November 2020, Sheikh Mansour bin Zayed, the Deputy Prime Minister, the Minister of Presidential Affairs, and the Abu Dhabi Judicial Department Chairman, decided to establish a court to combat money laundering and tax evasion.[228] At the same time, Abdulla bin Touq, the Minister of Economy, decided to create a specific department for the AML.[229] U.A.E confirmed in 2021 that its laws against money laundering and supporting terrorism were effective by seizing approximately 634.4 million dollars.[230] According to the legal and regulatory framework in the U.A.E, people who are found guilty of money laundering may face fines between AED 100.000 and AED 5.000.000 and a prison sentence of up to ten years.[231] In addition, anyone found guilty of a crime that poses a risk of financing terrorism faces a mandatory minimum sentence of ten years in jail or life.[232]

The legal frameworks of the nations mentioned above do not suggest that only those nations or nations not mentioned have the similar laws. Each receiving and sending country may have common goals in the fight against terrorism or money laundering, but each also has its own strategy for doing this. For instance, Afghanistan is a unique case of receiving- *hawāla* country where the self-regulation of the *hawāla* has been used in an unprecedented manner. Before the *Tālibān* took control of Afghanistan in August 2021, registered hawaladar operators operated under a framework that allowed them to self-regulate.[233] An eight-person Executive Committee oversaw the system's operations.[234] The number of unregistered operators still remained still substantial despite efforts to control them. Furthermore, the Afghan banking system is now crumbling, making it crucial for Afghan migrants to use *hawāla* transactions to send money to their families still residing in Afghanistan. One of the factors contributing to this

[227] CBUAE, *OUTREACH EVENT on the AML/CFT Guidance for Registered Hawala Providers*, 26 August 2021.
[228] "Abu Dhabi establishes dedicated court to tackle money laundering and tax evasion," *The National UAE*, November 10, 2020, https://www.thenationalnews.com/uae/courts/abu-dhabi-establishes-dedicated-court-to-tackle-money-laundering-and-tax-evasion-1.1109308.
[229] *Ibid.*
[230] CBUAE, *OUTREACH EVENT on the AML/CFT Guidance for Registered Hawala Providers, cit.*
[231] *Ibid*.
[232] *Ibid*.
[233] El Qorchi et al*., Informal Funds Transfer Systems: An Analysis of the Informal Hawala System,* cit., p. 112-113.
[234] *Ibid*.

nation's struggles in building a robust formal banking system is the continuous usage of *hawāla* and the accompanying lack of regulation.[235] In 2018, according to the WB, only one in six Afghans had a bank account, and "upwards of $788 million in formal remittances were sent to Afghanistan in 2020, about 4% of Afghanistan's overall GDP." [236] One of the claims made by the new *Tālibān* administration was that the previous administration's attitude to the *hawāla* system would be maintained.[237] Interestingly, the *Tālibān*'s fight to control the *hawāla* system extends to limiting the flow of drug-related funds which they have historically benefited from. The *Tālibān* appear keen to earn credibility and universal acclaim. They help on two levels, with their decision to control the *hawāla* system. Firstly, the *Tālibān* can collect a substantial sum of money, which is necessary to fund their operations, by increasing the registration of money and monetary exchange services, according to the first argument. Their decision to take this action aligns with their requirement for financial resources to maintain their government and ongoing operations.[238] The second justification has to do with their recognition on a global scale. The *hawāla* regulation could be viewed as an effort to show their willingness to follow international laws against money laundering and supporting terrorism. Gaining the confidence and acceptance of other nations and international institutions may be facilitated by this action.[239] Despite this, the *Tālibān*'s regulation of *hawāla* is probably not going to be properly adhered to, whatever their stated intentions.

*Hawāla* regulation laws are multiple and intricate to increase the financial system's transparency. While some nations, like India and Pakistan, have enacted stringent legislation to combat the misuse of the *hawāla* system by criminal and terrorist organisations, other countries have attempted to include this money transfer method into the established banking system to encourage financial inclusiveness. For instance, Germany has focused on ways to track money laundering and identify the actual beneficiaries of *hawāla* transactions. Furthermore, following the COVID-19 pandemic, in 2019, the use of remittances increased considerably. The number of remittances sent to low and middle-income countries increased by 8% in 2022, totaling $647

[235] Qayoom Suroush, "Gray Cash: How the U.S. and the Taliban Have Tried and Failed to Fix Afghanistan's Informal Banking System," *New America*, September 14, 2022, https://www.newamerica.org/future-frontlines/briefs/gray-cash-how-the-us-and-the-taliban-have-tried-and-failed-to-fix-afghanistans-informal-banking-system/.
[236] World Bank Report, *International Development Association Project Appraisal Document on a Proposed Grant in the amount of US$40 Million Equivalent to the Islamic Republic of Afghanistan for a Modernising Afghan State Owned Banks Project*, No: PAD2481, March 6, 2018, https://documents1.worldbank.org/curated/en/644081522461645615/pdf/Afghanistan-Afghan-State-Owned-Banks-PAD-PAD2481-03142018.pdf; IOM, *Remittances to Afghanistan are Lifelines: They are Needed More than Ever in a Time of Crisis*, United Nations (2020) https://weblog.iom.int/remittances-afghanistan-are-lifelines-they-are-needed-more-ever-time-crisis.
[237] *Ibid*.
[238] *Ibid*.
[239] *Ibid*.

billion.[240] Despite the consistent increase in remittances, the WB forecasted a modest decline for the year 2023 with moderate growth of 1.4% and "on a global scale, the remittances growth rate is projected to increase to 2.0% in 2024, increasing inflows by $18 billion."[241]

The approaches adopted by sending and receiving countries so far are not final; they are constantly changing to consider how the global financial system and security are developing.

[240] Dilip Ratha, Sonia Plaza, Eung Ju Kim, Vandana Chandra, Nyasha Kurasha, and Baran Pradhan (June 2023), Migration and Development Brief 38: Remittances Remain Resilient But Are Slowing, KNOMAD - World Bank, Washington, DC. https://knomad.org/sites/default/files/publication-doc/migration_development_brief_38_june_2023_0.pdf.
[241] *Ivi*, p. 1.

# CHAPTER IV.

# CRYPTOCURRENCIES AND MONEY LAUNDERING

## 4.1 Introduction to Cryptocurrencies

Blockchains, the most well-known of which is Bitcoin, have grown in popularity over the past ten years. These structures serve as a decentralised database where data is kept in blocks connected using sophisticated cryptographic methods. Without the need to re-enter the following blocks in the chain, the data becomes resistant to changes after it has been input. Blockchains increase their resilience to possible assaults by removing sources of weakness due to their distributed nature across several computer nodes.[242]

People's perceptions of security and trust in transaction and data have changed as a result of blockchain technology. This is already apparent in the development of bitcoins, which, as stated in their specifications, have "social scalability" as their key feature rather than computing performance.[243] According to Szabo, the term "refers to the ability of a technology or institution to expand and function effectively with the entry of increasing numbers of participants, overcoming the cognitive and behavioural limitations of humans."[244] As a result, traditional security, which depends on finite individuals and organisations, is replaced with automated and computationally expensive security, reducing vulnerability to harmful action by participants and other parties. The trust between several parties ensures the reliability of blockchains. Decentralisation provides more security, particularly regarding priceless resources like money.[245]

Blockchain technology has been used in various industries, including the financial sector and the arts, to assure authentication by supporting the widely discussed and wide field of cryptocurrencies. In light of this, cryptocurrencies undoubtedly improve global technology and the financial scene. Although they provide privacy and interference-resistance benefits, they could also be abused for money laundering and assisting criminal organisations.[246]

---

[242] Financial Action Task Force, *Virtual Currencies – Key Definitions and Potential AML/CFT RISKS,* Paris: FATF/OECD, 2014, https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf.coredownload.pdf.

[243] Erik H.B. Feyen, Yusaku Kawashima and Raunak Mittal, "Crypto-Assets Activity Around the World: Evolution and Macro-Financial Drivers," *World Bank Policy Research Working Paper 9962*, March 2022, https://doi.org/10.1596/1813-9450-9962.

[244] Nick Szabo, "Money, Blockchains, and social scalability," *Unenumerated*, 2021, https://doi.org/10.1596/1813-9450-9962.

[245] *Ibid*.

[246] FATF, *Virtual Currencies – Key Definitions and Potential AML/CFT Risks, cit.,* p. 9-10.

### 4.1.1 The Digital Gold Rush: Tracing the Path of Cryptocurrencies

Recent conversations concerning the digital financial sector have focused heavily on concepts like "blockchain," "virtual currency," and "cryptocurrency." However, there is a propensity to mix up these terms or to view them as interchangeable, leading to misunderstandings. The FATF has seen fit to explain and detail the subtleties and specificities of each of these ideas to address such ambiguities. The FATF has decided it is essential to define and describe the intricacies and particulars of each of these concepts to address such misconceptions. Virtual currency is the first term to be analysed, and it is "a digital representation[247] as a medium of value that can be digitally traded and functions as a medium of exchange, and/or a unit of account; and/or a store of value but does not have legal tender status 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."[248] Since no government agency provides a guarantee, such currencies' value is volatile and influenced by market forces like supply and demand. Virtual currencies are distinct fiat currencies, also known as real or national currencies, the electronic representation of conventional cash (such as the dollar or the euro).[249] Moreover, virtual currency "is distinct from e-money, a digital representation of fiat currency used to transfer value denominated in fiat currency electronically. E-money is a digital transfer mechanism for fiat currency."[250] Paypal or Satispay are just a couple of examples.

Virtual currencies can be divided into two groups: convertible and non-convertible. A convertible virtual currency, like Bitcoin, "has an equivalent value in real currency and can be exchanged back-and-forth for real currency."[251] A virtual currency is therefore convertible if there are private actors eager to trade it for other currencies, some of which may be fiat currencies. However, the virtual currency cannot be regarded as convertible if no one is eager to participate in the trade. Non-convertible virtual currencies are exclusive to a specific domain or virtual environment, like Amazon.com. Unlike convertible virtual currencies, they cannot be converted into fiat currency and are subject to the restrictions governing their use.

---

[247] This definition differs from that offered in 2012 by the European Central Bank (ECB), which defined virtual currency "as a type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community" ECB, *Virtual Currency Schemes* (October 2012), p. 6. The ECB recognised on p.13 of its report that its "definition may need to be adapted in future if fundamental characteristics change." Its definition now appears too limited, since math-based, decentralised virtual currencies like Bitcoin are not issued and controlled by a central developer, and some jurisdictions (e.g., the United States, Sweden, and Thailand) now regulate virtual currencies.
[248] Financial Action Task Force, *Virtual Currencies – Key Definitions and Potential AML/CFT Risks, cit.,* p. 4.
[249] *Ibid*.
[250] *Ivi*, p. 5.
[251] *Ivi*, p. 4.

The FATF's analysis is detailed and distinguishes between two subcategories of convertible virtual currencies: centralised and decentralised.[252] The operator, a single administrative authority, controls centralised virtual currencies. They are responsible for issuing the money, outlining its usage guidelines, operating a centralised payment system, and, most importantly, have the power to remove it from circulation. The market may impact the exchange rate for a convertible virtual currency, or the controlling body may set the rate based on a predetermined value, such as a traditional currency or other valuable assets, like gold. The majority of virtual currency transactions currently take place with centralised virtual currencies. Gold for World of Warcraft is one illustration.[253] On the other hand, decentralised virtual currencies, better known as cryptocurrencies, are based on open-source platforms that utilise peer-to-peer technology without an administration or regulating authority.[254]

Cryptocurrencies can be described as decentralised digital money protected by cryptographic methods and built on mathematical foundations.[255] The first operational example of such a currency, BTC, set the path for others.[256] These digital assets work in a distributed system, which is how they differ from traditional currencies. Public and private cryptographic keys in this system guarantee the security of ownership and the accuracy of transactions.[257] A cryptographic seal confirms the legitimacy of a transaction once it has been completed. The blockchain, the primary ledger in this system, owes its reliability to a group known as "miners" in the context of BTC.[258] To solve challenging mathematical problems and confirm and record transactions on the blockchain, miners use specialised hardware. This process is essential for maintaining the reliability and security of transactions across Bitcoin and its cryptocurrency competitors. Miners receive newly created BTC, known as the "block reward," as payment for their computing efforts.[259] They can also earn profit via transaction fees, an optional premium consumers pay to have their transactions processed faster within the network.

The history of cryptocurrencies dates back to October 31, 2008, when a paper entitled "Bitcoin: A Peer-to-Peer Electronic Cash System,"[260] written under the pseudonym Satoshi Nakamoto, became known as the "Bitcoin White Paper". This paper outlines the operation of

---

[252] *Ivi*, p. 5.
[253] *Ibid*.
[254] *Ibid*.
[255] *Ibid*.
[256] Zac Zimmer, "Bitcoin and Potosí Silver: Historical Perspectives on Cryptocurrency," *Technology and Culture* 58, 2 (2017): 310-312, http://www.jstor.org/stable/26406179.
[257] Financial Action Task Force, *Virtual Currencies – Key Definitions and Potential AML/CFT Risks, cit.,* p. 9-10
[258] *Ibid*.
[259] *Ibid*.
[260] Satoshi Nakamoto, *Bitcoin A Peer-to-Peer Electronic Cash System*, October 31, 2008, https://www.ussc.gov/sites/default/files/pdf/training/annual-national-training-seminar/2018/Emerging_Tech_Bitcoin_Crypto.pdf.

the blockchain network utilised by BTC. This novel digital currency kept track of transactions using a decentralised network of nodes known as the blockchain. The Genesis Block, or the initial blockchain block of Bitcoin, was created by Nakamoto on January 3, 2009. Nakamoto placed a symbolic message in the first block that referred to the headline of an article published the same day in *The Times* newspaper with the heading "Chancellor Alistair Darling on Brink of Second Bailout for Banks."[261] The message emphasised the need for reform while criticising the old banking system's volatility. The blockchain got a reward each time a new block was added. Fifty bitcoins were given to Nakamoto for creating the Genesis Block. This was done to demonstrate that individuals who broke a block were paid in bitcoins and also to entice users to invest IT resources in the upkeep and security of the network.

Nakamoto undoubtedly contributed to the success of BTC, although there had also been some earlier concepts for cryptocurrencies in the 1980s. In 1983, the American cryptographer David Chaum published a paper titled "Blind Signature for Untraceable Payments", explaining an early version of anonymous cryptocurrency.[262] Chaum's concept was centred on a currency that could be transferred without leaving a trail and without requiring centralised organisations like banks. In 1995, Chaum created a prototype cryptocurrency called Digicash.[263] It required using particular software to enable money withdrawals from banks and the use of encrypted keys before delivering money to the destination. But three years later, Chaum declared Digicash failed because of problems with interaction and collaboration with financial institutions. In 1998, the computer scientist Nick Szabo subsequently created BitGold, a global payment system that required a participant to carry out computational labour and solve cryptographic puzzles as proof of work done in exchange for receiving a specific amount of the cryptocurrency.[264] Szabo's BitGold is frequently seen as Bitcoin's immediate precursor. However, BitGold, failed to become a complete cryptocurrency due to the problem of "double spending."[265] This issue stemmed from the simplicity with which digital data could be copied and the possibility of different uses of the same digital currency. BitGold could not develop if there were no central body to control this duplication's problem.[266]

---

[261] Francis Elliot and Gary Duncan, "Chancellor Alistair Darling on Brink of Second Bailout for Banks," *The Times*, January 3, 2009, https://www.thetimes.co.uk/article/chancellor-alistair-darling-on-brink-of-second-bailout-for-banks-n9l382mn62h.
[262] David Chaum, "Blind Signature for Untraceable Payments," In: Chaum, D., Rivest R.L. and Sherman, A.T., Eds., Advances in Cryptology Proceedings of Crypto 82, Plenum (Springer-Verlag), New York, 199-203, https://sceweb.sce.uhcl.edu/yang/teaching/csci5234WebSecurityFall2011/Chaum-blind-signatures.PDF.
[263] David S. Kerr et al., "Cryptocurrency Risks, Fraud Cases, and Financial Performance," *Risks* 11, no. 51 (February 23, 2023): 2, https://doi.org/10.3390/risks11030051.
[264] Nick Szabo, "Bit Gold," *Unenumerated*, December 27, 2008, http://unenumerated.blogspot.com/2005/12/bit-gold.html.
[265] Gheorghe Matei, "Blockchain Tecnology – Support for Collaborative Systems," *Informatica Economica* 24, no. 2 (2020): 15-16, http://dx.doi.org/10.24818/issn14531305/24.2.2020.02.
[266] *Ibid*.

In comparison to Digicash and BitGold, BTC marked a significant breakthrough since it was introduced in 2009. This cryptocurrency altered the financial international setting and also how people perceived cryptocurrencies highlighting their multiple applications. Besides that, Bitcoin's price history has not been straightforward. **Figure 11** below illustrates BTC's price history from 2009 until 2023. In 2009, "the Bitcoin price was barely above zero."[267]


**Figure 11**. Bitcoin valuation over the years; Source: Social Finance Inc. (2023).

Only in 2011, BTC's value approached parity with the US dollar, with a value of $1, despite being almost worthless in the years immediately following its introduction. On one of the biggest cryptocurrency exchange sites, Mt. Gox, the value subsequently increased to $10 and then to $30.[268] This price rise was 100 times greater than the original value of 30 cents. However, towards the end of 2011, the price of BTC fell below $5, perhaps due to the introduction of alternative cryptocurrencies such as Litecoin, created by the engineer Charlie Lee.[269] The incentive for each new block contributed to the blockchain was reduced by half in the succeeding year, from 50 to 25 BTC by 2012.[270] The process Nakamoto invented to cut the issuance of new coins over time is better referred to as a "halving" mechanism.[271] Nakamoto created a system that generates a form of programmed deflation to prevent inflation as much as possible. Rather than raising the money supply, this process reduces the production of new

[267] Brian Nibley, "Bitcoin Price History: 2009 – 2023," *Social Finance Inc.*, March 1, 2023, https://www.sofi.com/learn/content/bitcoin-price-history/.
[268] *Ibid.*
[269] *Ibid.*
[270] *Ibid.*
[271] Nakamoto, *op. cit.*

BTC.[272] The fact that there are fewer BTC than traditional currencies, which do not have a cap placed on their supply by financial institutions, is one of its most intriguing qualities since it enables long-term preservation or, in some instances, growth of the BTC's purchasing power by users. The price of BTC increased by approximately 6.600% in 2013 thanks mainly to the adoption of this cryptocurrency by the non-profit organisation Electronic Frontier Foundation, which campaigns for digital rights like online privacy and freedom of expression.[273] However, 2013 also had a significant amount of volatility, with the underlying cryptocurrency initially moving through a range of highs and lows before eventually peaking at about $1.100 near the end of the year. Moreover, the first Bitcoin ATM in the world was developed in Vancouver, Canada, enabling users to convert fiat currency into cryptocurrency. The price of BTC has been relatively stable since 2016, fluctuating between $200 and $400. Furthermore 2016, the second halving occurred from 25 to 12.5 BTC.[274] Following the second halving, the price reached around $20.000 in December 2017. As the line graph above reports, the popularity of BTC and other cryptocurrencies has increased that year. Like every novelty, cryptocurrencies were the focus of several newspaper articles. However, other people believed cryptocurrencies were nothing more than a hoax and should be avoided in favour of future investments. Generally speaking, cryptocurrency experienced a drop in the years before the Covid-19 epidemic. As an illustration, BTC had a 39% decline in value in a single day in March 2020.[275] Being forced to stay at home due to the pandemic has also had beneficial effects, with Bitcoin reaching $68,500 in November 2021 due to increased interest in the cryptocurrency trend. Due to growing financial system uncertainty, undoubtedly made worse by the start of the war between Russia and Ukraine, 2022 was an awful year for cryptocurrencies. With a value of roughly $23,300 in 2023, BTC and other cryptocurrencies started to show signs of revival.[276]

Since the launch of BTC, a growing number of cryptocurrencies have entered the dynamic digital universe. According to the renowned *Forbes* magazine, as of March 15, 2023, there were about 22,932 cryptocurrencies in use.[277] Nonetheless, many cryptocurrencies are no longer active or have been discontinued and are no longer in circulation. By 2023, only 9,321of

[272] *Ibid*.
[273] Cindy Cohn et al., "EFF Will Accept Bitcoins to Support Digital Liberty," *Electronic Frontier Foundation*, May 17, 2013, https://www.eff.org/it/deeplinks/2013/05/eff-will-accept-bitcoins-support-digital-liberty.
[274] Nibley, *op. cit*.
[275] *Ibid*.
[276] *Ibid*.
[277] Kat Tretina and Michael Adams, "Top 10 Crypocurrencies of 2023," *Forbes Advisor*, August 22, 2023, https://www.forbes.com/advisor/investing/cryptocurrency/top-10-cryptocurrencies/.

the 22,932 cryptocurrencies are in circulation and use, as reported in **Figure 12** below.[278] As a result, the current number of cryptocurrencies is significant, considering that there were just 66 cryptocurrencies in use at their inception.[279] The following bar graph displays the total number of cryptocurrencies from August 2013 to August 2023. Until February 2022, the number of cryptocurrencies had been steadily rising, but the Ukraine War and other global imbalances have caused the number of active cryptocurrencies to fall. Recent data during August indicates a gradual growth.

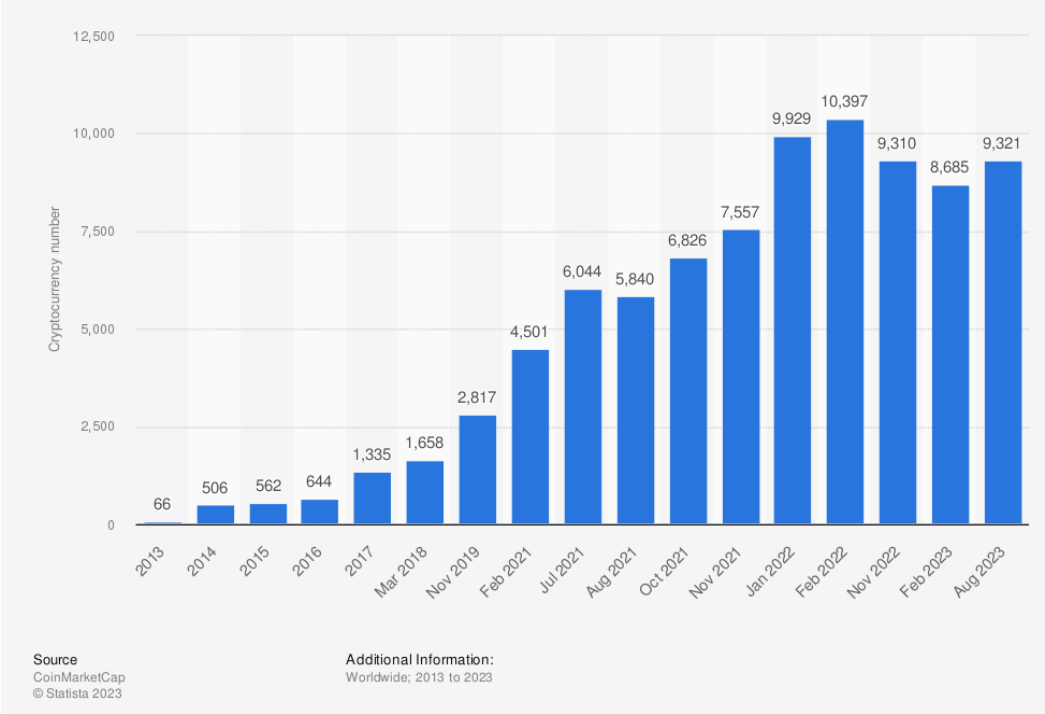



**Figure 12**: Cryptocurrencies: A numerical evolution from 2013 to August 2023; Source: Statista (2023).

The ease with which cryptocurrencies can be generated has undoubtedly contributed to their rise over time. Theoretically, anyone who knows how to code a blockchain program can develop a new cryptocurrency. However, this does not guarantee its success, and it can frequently disappear from the market for lack of interest or lack of practical utility in the digital financial ecosystem.

Although the concept behind creating these cryptocurrencies is the same as BTC, each cryptocurrency has a distinct value. This value is measured by market capitalisation, which

[278] GP Bullhound, und The Motley Fool, und Investing.com, "Number of cryptocurrencies worldwide from 2013 to August 2023, Chart, Statista, August 9, 2023, https://www-statista-com.ezprimo1.runi.ac.il/statistics/863917/number-crypto-coins-tokens/.
[279] *Ibid.*

indicates the total value of the cryptocurrency in circulation compared to other cryptocurrencies. Market capitalisation is calculated by multiplying the current price of the individual digital currency by the total number of digital currencies in circulation. [280]

On August 22, 2023, *Forbes* magazine employed this parameter to rank the top cryptocurrencies currently trading.[281] At the top of the ranking is Bitcoin, with a market capitalisation of $506,5 billion. [282] Bitcoin's price has seen a significant increase since 2009. In May 2016, the price for one Bitcoin was worth approximately $500, but as of August 22, 2023, it was valued at roughly $26,022, an increase of 5.104%.[283]

Following Bitcoin, Ethereum, is the second top cryptocurrency of 2023.[284] It is a decentralised digital platform similar to Bitcoin, whose currency, dubbed Ether (ETH), "has no intrinsic value, has no centralised issuer, and uses blockchain technology to record transaction history."[285] Programmer and co-founder of Bitcoin Magazine, Vitalik Buterin, who created Ethereum in 2013, was able to launch the cryptocurrency in 2015 owing to a crowdsourcing effort in 2018.[286] Since then, it has expanded to become the second-largest cryptocurrency platform worldwide. The peculiarity of ETH lies in the so-called "smart contract."[287] These are self-executing programs or instructions directly written on the blockchain.[288] Moreover, once a smart contract has been posted to the blockchain, it cannot be changed, making it trustworthy.[289] Smart contracts let you carry out transactions without the need for mediators or outside influence, which cuts down on expenses and waiting periods. In this context, the importance of the ERC20 standard on Ethereum emerges. Tokens must conform to a set of protocols defined by the ERC20 to function consistently throughout the platform.[290] This standard outlines several requirements for every token to ensure its predictable and efficient maintenance inside the various Ethereum applications. With a market cap of $199,6 billion, ETH has seen substantial growth due to these special characteristics.[291] Its price increased by 14,997% between April 2016 and late August 2023, from around $11 to about $1,661.[292]

---

[280] Dr. Andrea Sestino interview by Anna Miccoli, September 12, 2023, audio, 31:22.
[281] Tretina and Adams, *op. cit*.
[282] *Ibid*.
[283] *Ibid*
[284] Kerr et al., *op. cit*., p. 3.
[285] *Ibid*.
[286] *Ibid*.
[287]Cheng-Ting Tsai et al., "Design and Development of a Blockchain-Based Secure Scoring Mechanism for Online Learning," *Educational Technology & Society* 25, no. 3 (2022): 105–21. https://www.jstor.org/stable/48673728.
[288] *Ibid*.
[289] *Ibid*.
[290] *Ibid*.
[291] Tretina and Adams, *op. cit*.
[292] *Ibid*.

Tether (USDT) is the third top cryptocurrency of 2023. It was created in Santa Monica in 2014 by the company iFinex. Tether owes its popularity to the fact that it is one of the first "stablecoin" cryptocurrencies, i.e. digital coins that try to keep their value constant by attaching it to a currency issued by the government or another stable benchmark. This is done to reduce price volatility, an issue many other cryptocurrencies suffer from. Tether's value is primarily correlated with the US dollar. The US Commission for Future Trade in Goods (CFTC) imposed a $41 million fine on Tether in 2021. According to the CFTC, "Tether held sufficient fiat reserves in its accounts to back USDT tether tokens in circulation for only 27.6% of the days in a 26-month sample time period from 2016 through 2018."[293] In addition, USDT's market capitalisation amounted to $82.8 billion.[294]

With a $33.5 billion market valuation, Forbes magazine rated the Binance platform fourth.[295] The Binance trading platform's cryptocurrency, Binance Coin (BNB), was initially introduced in 2017 to manage commissions. In August 2023, it had a value of $218, a remarkable 217,730% rise from its original $0.10 value.[296] This growth is unquestionably attributable to the platform's status as the biggest cryptocurrency exchange in the world based on daily trading volume, its comparatively low commissions, and the prospect of earning BNB as compensation for promoting it.[297] Since 2017, BNB has increased its range of capabilities and can now, for example, be used to book vacations and be traded for other cryptocurrencies like Bitcoin.[298] Despite the cryptocurrency's clear appeal, it has also come under fire for what some users claim is its complex use and for having legal problems. Due to investigations into suspected money laundering and fraud by US regulators, the BNB has not been directly accessible in the US since 2019. However, Americans can use Binance US, a distinct version with fewer features.[299]

The Ripple company's creation, XRP, is the fifth most popular cryptocurrency in 2023. Three engineers, David Schwartz, Jed McCaleb, and Arthur Britto created XRP in 2011 while working on the XRP Registry (XRPL).[300] The project aimed to develop a more advanced version of Bitcoin that exceeded its restrictions to produce a long-lasting digital asset specially

[293] Commodity Futures Trading Commission (2021), CFTC Orders Tether and Bitfinex to Pay Fines Totaling $42.5 Million, CFTC, https://www.cftc.gov/PressRoom/PressReleases/8450-21.
[294] Tretina and Adams, *op cit*.
[295] *Ibid*.
[296] *Ibid*.
[297] Kerr et al., *op cit*., p. 3-4.
[298] Tretina and Adams, *op cit*.
[299] Kerr et al., *op cit*., p. 4.
[300] Marcel T. Rosner and Andrew Kang, "Understanding and Regulating Twenty-First Century Payment Systems: The Ripple Case Study," *Michigan Law Review* 114, no. 4 (2016): 649–81. http://www.jstor.org/stable/24770875.

made for payments. XRP was authorised in 2012.[301] Chris Larsen soon joined the group, and in September 2012, the corporation known initially as Newcoin was founded. The name rapidly shifted to Opencoin and finally to Ripple, the company name.[302] With this network, XRP can enable the exchange of other currencies, including fiat currencies and other significant cryptocurrencies, and it was created with the same vision as Ripple's founders. Like Binance Coin, XRP has grown significantly since 2017, when its value was only $0.006, reaching $0.52 on August 29, 2023, registering an 8.511% increase.[303] It has a $27.3 billion market capitalisation.[304]

The five cryptocurrencies listed above represent a tiny portion of the vast world of virtual currency. Despite their smaller scale, numerous other cryptocurrencies significantly impact the digital economy. For instance, Dogecoin, first intended as a straightforward parody, has grown immensely popular and gathered a devoted following, making it one of the most recognisable cryptocurrencies in circulation today. Then there is Cardano, renowned for its scientific approach and founded on peer-reviewed research, making it one of the most advanced blockchain projects with regard to sustainability and security. It is important to note how quickly market dynamics can shift and how broad, diverse, and ever-changing the world of cryptocurrencies is.

### 4.1.2 A Comprehensive Look at Cryptocurrencies: From Benefits to Concerns

The rise of BTC, promptly followed by other cryptocurrencies, has resulted in significant and unprecedented economic and technological advancement. The freedom from the established banking system and the speed of transactions have drawn a lot of consumers to cryptocurrencies. However, despite the clear benefits it provides, cryptocurrencies also have drawbacks. Like any new technology, cryptocurrencies should be handled carefully, balancing their great promise with their inherent difficulties.

Among the distinct advantages of cryptocurrencies is the *transactional speed*: unlike traditional banking systems, you can make transactions in a few minutes or a maximum of one day, regardless of the geographical distance between issuer and recipient.[305] Usually, domestic transactions can take place immediately or are processed in one or two days, whilst in the case

[301] *Ibid*.
[302] *Ibid*.
[303] Tretina and Adams, *op. cit*.
[304] *Ibid*.
[305] Nikita Tambe and Aashika Kain, "Advantages and Disadvantages of Cryptocurrencies in 2023," *Forbes Advisor*, June 14, 2023, https://www.forbes.com/advisor/in/investing/cryptocurrency/advantages-of-cryptocurrency/.

of international transactions, the wait can be longer, up to five or more working days, as it is necessary to carry out regulatory checks and follow up checks recycling to verify the security of transactions. These controls are reserved for traditional currencies as regulated by central banks and governments, while the *decentralised nature* of cryptocurrencies means that there is no central entity controlling transactions, but it is distributed among the many participants.[306] This reduces the monopolistic power of banking institutions and promotes more *transparency*.[307] Cryptocurrencies' *resistance to inflation* is unquestionably one of their most appealing features.[308] According to the IMF, inflation is the growth rate in product and service prices over a specific period.[309] A widespread increase in the cost of goods and services occurs when the traditional currency loses purchasing power due to inflation. Fewer items and services may currently be purchased with the same amount of money as in the past. Central banks' excessive printing of fiat currencies is one of the most frequent causes of inflation. Due to the devaluation of traditional currencies, more currency will be in circulation than products and services available. In contrast to conventional currencies, cryptocurrencies have a limit that protects them from inflation. For instance, BTC resists inflation since there is a cap of 21 million coins, and no new BTC is created. In addition, compared to banks and other financial institutions, cryptocurrencies *charge less* for transactions. As opposed to 2% or 3% for currency transfers, they typically charge a fee for each trade between 0.5% and 1.5%.[310] The prices are not constant and can change depending on the type of cryptocurrency used and the network congestion at the time of the transaction for both cryptocurrencies and traditional currencies. However, cryptocurrencies still offer a lower percentage cost.

Additionally, because they provide financial services to people who live in areas without access to or without banking systems, cryptocurrencies support *financial inclusion* by enabling it. Consequently, sending money is made simple for everyone with an internet connection. In addition to financial inclusion, using cryptocurrencies allows a specific *diversification of the investment portfolio*. Cryptocurrencies have grown significantly in recent years, and price variations are not directly related to changes in other markets. This enables the investor to combine assets, such as tangible and intangible assets, that have lower price correlations with one another. As a result, an investor may lower the volatility of the entire portfolio and aim for more steady returns. For instance, a cryptocurrency owner's shares might decline when its

[306] *Ibid*.
[307] *Ibid*.
[308] *Ibid*.
[309] Ceyda Oner, "Inflation: Prices on the Rise," *Finance & Development* 47, n. 001 (March 2010): 31, https://0-doi-org.library.svsu.edu/10.5089/9781451922257.022.A017.
[310] Tambe and Kain, *op. cit*.

cryptocurrency might increase, and vice versa.[311] The *high level of security and anonymity* that cryptocurrencies provide is one last fantastic benefit.[312] First, blockchain, the technology that powers cryptocurrencies, is considered one of the safest systems. Each transaction is thus recorded in blocks, and as each block is added to the chain, the data becomes unchangeable. Every investor also has a private key for their encrypted wallet, making it secure unless an outsider can access it. Since every investor maintains an encrypted asset in their wallet, security is paramount. A *high level of privacy* is also permitted because only a cryptographic address is used to identify the individuals responsible for the transitions.[313]

The phenomenon of cryptocurrencies, however, has, on the other hand, some disadvantages that can also lead to severe problems. On the one hand, the cryptocurrency's *volatility* is a benefit, but it may also result in significant losses when it becomes high. Since not all cryptocurrencies are precisely the same, predicting whether one will be more or less volatile is impossible.[314] However, investors risk significant losses when a cryptocurrency's value falls sharply. This may discourage potential investors or businesses that want to use cryptocurrencies as a form of payment but are hesitant due to the currency's potential for a fast value fall. Furthermore, the 51% *attack* is another possible cryptocurrency's disadvantage.[315] Participants in blockchain networks must agree before a block or transaction can be added. If most participants consent, the block or transaction is valid. It may or may not impact consent, though, if a person or group of players succeeds in taking over 50% of the network's processing capacity. There are three outcomes for this attack. First, whoever launches the attack can spend the virtual currency, immediately reverse the transaction, and then spend the same currency again. Another possibility is that the organisation that organised the attack blocks and censors transactions to prevent them from being confirmed. Additionally, the attackers could go back and modify some blocks or cancel past transactions if they held the bulk of the computational power. As well as the concept of volatility, the *irreversible nature of transactions* represents an advantage but, at the same time, can lead to errors, too. When the sender and recipient conclude the transaction, it is confirmed and recorded on the blockchain as definitive. Users risk losing funds if they transfer money to the wrong address because there is no way to reverse the transaction or no customer service support, such as banks provide.[316]

[311] *Ibid*.
[312] *Ibid*.
[313] *Ibid*.
[314] *Ibid*.
[315] *Ibid*.
[316] *Ibid*.

Moreover, cryptocurrencies can have a negative impact not only on people but also on the environment around them.[317] The *high use of energy* to add blocks to the network can become excessive for the environment and, consequently, for humans. However, the biggest drawback is that cryptocurrencies may be used illegally, especially for money laundering and terrorism financing.[318] While cryptocurrencies have numerous benefits, they can also be used for criminal activities like tax evasion, disguising income to avoid paying taxes or purchasing illicit commodities like drugs. Because they ensure identity anonymity and make it more difficult for the authorities to find illegal transactions promptly, criminals use digital currencies more frequently.

Cryptocurrencies are a financial instrument that attracts many investors because of their decentralised nature and because they are fast. Only through responsible use and deep knowledge of the mechanisms of cryptocurrencies can you make the most of the opportunities this new financial system offers. In addition, the risks resulting from the wrong use of cryptocurrencies have severe consequences for a single individual and the entire network, causing irreversible repercussions.

### 4.2 The Use of Cryptocurrencies in Terror Financing

The continuous technological innovation from artificial intelligence to social media constantly tests the world's governments, which try to promote conscious consumption to avoid illicit use. Cryptocurrencies are one of the main obstacles nations face in the technological world. The importance of cryptocurrencies is growing, offering opportunities on the one hand while continuing to pose hazards to organisations, governments, and people on the other. Due to their decentralised and anonymous nature, digital currencies create the greatest difficulty because they can circumvent conventional control and monitoring systems. This new digital tool allows non-state actors, particularly terrorist organisations, to purchase, finance, and transfer illicit funds more swiftly and easily than they could with conventional banking tools. At first, most cryptocurrency used in criminal activity was reserved for cybercrime. Today, it covers any criminal acts involving the transfer of money.

Foley et colleagues (2019) conducted targeted research on blockchain transactions between 2009 and April 2017 and identified all addresses related to seizures and darknet

[317] *Ibid*.
[318] Zachary K. Goldman et. al., "Virtual Currency Abuse in the Future: Criminals vs. Terrorists," *TERRORIST USE OF VIRTUAL CURRENCIES: Containing the Potential Threat*, Center for a New American Security, 2017, https://www.jstor.org/stable/resrep06423.

enterprises.[319] According to the analysis, "25 percent of all BTC users were engaged in criminal activity, accounting for around 23 (respectively, about 17) percent of all transactions by number (by value) and holding around half of all BTC."[320] The data reported by the research demonstrated that "a significant component of BTC's value as a payment system derives from its use in facilitating illegal trade."[321]

Although traditional techniques, such as *hawala*, bank transfers, and cash, continue to be the primary methods through which terrorists manage and move money, there has been a growing trend towards combining these techniques with modern payment technology. The range of options for transferring money has increased due to combining conventional and technical methods. A prime example of this is the *hawala*, which is being used to finance terrorism along with cryptocurrency.[322]

### 4.2.1 Crypto Crimes: The Many Faces of Illicit Digital Transactions

Svetlana Martynova, Senior Jurist at the Executive Board of the UN Counter-Terrorism Committee, during her speech at the Counter-Terrorism Committee's Security Council Special Meeting in October 2022, confirmed that the use of cryptocurrencies in terrorist financing has increased from a value of less than 5% in the past few years to about 20% in 2022.[323] This development is driven by the fact that more terrorist organisations are choosing to commit crimes online using cryptocurrencies.

The decision to employ more cryptocurrencies instead of conventional bank transfers is based on the features of cryptocurrencies that could make such actions easier. These characteristics include *anonymity*, which refers to the capability to protect the user's identity; usability, or the ease with which transactions can be made; *security*, which deals with the protection of transaction confidentiality and integrity; *acceptance*, which describes the degree to which a community of users adopts a cryptocurrency; *reliability*, which considers the speed and availability of transactions; and finally, *volume*, which refers to the overall value of a cryptocurrency.[324] **Table 2** examines how these cryptocurrency's properties help terrorist

[319] Sean Foley et al., "Sex, Drug, and Bitcoin: How Much Illegal Activity is Financed through Cryptocurrencies?", *The Review of Financial Studies* 32, no. 5, (May 2019): 1798-1853, https://doi.org/10.1093/rfs/hhz015.
[320] *Ibid*.
[321] *Ivi*, p. 1802.
[322] United Nations Security Council Counter-Terrorism Committee Executive Directorate (CTED), "Informing Security Council Counter-Terrorism Committee's Special Meeting," Mumbai and New Delhi, India (October 28-29, 20229, https://www.un.org/securitycouncil/ctc/news/cted's-tech-sessions-highlights-"threats-and-opportunities-related-new-payment-technologies-0.
[323] *Ibid*.
[324] Cynthia Dion-Schwarz et al., "Terrorist Use of Cryptocurrencies: Technical and Organisational Barriers and Future Threats," (Santa Monica, Calif: *Rand Corporation*, 2019): 13, https://rusi.org/explore-our-research/publications/occasional-papers/bit-bit-impacts-new-technologies-terrorism-financing-risks.

finance activities. The relevance of each box in the table is indicated by its classification and colour, which ranges from "critical importance" (dark grey) to "moderate importance" (light grey) to "minor importance" (white).[325] *Security* is a paramount feature in all activities involving terrorist financing. While fund-raising relies moderately on this, the other four activities deem *security* indispensable. *Anonymity* and *reliability* are crucial for the actors involved due to the weaknesses of illegal trafficking and the high stakes in obtaining funds for attacks. Moreover, *anonymity* given by cryptocurrencies is essential for illegal trafficking and attack fund-raising, which are complex activities that are simple to identify. Despite this, things change regarding operational funding since the necessity for *anonymity* is overcome by the *reliability* of a cryptocurrency, which takes on an increasingly significant role. This demonstrates how, despite the presence of the same entities, the traits they seek can vary greatly depending on the activity.

Furthermore, *acceptance* is one of the aspects that is less important than *reliability* or *security*. Nonetheless, it still has some significance when it comes to supporting both operations and fund-raising for attacks. On the other hand, *usability* is the primary concern when raising money, emphasising the need for user-friendly platforms that can efficiently handle these covert financial transactions. *Volume*, instead, is of moderate importance in relation to *security* and *anonymity* but more critical in terms of remittance, transfer and operational funding. Even while different cryptocurrencies have various features, it doesn't appear to be case that a single cryptocurrency that precisely satisfies all the requirements of terrorist organisations.[326]

| | Fundraising | Illegal Drug and Arms Trafficking | Remittance and Transfer | Attack Funding | Operational Funding |
|---|---|---|---|---|---|
| Anonymity | Moderate importance | Critical importance | Moderate importance | Critical importance | Lesser importance |
| Usability | Critical importance | Lesser importance | Lesser importance | Lesser importance | Lesser importance |
| Security | Moderate importance | Critical importance | Critical importance | Critical importance | Critical importance |
| Acceptance | Lesser importance | Lesser importance | Lesser importance | Moderate importance | Moderate importance |
| Reliability | Lesser importance | Moderate importance | Critical importance | Critical importance | Moderate importance |
| Volume | Moderate importance | Lesser importance | Critical importance | Lesser importance | Critical importance |

**Table 2**: Evaluating cryptocurrency features in the context of terrorist financing; Source: Rand (2019).

[325] *Ibid*.
[326] *Ibid*.

While several aspects of cryptocurrencies set them apart from more conventional forms of TF, the phases of the financing process are notably comparable. This continuity shows that terrorist organisations are highly resilient and flexible in responding to economic and technological advancements. The stages of TF through traditional methods are raise, move, and ultimately use. Four major phases may be identified when examining the stages in the context of cryptocurrencies: *collect, store, move, and use*.

*Collect* is the initial stage, which operates similarly to conventional terrorist fundraising. The most frequent sources of finance are charitable or individual contributions, criminal activity, and legitimate business activity. Illegal activity includes drug trafficking and other types of smuggling, fraud, extortion, and petty crimes. Donations may once again play a key role in financing terrorism since people who had previously funded these terrorist organisations switched to cryptocurrency because they are reliable, secure, and anonymous. Darknet markets, which may be accessed through private networks like I2P (Invisible Internet Project),[327] are used to sell drugs and other illegal commodities. Law enforcement organisations find it challenging to locate and prosecute users due to the anonymity of darknet markets and the use of cryptocurrencies.

After the funds have been raised, the terrorists *store* them. Terrorists frequently utilise prepaid cards, accounts with bogus identities, and expensive items like precious metals and valuable stones. However, in the case of cryptocurrency, terrorist groups employ digital wallets to hold their digital currency. Terrorists utilise online wallets the most because they are the most practical in ease of access and money transfers among digital wallets. Terrorists can lose money if the site is compromised, though. Using "mixing" or "tumbling" tactics to further obscure transaction histories and make the tracking of cash more challenging is an option for diversifying the storage of funds in various types of portfolios.

The third phase involves the *movement* of funds from one user to another through online. This stage establishes which terrorist groups may utilise cryptocurrencies and which ones should continue to rely on conventional tactics. Moving cryptocurrencies between portfolios might become very complicated for an organisation that is not technologically advanced. Cryptocurrencies might pose technical difficulties even though they provide more privacy and speed than traditional channels. For instance, the requirement to exchange cryptocurrencies for fiat money when making certain purchases, the volatility of a cryptocurrency's value, and the

[327] I2P was created and first made available in 2003. The "Invisible Internet Project" (I2P), which goes by the abbreviation, is a decentralised, anonymous overlay network. This network has been built for internet communications to offer a high level of privacy and anonymity.

secure storage of private keys. However, using cryptocurrencies allows users to send money straight to another person without using an intermediary. The traditional TF provides for the transfer of funds by mail services, bank transfers, and unofficial money transfer services like hawala. Regardless, this can come with a persistent danger because it can be challenging to move large transactions, and authorities can easily detect them.

The *use* of funds is the final phase. While the form of payment has changed, the goal of the terrorist organisations has not, and there are currently no significant distinctions between the traditional TF and the one using cryptocurrencies. The gathered funds are used to organise an attack, pay members' salaries, buy training supplies, and purchase weapons. However, using cryptocurrencies for funding has some drawbacks compared to traditional TF because terrorists can operate where cryptocurrencies are not well-known and occasionally need to change them into fiat money. Additionally, the value of cryptocurrencies might vary considerably. Because of this, when the circumstances are convenient, terrorists employ cryptocurrencies instead of conventional funds; otherwise, they transfer the cryptocurrencies into traditional currencies before using them.

Despite their evident advantages in the TF, not all terrorist organisations employ cryptocurrencies. The leading terrorist groups employing cryptocurrencies in 2021 are depicted in **Figure 13**. Among the terrorist organisations that have decided to use cryptocurrencies in TF are *Al-Qāʿida*, *Al-Qāʿida-related exchange*, *Hamās*, *ISIS*, and the *Saudi-led Jihadi activist movement*. These groups primarily employ XRP, ETH, ERC20, and BTC as cryptocurrencies.[328]

[328] Heidi Wilder, "An Overview of the Use of Cryptocurrencies in Terrorist Financing," *Coinbase Company*, September 21, 2021, https://www.coinbase.com/blog/an-overview-of-the-use-of-cryptocurrencies-in-terrorist-financing.

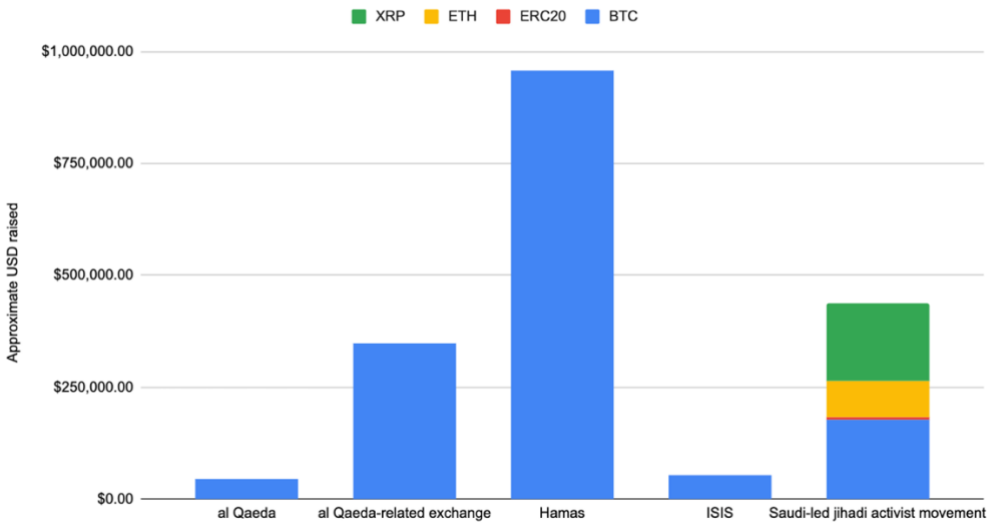



**Figure 13**: Dominant cryptocurrency preferences among high-activity terror funding organisations; Source: Coinbase (2021).

The graph highlights how *Hamās*, through its website and other Telegram channels, raises more money than anyone else, nearly $1,000,000.00, using only BTC. The second group, the *Saudi-led Jihadi activism movement*, has raised approximately $500,000 using all four cryptocurrencies, primarily BTC and XRP. Exchanges involving *Al-Qāʿida* had a volume of more than $250,000. *Al-Qāʿida* and *ISIS* also exclusively use BTC, although at a smaller level than *Hamās*.[329]

Moreover, *Al-Qāʿida*, *Al-Qāʿida-related exchanges*, *Hamās*, ISIS, and the *Saudi-led jihadist activist movement* began engaging in the TF organisation's fundraising efforts between 2018 and 2021, as reported by **Figure 14** below.[330] The first known cryptocurrency exchanges were those connected to *Hamās* and *Al-Qāʿida*. In 2020, *ISIS* and *Al-Qāʿida* started using cryptocurrencies more frequently. *Hamās* has been requesting BTC donations since January 2018, using a single donation address. Within a short period, their fundraising strategies have advanced. They now try to conceal the gathered funds by providing fresh donation addresses whenever they visit their dedicated page. The graph demonstrates that from 2018 to 2021, *Hamās* is the organisation that adopted cryptocurrencies most actively.[331] Up until the whole purpose of usage was declared on April 27, 2023, *Hamās* had gradually decreased its use of cryptocurrencies and, more broadly, digital tools for its finance operations since August 2021.[332]

[329] *Ibid.*
[330] *Ibid.*
[331] *Ibid.*
[332] *Ibid.*

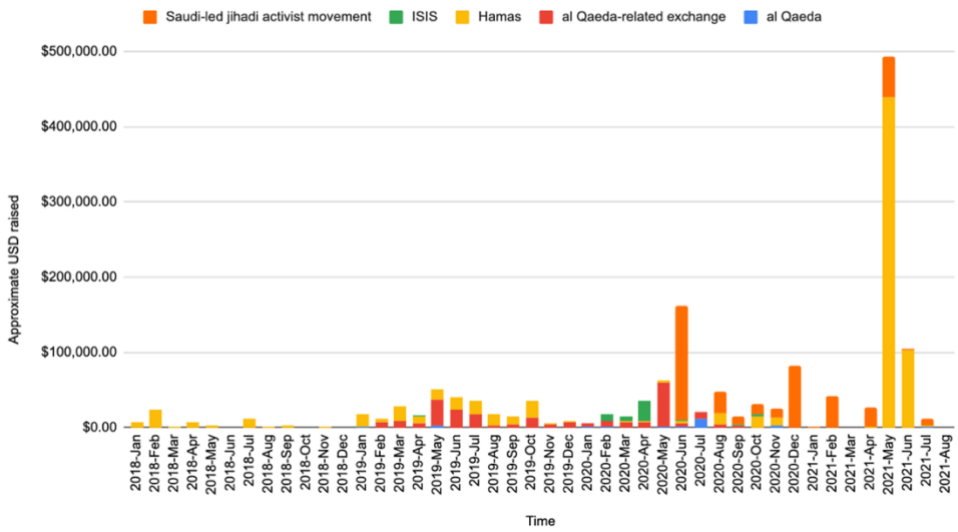



**Figure 14**: Evolving fundraising trends among most active TF-associated organisations; Source: Coinbase (2021).

*Al-Qassam Brigades* (AQB), the armed wing of *Hamās,* has in the past run social media campaigns and websites to request such contributions.[333] They accomplish this by offering specific donation addresses and comprehensive instructions on how to get and donate cryptocurrencies. US officials learned about these operations when they seized bitcoins worth more than $1 million linked to AQB donations from an unlicensed cryptocurrency company in the Gaza Strip in 2020.[334] When donations to *Hamās* peaked in July 2021, the Israeli government seized an undisclosed sum from several BTC wallets used by the AQB.[335] This demonstrates that, like conventional TF systems, cryptocurrencies are subject to government monitoring, regulation, and interference.

Terrorist and criminal organisations generally employ cryptocurrency to conceal the source of their funds' illegal activity. This mechanism is better defined as cryptolaundering which refers to money laundering using cryptocurrencies.[336] As for TF's steps, money laundering follows cryptocurrency TF's three conventional placement steps: collocation, stratification, and integration. The UNODC is working on a project that is expressly focused on cryptocurrencies and money laundering, and it has found some common characteristics of cryptocurrencies that facilitate money laundering for criminal organisations and to which we

[333] Chainalysis Team, "Hamas' Al-Qassam Brigades Announces End of Cryptocurrency Donation Efforts," *Chainalysis*, April 27, 2023, https://www.chainalysis.com/blog/hamas-al-qassam-brigades-cryptocurrency-donations-shutdown/.
[334] *Ibid*.
[335] *Ibid*.
[336] United Nations Office on Drugs and Crime, "Money Laundering Through Cryptocurrencies," United Nations, https://syntheticdrugs.unodc.org/syntheticdrugs/en/cybercrime/launderingproceeds/moneylaundering.html.

should pay more attention.[337] First, in banking systems, it is simpler to determine the first stage, the placement of illegal earnings, in the traditional financial system. In contrast, most cryptocurrencies are anonymous, making recognising them more challenging. The ease of creating an address or account in a blockchain takes seconds and, above all, does not require any cost. However, each address can only be used twice: once to receive funds and once to transfer them.

Moreover, the UNODC highlights that cryptocurrencies allow the deployment of very complex recycling schemes, with thousands at a minimum cost. All this can be done automatically through computer scripts, making the layering process quick. A further peculiarity lies in the volatility of cryptocurrencies: the exponential increase in their value in short periods can easily mask and justify an unexpected enrichment.[338]

Since 2015, there has been a sharp rise in the number of illicit addresses used to transfer money for recycling.[339] **Figure 15** shows the money laundering trends by year from 2015 to 2022. Cryptocurrencies worth about $0.4 billion were sent at the beginning of 2015. Illegal addresses sent roughly $23.8 billion worth of cryptocurrencies in 2022, a 68.0% increase from 2021.[340]

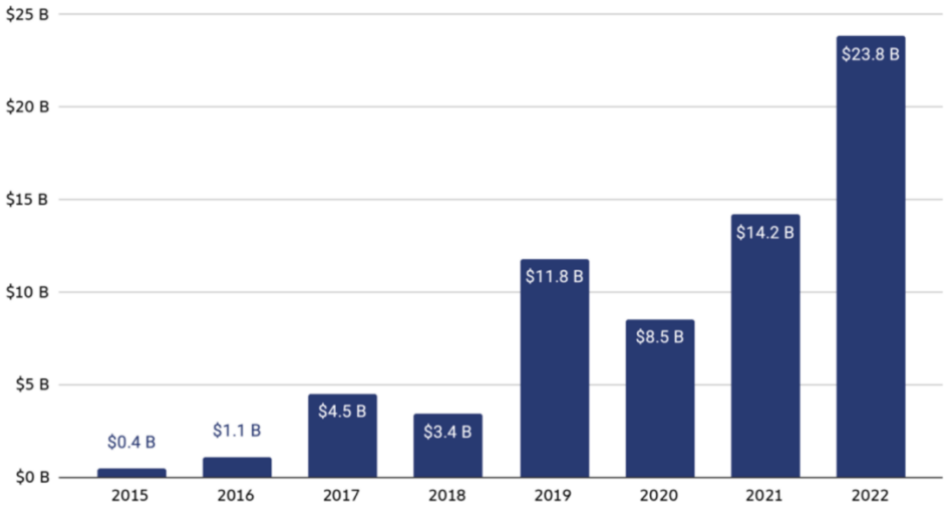



**Figure 15**:Cryptocurrency laundering trends from 2015 to 2022; Source: Chainalysis (2023).

There are many technologies and methods that can be used to launder money in the cryptocurrency world. Using supposedly "privacy coins" is one of the most well-known strategies. These virtual currencies are "cryptocurrency untraceable by design" since they are

[337] *Ibid*.
[338] *Ibid*.
[339] Chainanalysis Team, "Crypto Money Laundering: Four Exchange Deposit Addresses Received Over $1 Billion in Illicit Funds in 2022," *Chainanalysis*, January 26, 2023, https://www.chainalysis.com/blog/crypto-money-laundering-2022/.
[340] *Ibid*.

made to provide significantly more anonymous transactions than conventional cryptocurrencies.[341] Privacy coins conceal the transaction amount, issuer, and recipient. However, sales are publicly viewable in the blockchain even though traditional cryptocurrencies, such as the BTC, do not reveal the identity of address owners. Blending or mixing is another technique. One address is used to combine funds from various sources.[342] The money is pooled, divided, and distributed before being transmitted to multiple addresses. Linking funds to their source is very difficult when using this method because the funds are combined, divided, and distributed across many addresses. Tracing monies back to their original source is challenging in this situation. Cryptomixers can be used lawfully to boost transaction anonymity or safeguard financial information despite being frequently linked to illicit activities. Cryptomixers handled roughly $7.8 billion in 2022, of which 24% came from unlawful addresses, down from $11.5 billion in 2021, of which 10% came from illicit addresses.[343] The likelihood explains the considerable disparity between 2021 and 2022 that more substantial constraints have decreased legitimate users' use of cryptocurrency mixers while allowing illegal users to continue doing so.[344]

The third choice is what is known as "Fiat off-ramps," or the businesses that enable the conversion of cryptocurrencies into fiat money. Through this option, the converted funds leave the blockchain realm and are then harder to track. Most of these "off-ramps" are centralised exchanges, but peer-to-peer platforms and other services can also serve this purpose.[345]

The world of cryptocurrencies drew more and more users between 2022 and 2023 via both legitimate and illegal accounts.[346] Terrorist organisations use cryptocurrencies to finance their operations and launder finances. Still, during the past two years, most money held by criminals on the blockchain has come through hacks against cryptocurrency exchanges or outright theft of virtual currency.[347] The UN has emphasised how crucial it is to combat illicit gains using cryptocurrency while also keeping in mind the more conventional strategies used by terrorists to further their objectives.

[341] United Nations Office on Drugs and Crime, *op. cit.*
[342] *Ibid*.
[343] Chainanalysis Team, *Crypto Money Laundering: Four Exchange Deposit Addresses Received Over $1 Billion in Illicit Funds in 2022*, *cit*.
[344] *Ibid*.
[345] *Ibid*.
[346] *Ibid*.
[347] United Nations Office on Drugs and Crime, *op. cit.*

### 4.2.2 Hawāla and Cryptocurrency

Terrorist organisations need resources to continue to function. Such resources are gained through illegal, and sometimes even legitimate, operations like drug trafficking, money laundering, or charitable organisations. Activities like this are significant because they help to keep terrorists loyal by paying them salaries and providing advantages or additional rewards. They also help raise the money needed for terrorist operations. For this reason, the choice of means by which to raise funds is crucial. Terrorist groups have, on the one hand, taken advantage of technology, including cryptocurrency, but on the other hand, they have not entirely given up on more conventional techniques like *hawāla*. Both approaches are founded on similar ideas, like discretion, mutual trust, and effectiveness in resource transfers outside formal channels.

Terrorists can employ cryptocurrencies and *hawāla* in many different ways. They can be employed as separate transfer mechanisms.[348] In this regard, terrorists choose to use cryptocurrency instead of *hawāla* due to the sudden and significant loss of physical territory or the presence of military operations by international organisations and governments.[349] This could restrict their access and make transferring finances across borders and distances more challenging or engaging in conventional *hawāla* transactions, encouraging terrorists to adopt the new technologies.[350]

In contrast, others decide to combine the two to finance their operations. The process mirrors the conventional *hawāla* method. A funder in a nation wishes to transmit money to a group or person in another country. The sender may begin by purchasing cryptocurrency online, guaranteeing anonymity. Then, cryptocurrency is sent to a digital wallet associated with the recipient, for instance, a terrorist or a reliable member of the same organisation. After receiving the cryptocurrency, the recipient might keep it as is or transfer it across multiple digital addresses to strengthen anonymity further.[351]

When converting these cryptocurrencies into local currency, the recipient approaches a hawaladar as a broker. After receiving the cryptocurrency, this broker, relying on mutual trust and previous agreements, pledges to provide the equivalent in local currency in another region. This hawaladar contacts the hawaladar of the sending nation where the cryptocurrency was

[348] Marco Valeri et al., "The Use of Cryptocurrencies for Hawala in the Islamic Finance," *European Journal of Islamic Finance*, October 11, 2020, https://doi.org/10.13135/2421-2172/4145.
[349] Raihan Zahirah Mauludy Ridwan, "The Utilisation of Cryptocurrencies by the Terrorist Group as an Alternative Way of Hawala for Illicit Purposes," *University Katolik Parahyangan* 2, (2018): 5, https://journal.unpar.ac.id/index.php/Sentris/article/view/4183/3101.
[350] Antonia Ward, "Bitcoin and the Dark Web: The New Terrorist Threat?" *The RAND Blog*, January 22, 2018, https://www.rand.org/blog/2018/01/bitcoin-and-the-dark-web-the-new-terrorist-threat.html.
[351] Ridwan, *op. cit*.

sent, requesting that they pay the recipient in that nation's local currency. The second hawaladar is supposed to accept payment while hoping to receive reimbursement later. The two hawaladars may use cryptocurrencies rather than traditional transactions to pay off their debt. The first hawaladar settles its balance sheet by sending the second hawaladar an amount of bitcoin equal to the debt. To determine their balance, the initial hawaladar may transmit an amount of cryptocurrency equal to the debt to the second hawaladar. While the initial transaction and subsequent settlement between the two hawaladars occurred using cryptocurrencies, the ultimate recipient has now acquired the money in traditional currency, making it much harder for authorities to trace.[352]

*Hawāla* and cryptocurrency can be used together because of significant similarities in their features. In this regard, three specialists were asked about their opinions of the *hawāla* system and cryptocurrencies in the context of financing terrorism: Prof. Azani, Prof. Shaanan and Prof. Sestino.

[352] *Ibid*.

| | Respondent 1 Prof. Azani | | Respondent 2 Prof. Shaanan | | Respondent 3 Prof. Sestino | |
|---|---|---|---|---|---|---|
| | ***Hawāla*** | **Cryptocurrency** | ***Hawāla*** | **Cryptocurrency** | ***Hawāla*** | **Cryptocurrency** |
| **Easy Accessibility** | For *Hawāla* , it is easily accessible in regions with limited bank access. | As for cryptocurrencies, anyone with the internet can access it. | It is common in regions with limited bank access and a long tradition entrenched in many cultures and areas. | It is all about having internet access so if a terror organisation does not have it, it will probably use *hawāla* […]. | *Hawāla* is popular in regions with a high percentage of workers emigrants. | Cryptocurrencies are easy to access, and with low cost of transaction [...], so anyone can use it. |
| **Low Cost** | *Hawāla* has a lower cost compared to traditional banking systems. | […] Cryptocurrencies, too, offer a cost advantage over traditional financial systems. | The *hawāla*'s transactions are less expensive than traditional banking transfers. | The price is less expensive than banking systems, although it may change depending on whether the network is congested. | The transactions are low and sometimes are free among familiar connections. | When compared to other financial instruments, or even to cash, also by considering the black market and similar, crypto may be most "suitable" to be not controlled |
| **Decentralisation** | *Hawāla* is decentralised, and it challenges traditional financial systems. | Cryptocurrencies, as well, are decentralised and not regulated under the law. | *Hawāla* works in a decentralised manner because it is built on a reliable network with an established connection. | Decentralisation is the key characteristic that sets cryptocurrencies apart from conventional ways of money transfer. | *Hawāla* works outside the traditional banking system, there is no unique organisation that regularise it | Despite some timid attempts to regularise such forms of money transfer, even in Western economics, in Middle Eastern Countries, there is no regulation, so crimes may increase […]. Decentralisation should be monitored because, in this case is not a positive feature of such technology. |
| **Privacy** | *Hawāla* ensures anonymity and privacy. | As for *hawala, it* also cryptocurrencies guarantee a high level of privacy for the accounts | It provides more anonymity than other financing method. | Cryptocurrencies are not entirely anonymous […]. For instance, Ethereum allows for pseudonyms, but the transactions are visible on blockchain. | It allows for anonymous transactions. | It's all about traceability, because actually crypto are not so anonymous because traceable e.g., by leveraging on computer IPs addresses and so on. |
| **Regulation** | The lack of regulation is evident, despite some countries are | In the future there will be more regulations. | Maybe in the future there will not be the need of regulations because | Agrees on the increasing regulation. | In countries were originated like India there are a growing number of regulations. | The lack of regulation is clear: If in certain cases it may be partially positive, by considering |

| | | | | | | |
|---|---|---|---|---|---|---|
| | trying to regulate it […]. Maybe in the future more countries will regularise *hawāla* . | | terrorists' groups will use other instruments. | | | unethical practices, the absence of regulation may in turn increase criminality. |
| **Speed** | The speed is based on trust and on the transactions' destination. | The speed varies depending on the internet. | Speed base on connections between the parts. | Speedy transactions when the internet is not blocked. | It is quicker than the traditional transaction systems, however, it is fundamental that all the operators work in order to complete the transaction. | It's really speed […] and combined with crypto feasibility to access, an evident issue clearly emerges. |
| **Trust** | High trust based on strong personal relationships. | I think it is more trustable than *hawāla* thanks to the continuous evolution of technology. | It relies on personal and familiar ties, that may be interrupted. | Technology and mathematics that underlie cryptocurrency are trusted. | The people that are involved in the *Hawāla* transaction have to be reliable at 100%. | As a technology is trustable for definition, because based on blockchain systems. |
| **Usability** | It is a type of informal value system which is not difficult to use or understand […]. Easy for those familiar with it. | Cryptocurrencies are more complex than *hawāla* . | At first glance, *hawāla* can seem intricate, but once, understood, it is straightforward | More and more people are attracted by the cryptocurrencies' world and want to learn how to use them. | It is easy to use. | It is extremely easy to use, and as we said before, to access. |

**Table 3:** Findings from the in-depth interviews (2023).

*Note.* R1 = Professor Azani, 65 y.o.; R2 = Professor Shaanan, 40 y.o.; R3= Professor Sestino, 30 y.o.

All respondents concur that *hawāla* and cryptocurrencies have several advantages over conventional financial systems, although they operate in distinct ways. Indeed, R1 notes that while cryptocurrencies are available to anyone with an internet connection, *hawāla* is simple to use in areas with little access to banking services. R3 underlines the popularity of the *hawāla* system, especially in countries with a high rate of workers abroad. All parties agree that *hawāla* and cryptocurrencies offer cost advantages over conventional banking systems. R2 broadens this perspective by highlighting the profound cultural roots of *hawāla*. Moreover, R2 also points out that cryptocurrency costs may change based on network congestion. Although R1, R2 and R3 emphasise how decentralised *hawāla* and cryptocurrencies are, R1 argues that cryptocurrencies still need to be regulated despite being decentralised. R1, R2 and R3 concur that *hawāla* provides a high level of privacy. R2 contends that cryptocurrencies are not entirely anonymous, contrary to R1's assertion that they offer comparable privacy. Furthermore, R1 says that in the future more countries will regularise the *hawāla* system, while R2 affirms that maybe in the future there will be no need for regulations because criminal organisations, such as cryptocurrencies will employ other instruments. Furthermore, R3 highlights that neither Western countries nor Middle Eastern countries still have no regulation regarding the use and implementation of cryptocurrencies, so it is easier for criminals to use them. All the experts noted that trust and interpersonal connections are the foundation of *hawāla*'s quickness. Otherwise, while R1 claims that the speed of cryptocurrencies varies, R2 links it to the accessibility of internet connections. Both experts agree that the foundation of *hawāla* is firmly rooted in interpersonal and familiar connections, but R2 points out the possibility of eventual interruption of these ties with hawaladar due to the intervention of the authorities. Besides this, R3 points out that the *hawāla* transaction can be considered trustworthy only if the hawaladars, operating inside are known by the costumers and are involved in this type of transactions since lots of time.

On the other hand, according to R2 cryptocurrencies are founded on faith in science and math. As an expert of blockchains, R3 considers cryptocurrencies trustworthy because based on a technology that use advanced cryptographic techniques to ensure the security and integrity of data.

In contrast to more sophisticated cryptocurrencies, R1 and R3 view *hawāla* as an informal value system that is simple for those who understand it. R2 concurs but adds that interest in cryptocurrencies is rising and that *hawāla* is simple to learn and use.

The ongoing transformation of terrorist finance strategies demonstrates the capacity of extremist organisations to take advantage of old customs and emerging technologies. The

juxtaposition of cryptocurrency, the symbol of the digital revolution, and *hawala*, a practice anchored in many civilisations' histories and sociocultural fabric, illustrates such organisations' creativity and adaptability.

Cryptocurrencies promise anonymity and security through technology, and the *hawala*, with its deep roots in trust and interpersonal relationships and community, is at variance. However, both provide ways to get through conventional financial surveillance systems, making them valuable tools for people who operate on the edge of legality: the interaction between these approaches highlights the depth of the task facing international institutions and shows the strategic tenacity of terrorist organisations. Understanding the technological dynamics of new transaction modalities and the trust networks that underpin a system like *hawāla* is crucial for responding to this evolving threat.

### 4.3 Cryptocurrency in Terrorism: Case Studies on Al-Qāʿida and Al-Qassam Brigades

Following a joint investigation by the Federal Bureau of Investigation (FBI), Homeland Security Investigations (HIS), and the Internal Revenue Service – Criminal Investigation (IRS-CI), the US Department of Justice (DOJ) stated in 2020 that two terrorist funding operations that accepted cryptocurrency donations had been shut down: *Al-Qāʿida and* the *Al-Qassam Brigades* (AQB), the armed wing of *Hamās*. Both organisations frequently moved their funds using the *hawāla* method before switching to cryptocurrency.[353]

*Al-Qāʿida* is a terrorist group that Osama bin Laden founded in the late 1980s to support Islamic guerrilla warfare against the Soviet occupation of Afghanistan. Over the years, *Al-Qāʿida* has been responsible for numerous international and local attacks, including the 2005 London bombing. The *hawāla* system, formerly used to transmit money for these goals but later replaced by cryptocurrencies to receive and repurpose donations for the funding of terrorism, was frequently the route by which these funds were transported. The FBI, HSI, and IRS-CI tracked down the "Bitcoin Transfer Office," which appeared to be merely a standard cryptocurrency trading platform, in Idlib, Siria, which served as the focal point of transactions. Approximately $280,000 in BTC has been transferred using this platform since it was established in December 2018.[354] A Telegram fundraiser in 2019 that offered a BTC connection for donations was found to have been used to purchase guns. Agents tracked the address and

[353] Chainanalysis Team, "Chainalysis in Action: Department of Justice Announces Takedown of Two Terrorism Financing Campaigns with Help from Blockchain Analysis," *Chainalysis*, August 31, 2020, https://www.chainalysis.com/blog/cryptocurrency-terrorism-financing-al-qaeda-al-qassam-brigades-bitcointransfer/#:~:text=Al%2DQaeda%20specifically%20relied%20on,our%20newest%20intelligence%20brief%20here.
[354] *Ibid.*

discovered that when contributions were made, the money was sent to a different BitcoinTransfer-hosted address designated as "Defendant Property AQ2" to obtain further processing.[355] US investigators have found other funding operations run by *Al-Qāʿida*-related groups, including *Al Sadaqah*, a Syrian organisation active on social media, as well as on Telegram and Facebook. Even though she claims to be a charity, she has financed terrorism. The DOJ started seizing money linked to addresses under *Al-Qāʿida* control.[356]

The military arm of *Hamās*, also known as *Ḥaraka al-muqāwama al-islāmiyya* (literally, "Islamic resistance movement"), was established in 1987 to liberate Palestine from Israeli occupation to select an Islamic state. AQB is the abbreviation for this organisation. The *hawāla* system was the foundation for most of AQB's fundraising until 2018 when it heavily relied on BTC. AQB began an operation in 2019 deemed unprecedented by the DOJ due to its complexity and extent.[357] When AQB's website started pushing a QR code connected to a single BTC address to pay for jihad, the campaign was officially launched in early 2019. This address was initially linked to a US-based regulated stock exchange account, but U.S. officials quickly learned about this. After making an initial attempt to use cryptocurrencies, AQB has since used BTCs by switching out the original address with a new one that is connected to a private non-custodial wallet, where only the user has complete control and can authenticate transactions without the need for an intermediary. Thanks to techniques and companies like Chainalysis, the technology company that provides blockchain data and analysis, the DOJ could also track donations in this second attempt. With the third UnderCamp, the actual change occurred: AQB included a BTC wallet on their website, producing a unique BTC address for each donor.[358]

Additionally, they offered thorough video training to walk donors through the donation process while maintaining the highest level of privacy. The use of *hawāla* was recommended in one of the approaches. Donors could send cash to *hawāla*, who would subsequently send an equal amount in BTC to the address specified by AQB. In this instance, the fundraising was also uncovered.[359]

As demonstrated by AQB and *Al-Qāʿida*, terrorist organisations also adopt modern technologies in various ways. Although both terrorist groups had prior expertise with the *hawāla* system, they started using BTC to accept donations. While AQB began a genuine campaign through its website using a QR code, a portion of *Al-Qāʿida* used a Telegram channel

[355] *Ibid*.
[356] *Ibid*.
[357] *Ibid*.
[358] *Ibid*.
[359] *Ibid*.

that routed donations to a BTC address. The complexity of the strategies used by the two organisations is another important distinction. While AQB has shown greater flexibility and adaptation, moving from an associated address to a regulated stock exchange in the USA, to a non-custodial portfolio, to the integration of a portfolio on its website that generates unique lessons for each donor, *Al-Qāʿida* has adopted a more straightforward approach because the BTC's focus was unique and was primarily exposed to the authorities. This tactic has made it more difficult for the government to track donations. Finally, the videos that walked donors through the donation procedure showed that AQB had a more sophisticated strategy than *Al-Qāʿida.*

Both cases demonstrate that despite the availability of instruments to stop the financing of terrorism, organisations are becoming more adept at utilising new technologies.

# CHAPTER V.

# INTERNATIONAL EFFORTS AND REGULATORY FRAMEWORKS

## 5.1 Evaluation of International Efforts

The international community has stepped up its efforts to combat money laundering and terrorist funding in response to the mounting threats these practices pose. Globalisation and digitalisation have amplified these dangers by enabling terrorist organisations that use illegal weapons to open up new, more dangerous fronts. The necessity of concerted action is highlighted by their capacity to destabilise governance structures and "jeopardise" their economic stability. International organisations and central governments have turned their focus to the ways that terrorists fund themselves, including those that are intrinsic to a nation's culture or history, like *hawāla* in Asia and the Middle East. In this regard, the ongoing efforts and commitment made by organisations like United Nations, Financial Action Task Force, the International Monetary Fund, World Bank, and many others have been and continue to be crucial in halting all those phenomena that have the potential to upset the balances on the international and national levels. A strong and compelling framework to combat money laundering and terrorist financing has been laid out in recent strategies like the "Eighth Biennial Review of the United Nations Global Counter-Terrorism Strategy" of 2023 and the "Recommendations" of the FATF of February 2023, demonstrating how the fight against this phenomenon is keeping up with new terrorist tactics. [360]

Governments and international organisations initially implemented anti-money laundering and counter-terrorism financing practices in collaboration, with a unified approach and shared policy. However, following the September 11, 2001, assault and in response to the rising issue of money laundering, the two Executive Directors of the World Bank and the International Monetary Fund made the joint decision to step up AML and CTF activities. Coherently, the "Reference Guide on Anti-Money Laundering and Combating the Financing of Terrorism" was produced in 2003 through a collaborative effort: This guide offers concrete recommendations to help countries create an AML CTF system following international norms.

[360] U.N. GAOR, 77th Sess., U.N. Doc A/77/718 (February 2, 2023), https://documents-dds-ny.un.org/doc/UNDOC/GEN/N23/033/29/PDF/N2303329.pdf?OpenElement; FATF (2012-2023), International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, FATF, Paris, France, www.fatf-gafi.org/recommendations.htm.

The guide serves as a foundation for the ongoing evolution and modification of tactics in response to new difficulties in money laundering and terrorist financing. It is crucial to examine in particular the rules implemented by two organisations, the UN and the FATF, which have evolved more and more in the battle against money laundering and terrorism.

### 5.1.1 The United Nations Resolutions

Although combating terrorism and dealing with money laundering was not the UN's top priority when it was founded, the rise of these worldwide dangers has caught its attention. The UN was established in 1945, following the end of World War II, with the main goals of combating future major conflicts and fostering international cooperation. In the beginning, 51 nations ratified the UN Charter in San Francisco on June 26, 1945, and the organisation's operations began on October 24.[361] At the moment, the UN counts a total of 193 members. By referring to the period before the terrorist attack at the Twin Towers and the one that followed, it is possible to assess the United Nations' engagement in the fight against terrorism and money laundering.

The first significant event before 9/11 was the adoption of the "Vienna Convention", which, despite emphasising combating illicit drug trafficking and associated law enforcement difficulties, also refers to the criminalisation of the idea of money laundering. As another fundamental step in the fight against money laundering and terrorism, in 2000, the UN adopted the "Palermo Convention".[362] The Convention "contains a broad range of provisions to fight organised crime and commits countries that ratify this convention to implement its provisions through the passage of domestic laws."[363] Towards the end of the nineties, the United Nations began to take an interest in the financing of terrorists and 1999 adopted the so-called "International Convention for the Suppression of the Financing of Terrorism", which entered into force on April 10, 2002.[364] According to this agreement, anyone who seeks donations for organisations that support terrorism or engage in terrorism can be convicted of a crime.

The UN Security Council (UNSC) adopted Resolution 1373 immediately following the Twin Towers attack, which "calls on all Member States to find ways to intensify and accelerate the exchange of operational information on the use of information and communication technologies (ICT) by terrorist groups and to suppress the recruitment of terrorists."[365] Additionally, the Counter-Terrorism Committee (CTC) has been established as a body to assist

[361] United Nations, *Charter of the United Nations*, 1945, 1 UNTS XVI, https://treaties.un.org/doc/publication/ctc/uncharter.pdf.
[362] *The Palermo Convention op. cit*.
[363] P. Schott, *op. cit*.
[364] *International Convention for the Suppression of the Financing of Terrorism*, *op. cit*.
[365] UN S/RES/1373.

Member States in enhancing their capability in the fight against terrorism.[366] Other significant resolutions have been issued, such as Resolution 1624 of 2005, which calls on member nations to establish adequate measures to outlaw and prevent the incitement of terrorism.[367]
Additionally, to face the challenges posed by international terrorism, the UN launched the Global Counter-Terrorism Strategy in 2006 through Resolution 60/288.[368] This strategy is structured around four major pillars, each of which focuses on a distinct aspect of the war on terrorism:[369]

*i. Measures to address the conditions conducive to the spread of terrorism.*

*ii. Measures to prevent and combat terrorism.*

*iii. Measures to build States' capacity to prevent and combat terrorism and to strengthen the role of the United Nations system in that regard.*

*iv. Measures to ensure respect for human rights for all and the rule of law as the fundamental basis of the fight against terrorism.*

The first pillar concentrates on the underlying factors contributing to terrorism, such as protracted conflicts, a lack of the rule of law, economic unrest, corruption, and discrimination.[370] The second pillar emphasises practical and operational counterterrorism measures. This includes enhancing the capabilities of Member States, fostering global cooperation, and avoiding recruitment and radicalisation.[371] The third pillar focuses on assisting Member States to develop their institutional and operational capabilities to combat terrorism more effectively. [372] The fourth one states that all efforts to combat terrorism must respect human rights and the rule of law; More importantly, this pillar stresses the meaning of weighing security measures against respect for civil liberties and democratic principles.[373] Since 2006, the UN General Assembly has reviewed the Global Counter-Terrorism Strategy every two years to keep it current with emerging threats and Member States' top objectives. This gives a chance to reaffirm global support for multilateral counter-terrorism initiatives, evaluate the implementation's success, and pinpoint any new problems that need to be addressed.

In 2013, Security Council Resolution 2129 underlined the necessity for international collaboration to stop terrorists from abusing technology whilst always respecting human rights.

---

[366] *Ibid*.
[367] UNSC Res 1624 (14 September 2005) UN Doc S/RES/1624.
[368] UNGA Res 60/288 (20 September 2006) UN Doc A/RES/60/288.
[369] *Ibid*.
[370] UN Global Counter-Terrorism Strategy, Pillar I.
[371] UN Global Counter-Terrorism Strategy, Pillar II.
[372] UN Global Counter-Terrorism Strategy, Pillar III.
[373] UN Global Counter-Terrorism Strategy, Pillar IV.

It also highlighted the significance of analysing the threat posed by ICT.[374] Furthermore, the international community faces the growing problem of foreign terrorist fighters who cross borders to support or join terrorist organisations. Consequently, the UNSC approval for this addressed in Resolution 2178, also known as the "Foreign Terrorist Fighter Resolution" (2014), to emphasise the necessity of increasing global collaboration and cooperation.[375] In 2015, the UNSC adopted Resolution 2242, which addressed how gender affects terrorism and counterterrorism efforts.[376] This resolution is significant because it emphasises women's importance in maintaining peace and preventing conflict. Other resolutions, including Resolution 2341 and Resolution 2354 emphasise the value of public-private partnerships in preventing terrorists from using ICT, creating counter-narratives, and developing technology solutions that fully protect human rights. [377] In 2019, the UN has grown increasingly concerned about the prepaid cards and cryptocurrency that terrorists use as payment methods. It highlights the development of payment mechanisms that terrorists use through Resolution 2462.[378]

One of the latest actions the UN took was on June 22, 2023, when the General Assembly passed Resolution 77/298 to request that the Secretary-General provide a report on the Global Counter-Terrorism Strategy's implementation at its eightieth session.[379] This schedule differs from the previous biennial one because the ninth revision of the Strategy set for 2026 will occur in the same year as its twentieth adoption anniversary.[380] In the complex international context, not only the UN but also other institutions have stepped up their efforts, including the FATF.

### 5.1.2 Financial Action Task Force on Money Laundering

The United Nations are not just waging the fight against terrorism and money laundering. The G-7 nations established the FATF in 1989, formally, as "an intergovernmental body whose purpose is to develop and promote an international response to combat money laundering."[381] Furthermore, the FATF has increased its efforts to combat terrorism since 2001. The FATF's first duties include monitoring members' progress in implementing anti-money laundering measures, reviewing and reporting on laundering trends, techniques and countermeasures, and promoting the adoption and implementation of FATF anti-money laundering standards

[374] UNSC Res 2129 (17 December 2013) UN Doc S/RES/2129.
[375] UNSC Res 2178 (24 September 2014) UN Doc S/RES/2178.
[376] UNSC Res 2242 (13 October 2015) UN Doc S/RES/2242.
[377] UNSC Res 2341 (13 February 2017) UN Doc S/RES/2341; UNSC Res 2354 (24 May 2017) UN Doc S/RES/2354.
[378] UNSC Res 2462 (28 March 2019) UN Doc S/RES/2462.
[379] UNGA Res 77/298 (17 August 2022) UN Doc A/RES/77/298.
[380] *Ibid*.
[381] Schott, *op. cit.,* p. 38-39.

globally.[382] Today, FATF counts 39 members and has a strong network of 9 FATF-style regional bodies (FSRBs), which encourage the adoption of FATF recommendations among their members and participate in formulating FATF policy.[383] The Asia/Pacific Group on Money Laundering (APG), located in the Pacific Region, the Eurasian Group (EAG), the Financial Action Task Force of Latin America (GAFILAT), the Intergovernmental Action Group against Money Laundering in West Africa (GIABA), the Middle East and North Africa Financial Action Task Force (MENAFATF), and the Expert Committee on the Evaluation are among the nine FSRBs. About 200 nations have been estimated to have complied with the FATF Recommendations due to the global network of FSRBs and the FATF.[384]

About a year after its establishment in April 1990, the FATF issued a report with *Forty Recommendations* aimed to combat money laundering.[385] The FATF also made *Eight Special Recommendations* in October 2001 in response to the escalating terrorism issue. These recommendations brought to the global community's attention to the fact that limiting financial resources to terrorist groups was as crucial as pursuing them. FATF has, however, modified its list of recommendations over time, continuously keeping updated on emerging challenges. For instance, it changed the submissions in 2003 to consider the growing funding issue through methods like *hawala*.[386]

In order to prevent the illicit use of such tools for money laundering, the FATF emphasised the significance of openness in identifying the actual beneficiaries of trusts and legal companies. The *Ninth Special Recommendation* on financing terrorism was introduced the following year.[387] Additionally, several of its recommendations had to be revised in 2012 because the obstacles surrounding money laundering and terrorism had altered even more, including, for instance, issues like financing the spread of weapons of mass destruction (WMD).[388] Due to the need to balance innovation and security, the FATF modified its guidelines in 2019 to incorporate binding measures relating to virtual or crypto assets.[389] This is in line with UNSCR Resolution 2462, which stipulates that the FATF is crucial to the fight against money laundering, terrorism financing, and the use of WMD globally.[390] This resolution

---

[382] *Ibid.*
[383] FATF, "Methods and Trends," accessed September 12, 2023, https://www.fatf-gafi.org/en/topics/methods-and-trends.html.
[384] *Ibid*.
[385] FATF, "The Forty Recommendations of the Financial Action Task Force on Money Laundering," Paris, 1990.
[386] FATF, "The Forty Recommendations of the Financial Action Task Force on Money Laundering," Paris, June 20, 2003, https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202003.pdf.
[387] FATF, "History of the FATF," accessed September 12, 2023, https://www.fatf-gafi.org/en/the-fatf/history-of-the-fatf.html#:~:text=In%20April%201990%2C%20less%20than,Special%20Recommendations%20on%20terrorist%20financing.
[388] *Ibid*.
[389] *Ibid*.
[390] UN Doc S/RES/2462.

calls for the adoption of FATF recommendations by all nations. For global security, FATF and the UN's collaborative efforts to assist nations in fighting against these threats have become essential.

Moreover, in 2022, it will toughen global ownership rules to stop criminals from concealing their illegal operations and illicit riches behind covert company facilities.[391] The last update of the FATF Recommendations was in February 2023.

The FATF uses the mutual evaluation procedure for each country's AML/CFT system to determine whether recommendations are being adopted correctly by each nation. Every member of the FATF jurisdiction has had a mutual evaluation since 2004.[392] These assessments go into great depth about the AML/CFT system the country has implemented and the degree to which it complies with the FATF Recommendations. If a nation is given a low score for a particular recommendation, the FATF monitors it and asks for several periodic reports on steps taken to increase compliance. The mutual review process encourages member and non-member countries to enhance their AML/CFT systems despite the FATF's small membership and the lack of treaty-like power of its standards. As a result of criticism that this technique, which offered only a limited study of the efficacy and application of the AML/CFT system in each country beyond the legal framework, received in 2013, FATF made improvements to it.[393] The new evaluation procedure consists of two associated components: An evaluation of technical compliance, which focuses on the specific FATF Recommendations as they relate to the nation's relevant legal and institutional framework, and an evaluation of effectiveness, which assesses how well the legal and institutional elements cooperate when these are put into practice to achieve a set of defined outcomes that are essential to a strong AML/CFT system.[394]

FATF analysed the data in 1999 to identify which nations have AML/CFT gaps. In the global fight against money laundering and terrorist funding, 23 countries have been identified as "non-cooperative countries or territories" after a general assessment.[395] Numerous nations on the "black list" have hit their predicted FATF goals over time. In June 2023, when it was last updated, the FATF investigated over 125 nations and regions and made 98 publicly known.[396] Of these, 98 later implemented the necessary changes to remedy their AML/CFT

[391] *Ibid*.
[392] Leonardo Borlini, "The Financial Action Task Force: An Introduction," *Anti-Corruption Resource Centre*, January 2015, https://www.u4.no/publications/the-financial-action-task-force-an-introduction.pdf.
[393] *Ibid*.
[394] *Ibid*.
[395] *Ibid*.
[396] FATF, "High-Risk Jurisdictions Subject to a Call for Action," accessed September 12, 2023, https://www.fatf-gafi.org/en/publications/High-risk-and-other-monitored-jurisdictions/Call-for-action-June-2023.html.

flaws and were eliminated.[397] The Democratic People's Republic of Korea, Iran, and Myanmar are the nations with the greatest difficulties in preventing money laundering and terrorism, according to the FATF.[398] Countries, including Albania, Jordan, Mozambique, Vietnam, and others, are listed on the "grey list" because they have evident AML/CFT compliance issues but are working with FATF to address them.[399]

### 5.2 The Creation of an International AML/CFT Assessment Methodology

The policies and recommendations of the UN and FATF today represent a fundamental component of the global campaign against AML and CFT. They establish international standards in the fight against AML/CFT, the WB and the IMF have adopted measures like the FATF's *Forty Recommendations on Money Laundering* and the *Special Recommendations on Terrorist Financing*.[400] In this regard, the IMF and the WB have organised several Regional Policy Global Dialogues on AML/CFT. These discussions allowed specialists, government representatives, and representatives of regional and international groups to converse and share knowledge on AML/CFT concerns. This has made it feasible to draw attention to issues both at the regional and global levels, promoting greater international collaboration. The topics covered include the challenges countries face in the battle against illicit money flows, sharing the lessons learned, identifying specific problems for those countries, and understanding the kind of assistance countries need to halt money laundering and terrorist funding.

Furthermore, to create a unique and comprehensive AML/CFT validation methodology, the WB and the IMF convened a plenary meeting in October 2002 with the FATF, the Basel Committee on Banking Supervision, the International Association of Securities Commissions, the International Association of Insurance Supervisors, and the Egmont Group.[401] This approach assesses a nation's AML/CFT legal and institutional framework by creating the Financial Intelligence Unit, central organisations that are in charge of gathering, analysing, and disseminating financial data about alleged money laundering and terrorism funding activities.[402] The relevant UN Security Council Resolutions are also taken into consideration.[403]

---

[397] *Ibid*.
[398] *Ibid*.
[399] FATF, "Jurisdictions Under Increased Monitoring – 23 June 2023," accessed September 12, 2023, https://www.fatf-gafi.org/en/publications/High-risk-and-other-monitored-jurisdictions/Increased-monitoring-june-2023.html.
[400] Schott, *op. cit.,* p. 138.
[401] *Ibid*.
[402] IMF and WB, "Financial Intelligence Units: An Overview," *International Monetary Fund Publication Services*, Washington D.C., July 23, 2004, https://www.imf.org/external/pubs/ft/fiu/fiu.pdf.
[403] Schott, *op. cit.,* p. 138.

The WB and the IMF have expanded the types of technical assistance (TA) they offer to countries over time so that they can improve their internal AML and CFT frameworks. They include: creating AML/CFT legislation and regulations that adhere to global best practices; putting laws, regulations, policies, and procedures into effect by financial sector supervisors and other similarly qualified authorities in charge of enforcing AML/CFT measures; the development of training and awareness programmes to address AML/CFT problems in the public and private sectors; building of legal frameworks for financial intelligence units (FIUs) that adhere to worldwide best practices; production of computer-based training materials; partnership with other parties in international training programmes.[404]

The IMF and WB's commitment is still more than essential and is evolving quickly. The cornerstone of their strategy in the war on terrorism and money laundering continues to be FATF recommendations. In addition, when new digital frontiers like cryptocurrencies have emerged, the IMF and WB have expanded their activities. Because cryptocurrency transactions are decentralised and frequently anonymous, they could be a desirable tool for illegal activity. The IMF and WB have taken steps to comprehend, monitor, and provide recommendations on successfully addressing these difficulties while continuing to engage with the UN, FATF, and other organisations. Both bodies are aware of the changing financial landscape and the new vulnerabilities that this brings.

### 5.3 Future Challenges and Opportunities

As the world community tries to rapidly find answers to counteract any new global threats, emerging risks continue to appear. While constantly considering potential risks and vulnerabilities, the IMF and the WB have been detailing their shared AML/CFT approach for years. The most well-known of the biggest dangers is undoubtedly terrorism's use of social media. Terrorist groups aggressively employ social media to disseminate their message and connect with supporters worldwide. To raise the money needed for their criminal actions, terrorists frequently use social media sites such as Facebook, Instagram, and Twitter for crowdfunding. Indeed, social networks are particularly dangerous because extremist and terrorist groups can use them to disseminate propaganda, recruit new members, and radicalise people. They may easily connect with a broad audience, including children and others prone to being hooked, using compelling content and powerful messages. The U.S. government revised its National Risk Assessment on Terrorist Financing in 2018, noting the dangers related to

[404] *Ivi*, p 140.

social media use by several significant international terrorist organisations, including *ISIS*, *Al-Qaeda in the Arabian Peninsula* (AQAP), and *Al-Shabaab*.[405] The MENAFATF and the APG jointly issued a study on this subject in 2019. This investigation highlights how easy it is to create new personas and accounts while also being simple for these terrorist organisations to track their actions. Governments need to develop new, quicker methods to block suspected profiles.[406] The payment method for many of these transactions is cryptocurrency, although most still use bank transfers, prepaid cards, or other more conventional ways. Other technology-related services that do not specifically deal with social media include anonymous hosting services that allow users to host websites secretly or other programs like Telegram that provide extensive encryption features out of the reach of law enforcement.[407]

One emerging and less well-known risk is the exploitation, trade, and trafficking of natural resources to finance terrorism. This kind of natural resources, which for instance may include metals like gold, silver, diamonds, and copper, represent a significant source of income for terrorists who seek to integrate themselves into the legitimate economic sectors of natural resources to obtain regular income and diversify their funding sources. Through Resolutions 2195 (2014), 2462 (2019), and 2482 (2019), the UNSC has expressed its concerns regarding the use of sources of illegal exploitation and trafficking of natural resources by organised crime organisations, terrorist groups, and other groups that support them.[408] Additionally, the FATF stated in 2021 that environmental crimes occurred to aid in financing terrorist activities. The areas affected, which are most vulnerable to climate disaster, suffer from the misuse of environmental resources. For instance, in the Horn of Africa, where extreme weather events occur more frequently, this significantly impacts food security by depleting water supplies and destroying crops.[409] Competition for natural resources, which can turn violent when used by terrorist organisations, is another harmful component of environmental crimes.

The fact that many states fail to give unlawful exploitation of natural resources the attention it deserves is one of the most concerning elements. In this context, on June 22, 2022, the CTED published the *Trends Alert* in compliance with Security Council Resolution 2395 of

---

[405] "National Terrorist Financing Risk Assessment," *U.S. Department of the Treasury*, 2018, https://home.treasury.gov/system/files/136/2018ntfra_12182018.pdf.
[406] APG and MENAFATF, "Social Media and Terrorism Financing Report," *Asia/Pacific Group on Money Laundering*, 23 January 2019, https://apgml.org/methods-and-trends/news/details.aspx?pcPage=1&n=1142.
[407] Tom Keatinge and Florence Keen, "Social Media and (Counter) Terrorist Finance: A Fund – Raising and Disruption Tool," *Studies in Conflict & Terrorism* 42, no. 1-2 (2019): 178-205, https://doi.org/10.1080/1057610X.2018.1513698.
[408] S/RES/2195 (2014), preamble; S/RES/2462 (2019), preamble; S/RES/2482 (2019), para. 14. See also preamble and paras. 13 and 15 (e).
[409] United Nations High Commissioner for Refugees (UNHCR), "Somalia: Internal Displacements Monitored by Protection and Return Monitoring Network (PRMN)", 2021, https://data.unhcr.org/en/documents/details/88558.

2017.[410] The goal of the *Trends Alert*, which the CTED creates, is to inform and update the Security Council's Counter-Terrorism Committee and other UN bodies. To guarantee that Security Council decisions are efficiently implemented, these cautions concentrate on specific and topical challenges, relying on the CTED's continuing interaction with member states. A few examples in CTED *Trends Alert* illustrate environmental crimes. *ISIS*, for example, despite having recently gained control of several territories between the Syrian Arab Republic and Iraq, reduced access to oil and natural gas through "extortion of oil networks in the Eastern Syrian Arab Republic as late as 2021."[411] Furthermore, terrorist organisations like *Boko Haram* and *Islamic State West Africa Province* (ISWAP) "have also been reported to profit from trade in smoked fish and red pepper or to extort communities involved in farming and fishing activities" in the Lake Chad Basin, which is primarily based on fishing and agriculture. [412]

Moreover, Boko Haram also employs wildlife trafficking as a source of funding.[413] This commerce involves capturing and selling wild animals and the items that can be made from them, such as horns, skins, and bones. Given that numerous species, including tigers, are in danger of extinction, this trade endangers biodiversity. The trafficking of precious metals and minerals is another way of terrorist funding covered by CTED. Mali is one of the areas that terrorists are most interested in. Burkina Faso and Niger.[414] The management of mines from which minerals and precious metals are extracted and sold on the black market or even legally through a network of intermediaries is typically how terrorists obtain their funding. Terrorist organisations can further conceal their funding sources by reinvesting the money they make in other legitimate mining firms or other sectors of the economy.[415]

Cryptocurrency use gives terrorists an essentially anonymous avenue to fund themselves in addition to social media and other technology tools, making it much harder for law enforcement organisations to identify and stop these money flows. These organisations make a sizable amount of money from the illegal trade in natural resources, including precious metals and minerals, encrypted messaging services, and anonymous hosting services. This allows them

[410] UNSC Res 2395 (21 December 2017) UN Doc S/RES/2395.

[411] *Ibid*.

[412] Etienne Tabi Mbang, "Raising Funds for Terrorists Purposes Through Exploitation of Natural Resources," (2021) Joint special meeting of the Counter-Terrorism Committee and the 1267/1989/2253 ISIL (Da'esh) and Al-Qaida Sanctions Committee on the latest terrorism- financing trends and threats, as well as the implementation of Security Council resolution 2462 (2019). https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/gabac.pdf.

[413] See e.g., the analysis of the United States Institute of Peace: https://www.usip.org/events/wildlife-poaching-and-trafficking-combating-source-terrorist-funding ; National Geographic, "How Killing Elephants Finances Terror in Africa" (2015): https://www.nationalgeographic.com/tracking-ivory/article.html. See also the record of the Hearing before the Subcommittee on Terrorism, Non-Proliferation and Trade of the Committee on Foreign Affairs of the U.S. House of Representatives, April 2015: https://www.govinfo.gov/content/pkg/CHRG-114hhrg94308/html/CHRG-114hhrg94308.htm.

[414] *Ibid*.

[415] *Ibid*.

to enter reputable industries and diversify their funding sources. Through sustained international cooperation, technology to monitor and track these actions, and new rules, it is possible to think of ways to limit the financing of terrorism and money laundering despite the complexity and constant variation of terrorist financing tactics.

### 5.4 Limitations and Future Research Avenues

This Thesis has highlighted several significant approaches that various international organisations and jurisdictions use in assessing the risk associated with using cryptocurrencies and *hawāla* in the context of terrorist financing and money laundering. However, despite these promising results, this study, is not exempt from limitations, however useful in suggesting future research. For instance, the legal landscape in this field is continuously changing, so a strategy that proves effective now might become different. Additionally, this Thesis is based on qualitative research design consisting of three in-depth interviews conducted among experts in the field. Despite this preliminarily findings, future research may try to enrich the sample, by collecting expert participants from different cultures, and international settings. Thus, future research, may also add valuable and interesting highlights, by incorporating more insights deriving by respondents from other geographical locations, or by proposing quantitative-based studies aimed to shed light on hidden variables feeding the unethical usage of crypto-based technologies for illicit money exchange. The relevance of this Thesis in the context of the research landscape also needs to be recognised, notwithstanding the limitations that have been emphasised. In a world that is becoming increasingly globalised, it is essential to comprehend the risks and difficulties associated with using cryptocurrency and *hawāla* to finance terrorists and commit money laundering.

# CONCLUSION

In the current era characterised by a constant global connection and the predominance of technology, the strategies of terrorist organisations consequently evolve, negatively benefiting of such technologies by merging elements of the old with the new frontiers of the digital.

The current financial landscape is characterised by the growing use of informal systems such as *hawala*, with ancient roots and emerging cryptocurrencies, by terrorists challenging the authorities' controls. Terrorist organisations, such as the organisation of a terrorist attack, need funding to support themselves and achieve their objectives. The terrorist financing process is not limited to supporting organisations. The process of raising and using money is more complex than expected. The sources or purposes of finances are frequently highlighted, but the transfer methods of those funds have begun to receive a greater significance. Because of technological advances, transactions have become more complex, untraceable, and frequently hidden. In addition, several variables, including volume, risk, convenience, simplicity, costs, and speed, influence the choice of transfer route. Both official and informal transfer services share these characteristics. Conventional channels include bank transfer services. IFTs serve as an intermediary for people who need to transmit money across borders or even inside the same country, and they have their roots in the culture of the area of origin. They are based on a fabric of trust and personal relationships. IFT is known as *Fei-Ch'ien* in China, whereas *hawāla* is used in Asia and the Middle East. This system is one of the most well-known: It is frequently used to transfer money for terrorist purposes because it exhibits the qualities needed to make it a valuable tool for terrorist organisations, including speed, cost savings over conventional banking methods, usability in challenging environments like war zones, and, most importantly, anonymity. By considering Afghanistan as a scenario, *hawāla* not only allow to move money to a nation with a virtually nonexistent banking system, but it is also closely associated with the drug trade, which accounts for a sizeable share of all monetary transfers. To date, nearly 60% of all money transactions go to the Afghan drug trade.

Alongside the financing of terrorism, another illegal phenomenon emerges, money laundering. This is based on three stages: Placement, the first stage in which funds from unlawful activity are injected into the financial system; layering, which tries to conceal the source of funds' illicit income; and integration, which refers to the integration of recycled funds into the global economy. Johnson pointed out that the former is essential in order to fight the war against terrorism, after the 9/11 terrorist attacks, not because they are two completely different processes.

The introduction of BTC in 2008, which constituted an unparalleled advance in the legal and illegal financial landscape, marked the beginning of a genuine economic revolution. Although a radical innovation, cryptocurrencies have many characteristics in common with the *hawāla* system, including secrecy, lower costs, trust, and, most importantly, effective resistance to conventional control mechanisms. Taking advantage of cryptocurrencies' digital character, specific terrorist organisations have integrated both systems due to their complementary nature or, in other circumstances, have entirely replaced *hawāla* with them. The UN, FATF, the IMF, and other international organisations are stepping up their efforts to comprehend, track, and, when possible, regulate these flows. In addition to stopping terrorist attacks, the goal is to safeguard the reliability of the world's financial institutions. These organisations have been devoted to the war against terrorism ever since the combined AML/CFT policy was adopted. However, these tactics are frequently upgraded to stay ahead of new dangers that need more precise and potent comparison tools. It may have seemed unimaginable a few years ago that a system as old as *hawala*, utilised for legal purposes, could become the ideal weapon for terrorists. On the other hand, technology enables innovation and the discovery of methods to simplify every part of life, such as transmitting money more straightforwardly. Still, if misused, it can result in the completion of illegal actions.

Thus, by considering the goal of this Thesis delve into the role of cryptocurrencies and *hawāla* in facilitating money laundering and the financing of terrorism, and the potential of cryptocurrencies to exceed the *hawāla* in the future. The qualitative research performed on the basis of the three in-depth interviews (see Chapter IV), demonstrate that despite the evident efficiency of *hawāla*, cryptocurrencies, which are built on blockchain technology, offer more resilience, eliminating the need for intermediaries and increasing the difficulty of intercepting or blocking transactions. Additionally, global integration and digitalisation are accelerating the use of cryptocurrency-based technology for everyone. The financial environment will undoubtedly continue to change in the years to come, and terrorist organisations will use a wide range of methods. Even though both *hawāla* and cryptocurrencies are already used to finance terrorism, technological advancements appear to be driving terrorist outfits to adopt cryptocurrencies more frequently. The *hawāla* may still exist, but with the help of technology, cryptocurrencies are influencing how terrorists will be funded in the future. To create a safer world, it is now essential for international authorities to comprehend, monitor, and, where possible, adapt these new dynamics.

# REFERENCES


"Abu Dhabi establishes dedicated court to tackle money laundering and tax evasion." *The National UAE*. November 10, 2020. https://www.thenationalnews.com/uae/courts/abu-dhabi-establishes-dedicated-court-to-tackle-money-laundering-and-tax-evasion-1.1109308.

Ali Abbas J., Abdulrahman Al-Aali, and Abdullah Al-Owaihan, "Islamic Perspectives on Profit Maximasation," *Journal of Business Ethics* 117, (November 2012): 467-475, https://doi.org/10.1007/s10551-012-1530-0.

APG and MENAFATF. "Social Media and Terrorism Financing Report." *Asia/Pacific Group on Money Laundering*, 23 January 2019. https://apgml.org/methods-and-trends/news/details.aspx?pcPage=1&n=1142.

BaFin (2002). https://www.bafin.de/EN/Homepage/homepage_node.html.

BaFin checklist "Authorisation as a credit institution" of 20.08.2017, amended on 14.11.2017, available at: https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/2017/rs_1709_marisk_ba.html.

Bank Secrecy Act, 31 U.S.C. § 5311 et seq. (1970).

Belk, Russell, Eileen Fischer and Robert V. Kozinets. *Qualitative Consumer and Marketing Research*. Los Angeles: SAGE, 2012.

Black Money (Undisclosed Foreign Income and Assets) and Imposition of Tax Act, § 22 (2015).

Boku and Juniper Research, *2021 Mobile Wallets Report*, San Francisco, 2021: 9, https://www.paymentscardsandmobile.com/wp-content/uploads/2022/02/Mobile-Wallets-Report-2021.pdf.

Borlini, Leonardo. "The Financial Action Task Force: An Introduction." *Anti-Corruption Resource Centre*, January 2015. https://www.u4.no/publications/the-financial-action-task-force-an-introduction.pdf.

Bouveret, Antoine and Vikram Haksar. “What are cryptocurrencies.” *Finance and Development* 55 no. 2 (2018): 26-29.

Brauer, Jurgen. “The Terrorist Firm: Innovation, Substitution and Productivity.” in *Fighting Terrorism: Financial and Economic Aspects*, *Occasional Paper NATO Defence College.* (2004).

Brian, Nibley. “Bitcoin Price History: 2009 – 2023,” *Social Finance Inc*. March 1, 2023. https://www.sofi.com/learn/content/bitcoin-price-history/.

Buchanan, Bonnie. “Money Laundering – a Global Obstacle.” *Research in International Business and Finance*, 18, no. 1 (2004): 115-127.

Buddenberg, Doris and William A. Byrd (editors). *Afghanistan’s Drug Industry: Structure, Functioning, Dynamics, and Implications for Counter-Narcotics Policy*. UNODC and the World Bank. 2006, p.15.

Burns, John F. “Riot Scars Are Gone, but Bombay Is Still Healing.” *New York Times*, April 17, 1994. https://www.nytimes.com/1994/04/17/world/riot-scars-are-gone-but-bombay-is-still-healing.html.

Bush, W. George. “A Joint Session of Congress and the American People.” September 20, 2001. https://www.whitehouse.gov/briefing-room/.

Cabinet Decision No. 10 (2019) concerning the Executive Regulations of Federal Decretal-Law No. 20 (2018) on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations.

CBUAE, *Registered Hawala Providers Regulation*, Circular No. 24/2019.

CBUAE. *OUTREACH EVENT on the AML/CFT Guidance for Registered Hawala Providers*, 26 August 2021.

Central Bank of Bahrain. *Combating the Financing of Terrorism: Guidance for Financial Institutions*, Bahrain, November 2020.

Chainanalysis Team. “Crypto Money Laundering: Four Exchange Deposit Addresses Received Over $1 Billion in Illicit Funds in 2022.” *Chainanalysis*, January 26, 2023. https://www.chainalysis.com/blog/crypto-money-laundering-2022/.

Chainalysis Team. “Hamas’ Al-Qassam Brigades Announces End of Cryptocurrency Donation Efforts.” *Chainalysis*, April 27, 2023. https://www.chainalysis.com/blog/hamas-al-qassam-brigades-cryptocurrency-donations-shutdown/.

Chaum, David. “Blind Signature for Untraceable Payments.” In: Chaum, D., Rivest R.L. and Sherman, A.T., Eds., Advances in Cryptology Proceedings of Crypto 82, Plenum (Springer-Verlag), New York, 199-203. https://sceweb.sce.uhcl.edu/yang/teaching/csci5234WebSecurityFall2011/Chaum-blind-signatures.PDF.

Cherniavskyi, Serhii S., Bohdan M. Holovkin, Yuliia M. Chornous, Vasyl Y. Bodnar, and Ilona V. Zhuk. “International Cooperation in the Field of Fighting Crime: Directions, Levels and Forms of Realization.” *Journal of Legal, Ethical and Regulatory Issues* 22, no. 3 (2019): 1–11. https://www.abacademies.org/articles/international-cooperation-in-the-field-of-fighting-crime-directions-levels-and-forms-of-realization-8346.html.

Clarke, Colin P. *Terrorism, Inc.: the financing of terrorism, insurgency, and irregular warfare*. Praeger Security International, 2015, 109; Adam Dolnik, Anjali Bhattacharjee, ‘Hamas: suicide bombings, rockets, or WMD?’ *Terrorism and Political Violence*, 2002. 14:3:13.

Cohn, Cindy, Peter Eckersley, Rainey Reitman and Seth Schoen. “EFF Will Accept Bitcoins to Support Digital Liberty.” *Electronic Frontier Foundation*. May 17, 2013. https://www.eff.org/it/deeplinks/2013/05/eff-will-accept-bitcoins-support-digital-liberty.

Commodity Futures Trading Commission (2021). CFTC Orders Tether and Bitfinex to Pay Fines Totaling $42.5 Million. CFTF. https://www.cftc.gov/PressRoom/PressReleases/8450-21.

Council Directive 2017/541/EC of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA (OJ L 88/6), 31 March 2017, 12.

Crenshaw, Martha. *Explaining Terrorism: Causes, Process and Consequences.* 1st ed, Oxford: Routledge, 2011.

Daudi, Adil Anwar. "The Invisible Bank: Regulating the Hawala System in India, Pakistan and the United Arab Emirates." *Indiana International & Comparative Law Review* 15, no. 3 (2005): 622. https://research.amanote.com/publication/EZFX1XMBKQvf0Bhi4Jlk/the-invisible-bank-regulating-the-hawala-system-in-india-pakistan-and-the-united-arab.

Da Silva Filho, Tito Nicias Teixeira. "IMF Working Paper: No Easy Solution A Smorgasbord of Factors Drive Remittance Costs," *International Monetary Fund* 21, 199 (July 2021): 8-9. https://doi.org/10.5089/9781513592954.001.A000.

De Robespierre, Maximilien. *Virtue and Terror.* Reviewed by Slavoj Zizek, edited by Jean Ducange and translated by John Howe. Brooklyn: Verso Books, 2017.

Dion-Schwarz, Cynthia, and David Manheim and Patrick B. Johnston, "Terrorist Use of Cryptocurrencies: Technical and Organisational Barriers and Future Threats," (Santa Monica, Calif: *Rand Corporation*, 2019): 13, https://rusi.org/explore-our-research/publications/occasional-papers/bit-bit-impacts-new-technologies-terrorism-financing-risks.

Directive (EU) 2015/849 of the European Parliament and of the Council of May 20, 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC—Official Journal of the European Union (L 141/73).

Doshi, Vidhi. "India Withdraws 500 and 1000 Rupee Notes in Effort to Fight Corruption." *The Guardian*. November 8, 2016. https://www.theguardian.com/world/2016/nov/08/india-withdraws-500-1000-rupee-notes-fight-corruption.

Dulce M. Redin, Reyes Calderon and Ignacio Ferrero, "Exploring the Ethical Dimension of "Hawala," *Journal of Business Ethics* 124, no. 2 (2014): 328, https://www.jstor.org/stable/24033272.

El Qorchi, Mohammed and International Monetary Fund. "Hawala: How does this Informal Funds Transfer System Work, and Should it be regulated?" *Finance & Development* 39, no. 4 (2002). https://www.imf.org/external/pubs/ft/fandd/2002/12/elqorchi.htm.

El Qorchi, Mohammed, Samuel Munzele Maimbo, and John F Wilson. "Informal Funds Transfer Systems: An Analysis of the Informal Hawala System." *IMF-World Bank Paper*, no. 222 (August 2003): 30-64.

Elliot, Francis and Gary Duncan. "Chancellor Alistair Darling on Brink of Second Bailout for Banks." *The Times*, January 3, 2009. https://www.thetimes.co.uk/article/chancellor-alistair-darling-on-brink-of-second-bailout-for-banks-n9l382mn62h.

European Union Agency for Criminal Justice Cooperation. *Eurojust Report on Money Laundering*. (Luxembourg, Publication Office of the European Union, 2022). https://www.eurojust.europa.eu/sites/default/files/assets/eurojust-report-money-laundering-2022.pdf.

Fanusie, Yaya J. and Tom Robinson, "Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services." *Foundation for Defense of Democracies and Elliptic* (12 Jan. 2018): 1–7. https://doi.org/10.1080/00431672.2019.1538758.

FATF (2003-2004). *FATF 40 Recommendations*. FATF, Paris. https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Standards%20-%2040%20Recommendations%20rc.pdf.coredownload.pdf.

FATF and GAFI (2006). *Trade Based Money Laundering*. FATF, Paris. https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Trade%20Based%20Money%20Laundering.pdf.coredownload.pdf.

FATF and MENAFATF (2015). *Money Laundering through the Physical Transportation of Cash*. FATF, Paris, France and MENAFATF, Manama, Bahrain, 26. https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/money-laundering-through-transportation-cash.pdf.coredownload.pdf.

FATF (2019). *Terrorist Financing Risk Assessment Guidance.* FATF, Paris. https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Terrorist-Financing-Risk-Assessment-Guidance.pdf.coredownload.pdf.

FATF (2012-2023). *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation*, FATF, Paris. https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf.

Federal Decretal-Law No. 20 (2018) on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations.

Federal Law No. 10 (1980) concerning the Central Bank, monetary system, and organisation of banking.

Feyen, Erik H.B., Yusaku Kawashima and Raunak Mittal. "Crypto-Assets Activity Around the World: Evolution and Macro-Financial Drivers." *World Bank Policy Research Working Paper 9962*, March 2022. https://doi.org/10.1596/1813-9450-9962.

Foley, Sean, Jonathan R. Karlsen and Talis J. Putnins. "Sex, Drug, and Bitcoin: How Much Illegal Activity is Financed through Cryptocurrencies?" *The Review of Financial Studies* 32, no. 5. (May 2019): 1798-1853, https://doi.org/10.1093/rfs/hhz015.

Foreign Exchange Regulation Act, § 46 (1973).

Foreign Exchange Management Act, § 42 (1999).

Foreign Exchange Regulation Ac, art. 8.

Foreign Exchange Regulation Ac, art. 9.

Forest, James J. F. "Crime-Terror Interactions in Sub-Saharan Africa." *Studies in Conflict & Terrorism* 45, no. 5-6 (17 October 2019): 372-375. https://doi.org/10.1080/1057610X.2019.1678881.

Freeman, Michael. "The Sources of Terrorist Financing: Theory and Typology." Journal Studies in Conflict & Terrorism 34, no. 6 (2011): 461.

Freeman, Michael and Moyara Ruehsen, "Terrorism Financing Methods: An Overview." *Perspectives on Terrorism* 7, no. 4 (2013): 5-15, http://www.terrorismanalysts.com/pt/index.php/pot/article/view/279/html.

Goldman, Zachary K., Ellie Maruyama, Elizabeth Rosenberg, Edoardo Saravalle, and Julia Solomon-Strauss. "Virtual Currency Abuse in the Future: Criminals vs. Terrorists." *TERRORIST USE OF VIRTUAL CURRENCIES: Containing the Potential Threat*. Center for a New American Security, 2017. http://www.jstor.org/stable/resrep06423.7.

GP Bullhound, und The Motley Fool, und Investing.com. "Number of cryptocurrencies worldwide from 2013 to August 2023. Chart, Statista. August 9, 2023. https://www-statista-com.ezprimo1.runi.ac.il/statistics/863917/number-crypto-coins-tokens/.

GwG (1993). https://www.bafin.de/SharedDocs/Downloads/EN/Aufsichtsrecht/dl_gwg_en.pdf?__blob=publicationFile&v=1.

Haslerud, Gjermund and Bent Sofus Tranoy. *Fighting Terrorist Finance – Issues, Impacts and Challenges*. Kjeller: Norwegian Defence Research Establishment, 2005. https://ffi-publikasjoner.archive.knowledgearc.net/bitstream/handle/20.500.12242/1874/05-02100.pdf.

Hernandez- Coss, Raul. "Regulatory Frameworks for Hawala and Other Remittance System." Paper presented to the Second International Conference on Hawala, Abu Dhabi, 3-5 April 2004. https://www.imf.org/external/pubs/nft/2005/hawala/hawala.pdf.

Hoffman, Bruce. "Change and Continuity in Terrorism," *Studies in Conflict & Terrorism* 24, no. 5 (2001): 417-429. https://dx.doi.org./10.1080/105761001750434268.

IMF and WB. "Financial Intelligence Units: An Overview," *International Monetary Fund Publication Services*, Washington D.C., July 23, 2004. https://www.imf.org/external/pubs/ft/fiu/fiu.pdf.

Institute for Economics & Peace. *Global Terrorism Index 2023: Measuring the Impact of Terrorism*. (Sydney: March 2023). https://www.visionofhumanity.org/resources/.

*International Convention for the Suppression of the Financing of Terrorism*, G.A. Res. 54/109, U.N. GAOR, 54th Sess., 76th mtg., Supp. No. 49, U.N. Doc. A/Res/53/108 (1999), https://treaties.un.org/doc/db/terrorism/english-18-11.pdf.

International Monetary Fund. "Abu Dhabi Declaration on Hawala." Declaration presented to the First International Conference on Hawala, Abu Dhabi, 16 May 2002. https://digitallibrary.un.org/nanna/record/467698/files/A_56_993-EN.pdf?withWatermark=0&withMetadata=0&version=1&registerDownload=1.

IOM, *Remittances to Afghanistan are Lifelines: They are Needed More than Ever in a Time of Crisis*, United Nations (2020) https://weblog.iom.int/remittances-afghanistan-are-lifelines-they-are-needed-more-ever-time-crisis.

Jacobson, Michael. "Terrorist Financing and the Internet." *Studies in Conflict & Terrorism* 33, no. 4 (2010): 353–63.

Johnson, Jackie. "Is the Global Financial System AML/CFT Prepared?" *Journal of Financial Crimes* 15, no. 1 (2008): 7-14. http://dx.doi.org/10.1108/13590790810841662.

Johnston, R. Barry. "Regulatory Frameworks for Hawala and Other Remittance System." Paper presented to the First International Conference on Hawala, Abu Dhabi, 15-16 May 2002. https://www.imf.org/external/pubs/nft/2005/hawala/hawala.pdf.

Jongman, Albert J. and Alex P. Schmid. *Political Terrorism: A New Guide to Actors, Authors, Concepts, Data Bases, Theories, and Literature.* 1st ed, New York: Taylor & Francis Group, 2005.

Jost, Patrick M. and Harjit Singh Sandhu. *The Hawala Alternative Remittance System and its Role in Money Laundering*. Lyon: Interpol General Secretariat, 2000. https://www.assetsearchblog.com/wp-content/uploads/sites/197/2013/06/FinCEN-Hawala.pdf.

Keatinge, Tom and Florence Keen, "Social Media and (Counter) Terrorist Finance: A Fund – Raising and Disruption Tool." *Studies in Conflict & Terrorism* 42, no. 1-2 (2019): 178-205. https://doi.org/10.1080/1057610X.2018.1513698.

Kerr, David S., Karen A. Loveland, Katherine Taken Smith, and Lawrence Murphy Smit. "Cryptocurrency Risks, Fraud Cases, and Financial Performance." *Risks* 11, no. 51 (February 23, 2023): 2. https://doi.org/10.3390/risks11030051.

Khalil, Shamaimaa "Pakistan Taliban: Peshawar School Attack Leaves 141 Dead." *BBC News.* December 16, 2014. https://www.bbc.com/news/world-asia-30491435.

KWG § 54 (1998).

Martis, Genesis J. "A Guidance to Understand Hawala and to Establish the Nexus with Terrorist Financing." *Association of Certifed Anti-money Laundering Specialists.* March 18, 2018. https://www.acams.org/en/media/document/9406.

Matei, Gheorghe. "Blockchain Tecnology – Support for Collaborative Systems." *Informatica Economica* 24, no. 2 (2020): 15-25. http://dx.doi.org/10.24818/issn14531305/24.2.2020.02.

McAuliffe, Marie and Anna Triandafyllidou. *World Migration Report 2022*. Geneva: International Organization for Migration (IOM) (eds.), 2021. https://publications.iom.int/books/world-migration-report-2022.

"Money Laundering." United Nations Office on Drugs and Crime. Accessed July 21, 2023. https://www.unodc.org/unodc/en/money-laundering/overview.html.

National Action Plan, https://nacta.gov.pk/nap-2014/.

"National Terrorist Financing Risk Assessment." *U.S. Department of the Treasury*, 2018. https://home.treasury.gov/system/files/136/2018ntfra_12182018.pdf.

Norton, Simon and Paula Chadderton. "*Detect, Disrupt and Deny: Optimising Australia's Counterterrorism Financing System*. Australian Strategic Policy Institute, December 2016. https://ad-aspi.s3.ap-southeast-2.amazonaws.com/import/SR98_countering_terrorism_funding.pdf?VersionId=B5pF0o5WRfLNUJ6BfG5fuqzkona9UrI5.

Office of Public Affairs. "Western Union Admits Anti Money Laundering and Consumer Fraud Violations, Forfeits $586 Million In Settlement With Justice Department and Federal Trade Commission." U.S. Department of Justice, accessed July 11, 2023, https://www.justice.gov/opa/pr/western-union-admits-anti-money-laundering-and-consumer-fraud-violations-forfeits-586-million.

Oftedal, Emilie. "The Financing of Jihadi terrorist cells in Europe." *Norwegian Defence Research Establishment FFI-rapport 2014/02234* (16 January 2015): 16-20. https://www.ffi.no/en/publications-archive/the-financing-of-jihadi-terrorist-cells-in-europe.

Oner, Ceyda. "Inflation: Prices on the Rise." *Finance & Development* 47, n. 001 (March 2010): 31. https://0-doi-org.library.svsu.edu/10.5089/9781451922257.022.A017.

Passas, Nikos. "Hawala and Other Informal Value Transfer Systems: How to Regulate Them?" *Risk Management* 5, no. 2 (2003): 49–59. http://www.jstor.org/stable/3867818.

Passas, Nikos. "Informal Value Transfer Systems and Criminal Organizations; A Study into So-Called Underground Banking Networks." *SSRN Electronic Journal*, 1999. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1327756.

Passas, Nikos. "Informal Value Transfer Systems, Terrorism and Money Laundering." *SSRN Electronic Journal, 2003*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1327839.

Poulain, Jean-Guillame and Julien Reynald. “IMF Working Paper: IMF Lending in an Interconnected World.” *International Monetary Fund*, 17. no. 155 (2017): 8-15. https://doi.org/10.5089/9781484305867.001.

Radil, Steven M. “Global Patterns of Terrorism, 1998-2005: A Geographic Overview and Root Cause Analysis,” Dissertation. (University of Colorado at Colorado Springs, 2006).

Rapoport, David C. “The Four Waves of Modern Terrorism.” In *Attacking Terrorism: Elements of a Grand Strategy*, edited by Audrey Kurth Cronin and James M. Ludes, 46-73. Washington, DC: Georgetown University Press, 2004.

Rapoport, David C. “The Four Waves of Rebel Terror and September 11.” In *Anthropoetics* 8, no. 1 (Spring/Summer 2002): 1-16.

Ratha, Dilip Sonia Plaza, Eung Ju Kim, Vandana Chandra, Nyasha Kurasha, and Baran Pradhan (June 2023). Migration and Development Brief 38: Remittances Remain Resilient But Are Slowing. KNOMAD - World Bank, Washington, DC. https://knomad.org/sites/default/files/publication-doc/migration_development_brief_38_june_2023_0.pdf.

Raveenran, K. “U.A.E. Takes Unprecedent Action on Hawala.” *The Daily Star*. October 25, 2003, at 5. http://goldismoney.info/forums/archive/index.php/t-4556.html.

Raza, MS, Muhammad Fayyaz and Haseeb Ijaz. “The Hawala System in Pakistan: A Catalyst for Money Laundering & Terrorist Financing.” *Forensic Research and Criminology International Journal* 5 no.4 (2017): 368-369. 10.15406/frcij.2017.05.00167.

Reimer, Stephen and Matthew Redhead, “Bit by Bit: Impacts of New Technologies on Terrorism Financing Risks,” *Royal United Services Institute for Defence and Security Studies, RUSI Occasional Paper* (April 2022): 9-10, https://rusi.org/explore-our-research/publications/occasional-papers/bit-bit-impacts-new-technologies-terrorism-financing-risks.

Resolution No. 123/7/92 regarding the regulation of the money changing business in the U.A.E.
Resolution No. 123/7/92 regarding the regulation of the money changing business in the U.A.E.

Resolution No. 31/2/1986 regarding the regulation of money changing business in the U.A.E.

Resolution No. 31/2/1986 regarding the regulation of money changing business in the U.A.E.

Ridwan, Raihan Zahirah Mauludy. "The Utilisation of Cryptocurrencies by the Terrorist Group as an Alternative Way of Hawala for Illicit Purposes." *University Katolik Parahyangan* 2, (2018): 5. https://journal.unpar.ac.id/index.php/Sentris/article/view/4183/3101.

Roach, Kent. *Due Process and Victims' Rights: The New Law and Politics of Criminal Justice*. 1st ed, Toronto: University of Toronto Press, 1999.

Rosner, Marcel T., and Andrew Kang. "Understanding and Regulating Twenty-First Century Payment Systems: The Ripple Case Study." *Michigan Law Review* 114, no. 4 (2016): 649–81. http://www.jstor.org/stable/24770875.

Roth, John, Douglas Greenburg and Serena Wille. *Monograph on Terrorist Financing*. National Commission on Terrorist Attacks Upon the United States, 2004. https://govinfo.library.unt.edu/911/staff_statements/911_TerrFin_Monograph.pdf.

Savrul, Mesut and Incekara, Ahmet. "The Effect of Globalisation on International Trade: The Black Sea Economic Cooperation Case" paper presented to the *International Conference on Eurasian Economies*, (9-11 Sept. 2015): 88-94.

Schott, Paul A. *Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism*. Washington D.C.: The World Bank, 2003.

Sestino, Andrea, Luca Giraldi, Elena Cedrola, Seyedeh Zahra Zamani and Gianluigi Guido. "The Business Opportunity of Blockchain Value Creation among the Internet of Value." *Global Business Review* (2022). https://doi.org/10.1177/09721509221115012.

Seth, Shivangi and Gatra Priyandita. "Combating the Cyber Heists that are Costing the Global Economy." *Australian Strategic Policy Institute* (June 2023). https://www.aspistrategist.org.au/combating-the-cyber-heists-that-are-costing-the-global-economy/.

StGB (1998), https://www.iuscomp.org/gla/statutes/StGB.htm#86a.

Suroush, Qayoom. "Gray Cash: How the U.S. and the Taliban Have Tried and Failed to Fix Afghanistan's Informal Banking System." *New America*. September 14, 2022. https://www.newamerica.org/future-frontlines/briefs/gray-cash-how-the-us-and-the-taliban-have-tried-and-failed-to-fix-afghanistans-informal-banking-system/.

Sustainable Development Goals. United Nations (2015). https://www.undp.org/sustainable-development-goals.

Szabo, Nick. "Bit Gold." *Unenumerated*, December 27, 2008. http://unenumerated.blogspot.com/2005/12/bit-gold.html.

Szabo, Nick. "Money, Blockchains, and social scalability." *Unenumerated*, 2021. https://doi.org/10.1596/1813-9450-9962.

Tabi Mbang, Etienne. "Raising Funds for Terrorists Purposes Through Exploitation of Natural Resources." (2021). https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/gabac.pdf.

Tambe, Nikita and Aashika Kain. "Advantages and Disadvantages of Cryptocurrencies in 2023." *Forbes Advisor*, June 14, 2023. https://www.forbes.com/advisor/in/investing/cryptocurrency/advantages-of-cryptocurrency/.

Teichmann, Fabian and Chiara Wittmann. "The Abuse of Hawala Banking for Terrorist Financing in German-speaking Countries." *Journal of Money Laundering Control* Vol. ahead-of-print No. ahead-of-print. 10.1108/JMLC-01-2022-0013.

The Anti-Terrorism Act, § 27 (1997).

The Department of Treasury. Office of Inspector General. *Operation Inherent Resolve – Summary of Work Performed by the Department of the Treasury Related to Terrorist Financing, ISIS, and Anti-Money Laundering for First Quarter Fiscal Year 202*. January 4, 2021. https://oig.treasury.gov/sites/oig/files/2021-01/OIG-CA-21-012.pdf.

The Department of Treasury. *Treasury Disrupts International Money Laundering and Sanctions Evasion Network Supporting Hezbollah Financier*. April 18, 2023. https://home.treasury.gov/news/press-releases/jy1422.

The Economic Declaration, Paris, 16 July 1989, G7 Research Group, http://www.g8.utoronto.ca/summit/1989paris/communique/index.html.

The Securities and Exchange Commission Pakistan Act, § 42 (1997).

Tretina, Kat and Michael Adams. "Top 10 Cryptocurrencies of 2023," *Forbes Advisor*. August 22, 2023. https://www.forbes.com/advisor/investing/cryptocurrency/top-10-cryptocurrencies/.

Trozze, Arianna Josh Kamps, Eray Arda Akartuna, Florian J. Hetzel, Bennett Kleinberg, Toby Davies and Shane D. Johnson. "Cryptocurrencies and Future Financial Crime." *Crime Science* 11, no. 1 (2022): 1-37. https://doi.org/10.1186/s40163-021-00163-8.

Tsai, Cheng-Ting, Ja-Ling Wu, Yu-Tzu Lin, and Martin K.-C. Yeh. "Design and Development of a Blockchain-Based Secure Scoring Mechanism for Online Learning." *Educational Technology & Society* 25, no. 3 (2022): 105–21. https://www.jstor.org/stable/48673728. *United Nation Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances*, New York, 20 December 1988, United Nations Doc. E/CONF.82/15, https://www.unodc.org/pdf/convention_1988_en.pdf.

*United Nations Convention against Transnational Organised Crimes*, New York, 12 December 2000, United Nations A/RES/55/25, https://treaties.un.org/doc/source/docs/A_RES_55_25-E.pdf.

United Nations High Commissioner for Refugees (UNHCR). "Somalia: Internal Displacements Monitored by Protection and Return Monitoring Network (PRMN)". 2021, https://data.unhcr.org/en/documents/details/88558.

United Nations Security Council Counter-Terrorism Committee Executive Directorate (CTED), "Informing Security Council Counter-Terrorism Committee's Special Meeting," Mumbai and New Delhi, India (October 28-29, 20229, https://www.un.org/securitycouncil/ctc/news/cted's-tech-sessions-highlights-"threats-and-opportunities-related-new-payment-technologies-0.

U.N. GAOR, 77th Sess., U.N. Doc A/77/718 (February 2, 2023). https://documents-dds-ny.un.org/doc/UNDOC/GEN/N23/033/29/PDF/N2303329.pdf?OpenElement.

U.S. Department of State. *Country Reports on Terrorism*. 2019. https://www.state.gov/reports/country-reports-on-terrorism-2019/.

U.S. States Department of the Treasury Financial Crimes Enforcement Network. *Informal Value Transfer Systems*. March 2003. https://www.fincen.gov/sites/default/files/advisory/advis33.pdf.

UNGA (27th Session) "Questions Relating to International Terrorism" (1972) UN Doc A/8791, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N72/173/18/PDF/N7217318.pdf?OpenElement.

UNGA Res 60/288 (20 September 2006) UN Doc A/RES/60/288.

UNGA Res 77/298 (17 August 2022) UN Doc A/RES/77/298.

UNSC Res 1373 (28 September 2001) UN Doc S/RES/1373.

UNSC Res 2129 (17 December 2013) UN Doc S/RES/2129.

UNSC Res 2178 (24 September 2014) UN Doc S/RES/2178.

UNSC Res 2242 (13 October 2015) UN Doc S/RES/2242.

UNSC Res 2341 (13 February 2017) UN Doc S/RES/2341.

UNSC Res 2354 (24 May 2017) UN Doc S/RES/2354.

UNSC Res 2395 (21 December 2017) UN Doc S/RES/2395.

UNSC Res 2462 (28 March 2019) UN Doc S/RES/2462.

United States v. $4,255,625.39, 551 F. Supp. 314 (S.D. Fla. 1982).

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001. Pub. L. No. 107–56, 115 Stat. 272 (2001). https://www.govinfo.gov/content/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf.

Vaccani, Matteo. "Alternative Remittance Systems and Terrorism Financing." World Bank Working Paper. no. 180, 2010: 7. https://doi.org/10.1596/978-0-8213-8178-6.

Valeri, Marco, Rosario Fondacaro, Cinzia De Angelis, and Andrea Barella. "The Use of Cryptocurrencies for Hawala in the Islamic Finance." *European Journal of Islamic Finance*. October 11, 2020. https://doi.org/10.13135/2421-2172/4145.

Ward, Antonia. "Bitcoin and the Dark Web: The New Terrorist Threat?" *The RAND Blog*, January 22, 2018. https://www.rand.org/blog/2018/01/bitcoin-and-the-dark-web-the-new-terrorist-threat.html.

Wilder, Heidi. “An Overview of the Use of Cryptocurrencies in Terrorist Financing.” *Coinbase Company*, September 21, 2021. https://www.coinbase.com/blog/an-overview-of-the-use-of-cryptocurrencies-in-terrorist-financing.

Wilson Center, The 3/11 Madrid bombings: an assessment after 5 years, 10 April 2009, https://www.wilsoncenter.org/article/the-311-madrid-bombings-assessment-after-5-years.

World Bank Report, *International Development Association Project Appraisal Document on a Proposed Grant in the amount of US$40 Million Equivalent to the Islamic Republic of Afghanistan for a Modernising Afghan State Owned Banks Project*, No: PAD2481, March 6, 2018, https://documents1.worldbank.org/curated/en/644081522461645615/pdf/Afghanistan-Afghan-State-Owned-Banks-PAD-PAD2481-03142018.pdf.

Zarate, Juan C. *Treasury's War: The Unleashing of a New Era of Financial Warfare.* New York: PublicAffairs Book, 2013.

Zimmer, Zac. “Bitcoin and Potosí Silver: Historical Perspectives on Cryptocurrency.” *Technology and Culture* 58, 2 (2017): 307–34. http://www.jstor.org/stable/26406179.