

Cryptocurrency and its Nexus with Money Laundering and Terrorism Financing within the Framework of FATF Recommendations

How to cite this article [Chicago]: Anggriawan, Rizaldy and Muh. Endriyo Susila. "Cryptocurrency and Its Nexus with Money Laundering and Terrorism Financing within the Framework of FATF Recommendations." *Novum Jus* 18, no. 2 (2024): 249–277. <https://doi.org/10.14718/NovumJus.2024.18.2.10>.

Rizaldy Anggriawan /
Muh. Endriyo Susila



Código: 1326770854 • Autor: istockphoto.com

Cryptocurrency and its Nexus with Money Laundering and Terrorism Financing within the Framework of FATF Recommendations

Rizaldy Anggriawan*
University of Szeged (Szeged, Hungary)

Muh. Endriyo Susila**
Universitas Muhammadiyah Yogyakarta (Special Region of Yogyakarta, Indonesia)

Received: September 24, 2023 | **Evaluated:** February 08, 2024 | **Accepted:** February 13, 2024

Abstract

Cryptocurrency has emerged as a viable alternative to conventional payment systems, offering its users notable advantages such as cost efficiency and rapid transaction processing. However, cryptocurrencies' decentralized nature, anonymity, and susceptibility to cyber threats introduce the potential for their exploitation in illicit activities, notably money laundering and terrorism financing (ML/TF). This scholarly investigation seeks to investigate the roles played by international organizations actively combating such criminal activities. In this academic context, a meticulous consideration of the inherent risks associated with the aforementioned criminal endeavors is undertaken, aligning with the guidelines and recommendations set forth by the Financial Action Task Force (FATF). The study underscores a significant finding that cryptocurrency accounts can be opened anonymously, with no centralized registry to monitor cryptocurrency ownership. This characteristic poses a formidable challenge in confiscating funds linked to terrorist activities. Even in instances where cryptocurrency transactions may be traced, accessing this critical data necessitates the involvement of third-party entities, given that cryptocurrency transactions are recorded in decentralized ledgers spanning multiple jurisdictions. Furthermore, the study underscores the imperative of coordination and information exchange as indispensable elements in the ongoing battle against organized and transnational criminal activities, specifically ML/TF. Moreover, the study elucidates the incongruence between cryptocurrency and FATF regulations governing electronic fund transfers, as cryptocurrencies can make transactions through opaque and unregulated conduits, such as the deep web.

Keywords: cryptocurrency, FATF recommendations, international cooperation, money laundering, terrorism financing

* Ph.D. Student, Faculty of Law and Political Science, Institute of Criminal Science, University of Szeged, 6720, Dugonics tér 13, Szeged, Hungary. ORCID: 0000-0002-7195-769X. Scopus ID: 57315935700. E-mail: anggriawan.rizaldy@stud.u-szeged.hu

** Associate Professor, Faculty of Law, Department of Criminal Law, Universitas Muhammadiyah Yogyakarta, 55183, Jl. Brawijaya, Daerah Istimewa Yogyakarta, Indonesia. ORCID: 0000-0002-1226-3321. Scopus ID: 57201999280. E-mail: endriosusilo@umy.ac.id

Las criptomonedas y su nexo con el lavado de dinero y la financiación del terrorismo en el marco de las recomendaciones del GAFI

Rizaldy Anggriawan*
University of Szeged (Szeged, Hungary)

Muh. Endriyo Susila**
Universitas Muhammadiyah Yogyakarta (Special Region of Yogyakarta, Indonesia)

Recibido: 24 de septiembre de 2023 | **Evaluado:** 8 de febrero de 2024 | **Aceptado:** 13 de febrero de 2024

Resumen

La criptomoneda se ha convertido en una alternativa viable a los sistemas de pago tradicionales al ofrecer a los usuarios ventajas importantes como la rentabilidad y el procesamiento rápido de transacciones. Sin embargo, la naturaleza descentralizada de las criptomonedas, junto con la capacidad de anonimato y la susceptibilidad a las amenazas cibernéticas, tiene el potencial de explotarse en actividades ilícitas, en particular el lavado de dinero y la financiación del terrorismo. Esta investigación académica busca profundizar en el papel que desempeñan las organizaciones internacionales que participan activamente en la lucha contra este tipo de actividades criminales. En este contexto académico, se lleva a cabo una consideración meticulosa de los riesgos inherentes asociados con los esfuerzos criminales antes mencionados, la cual se alinea con las pautas y recomendaciones establecidas por el Grupo de Acción Financiera Internacional (GAFI). El estudio subraya un hallazgo importante: las cuentas de criptomonedas se pueden abrir con un alto grado de anonimato, sin un registro centralizado para hacer seguimiento de la propiedad de las criptomonedas. Esta característica representa un desafío formidable en términos de confiscación de fondos vinculados a actividades terroristas. Incluso en los casos en los que se pueden rastrear las transacciones de criptomonedas, el acceso a estos datos críticos requiere la participación de terceros, dado que las transacciones con criptomonedas se registran en libros de contabilidad descentralizados que abarcan diferentes jurisdicciones. Además, el estudio subraya el imperativo de coordinar e intercambiar información como elementos indispensables en la batalla en curso contra las actividades criminales organizadas y transnacionales, en especial en los ámbitos del lavado de dinero y la financiación del terrorismo. Por otra parte, el estudio aclara la incongruencia entre las criptomonedas y los reglamentos del GAFI que rigen las transferencias electrónicas de fondos, puesto que las criptomonedas ofrecen los medios para ejecutar transacciones a través de conductos opacos y no regulados, como la internet profunda.

Palabras clave: criptomoneda, recomendaciones del GAFI, cooperación internacional, lavado de dinero, financiación del terrorismo

Introduction

The Financial Action Task Force (FATF), established under the aegis of the Organisation for Economic Co-operation and Development (OECD) with the primary objective of combating money laundering and terrorism financing (ML/TF), has promulgated a compendium of regulatory measures incumbent upon its member states to counteract these illicit activities effectively. This pursuit of regulatory harmonization culminated in the 40 Recommendations issued in 1990. These recommendations encapsulate a comprehensive array of measures to safeguard the financial system against exploitation by unlawful criminal entities.¹ They underscore the imperative for member states to amend and augment their legal frameworks in consonance with these dictates to execute the stipulated measures effectively. FATF, serving as both a guiding beacon and an institution vested with substantial punitive authority in ML/TF within its member nations, engages in assessments of its member countries through a series of bilateral and regional deliberations. Subsequently, the organization disseminates annual reports that encapsulate the outcomes of these evaluations.²

Compliance with the recommendations published by the FATF is of great importance for member states. Indeed, as a corollary of these evaluations, jurisdictions found wanting in their adherence to the FATF recommendations or displaying a recalcitrant attitude toward cooperative engagement are categorically designated as “Non-Cooperating Countries.” It is important to underscore that such a designation carries the potential consequence of isolation from the international financial system, a measure of significance within the context of global financial interdependencies and the imperatives of international financial integrity. For this reason, new products and services emerging in the financial system are primarily evaluated within the framework of FATF recommendations, and the local legislation is shaped accordingly.³

¹ Helber Armando Noguera Sánchez, “Democracia Dirigida, Terrorismo Invertido: Normalización Del Terrorismo de Estado y de La Excepcionalidad En La Democracia,” *Novum Jus* 7, no. 2 (July 1, 2013): 129–56, <https://doi.org/10.14718/NovumJus.2013.7.2.5>

² Mark T. Nance, “The Regime That FATF Built: An Introduction to the Financial Action Task Force,” *Crime, Law and Social Change* 69, no. 2 (March 11, 2018): 109–29, <https://doi.org/10.1007/s10611-017-9747-6>

³ Eleni Tsingou, “Fighting Financial Crime: Who Designs Global Governance and Who Does The Work?,” *Fudan Journal of the Humanities and Social Sciences* 13, no. 2 (June 4, 2020): 169–79, <https://doi.org/10.1007/s40647-020-00278-3>

As the use and payment areas of cryptocurrencies, which emerged as a payment tool different from traditional payment methods, are becoming more and more widespread, it makes it necessary to determine the risks of these currencies and the measures to be taken to eliminate them within the framework of the standards specified by the FATF.⁴ In addition to the advantages of these currencies with their cost and fast transfer system, they can be used by illegal criminal organizations due to their decentralized structure, the ability to carry out transactions through anonymous accounts, insufficient identification of parties involved, and the inability to confirm the legitimacy of transactions.⁵

Using cryptocurrencies as a conduit for ML/TF has garnered considerable scholarly attention. In his analysis, Raymond Choo posits that individuals involved in acts of bribery and corruption invariably seek to exploit emerging circumstances and avenues to perpetrate illicit activities, including the laundering of proceeds acquired through corrupt practices, all the while evading scrutiny from law enforcement agencies and governmental bodies. Choo advances a theoretical framework centered on intelligence-driven strategies for Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) to confront this multifaceted criminal phenomenon. This strategic approach is advocated due to the potential utility of cryptocurrencies and other virtual mechanisms as instruments for concealing and laundering funds derived from corrupt activities.⁶

In addition, Wegberg et al. analyze five dark web mixing and exchange services and demonstrate how the proceeds of criminal activity can be laundered through various dark web services. Their research shows that reputation-based services can manage transactions for a cash-out strategy. According to the authors, Bitcoin is “already relatively anonymous,” and future developments in digital currencies may make ML much easier.⁷

⁴ Emmanuel Senanu Mekpor, Anthony Aboagye, and Jonathan Welbeck, “The Determinants of Anti-Money Laundering Compliance among the Financial Action Task Force (FATF) Member States,” *Journal of Financial Regulation and Compliance* 26, no. 3 (July 9, 2018): 442–59, <https://doi.org/10.1108/JFRC-11-2017-0103>.

⁵ Malcolm Campbell-Verduyn, “Bitcoin, Crypto-Coins, and Global Anti-Money Laundering Governance,” *Crime, Law and Social Change* 69, no. 2 (March 19, 2018): 283–305, <https://doi.org/10.1007/s10611-017-9756-5>.

⁶ Kim-Kwang Raymond Choo, “Cryptocurrency and Virtual Currency,” in *Handbook of Digital Currency* (Elsevier, 2015), 283–307, <https://doi.org/10.1016/B978-0-12-802117-0.00015-1>.

⁷ Rolf van Wegberg, Jan-Jaap Oerlemans, and Oskar van Deventer, “Bitcoin Money Laundering: Mixed Results? An Explorative Study on Money Laundering of Cybercrime Proceeds Using Bitcoin,” ed. Angela Futter, *Journal of Financial Crime* 25, no. 2 (March 7, 2018), <https://doi.org/10.1108/JFC-11-2016-0067>.

Moreover, as elucidated in the work of Fletcher et al., malefactors and individuals involved in terrorist activities expeditiously exploited the distinctive attributes inherent in Bitcoin, including its decentralized peer-to-peer architecture and the semblance of pseudonymity, to facilitate the execution of intricate ML/TF operations. The range of governmental responses aimed at safeguarding national security interests has exhibited a pronounced diversity, encompassing measures that span from explicit proscriptions to a stance of passive tolerance. This confluence of incongruous responses emanates from the ineffectual categorization and classification of Bitcoin within the regulatory framework.⁸

While extant literature has delved into the nexus between cryptocurrency employment and the perpetration of ML/TF activities, it is noteworthy that research endeavors focusing on a specific exploration and analysis of these crimes within the ambit of the FATF recommendations remain conspicuously sparse. Consequently, to bridge this lacuna, the present study endeavors to make a substantive contribution by dissecting the foundational concepts and operational protocols underpinning ML/TF. Moreover, this research delves into the scrutiny of international organizations actively immersed in crime prevention. In this vein, the potential perils associated with the discussed criminal activities are subjected to thorough examination, with a conscientious evaluation rendered under the prescriptive guidance provided by the FATF recommendations.

Methodology

This study employed doctrinal legal research methodologies, including statutory, historical, and conceptual approaches, to investigate the interaction of cryptocurrency and ML/TF within the framework established by the FATF. The study involved an in-depth analysis of primary legal texts, such as international treaties on AML/CFT. Furthermore, historical analysis is critical to understanding the evolution of regulatory actions and the creation of the 40 FATF Recommendations since their inception in 1990.

The research also relied on secondary legal materials from scientific journal articles, conference papers, and books. These sources offer scientific insights on cryptocurrency usage in criminal financial operations. In addition, qualitative data gathered

⁸ Emily Fletcher, Charles Larkin, and Shaen Corbet, "Countering Money Laundering and Terrorist Financing: A Case for Bitcoin Regulation," *Research in International Business and Finance* 56 (April 2021): 101387, <https://doi.org/10.1016/j.ribaf.2021.101387>.

through library research serves as the foundation for descriptive analysis, allowing for a study of the constraints and opportunities posed by cryptocurrencies inside the FATF regulatory framework. This study investigated theoretical frameworks from authors such as Raymond Choo and Wegberg et al., which synthesize existing knowledge while highlighting the importance of targeted analysis within FATF guidelines.

International Cooperation in Combating Money Laundering and Terrorism

The United Nations (UN)

In the aftermath of the Second World War, the UN was founded on the auspicious date of October 24, 1945, with the overarching mandate of upholding international peace, countering the scourge of terrorism, and safeguarding the welfare and security of civilian populations globally. Article 1 of the UN Convention, crafted with the overarching objective of forestalling prospective conflicts and fortifying international security, delineates a framework for adopting measures guided by principles of justice and international law to preserve and nurture international peace and security.⁹

It is possible to define the concept of TF as knowingly providing or helping real persons or organizations to commit a terrorist act with the financial resources necessary for them to continue their activities.¹⁰ Terrorist groups ultimately need funds to carry out their actions. Therefore, identifying terrorist funds and cutting funding sources through measures to be taken in the financial system is of vital importance in the fight against terrorism. Even though the UN has drawn up many resolutions and conventions for the prevention of terrorism, instead of making a single legal definition of terrorism, it has chosen to create a definition based on the actions of terrorist groups, such as hijacking and assassinating diplomats.¹¹

⁹ Jeremy Farrall et al., "Elected Member Influence in the United Nations Security Council," *Leiden Journal of International Law* 33, no. 1 (March 28, 2020): 101–15, <https://doi.org/10.1017/S0922156519000657>.

¹⁰ Ilias Bantekas, "The International Law of Terrorist Financing," *American Journal of International Law* 97, no. 2 (April 27, 2003): 315–33, <https://doi.org/10.2307/3100109>.

¹¹ Muhammad-Basheer A. Ismail, "Terrorist Attacks on Diplomatic Institutions: Jihad and Islamic Law Viewpoints," in *Islamic Law and Transnational Diplomatic Law* (New York: Palgrave Macmillan US, 2016), 139–64, https://doi.org/10.1057/9781137558770_6.

In Resolution 49/60, International Declaration on Measures to Eliminate Terrorism adopted by the UN in 1994, references are made to international and regional agreements, as well as expressing concern about the link between terrorist groups and drug traffickers. When the financial sources of terrorism are examined today, it is known that the illegal drug trade has reached a market of billions of dollars and that terrorist groups provide financing in this way.¹²

A further stride in the UN's concerted efforts to combat TF is evident in the International Convention for the Suppression of the Financing of Terrorism. This seminal instrument, promulgated by the UN General Assembly on December 9, 1999, and made available for the endorsement of member states commencing on January 10, 2000, operates within a multifaceted framework. It encompasses a prohibition against acts intended to instill fear in the public or coerce the actions of governments or international organizations, as delineated within the purview of the affiliated treaty and the stipulated definitional constructs. This prohibition extends to both civilian actors and belligerent parties during armed conflicts.¹³ Moreover, it is incumbent upon parties to this convention to be cognizant that their actions may be deemed as transgressions of the agreement should they, whether directly or indirectly, knowingly and unlawfully amass financial resources with the intention that these resources be utilized in the commission of acts designed to cause the death or severe injury of individuals who are not active participants in such activities.¹⁴

The contract, which consists of 18 articles, has accepted TF as a separate crime and will make it possible to seize the resources used in TF, whether they are obtained from legitimate sources such as associations, foundations, or companies or through illegal means such as arms smuggling, drug dealing, and kidnapping. Regulations have been implemented.¹⁵ In the contract, "fund" refers to tangible and intangible movable properties. Accordingly, "fund" means any document, whether material or immaterial, movable or immovable, including electronic or digital forms, proving a property right or interest in these assets, no matter how they were obtained. The

¹² Giuseppe Nesi, ed., *International Cooperation in Counter-Terrorism* (Routledge, 2016), <https://doi.org/10.4324/9781315589343>.

¹³ Heyder Alfonso Camelo, "Transformation of the Dynamics of Confrontation in the Armed Conflict," *Novum Jus* 5, no. 1 SE-Artículo de investigación científica, tecnológica o innovación (January 1, 2011): 55–78, <https://novumjus.ucatolica.edu.co/article/view/685>.

¹⁴ Marcello Di Filippo, "The Definition(s) of Terrorism in International Law," in *Research Handbook on International Law and Terrorism* (Edward Elgar Publishing, 2020), 2–15, <https://doi.org/10.4337/9781788972222.00008>.

¹⁵ Jorge Enrique Carvajal Martínez, "Public Safety and Policy," *Novum Jus* 4, no. 1 SE-Artículo de investigación científica, tecnológica o innovación (January 1, 2010): 9–32, <https://novumjus.ucatolica.edu.co/article/view/698>.

legal instruments encompassed by these provisions extend to a broad spectrum of financial mechanisms, including but not limited to bank loans, travelers' checks, money orders, stocks, guarantees, bonds, and letters of credit.

Furthermore, the endeavor to extirpate terrorism received augmented fortification through the instrumentality of the UN Convention Against Transnational Organized Crime. This convention, inaugurated for signature by the UN General Assembly in Palermo, Italy, in 2000, articulates an unwavering commitment to the battle against organized and transnational criminal enterprises. It promulgates substantive recommendations while underscoring the deleterious repercussions of such criminal activities on societal impoverishment. The convention aims to fight organized and transboundary crimes more effectively and increase cooperation between the parties. To this end, it is incumbent upon the contracting parties to prioritize and take concrete actions against activities encompassing affiliations with organized criminal syndicates, ML, acts of corruption, and the obstruction of justice as actionable crimes meriting concerted attention and countermeasures.¹⁶

The overarching objective of the Palermo Convention was to facilitate a harmonized understanding among member nations regarding the delineation of criminal activities in the context of the battle against ML/TF. By doing so, it sought to surmount the barriers that could impede the classification of a given act as criminal in one nation while evading such classification in another. In pursuit of this aim, the convention drew upon the foundational guidance provided by the 40 recommendations issued by the FATF. The imperative of intergovernmental cooperation and the establishment of legal consensus for the prevention of terrorist acts can, in turn, serve as a potent mechanism for the dismantling of internationally interconnected terrorist organizations.¹⁷

Financial Action Task Force (FATF)

Conceived in 1989 under the aegis of the Group of Seven (G-7) nations, within the framework of the OECD, the FATF came into existence with the overarching objective of galvanizing international collaboration. This initiative recognized that mitigating

¹⁶ Ioannis Chapsos and Steve Hamilton, "Illegal Fishing and Fisheries Crime as a Transnational Organized Crime in Indonesia," *Trends in Organized Crime* 22, no. 3 (September 30, 2019): 255–73, <https://doi.org/10.1007/s12117-018-9329-8>.

¹⁷ Maria Bergström, "The Many Uses of Anti-Money Laundering Regulation—Over Time and into the Future," *German Law Journal* 19, no. 5 (October 1, 2018): 1149–67, <https://doi.org/10.1017/S2071832200022987>.

ML/TF could not be efficaciously achieved through unilateral national efforts but necessitated a concerted, cross-border endeavor. It has not been established for an unlimited period due to its “power”; therefore, the working period is reviewed every five years.¹⁸ The organization systematically conducts comprehensive studies across a spectrum of domains germane to formulating recommendations directed at its member states. These investigations encompass the dynamic analysis of evolving typologies and a rigorous appraisal of the appropriateness and efficacy of domestic legislative frameworks within member countries, all geared toward the overarching imperative of fortifying the collective arsenal to combat the scourge of ML.¹⁹

The organization, driven by its commitment to bolstering the financial system’s resilience against the perils posed by ML, has promulgated a compendium of 40 recommendations to further this objective. These recommendations serve as a prescriptive framework, proffering guidance and proposals concerning the multifarious measures that can be implemented within AML/CFT initiatives. Know Your Customer (KYC), suspicious transaction reporting, additional measures regarding high-risk sectors and individuals, Politically Exposed Persons, electronic fund transfers, international cooperation and coordination, confiscation and interim measures, non-profit organizations, record keeping, correspondent banking, internal control and audit of the regulations have been put into practice.²⁰

Through the meticulous pursuit of these investigations, the FATF has endeavored to make a substantive contribution towards mitigating risks inherent within the financial system. Bolstered by its mandate, the FATF wields the authority to institute punitive measures directed at member nations to compel adherence to the recommendations it disseminates. This is complemented by periodic reviews and assessments by the FATF, with the outcomes meticulously documented in report form. Moreover, the FATF extends its consultative capacity, furnishing guidance and counsel through dedicated support mechanisms. In addition, within the scope of AML/CFT, it cooperates and exchanges information with many international organizations to increase compliance.

¹⁸ Mansour Rahmdel, “FATF and Money Laundering in Iran,” *Journal of Money Laundering Control* 21, no. 3 (July 2, 2018): 314–27, <https://doi.org/10.1108/JMLC-07-2017-0033>.

¹⁹ Deen Kemsley, Sean A. Kemsley, and Frank T. Morgan, “Tax Evasion and Money Laundering: A Complete Framework,” *Journal of Financial Crime* 29, no. 2 (March 14, 2022): 589–602, <https://doi.org/10.1108/JFC-09-2020-0175>.

²⁰ Nasir Sultan et al., “The Sustainability of the International AML Regime and the Role of the FATF: The Objectivity of the Greylisting Process of Developing Jurisdictions like Pakistan,” *Journal of Money Laundering Control* 27, no. 1 (April 11, 2023), <https://doi.org/10.1108/JMLC-12-2022-0166>.

40 Recommendations passed in 1990 to prevent laundering proceeds from crime were revised in 1996 due to new methods and technological developments in ML methods, and additional measures were introduced. FATF 40 recommendations mainly aim to protect the financial system against ML risk. However, the scope of the FATF underwent a significant expansion following the tragic events of the September 11 attacks, spurred by initiatives originating from the United States. In response to these events, in 2001, the FATF introduced eight distinct recommendations expressly tailored to address the intricate domain of countering TF. Subsequently, through a comprehensive revision in 2003, these recommendations coalesced with the original 40, culminating in establishing the 40+9 Recommendations. These meticulously crafted recommendations, disseminated by the FATF, subsequently garnered widespread recognition as standards of paramount significance. The embracement of these recommendations, especially by member states, and the concomitant efforts to develop national legislation aligned with these recommendations were met with substantial support from numerous international organizations, most notably the UN. Of salient note within these new regulatory frameworks is the profound emphasis on the alignment with UN resolutions as a cornerstone of the overarching strategy to combat TF.²¹

The FATF issued a call for the expeditious enactment of the International Convention for the Suppression of the Financing of Terrorism, ratified on December 9, 1999, with the overarching objective of instituting a uniform standard among its member states in the collective pursuit of counterterrorism financing measures.²² Before the tragic events of the September 11 attacks, the willingness of member states to endorse the aforementioned convention was met with circumspection. However, the proactive advocacy of the FATF, complemented by concerted efforts spearheaded by the United States and the UN, precipitated a significant shift in member-state attitudes. These events led to member states' acceptance and subsequent convention ratification. In the wake of the September 11 attacks and with the imperative of thwarting similar actions and severing the financial lifelines sustaining terrorist groups, the FATF embarked on a regulatory course aimed at ensuring member state ratification and stringent adherence to the stipulations of the agreement.²³ In

²¹ Shahr Hameiri and Lee Jones, "Regulatory Regionalism and Anti-Money-Laundering Governance in Asia," *Australian Journal of International Affairs* 69, no. 2 (March 4, 2015): 144–63, <https://doi.org/10.1080/10357718.2014.978737>.

²² Ilias Bantekas, "The International Law on Terrorist Financing," in *Research Handbook on International Law and Terrorism* (Edward Elgar Publishing, 2020), 97–108, <https://doi.org/10.4337/9781788972222.00014>.

²³ Jorge Carvajal, "The State of Security and International Policy," *Novum Jus* 4, no. 2 SE-Artículo de investigación científica, tecnológica o innovación (July 1, 2010): 55–76, <https://novumjus.ucatolica.edu.co/article/view/692>.

tandem with these measures, the FATF issued a resounding call to member states for immediate compliance with UN Security Council Resolution 1373. In concordance with Resolution 1373, it underscored a multifaceted array of imperatives, including the criminalization of TF and the delineation of corresponding criminal provisions. Moreover, recognizing the transnational nature of TF, it implored member states to foster solidarity and information exchange. A further directive pertained to the seizure of funds utilized by individuals and entities involved in the perpetration or attempted execution of terrorist activities. Lastly, the resolution enjoined member states to refrain from providing asylum and support to individuals who render financial aid or abetment to terrorist groups.²⁴

To interdict the financial resources underpinning the commission of terrorist acts and to impede the flow of these funds, member states are urged, in conformity with UN Resolutions, to institute the requisite measures for the expeditious freezing of the assets held by individuals and entities that engage in TF. Freezing of assets means converting funds based on a legal process initiated by an authority authorized by law or a court, prohibiting the disposition or movement by the owner. It is required by law to determine which authority is responsible for confiscating the assets of people who are determined to support terrorist organizations and are also announced by UN Security Council resolutions. Confiscation, as expressed by the FATF, is the permanent deprivation of funds and other assets of the owner and the freezing of these funds due to the decision of the competent authority or court.²⁵

Implementing the Nine Special Recommendations, designed with the overarching objective of combating TF, is fundamentally oriented towards augmenting international cooperation, elucidating the contours of criminal penalties, and achieving comprehensive identification of the culpable actors involved in this illicit endeavor. For this reason, in the recommendations, the obliged parties act within the framework of the principle of knowing your customer, and the obliged parties are obliged to identify the customer and confirm this information from reliable sources before establishing a business relationship. The said practices will ensure the identification

²⁴ Carlotta M. Minnella, "Counter-Terrorism Resolutions and Listing of Terrorists and Their Organizations by the United Nations," in *International Human Rights and Counter-Terrorism* (Singapore: Springer, 2019), 31–53, https://doi.org/10.1007/978-981-10-4181-5_4.

²⁵ Roberto Virzo, "Limits to Measures of Confiscation of Property Linked to Serious Criminal Offences in the Case Law of the European Court of Human Rights," *The Italian Yearbook of International Law Online* 30, no. 1 (November 10, 2021): 265–81, <https://doi.org/10.1163/22116133-03001015>.

of customers operating in the risky sector and thus enable the implementation of a risk-based approach.²⁶

The International Monetary Fund (IMF)

The IMF, established on December 27, 1945, is a global organization charged with the multifaceted mission of monitoring international financial markets, fostering international cooperation, ensuring financial stability, promoting robust employment, facilitating sustainable economic growth, and representing the interests of its vast constituency comprising 189 member countries. In addition to its primary mission, the IMF undertakes diverse initiatives to bolster financial market stability, curb financial malfeasance, and prevent the pernicious activities of ML/TF. Significantly, alongside the regulatory efforts directed at countering ML, the post-September 11 attacks witnessed the implementation of stringent regulations to address TF. In alignment with these evolving standards, the FATF published the 40+9 Recommendations in July 2002, subsequently accorded the status of international standards by the IMF. Furthermore, recognizing the imperative of advancing efforts in financial integrity, the IMF's Executive Board, in 2004, resolved to integrate work in this sphere as a routine component of its activities. Collaboratively with the World Bank, the IMF has embarked on a collective mission, manifest in activities aimed at enhancing institutional capacity through an enhanced dialogue framework, the refinement of methodologies for assessing the fight against international ML/TF, and the intensification of training initiatives in this domain.²⁷

The fundamental basis of the IMF's work in this area is the necessity of considering the financial system as a whole. Naturally, it is incumbent upon this institution, whose primary mandate revolves around preserving financial stability, to eschew indifference toward the pernicious phenomena of ML/TF. These nefarious activities, replete with profound societal and economic ramifications, serve as fertile conduits for the proliferation of other corrosive practices, such as corruption and bribery. For this purpose, the IMF has emphasized that terrorist activities cause suffering for individuals, families, and communities. It has stressed that tackling the financial flows that enable these actions is a primary responsibility. To combat these crimes,

²⁶ Mark T. Nance, "Re-Thinking FATF: An Experimentalist Interpretation of the Financial Action Task Force," *Crime, Law and Social Change* 69, no. 2 (March 18, 2018): 131–52, <https://doi.org/10.1007/s10611-017-9748-5>.

²⁷ Jon Truby, "Measuring Qatar's Compliance with International Standards on Money Laundering and Countering the Financing of Terrorism," *Journal of Money Laundering Control* 19, no. 3 (July 4, 2016): 264–77, <https://doi.org/10.1108/JMLC-04-2015-0011>.

there is a need to leverage the power of fintech to enhance the control and monitoring of financial transactions. The IMF cooperates with the FATF in this area.²⁸

The Dark Side of Cryptocurrency: Understanding the Risks

The ability to perform transactions through the anonymous accounts provided by cryptocurrency to its users allows this system to be exposed to certain risks in terms of fraud and ML/TF. Intensive use of the deep web, where access can be provided through private servers with special equipment, is among these risks. Cryptocurrency is based on advanced encryption techniques, i.e., cryptography. An increasing number of merchants accept cryptocurrencies for the sale of both real and digital goods and products. Traditional financial systems establish the necessary tools against abuse in their structures. These measures are because the currencies used have a central control mechanism. In contrast, there is no central registry in cryptocurrencies, so there is no authority to prevent and control the abuse of the system. Due to its decentralized structure, cryptocurrency faces the risks of ML/TF.²⁹

The ability to transact through anonymous accounts has always been a goal for cryptocurrency markets. Cryptocurrencies, however, are not always uniformly anonymous. During the account opening process, it is impossible to determine for whom and for what purposes the transactions are carried out, as the customer numbers are created using alphanumeric characters. The unique key generated for each transaction provides privacy to its users. Due to the ability to open accounts under pseudonyms and its deficiencies in identification, this system makes it attractive for launderers and those who want to finance terrorism. When the international regulations and standards regarding AML/CFT are examined, it is seen that identification is the primary measure that financial institutions should take within the scope of the KYC policy. The common point emphasized by the FATF, EU Directives, and Wolfsberg Standards is identifying and verifying identity in establishing business relationships. However, besides identification and confirmation in account openings to transact through cryptocurrency, these transactions can also be made directly through anonymous accounts. In the research conducted by the Federal Bureau of

²⁸ Nankpan Moses Nanyun and Alireza Nasiri, "Role of FATF on Financial Systems of Countries: Successes and Challenges," *Journal of Money Laundering Control* 24, no. 2 (July 31, 2021): 234–45, <https://doi.org/10.1108/JMLC-06-2020-0070>.

²⁹ Chad Albrecht et al., "The Use of Cryptocurrencies in the Money Laundering Process," *Journal of Money Laundering Control* 22, no. 2 (May 7, 2019): 210–16, <https://doi.org/10.1108/JMLC-12-2017-0074>.

Investigation (FBI), it was emphasized that it is not possible to know who is who and to obtain identity information for users of cryptocurrencies such as Bitcoin.³⁰

With cryptocurrencies, transfer transactions can be quickly and instantly transferred to the recipient's wallet via digital identities without central authority approval and control. The cost of transfer transactions is meager. Cost advantage and fast fund transfers through anonymous accounts cause this system to have ML/TF risks. In particular, launderers may prefer using cryptocurrency when separating the funds they include in the financial system. The fact that cryptocurrency offers fast transfer services allows transactions to occur confidentially without passing through legal authority control and, most importantly, using pseudonyms or anonymous accounts, triggering the risk of abuse. In addition, the high commissions received by money transfer agencies such as Western Union and the difficulties in accessing these systems in underdeveloped regions lead users to transfer via cryptocurrencies. The fact that this system is easily accessible via the internet and mobile channels is another advantage that makes its use attractive.³¹

Criminals introduce illegal income into the financial system in different ways during the placement stage; they can use these funds as a means of exchange in cryptocurrencies, thereby diverting the income from its original source through numerous transfers. In addition, criminal organizations may prefer these currencies as a payment method for the revenues they obtain from selling illegal goods or services. Proceeds from sales such as drugs and weapons can be received in cryptocurrencies; e.g., many dealers in Texas can accept Bitcoin payments for weapons sales. Therefore, as it is accepted as a means of payment in activities such as drug and weapon sales, this system can also be used by terrorist organizations that derive most of their income from these activities.³² Although cryptocurrencies offer attractive opportunities for laundering activities, no study has yet been conducted to show that they are used extensively by launderers. However, the National Crime Agency (NCA), the UK Financial Intelligence Unit, emphasized that cryptocurrencies carry

³⁰ Perri Reynolds and Angela S.M. Irwin, "Tracking Digital Footprints: Anonymity within the Bitcoin System," *Journal of Money Laundering Control* 20, no. 2 (May 2, 2017): 172–89, <https://doi.org/10.1108/JMLC-07-2016-0027>.

³¹ Alexia Maddox et al., "Constructive Activism in the Dark Web: Cryptomarkets and Illicit Drugs in the Digital 'Demimonde,'" *Information, Communication & Society* 19, no. 1 (January 2, 2016): 111–26, <https://doi.org/10.1080/1369118X.2015.1093531>.

³² Steven David Brown, "Cryptocurrency and Criminality," *The Police Journal: Theory, Practice and Principles* 89, no. 4 (December 3, 2016): 327–39, <https://doi.org/10.1177/0032258X16658927>.

significant risks in terms of AML, and it was stated that many lawsuits were filed in the Netherlands on this issue, whose details were not given.

Providing the opportunity to open accounts and make untraceable transactions through fake IDs, passports, or anonymous accounts, terrorist organizations can also prefer cryptocurrency. Terrorist organizations, which obtain the funds they need to carry out their actions, mostly from drug and weapons smuggling, prefer vehicles and regions where the financial system is weak or the measures are not tight to collect these funds and use them for payments. For this reason, it is known that they use the system called hawala for a long time in their financial transactions. Hawala is practically no different from traditional payment services and banks. However, it differs from the conventional financial system in that the transactions are not recorded; there is no information on who or on behalf of whom the payments are made, and the transaction purpose is unknown, causing the system to have ML/TF risk. When examined from this aspect, cryptocurrencies also offer privacy and unregistered transactions to their users, as in the hawala system. As a matter of fact, in the guides published by the FATF, it was emphasized that cryptocurrencies could be used in TF due to these features, and it was stated in the report that the Islamic State of Iraq and the Levant (ISIS) preferred cryptocurrencies instead of using remittance agencies in the Middle East. These transactions can be carried out through digital wallets like Dark Wallet, which offer anonymity and work with FinTech organizations under the FATF to develop products and services that can combat this with new financial instruments.³³

Cryptocurrency in the Framework of FATF Recommendations

The Vienna Convention was adopted by the UN General Assembly, which stipulates that the member states should take measures regarding ML and drug trafficking. It has enacted regulations encompassing a broad spectrum of domains, including but not limited to FATF recommendations, the customer onboarding process, fund transfers, and measures about high-risk countries and sectors, all with the overarching goal of safeguarding the financial system against various risks. Additionally, it actively endeavors to secure compliance by member countries with these regulations. Cryptocurrencies, which have emerged recently and become

³³ Joe Whittaker, "The Role of Financial Technologies in US-Based ISIS Terror Plots," *Studies in Conflict & Terrorism*, (October 12, 2022): 1–26, <https://doi.org/10.1080/1057610X.2022.2133345>.

increasingly widespread, are also discussed due to the ML/TF risks they contain and their advantages. Failure to implement the regulations regarding the measures to be taken in the customer acceptance process and transfer processes, as stated in the FATF recommendations, may lead to the use of these units by ML/TF groups.³⁴

Its report titled “Virtual Currencies Key Definitions and Potential AML/CFT Risks,” published by the FATF in June 2014, emphasizes the definition and operating system of cryptocurrencies and the ML/TF risks of cryptocurrency. It was seen as risky in terms of security, and the system is vulnerable to AML/CFT risks, emphasizing that cryptocurrency allows greater anonymity than traditional non-cash transfers. The fact that these units can be easily transacted through non-face-to-face channels such as the internet and mobile channels and that, unlike payment systems, they are transferred only through digital identity numbers without sender-receiver names makes this market highly vulnerable to ML/TF. The decentralized cryptocurrency is processed on the web without any centralized system or servers, without using terms such as name or customer definition, and there is no central supervisory body to control the transactions. Thanks to software, financial institutions can detect suspicious transactions within their bodies according to certain scenarios and distinguish them from ordinary financial transactions. However, there is no control or surveillance mechanism regarding whether the transactions in the cryptocurrency markets are suspicious. Cryptocurrencies are easily accessible through the internet, mobile, and ATM channels, and there are no checkpoints for these non-face-to-face channels.³⁵

Know Your Customer Policy

The KYC principle signifies a meticulous process that encompasses the collection of crucial information about a customer, encompassing details such as their identity, occupation, the intended use of the account, potential transaction types to be made through the account, and the channels to be employed. This process is instituted before establishing a business relationship and its documentation. Following the guidelines delineated by the FATF, obligated entities must adhere to a specific protocol in situations that involve transactions surpassing the monetary thresholds

³⁴ Emmanuel Senanu Mekpor, “Anti-Money Laundering and Combating the Financing of Terrorism Compliance,” *Journal of Money Laundering Control* 22, no. 3 (July 2, 2019): 451–71, <https://doi.org/10.1108/JMLC-09-2018-0057>.

³⁵ Georgios Pavlidis, “International Regulation of Virtual Assets under FATF’s New Standards,” *Journal of Investment Compliance* 21, no. 1 (July 8, 2020): 1–8, <https://doi.org/10.1108/JOIC-08-2019-0051>.

stipulated by member country legislation. This protocol applies when suspicions of ML/TF arise, irrespective of transaction amounts, and when there is ambiguity regarding the veracity of the customer's identity information.

These prescribed measures necessitate, firstly, the identification of the ultimate beneficiary associated with transactions and the corresponding account. If it is ascertained that transactions are conducted on behalf of an entity other than the account holder or the individual performing the transaction, this third party should be recognized as the actual beneficiary, and their identity must be corroborated. Additionally, the KYC process entails gathering comprehensive information concerning the intended purpose of the business relationship for individuals and legal entities that have initiated accounts with obligated entities. Furthermore, the process entails meticulously monitoring transactions integral to the business relationship, emphasizing a risk-based approach. This approach is forged within the framework of the information acquired about the customer.³⁶

Identifying the person conducting the transactions and ascertaining the ultimate recipient is unattainable when dealing with transactions conducted via an anonymous account. For this reason, one of the regulations introduced under KYC is the prohibition of anonymous account opening. Anonymous account openings are prohibited in FATF Recommendation No. 5 and EU Directives. Anonymous account openings likely to be used by criminal organizations are not permitted, and the account holder's identification is obligatory.³⁷

When cryptocurrencies are examined within the scope of the measures introduced by FATF under KYC, they contain ML/TF risks due to their structure. Since cryptocurrency transactions can be carried out through anonymous accounts, they do not comply with the identification regulations. ML/TF groups may find these units attractive, providing the advantage of pseudonyms and almost complete anonymity. In this respect, it is possible to say that it contradicts the FATF recommendation to ban anonymous account opening. In this context, member countries establish financial intelligence units whose powers and duties are determined under the laws. They are obliged to keep this information for the period stipulated by the laws of

³⁶ Joel Harry Clavijo Suntura, "Customer Identification in Currency Exchange Companies as per FATF Recommendations," *Journal of Money Laundering Control* 23, no. 1 (December 19, 2019): 96–102, <https://doi.org/10.1108/JMLC-05-2019-0036>.

³⁷ Nadine Kathrin Ostern and Johannes Riedel, "Know-Your-Customer (KYC) Requirements for Initial Coin Offerings," *Business & Information Systems Engineering* 63, no. 5 (October 8, 2021): 551–67, <https://doi.org/10.1007/s12599-020-00677-6>.

the relevant country and, if requested, to notify the competent authorities before initiating the commercial partnership. They can leave the control of the records kept to these institutions.³⁸

The issue of keeping records includes not only the identity of the customer but also the information obtained for the transaction purpose, the transactions made from the account, and AML/CFT training. In the research carried out by the US Foreign Relations Council, it has been stated that terrorist groups are financed with Bitcoin, which is a cryptocurrency, and Bitcoins are used to fund terrorist groups in Indonesia. The Council emphasized that the most significant factor in the use of Bitcoin as a payment tool in bomb-making and weapon purchases is the anonymity that these coins provide to their users and that companies such as Samurai, BitcoinFog, and Dark Wallet, which have become widespread in recent years and offer more privacy, pose serious risks in this context. As a result, the anonymity feature of cryptocurrencies, the lack of control for identification, and the ability to make transactions between accounts without supervision cause them to not comply with the recommendations made by FATF within the KYC principle.³⁹

The Issue of Legal Systems

Since ML/TF is an organized and transboundary crime, international cooperation is needed to prevent this crime, the framework of which is determined by law. For this purpose, the FATF, established within the OECD, recommended that member countries implement legal regulations, whose scope was determined under FATF recommendations, to define ML/TF crime among countries commonly and harmoniously. In formulating the parameters and extent of ML/TF offenses, the FATF draws substantially from the provisions articulated within the Vienna Convention. Per its commitment to combating these illicit financial activities, the FATF has formally embraced the UN Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances and the UN Convention Against Transnational Organized Crime, thereby affording legal recognition to the criminality of money laundering. This issue is also addressed in Special Recommendation No. 1 of the FATF, which

³⁸ Asim Jusic, "Kuwait's Administrative Risk-Based Model for the Prevention of Money Laundering: Costs and Benefits of Compliance with the Financial Action Task Force (FATF) Standards," *Arab Law Quarterly* 31, no. 2 (June 14, 2017): 101–33, <https://doi.org/10.1163/15730255-31020005>.

³⁹ Tju Liang Chua, "Strengthening AML/CFT Controls of Digital Payment Token Service Providers in Singapore," *Journal of Investment Compliance* 22, no. 4 (October 28, 2021): 370–76, <https://doi.org/10.1108/JOIC-08-2021-0035>.

will be covered in later chapters. In this respect, the UN significantly contributes to FATF studies to ensure international harmony and increase cooperation on ML/TF.⁴⁰

To define the revenues from crime, an income must first be used as a means of exchange. This income unit must be regulated within the relevant country's legislation framework. Units such as Dollar, Turkish Lira, and Euro are put into circulation by a central authority and traded under the control of the relevant countries. Therefore, the regulations made by the FATF cover regulated currencies. Considering this aspect, cryptocurrencies are out of traditional payment instruments due to their decentralized structure. At this point, cryptocurrencies are not transparent regarding accountability in an investigation by law enforcement or in a situation where ML/TF risk arises.⁴¹ Failure to do so constitutes an obstacle to regulation in this regard. The lack of legal regulations and control causes both ML/TF groups to use cryptocurrencies. As a matter of fact, in the terrorist attacks that took place in Paris in November 2015, it was stated that cryptocurrencies were also used in TF and emphasized the necessity of making regulations in this area. The European Commission noted that the rules in this area would be addressed in the Fifth Anti-Money Laundering Directive. As of today, there are no legal regulations made by organizations such as FATF and EU regarding cryptocurrency markets. Some countries, such as Finland and the United Kingdom, do not recognize these instruments as an official payment method, although they have taxed income from these currencies.⁴²

The Issue of Electronic Transfers

The regulations promulgated by the FATF about electronic fund transfers encompass a comprehensive gamut of provisions. These provisions encompass the mandatory inclusion of critical information such as the full names of both the sender and recipient, the transaction purpose, relevant account numbers, and address details within payment messages. One salient objective underlying these requirements is the imperative to ascertain the actual beneficiaries of these transfers. Notably,

⁴⁰ Natalia N. Reshetnikova et al., "Directions of Digital Financial Technologies Development: Challenges and Threats to Global Financial Security" (Cham: Springer, 2021), 355–63, https://doi.org/10.1007/978-3-030-69421-0_38.

⁴¹ Salwa Zolkafli, Sharifah Nazatul Faiza Syed Mustapha Nazri, and Normah Omar, "Asset Recovery Practices in Combating Money Laundering: Evidence from FATF Mutual Evaluation Report of FATF Member Countries of Asia Pacific Region," *Journal of Money Laundering Control* 26, no. 1 (January 2, 2023): 24–34, <https://doi.org/10.1108/JMLC-11-2021-0127>.

⁴² Agata Ferreira and Philipp Sandner, "EU Search for Regulatory Answers to Crypto Assets and Their Place in the Financial Markets' Infrastructure," *Computer Law & Security Review* 43 (November 2021): 105632, <https://doi.org/10.1016/j.clsr.2021.105632>.

the specific thresholds for the transaction amount may vary across different countries, with some nations imposing no monetary limit while others adhere to a predetermined threshold. Per FATF stipulations, member states are duty-bound to enact the prescribed measures on electronic fund transfers. Particular attention is accorded to the imperative of compliance with UN Security Council Resolutions 1267 and subsequent 1373, especially within the context of countering TF. Under these resolutions, the inclusion of pertinent information within payment messages is mandated to facilitate the execution of asset-freezing requests related to transactions implicated in TF.⁴³

It is also regulated in Wolfsberg and EU Directives.⁴⁴ In particular, the Wolfsberg Principles introduced necessary regulations, emphasizing that sender and receiver information should be included in SWIFT MT 202 COV messages. This information also contributes to identifying transactions by persons linked to organized crime or transactions that may be included in the scope of violations of international sanctions.⁴⁵

When the transfer transactions made through cryptocurrencies are examined, it is seen that the transfers made with these currencies are made over digital identity numbers, and the information of the sender and the receiver is not included in the payment messages. When evaluated in this context, it is incompatible with the regulations made by FATF, the Wolfsberg Principles, and EU Directives.⁴⁶ For this reason, it is seen that it is not possible to determine whether the sender and receiver information is not included in the transfers made with cryptocurrencies, on whose behalf and account the transaction is made, and whether their persons are connected with criminal organizations. For this reason, the New York Ministry of Foreign Affairs Department of Financial Services (NYDFS) recommendations to obtain licensing to detect and report suspicious transactions for institutions that

⁴³ George J. Andreopoulos, "The Quest for Accountability: The Resolution 1373 Process at the United Nations Security Council," in *The Rule of Law in an Era of Change* (Cham: Springer International Publishing, 2018), 73–101, https://doi.org/10.1007/978-3-319-89908-4_4.

⁴⁴ Sisira Dharmasri Jayasekara, "Challenges of Implementing an Effective Risk-Based Supervision on Anti-Money Laundering and Countering the Financing of Terrorism under the 2013 FATF Methodology," *Journal of Money Laundering Control* 21, no. 4 (October 1, 2018): 601–15, <https://doi.org/10.1108/JMLC-11-2017-0062>.

⁴⁵ Matthew Collin, Samantha Cook, and Kimmo Soramaki, "The Impact of Anti-Money Laundering Regulation on Payment Flows: Evidence from SWIFT Data," *SSRN Electronic Journal*, 2016, <https://doi.org/10.2139/ssrn.2893790>.

⁴⁶ Matthew Manning, Gabriel T. W. Wong, and Nada Jevtovic, "Investigating the Relationships between FATF Recommendation Compliance, Regulatory Affiliations and the Basel Anti-Money Laundering Index," *Security Journal* 34, no. 3 (September 22, 2021): 566–88, <https://doi.org/10.1057/s41284-020-00249-z>.

act as intermediaries in cryptocurrency trading have come to the fore. In payment messages, it is seen that there is a separate area where information about the purpose of the payment is included, as well as information about the parties to the transaction. Payment institutions serving as Money Services Businesses (MSB) and local money transfers also take precautions. However, cryptocurrency payments do not contain information about the parties, nor do they have a regulation showing the purpose of the payment.⁴⁷

International Cooperation and Coordination

The international coordination and cooperation issue should be ensured to combat ML and regulate TF in the FATF recommendation. Since ML/TF crime is trans-boundary and organized, cooperation becomes inevitable. For this reason, FATF cooperates with institutions and organizations such as the UN and the EU so that member states can collaborate on AML/CFT. It aims to ensure cooperation between the countries' financial intelligence units through formations such as the Egmont Group, as well as cooperation among member countries before international organizations. The main factor that obliges the cooperation is the organization of the ML/TF activity.

After launderers introduce the proceeds from crime into the financial system, they use the separation stage and transfer the funds to different countries and organizations to divert the funds from their source. Financial intelligence units can collaborate to track these funds, and this cooperation can be realized through the Egmont Group. One hundred sixty-eight regulations in international cooperation cover transactions that take place through regulated currencies and organizations whose jurisdiction is determined by law. Therefore, there will be obstacles to the realization of international cooperation in investigating the risks that may arise in cryptocurrencies, which have a centralized structure and are not subject to the laws of which country. Cryptocurrency transactions are recorded in different countries and on other servers. Based on the suspicion of ML/TF in the transactions, the uncertainty about which country will investigate the crime within the framework of judicial decisions and which institutions of the relevant country will be contacted is one of the biggest

⁴⁷ Aleksei Churilov, "Practical Aspects of Bitcoin Usage in Business," *SSRN Electronic Journal*, (November 3, 2015), <https://doi.org/10.2139/ssrn.2685646>.

obstacles to cooperation in this area. Determining the competent authority by law on the subject will significantly contribute to overcoming this obstacle.⁴⁸

Conclusion

The most critical factor in implementing FATF recommendations stems from the fact that transactions in financial institutions can be recorded at a single point. These records are collected within the body of financial institutions and reported to the competent authorities at regular intervals within specific scenarios. In the cryptocurrency markets, transactions cannot be recorded because the institutions issuing these currencies are not centralized. It is impossible to track transactions performed with anonymous accounts and alpha-numeric codes. When evaluated within the framework of the FATF Recommendations supported by the UN to combat TF, it is possible to see that cryptocurrencies contain risks. In the traditional financial system, terrorism-related funds can be confiscated at the request of competent authorities and judicial decisions. However, cryptocurrency markets do not have a central registry, and accounts can be opened anonymously. This does not make it possible to confiscate funds linked to terrorism. Even if funds can be identified, access to this information will require the cooperation of third countries, as transactions are recorded in ledgers located in different countries. The lack of regulations and bureaucratic obstacles in this area makes it difficult to seize funds that are found to be related to TF in cryptocurrency markets.

Another issue addressed in the FATF Special Recommendation is international cooperation in ML/TF. The fight against the crime of ML/TF, an organized and cross-border crime, requires cooperation and information exchange. The fact that cryptocurrencies can be used through untraceable tools such as the Deep Web, which is far from being controlled, causes it to conflict with the regulations of the FATF regarding electronic fund transfers. As a result, cryptocurrencies have risks in ML/TF since transactions with cryptocurrencies are made through anonymous accounts, and no central institution is issuing these currencies. They are frequently used on servers known as the deep web, where the illegal drug trade is widespread.

⁴⁸ Santha Vaithilingam, Mahendhiran Nair, and Thangarajah Thiyagarajan, "Managing Money Laundering in a Digital Economy," *Journal of Asia-Pacific Business* 16, no. 1 (January 2, 2015): 44–65, <https://doi.org/10.1080/10599231.2015.997626>.

References

- Albrecht, Chad, Kristopher McKay Duffin, Steven Hawkins, and Victor Manuel Morales Rocha. "The Use of Cryptocurrencies in the Money Laundering Process." *Journal of Money Laundering Control* 22, no. 2 (May 7, 2019): 210–16. <https://doi.org/10.1108/JMLC-12-2017-0074>.
- Andreopoulos, George J. "The Quest for Accountability: The Resolution 1373 Process at the United Nations Security Council." In *The Rule of Law in an Era of Change*, 73–101. Cham: Springer International Publishing, 2018. https://doi.org/10.1007/978-3-319-89908-4_4.
- Bantekas, Ilias. "The International Law of Terrorist Financing." *American Journal of International Law* 97, no. 2 (April 27, 2003): 315–33. <https://doi.org/10.2307/3100109>.
- Bantekas, Ilias. "The International Law on Terrorist Financing." In *Research Handbook on International Law and Terrorism*, 97–108. Edward Elgar Publishing, 2020. <https://doi.org/10.4337/9781788972222.00014>.
- Bergström, Maria. "The Many Uses of Anti-Money Laundering Regulation—Over Time and into the Future." *German Law Journal* 19, no. 5 (October 1, 2018): 1149–67. <https://doi.org/10.1017/S2071832200022987>.
- Brown, Steven David. "Cryptocurrency and Criminality." *The Police Journal: Theory, Practice and Principles* 89, no. 4 (December 3, 2016): 327–39. <https://doi.org/10.1177/0032258X16658927>.
- Camelo, Heyder Alfonso. "Transformation of the Dynamics of Confrontation in the Armed Conflict." *Novum Jus* 5, no. 1 SE-Artículo de investigación científica, tecnológica o innovación (January 1, 2011): 55–78. <https://novumjus.ucatolica.edu.co/article/view/685>.
- Campbell-Verduyn, Malcolm. "Bitcoin, Crypto-Coins, and Global Anti-Money Laundering Governance." *Crime, Law and Social Change* 69, no. 2 (March 19, 2018): 283–305. <https://doi.org/10.1007/s10611-017-9756-5>.
- Carvajal, Jorge. "The State of Security and International Policy." *Novum Jus* 4, no. 2 SE-Artículo de investigación científica, tecnológica o innovación (July 1, 2010): 55–76. <https://novumjus.ucatolica.edu.co/article/view/692>.
- Carvajal Martínez, Jorge Enrique. "Public Safety and Policy." *Novum Jus* 4, no. 1 SE-Artículo de investigación científica, tecnológica o innovación (January 1, 2010): 9–32. <https://novumjus.ucatolica.edu.co/article/view/698>.
- Chapsos, Ioannis, and Steve Hamilton. "Illegal Fishing and Fisheries Crime as a Transnational Organized Crime in Indonesia." *Trends in Organized Crime* 22, no. 3 (September 30, 2019): 255–73. <https://doi.org/10.1007/s12117-018-9329-8>.

- Choo, Kim-Kwang Raymond. "Cryptocurrency and Virtual Currency." In *Handbook of Digital Currency*, 283–307. Elsevier, 2015. <https://doi.org/10.1016/B978-0-12-802117-0.00015-1>.
- Chua, Tju Liang. "Strengthening AML/CFT Controls of Digital Payment Token Service Providers in Singapore." *Journal of Investment Compliance* 22, no. 4 (October 28, 2021): 370–76. <https://doi.org/10.1108/JOIC-08-2021-0035>.
- Churilov, Aleksei. "Practical Aspects of Bitcoin Usage in Business." *SSRN Electronic Journal*, 2015. <https://doi.org/10.2139/ssrn.2685646>.
- Clavijo Suntura, Joel Harry. "Customer Identification in Currency Exchange Companies as per FATF Recommendations." *Journal of Money Laundering Control* 23, no. 1 (December 19, 2019): 96–102. <https://doi.org/10.1108/JMLC-05-2019-0036>.
- Collin, Matthew, Samantha Cook, and Kimmo Soramaki. "The Impact of Anti-Money Laundering Regulation on Payment Flows: Evidence from SWIFT Data." *SSRN Electronic Journal*, 2016. <https://doi.org/10.2139/ssrn.2893790>.
- Farrall, Jeremy, Marie-Eve Loiselle, Christopher Michaelsen, Jochen Prantl, and Jeni Whalan. "Elected Member Influence in the United Nations Security Council." *Leiden Journal of International Law* 33, no. 1 (March 28, 2020): 101–15. <https://doi.org/10.1017/S0922156519000657>.
- Ferreira, Agata, and Philipp Sandner. "Eu Search for Regulatory Answers to Crypto Assets and Their Place in the Financial Markets' Infrastructure." *Computer Law & Security Review* 43 (November 2021): 105632. <https://doi.org/10.1016/j.clsr.2021.105632>.
- Filippo, Marcello Di. "The Definition(s) of Terrorism in International Law." In *Research Handbook on International Law and Terrorism*, 2–15. Edward Elgar Publishing, 2020. <https://doi.org/10.4337/9781788972222.00008>.
- Fletcher, Emily, Charles Larkin, and Shaen Corbet. "Countering Money Laundering and Terrorist Financing: A Case for Bitcoin Regulation." *Research in International Business and Finance* 56 (April 2021): 101387. <https://doi.org/10.1016/j.ribaf.2021.101387>.
- Hameiri, Shahar, and Lee Jones. "Regulatory Regionalism and Anti-Money-Laundering Governance in Asia." *Australian Journal of International Affairs* 69, no. 2 (March 4, 2015): 144–63. <https://doi.org/10.1080/10357718.2014.978737>.
- Ismail, Muhammad-Basheer A. "Terrorist Attacks on Diplomatic Institutions: Jihad and Islamic Law Viewpoints." In *Islamic Law and Transnational Diplomatic Law*, 139–64. New York: Palgrave Macmillan US, 2016. https://doi.org/10.1057/9781137558770_6.
- Jayasekara, Sisira Dharmasri. "Challenges of Implementing an Effective Risk-Based Supervision on Anti-Money Laundering and Countering the Financing of Terrorism under the 2013 FATF Methodology." *Journal of Money Laundering Control* 21, no. 4 (October 1, 2018): 601–15. <https://doi.org/10.1108/JMLC-11-2017-0062>.

- Jusic, Asim. "Kuwait's Administrative Risk-Based Model for the Prevention of Money Laundering: Costs and Benefits of Compliance with the Financial Action Task Force (Fatf) Standards." *Arab Law Quarterly* 31, no. 2 (June 14, 2017): 101–33. <https://doi.org/10.1163/15730255-31020005>.
- Kemsley, Deen, Sean A. Kemsley, and Frank T. Morgan. "Tax Evasion and Money Laundering: A Complete Framework." *Journal of Financial Crime* 29, no. 2 (March 14, 2022): 589–602. <https://doi.org/10.1108/JFC-09-2020-0175>.
- Maddox, Alexia, Monica J. Barratt, Matthew Allen, and Simon Lenton. "Constructive Activism in the Dark Web: Cryptomarkets and Illicit Drugs in the Digital 'Demi-monde.'" *Information, Communication & Society* 19, no. 1 (January 2, 2016): 111–26. <https://doi.org/10.1080/1369118X.2015.1093531>.
- Manning, Matthew, Gabriel T. W. Wong, and Nada Jevtovic. "Investigating the Relationships between FATF Recommendation Compliance, Regulatory Affiliations and the Basel Anti-Money Laundering Index." *Security Journal* 34, no. 3 (September 22, 2021): 566–88. <https://doi.org/10.1057/s41284-020-00249-z>.
- Mekpor, Emmanuel Senanu. "Anti-Money Laundering and Combating the Financing of Terrorism Compliance." *Journal of Money Laundering Control* 22, no. 3 (July 2, 2019): 451–71. <https://doi.org/10.1108/JMLC-09-2018-0057>.
- Mekpor, Emmanuel Senanu, Anthony Aboagye, and Jonathan Welbeck. "The Determinants of Anti-Money Laundering Compliance among the Financial Action Task Force (FATF) Member States." *Journal of Financial Regulation and Compliance* 26, no. 3 (July 9, 2018): 442–59. <https://doi.org/10.1108/JFRC-11-2017-0103>.
- Minnella, Carlotta M. "Counter-Terrorism Resolutions and Listing of Terrorists and Their Organizations by the United Nations," 31–53, 2019. https://doi.org/10.1007/978-981-10-4181-5_4.
- Nance, Mark T. "Re-Thinking FATF: An Experimentalist Interpretation of the Financial Action Task Force." *Crime, Law and Social Change* 69, no. 2 (March 18, 2018): 131–52. <https://doi.org/10.1007/s10611-017-9748-5>.
- Nance, Mark T. "The Regime That FATF Built: An Introduction to the Financial Action Task Force." *Crime, Law and Social Change* 69, no. 2 (March 11, 2018): 109–29. <https://doi.org/10.1007/s10611-017-9747-6>.
- Nanyun, Nankpan Moses, and Alireza Nasiri. "Role of FATF on Financial Systems of Countries: Successes and Challenges." *Journal of Money Laundering Control* 24, no. 2 (July 31, 2021): 234–45. <https://doi.org/10.1108/JMLC-06-2020-0070>.
- Nesi, Giuseppe, ed. *International Cooperation in Counter-Terrorism*. Routledge, 2016. <https://doi.org/10.4324/9781315589343>.

- Noguera Sánchez, Helber Armando. "Democracia Dirigida, Terrorismo Invertido : Normalización Del Terrorismo de Estado y de La Excepcionalidad En La Democracia." *Novum Jus* 7, no. 2 (July 1, 2013): 129–56. <https://doi.org/10.14718/NovumJus.2013.7.2.5>.
- Ostern, Nadine Kathrin, and Johannes Riedel. "Know-Your-Customer (KYC) Requirements for Initial Coin Offerings." *Business & Information Systems Engineering* 63, no. 5 (October 8, 2021): 551–67. <https://doi.org/10.1007/s12599-020-00677-6>.
- Pavlidis, Georgios. "International Regulation of Virtual Assets under FATF's New Standards." *Journal of Investment Compliance* 21, no. 1 (July 8, 2020): 1–8. <https://doi.org/10.1108/JOIC-08-2019-0051>.
- Rahmdel, Mansour. "FATF and Money Laundering in Iran." *Journal of Money Laundering Control* 21, no. 3 (July 2, 2018): 314–27. <https://doi.org/10.1108/JMLC-07-2017-0033>.
- Reshetnikova, Natalia N., Magomedgabib M. Magomedov, Sergey S. Zmiyak, Aleksandr V. Gagarinskii, and Dmitry A. Buklanov. "Directions of Digital Financial Technologies Development: Challenges and Threats to Global Financial Security," 355–63. Springer, Cham, 2021. https://doi.org/10.1007/978-3-030-69421-0_38.
- Reynolds, Perri, and Angela S.M. Irwin. "Tracking Digital Footprints: Anonymity within the Bitcoin System." *Journal of Money Laundering Control* 20, no. 2 (May 2, 2017): 172–89. <https://doi.org/10.1108/JMLC-07-2016-0027>.
- Sultan, Nasir, Norazida Mohamed, Jamaliah Said, and Azroz Mohd. "The Sustainability of the International AML Regime and the Role of the FATF. The Objectivity of the Greylisting Process of Developing Jurisdictions like Pakistan." *Journal of Money Laundering Control*, April 11, 2023. <https://doi.org/10.1108/JMLC-12-2022-0166>.
- Truby, Jon. "Measuring Qatar's Compliance with International Standards on Money Laundering and Countering the Financing of Terrorism." *Journal of Money Laundering Control* 19, no. 3 (July 4, 2016): 264–77. <https://doi.org/10.1108/JMLC-04-2015-0011>.
- Tsingou, Eleni. "Fighting Financial Crime: Who Designs Global Governance and Who Does The Work?" *Fudan Journal of the Humanities and Social Sciences* 13, no. 2 (June 4, 2020): 169–79. <https://doi.org/10.1007/s40647-020-00278-3>.
- Vaithilingam, Santha, Mahendhiran Nair, and Thangarajah Thiyagarajan. "Managing Money Laundering in a Digital Economy." *Journal of Asia-Pacific Business* 16, no. 1 (January 2, 2015): 44–65. <https://doi.org/10.1080/10599231.2015.997626>.
- Virzo, Roberto. "Limits to Measures of Confiscation of Property Linked to Serious Criminal Offences in the Case Law of the European Court of Human Rights." *The Italian Yearbook of International Law Online* 30, no. 1 (November 10, 2021): 265–81. <https://doi.org/10.1163/22116133-03001015>.
- Wegberg, Rolf van, Jan-Jaap Oerlemans, and Oskar van Deventer. "Bitcoin Money Laundering: Mixed Results? An Explorative Study on Money Laundering of Cybercrime Proceeds

- Using Bitcoin.” Edited by Angela Futter. *Journal of Financial Crime*, March 7, 2018, 00–00. <https://doi.org/10.1108/JFC-11-2016-0067>.
- Whittaker, Joe. “The Role of Financial Technologies in US-Based ISIS Terror Plots.” *Studies in Conflict & Terrorism*, October 12, 2022, 1–26. <https://doi.org/10.1080/1057610X.2022.2133345>.
- Zolkafil, Salwa, Sharifah Nazatul Faiza Syed Mustapha Nazri, and Normah Omar. “Asset Recovery Practices in Combating Money Laundering: Evidence from FATF Mutual Evaluation Report of FATF Member Countries of Asia Pacific Region.” *Journal of Money Laundering Control* 26, no. 1 (January 2, 2023): 24–34. <https://doi.org/10.1108/JMLC-11-2021-0127>.