ARTICLE

CRYPTOCURRENCIES AND NATIONAL SECURITY: THE CASE OF MONEY LAUNDERING AND TERRORISM FINANCING

Shlomit Wagman[*]

CONTENTS

INTRODUCTION

Cryptocurrencies can be a haven for criminals, terrorists, and sanction evaders. The early, romantic ideology underlying blockchain technology envisioned a decentralized currency without geographical boundaries, governmental supervision, central bank control, or any identification required. Cryptocurrency was meant to be a fast, cheap, and reliable way of transferring value among strangers.

In 2014, the Financial Action Task Force (FATF), an international organization dedicated to combating money laundering and the financing of terrorism, identified the risks associated with cryptocurrency. By 2018, it developed an overall strategy to manage these risks and countermeasures designed by the FATF were enacted into binding global standards that all jurisdictions must adopt. Since then, the FATF has been leading coordinated

[*] Research Fellow, Mossavar-Rahmani Center for Business and Government, Harvard Kennedy School and Faculty Associate, Berkman Klein Center, Harvard Law School. Former Director-General of the Israel Money Laundering and Terror Financing Prohibition Authority, head of the Israeli delegation to the Financial Action Task Force (FATF) from 2016 to 2022, Co-Chair of the FATF's Research, Typologies, and Methods Group from 2019 to 2022, and former Acting Director-General of the Israel Privacy Protection Authority. The author earned a B.A. from Hebrew University of Jerusalem and an L.L.M. and J.S.D. from Yale Law School. The author would like to thank Professor Howell Jackson, John Haigh, Katherine Ford, and David Izack-Haim for their valuable input and comments.

implementation efforts around the world. The FATF's response was the first global, coordinated regulatory response to cryptocurrency risks. Dozens of countries have already adopted the FATF's cryptocurrency-related measures. It is imperative that the remaining countries follow suit, and that the FATF holds them accountable if they fail to do so.

This Article reviews the anti-money laundering and counter-financing of terrorism (AML/CFT) framework and its application to cryptocurrencies. Then, it presents case studies demonstrating the important contributions that the AML/CFT toolkit has made to countries' security. The case studies include the seizing of cryptocurrency used by terrorists for fundraising, revealing the identity of attackers in a ransomware cyberattack, and arresting terrorists who were paid through cryptocurrency and tracked before completing their planned attack. The Article concludes with recommendations for further actions that the global community, individual countries, and the private sector should take to better tackle AML/CFT risks, including unaddressed cryptocurrency-related challenges posed by decentralized systems.

I. CRYPTOCURRENCY RISKS FOR MONEY LAUNDERING AND TERRORISM FINANCING

Cryptocurrencies are a rising trend in the global economy, recently reaching a market value as high as $2.9 trillion.[1] This innovative, decentralized financial technology has the potential to initiate a revolution in the way society transfers value. The transformation could parallel the revolution of the 1990s that altered the way society transfers data. Cryptocurrencies can facilitate international commerce and cross-border financial activities and decrease transaction costs and barriers.

However, cryptocurrencies also pose challenges to national security and the integrity of financial systems. Certain unique characteristics make them appealing for conducting illegal activities: (1) they are decentralized, unsupervised by any government or central bank, and therefore, like cash, preserve a high degree of anonymity; (2) they are virtual and therefore generally unbounded by geographical borders; and (3) they do not require transactions be conducted in-person. Criminals, terrorists, and sanctions evaders have identified opportunities in this field and started to use cryptocurrencies for their illicit activities.

[1] As of early October 2022, the market value of crypto assets was estimated at around $1 trillion, which is actually a dramatic decrease from their market value in November 2021 of around $2.9 trillion. *Global Cryptocurrency Charts*, COINMARKETCAP, https://coinmarketcap.com/charts/ (last visited Nov. 4, 2022) [https://perma.cc/D68J-TLEX].

Cryptocurrencies are increasingly used for illicit activities. They have become the payment method of choice for a variety of criminals. Hackers that hold data captive are asking for ransom in cryptocurrencies, as was seen in the Wannacry and Colonial Pipeline cases.[2] Nefarious actors are increasingly using cryptocurrencies to pay for illicit activities, such as when Iran paid an individual to facilitate an unsuccessful plot to assassinate former U.S. National Security Advisor John Bolton.[3] Weapons dealers, drug dealers, human traffickers, and child pornography distributors are also receiving payment in cryptocurrencies.[4] Terrorist organizations are also using cryptocurrencies to raise funds. For example, ISIL called for cryptocurrency donations in this memorable poster:[5]

[2] Samuel Gibbs, *WannaCry: Hackers Withdraw £108,000 Of Bitcoin Ransom*, THE GUARDIAN (Aug. 3, 2017), https://www.theguardian.com/technology/2017/aug/03/wannacry-hackers-withdraw-108000-pounds-bitcoin-ransom [https://perma.cc/6G2X-MV2H]; Press Release, U.S. Att'y's Off. for the N. Dist. of Cal., Dep't of Just., Department of Justice Seizes $2.3 Million In Cryptocurrency Paid to the Ransomware Extortionists Darkside (June 8, 2021), https://www.justice.gov/usao-ndca/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists [https://perma.cc/QK86-U7QC].

[3] Press Release, Off. of Pub. Affs., Dep't of Just., Member of Iran's Islamic Revolutionary Guard Corps (IRGC) Charged with Plot to Murder the Former National Security Advisor (Aug. 10, 2022), https://www.justice.gov/opa/pr/member-irans-islamic-revolutionary-guard-corps-irgc-charged-plot-murder-former-national [https://perma.cc/5R3F-4NLC].

[4] *See, e.g.*, Press Release, U.S. Att'y's Off. for the W, Dist. of Mich., Dep't of Just., Plainwell Man, Benjamin James Cance, Charged with Illegal Arms Exportation, Other Crimes (Aug. 11, 2015) https://www.justice.gov/usao-wdmi/pr/2015_0811_BCance [https://perma.cc/A7UP-5WJ3]; U.S. Govt. Accountability Off., *As Virtual Currency Use In Human And Drug Trafficking Increases, So Do The Challenges For Federal Law Enforcement*, WATCHBLOG (Feb. 24, 2022), https://www.gao.gov/blog/virtual-currency-use-human-and-drug-trafficking-increases-so-do-challenges-federal-law-enforcement [https://perma.cc/TCT8-4VV3]; Danny Nelson, *Crypto Payments for Child Porn Grew 32% In 2019: Report*, COINDESK (July 12, 2022), https://www.coindesk.com/markets/2020/04/21/crypto-payments-for-child-porn-grew-32-in-2019-report/ [https://perma.cc/45US-NGMS].

[5] Press Release, Off. of Pub. Affs., Dep't of Just., Global Disruption of Three Terror Finance Cyber-Enabled Campaigns (Aug. 13, 2020), https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns [https://perma.cc/579K-VD2F].

In their attempt to avoid being traced, illegal actors have adopted ever more sophisticated cryptocurrency technologies, such as using cryptocurrencies that operate over private ledgers (e.g., ISIL's use of Monero for its fundraising)[6] or non-custodial wallets and sophisticated software that generate unique addresses for every donation (e.g., Hamas's fundraising campaign).[7] Cryptocurrency anonymizing services, commonly referred to as mixers, prevent tracing a transaction back to its source. North Korea recently used the mixer Tornado Cash to evade sanctions.[8]

Currently, the volume of financial crimes identified as being conducted through cryptocurrency is low, especially when compared to "traditional" financial services.[9] However, as cryptocurrency comes to be used more frequently, the risks of its abuse increase in turn. These abuses could circumvent the AML/CFT regime. It is therefore important to identify the ways that cryptocurrencies may be abused and encourage the development of both technological and regulatory measures in the early stages of innovation. Unless the risks of cryptocurrency abuse are properly mitigated, the industry's development will suffer. Regulators could even outlaw cryptocurrency, as China has attempted to do.[10]

---

[6] Andrew Shevchenko, *ISIS-Affiliated News Website to Collect Donations with Monero*, COINTELEGRAPH (June 25, 2020), https://cointelegraph.com/news/isis-affiliated-news-website-to-collect-donations-with-monero [https://perma.cc/P46S-TZT5].

[7] Anna Baydakova, *Hamas Tapped Binance to Launder Bitcoin Donations, Blockchain Data Suggests*, COINDESK (Sept. 14, 2021), https://www.coindesk.com/policy/2021/06/08/hamas-tapped-binance-to-launder-bitcoin-donations-blockchain-data-suggests/ [https://perma.cc/4QCU-KVDK].

[8] The U.S. designated the virtual currency mixer Tornado Cash, which has been used to launder more than $7 billion worth of virtual currency since its creation in 2019. Press Release, U.S. Dep't of the Treasury, U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash (Aug. 8, 2022), https://home.treasury.gov/news/press-releases/jy0916 [https://perma.cc/7GUZ-KP7U]. This includes over $455 million stolen by a North Korea-sponsored hacking that was subject to sanctions, the laundering of more than $96 million of malicious cyber actors' funds derived from the Harmony Bridge Heist, and at least $7.8 million from the Nomad Heist. *Id.*

[9] FIN. ACTION TASK FORCE, SECOND 12-MONTH REVIEW OF THE REVISED FATF STANDARDS ON VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS 22 (2021), https://www.fatf-gafi.org/media/fatf/documents/recommendations/Second-12-Month-Review-Revised-FATF-Standards-Virtual-Assets-VASPS.pdf [https://perma.cc/YE5E-TPW2] [hereinafter FATF SECOND 12-MONTH REVIEW] (para. 70, based on data provided by seven blockchain analytic companies).

[10] Alun Jon, Samuel Shen & Tom Wilson, *China's Top Regulators Ban Crypto Trading and Mining, Sending Bitcoin Tumbling*, REUTERS (Sept. 24, 2021), https://www.reuters.com/world/china/china-central-bank-vows-crackdown-cryptocurrency-trading-2021-09-24/ [https://perma.cc/6G48-NPFU].

II. DESIGNING A UNIFIED GLOBAL RESPONSE

The international community identified the risks that cryptocurrencies pose to the integrity of the global financial system relatively early. It then developed a comprehensive response, led by the Financial Action Task Force (FATF).

The FATF is the international watchdog responsible for coordinating the global fight against money laundering, terrorism financing, and nuclear proliferation.[11] It is a proactive and robust organization that enjoys tremendous professional credibility and global influence over both member and non-member countries. The FATF is composed of thirty-nine member countries (including most of the G20 countries) and regional organizations, and together with its nine associated FATF-Style Regional Bodies (FSRBs), it encompasses over 200 jurisdictions.[12]

The FATF has defined forty standards, called "Recommendations," which are in fact mandatory measures that all countries and jurisdictions must implement into their national legal systems.[13] All jurisdictions, regardless of their membership status, must adopt the FATF Recommendations into their legal framework and implement them in an efficient manner or risk being cut off from the global financial system. The FATF and FSRBs conduct ongoing monitoring to review and evaluate the level of compliance of countries with these Recommendations.[14] When the FATF finds that a jurisdiction has a substantial deficiency or non-cooperation with the evaluation process, it may list that jurisdiction on its grey or blacklist.

---

[11] The organization was established in 1989 by the G7 countries with the aim of developing and promoting policies to combat money laundering at the national and global levels. After the terror attacks of September 11, 2001, its mandate was expanded to combat terrorism financing as well. For additional background on the FATF, see Juan Zarate & Sarah Watson, *The Lexicon of Terror: Crystallization of the Definition of "Terrorism" Through the Lens of Terrorist Financing & the Financial Action Task Force*, 13 HARV. NAT'L SEC. J. 369, 394–97, 403–08 (2022).

[12] *Id.*

[13] *See* FIN. ACTION TASK FORCE, INTERNATIONAL STANDARDS ON COMBATING MONEY LAUNDERING AND THE FINANCING OF TERRORISM & PROLIFERATION (2022), https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf [https://perma.cc/6XP8-9CAT] [hereinafter FATF RECOMMENDATIONS]. The Recommendations include the obligations for countries to set criminal offenses of money laundering and terrorism financing, set mechanisms for the seizure and forfeiture of illicit assets, conduct national risk assessments, develop capabilities to conduct financial investigations, establish a national Financial Intelligence Unit (FIU), and cooperate with international counterparts. *See generally id.*

[14] *See Mutual Evaluations*, FIN. ACTION TASK FORCE, https://www.fatf-gafi.org/publications/mutualevaluations/documents/more-about-mutual-evaluations.html (last visited Nov. 15, 2022) [https://perma.cc/UU4C-EEBT].

The "grey list" refers to the list of jurisdictions under increased monitoring. These are jurisdictions that are "actively working with the FATF to address strategic deficiencies in their regimes to counter money laundering, terrorist financing, and proliferation financing."[15] They have agreed to do so within agreed timeframes, and in the meantime are subject to increased monitoring by other jurisdictions. As of October 2022, there are twenty-three countries on this list.[16]

The "blacklist" refers to the list of high-risk jurisdictions that have "significant strategic deficiencies in their regimes to counter money laundering, terrorist financing, and financing of proliferation."[17] Toward countries on the blacklist, "the FATF calls on all members and urges all jurisdictions to apply enhanced due diligence, and, in the most serious cases, countries are called upon to apply counter-measures to protect the international financial system from the money laundering, terrorist financing, and proliferation financing risks (ML/TF/PF) emanating from the country."[18] As of October 2022, North Korea, Iran, and Myanmar are the only countries listed on the FATF's blacklist.[19]

These lists are powerful signaling tools that put severe pressure on the listed jurisdictions to quickly meet FATF Recommendations. Jurisdictions on the lists are marked as high-risk territories for AML/CFT purposes, limiting their respective financial sectors' ability to participate in the global market.[20] A place on the blacklist practically abolishes financial activities between the blacklisted country and other jurisdictions.[21]

The FATF was the first international organization to develop a holistic strategic response to cryptocurrency security risks. Compared to other regulators, the FATF acted relatively early in assessing the significant risks

---

[15] *Jurisdictions under Increased Monitoring*, Fin. Action Task Force. (Oct. 21, 2022), https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/increased-monitoring-october-2022.html [https://perma.cc/QS4Q-KN9B].

[16] *Id.*

[17] *High-Risk Jurisdictions subject to a Call for* Action, FIN. ACTION TASK FORCE (Oct. 21, 2022), https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/call-for-action-october-2022.html [https://perma.cc/CK35-UDHS].

[18] *Id.*

[19] *Id.*

[20] Zarate & Watson, *supra* note 11, at 405, 408. The philosophy behind the FATF's mandate rests on the notion that financial enforcement has the capability to supplement other coercive measures and effectively combat against crime and terrorism. The financial enforcement toolbox is a separate and complementary channel to the traditional criminal toolbox. Since funds are being funneled through global economies, and the global regime is as strong as its weakest link, global compliance is monitored closely.

[21] *See id.*

that cryptocurrencies pose to the AML/CFT regime. This astute assessment, along with the organization's dynamic and proactive nature, allowed the FATF to quickly bring the relevant experts together to design a holistic solution to the risks that cryptocurrencies pose to the AML/CFT field, while not holding off innovation.

In 2014 and 2015, the FATF published risk analysis and guidance specific to cryptocurrency.[22] In 2018, it amended its mandatory Recommendations to explicitly apply cryptocurrency to its rules.[23] The FATF has continued to be responsive to impending challenges by publishing clarifications and updates related to the application of the FATF Recommendations to the cryptocurrency industry.[24]

---

[22] In June 2014, the FATF issued a document which sets key definitions and maps potential AML/CFT risks regarding virtual assets in response to the emergence of virtual currencies and their associated payment mechanisms. FIN. ACTION TASK FORCE, VIRTUAL CURRENCIES: KEY DEFINITIONS AND POTENTIAL AML/CFT RISKS (2014), http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf [https://perma.cc/B3GD-EN5C]. In June 2015, the FATF issued guidance for a risk-based approach to virtual currencies as part of a staged approach to addressing their AML/CFT risks. FIN. ACTION TASK FORCE, GUIDANCE FOR A RISK-BASED APPROACH: VIRTUAL CURRENCIES (2015), https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf [https://perma.cc/YKD9-BBKD].

[23] In October 2018, the FATF adopted changes to Recommendation 15, explicitly clarifying that it applies to financial activities involving cryptocurrency and added two new definitions in the Glossary: "virtual asset" (VA) and "virtual asset service providers" (VASP). Press Release, Fin. Action Task Force, Regulation of Virtual Assets (Oct. 19, 2018), https://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets.html [https://perma.cc/B8VP-Q5ZS]; *see also* FATF RECOMMENDATIONS, *supra* note 13, at 17 (Recommendation 15).

[24] In June 2019, the FATF published further guidance on the application of a risk-based approach to the cryptocurrency industry. FIN. ACTION TASK FORCE, GUIDANCE FOR A RISK-BASED APPROACH TO VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS (2019), https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf [https://perma.cc/4FLE-RGWU]. This guidance was updated in October 2021. FIN. ACTION TASK FORCE, UPDATED GUIDANCE FOR A RISK-BASED APPROACH TO VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS (2021), https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf [https://perma.cc/7CG5-VQJ5] [hereinafter FATF UPDATED GUIDANCE]. In June 2020, the FATF published a report to the Financial Ministers of the G20 on "so-called stablecoins." FIN. ACTION TASK FORCE, FATF REPORT TO THE G20 FINANCE MINISTERS AND CENTRAL BANK GOVERNORS ON SO-CALLED STABLECOINS (2020), https://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-FATF-Report-G20-So-Called-Stablecoins.pdf [https://perma.cc/W5AZ-DH5K]. In June 2020, June 2021, and July 2022, the FATF published updates on the application of the FATF Recommendations to the virtual asset industry. FIN. ACTION TASK FORCE, 12-MONTH REVIEW OF THE REVISED FATF STANDARDS ON VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS (2020), https://www.fatf-gafi.org/media/fatf/documents/recommendations/12-Month-Review-Revised-FATF-Standards-Virtual-Assets-VASPS.pdf [https://perma.cc/B973-K4Z2]

A. The Essence of the AML/CFT Global Regime for Cryptocurrency

The FATF's regulatory approach to cryptocurrency is similar to the approach it has taken to regulating traditional financial activities. The FATF requires countries to impose the full AML/CFT framework, albeit with relevant modifications pertinent to cryptocurrencies' unique technological characteristics.

To ensure that the regulations are as effective as possible, and to avoid circumvention of its global Recommendations, the FATF defined cryptocurrency assets broadly. FATF chose the term "Virtual Assets" (VA) rather than "cryptocurrency" or "digital asset" to refer broadly to any "digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes."[25] The definition does not include the digital representation of fiat currencies.[26]

As it has done when regulating other financial activities, the FATF also identified virtual asset platforms capable of monitoring the financial activities conducted through their systems, termed "Virtual Assets Service Providers" (VASPs). This term was also defined broadly to capture all relevant services, including virtual currency exchanges and certain types of wallet providers.[27]

All jurisdictions must establish licensing or registration requirements for VASPs.[28] At a minimum, VASPS must be licensed where they were legally created.[29] Some jurisdictions may also require licensing or registration as a condition for conducting business.[30] VASPs should be subject to the full range of preventative measures and AML/CFT obligations, similar to other financial intermediaries. These obligations include, among others, the requirements of conducting customer due diligence and ongoing monitoring, recordkeeping, submitting of suspicious transaction reports (STR) to the designated Financial Intelligence Unit (FIU), and screening customers and transactions against

---

[hereinafter FATF FIRST 12-MONTH REVIEW]; FATF SECOND 12-MONTH REVIEW, *supra* note 9; FIN. ACTION TASK FORCE, TARGETED UPDATE ON IMPLEMENTATION OF THE FATF STANDARDS ON VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS (2022), https://www.fatf-gafi.org/media/fatf/documents/recommendations/Targeted-Update-Implementation-FATF%20Standards-Virtual%20Assets-VASPs.pdf [https://perma.cc/Q7ZG-3V3H] [hereinafter FATF TARGETED UPDATE].

[25] FATF RECOMMENDATIONS, *supra* note 13, at 132.

[26] *Id*.

[27] *See id.* at 133.

[28] FATF RECOMMENDATIONS, *supra* note 13, at 17 (Reccomendation 15), 76 (Interpretive Note to Recommendation 15); FATF UPDATED GUIDANCE, *supra* note 24, paras. 123–141.

[29] FATF RECOMMENDATIONS, *supra* note 13, at 76 (Interpretive Note to Recommendation 15); FATF UPDATED GUIDANCE, *supra* note 24, para. 125.

[30] FATF UPDATED GUIDANCE, *supra* note 24, para. 127.

designation lists.[31] In order to conduct the needed examinations as part of the consumer due diligence and licensing process, the FATF recommends using relevant tools and resources, such as blockchain analytic tools.[32]

Given the cross-border nature of VASPs' activities, the FATF Recommendations require them to impose additional preventive measures.[33] With respect to the Customer Due Diligence (CDD) requirements, set under Recommendation 10, the FATF adopted in 2019 a low $/€1,000 threshold for VA transfers that trigger FATF CDD obligations.[34] Most importantly, the FATF adopted a "Travel Rule" requirement for VASPs. The Travel Rule, a modification to FATF Recommendation 16 regarding wire transfers, requires VASPs to obtain, hold, and transmit required originator and beneficiary information, immediately and securely, when conducting VA transfers.[35] These are the same obligations traditional financial intermediaries are required to undertake when they transmit transaction information via SWIFT.[36] Countries are advised to ensure that their implementation of these requirements is compatible with data protection and privacy laws.[37]

Dozens of jurisdictions already adopted the FATF regime on VA, but many others still need to follow suit. As of June 2021, fifty-two jurisdictions reported to the FATF that they have enacted the VA-related Recommendations into their local legislation, and twenty-six additional jurisdictions reported that they are in the process of introducing the measures as legislation.[38] With respect to implementation of the Travel Rule, as of March 2022, only twenty-nine jurisdictions reported to the FATF they have implemented the Travel Rule in their domestic legislation and only eleven reported having begun enforcement.[39] This lack of uniform implementation enables jurisdictional

---

[31] *See id.* para. 85.
[32] *See id*. paras. 130(a), 234.
[33] *See* FATF RECOMMENDATIONS, *supra* note 13, at 76–77 (Interpretive Note to Recommendation 15).
[34] *Id.* at 77 (para. 7(a)). In other words, all VASPs around the globe should conduct CDD procedures for any transaction above the threshold of $/€1,000. Since these procedures are usually conducted remotely, the user's provided information is usually verified against governmental identification, and by cross-referencing that with biometric data, which is usually more reliable than face-to-face human verification.
[35] *Id*. (para. 7(b)).
[36] *See id.* at 79 (para. 6).
[37] *Id.* at 11.
[38] SECOND 12-MONTH REVIEW, *supra* note 9, at 10–11 (paras. 27–28).
[39] *See* FATF TARGETED UPDATE, *supra* note 24, at 10 (para. 12). Ninety-eight jurisdictions responded to the survey. *Id.* at 5 (para. 6). Around a quarter of those that responded reported they were in the process of passing the relevant legislation, while around a third (thirty-six out of ninety-eight) had not started implementing the Travel Rule into domestic legislation. *Id.* at 10 (para. 12). "Over half of FATF Global Network did not respond to the survey and it is assumed that those jurisdictions have not made progress in Travel Rule implementation." *Id.* at 3, n. 8.

arbitrage by criminals. When criminals find that one country has implemented the FATF Recommendations whereas another country has not, the criminals can locate their transactions in the jurisdiction with lax standards.

B. Law Enforcement and Cryptocurrency

Aside from the risks associated with virtual assets, their digital environment provides ample unique opportunities for law enforcement agencies (LEAs) to conduct financial investigations. Analysis of public blockchain ledgers allows both the private sector (VASPs and other financial institutions) and LEAs to trace financial activities over the public blockchain and identify connections to suspicious transactions and illegal activities even if the cryptocurrency holder is represented only by a wallet number.[40] The public ledgers allow analyzing and tracing a long history of transactions, thereby identifying whether the funds were involved in a known illicit activity, comingled with illegal funds, processed by an unregulated VASP, or were suspiciously treated (e.g., they were treated with an anonymity-enhancing mixer). In addition, because the data is available in digital format, analysts can apply sophisticated machine learning and artificial intelligence techniques to reveal hidden information. At the same time, it is important to note that blockchain analytics is not a silver bullet. Private ledger cryptocurrencies, such as Monero, provide very limited public information.[41]

When VASPs collect data pursuant to their AML/CFT obligations, the data can provide the linkage between pseudonymous wallets and identifiable entities, especially when virtual asset holders cash in/out from/to fiat currency. The information collected by VASPs as part of their customer due diligence obligations includes a vast repository of revealing data, including government-issued identification (which is often crossed with biometric data), geographical location, IP addresses, statements regarding the source of funds, beneficial owners, and VASP-identified concerns based on the consumer or transaction's nature. This information can be obtained by LEAs as a result of spontaneous reporting by VASPs to the relevant FIU, or following a request by an LEA (either a request for additional information by the FIU or a court-issued warrant). When the financial intelligence held by LEAs is combined with other relevant intelligence (such as open-source intelligence (OSINT)), signals intelligence (SIGINT), and human intelligence (HUMINT), it empowers LEAs to trace suspicious financial activities and unmask the lawbreakers.

---

[40] *See, e.g.*, John Bohannon, *Why Criminals Can't Hide Behind Bitcoin*, SCIENCE, (Mar. 9, 2016) https://www.science.org/content/article/why-criminals-cant-hide-behind-bitcoin [https://perma.cc/89KA-GF9M].

[41] These limitations pose tremendous challenges to LEAs in tracing such activities. This is among the reasons that international criminals have increasingly utilized private cryptocurrency ledgers. *See, e.g.*, Shevchenko, *supra* note 6 (discussing ISIL's use of a private ledger to collect donations).

III. CASE STUDIES

A few examples from the author's professional experience demonstrate how the unique combination of information collected by VASPs as part of their AML/CFT obligations, blockchain analytics, and additional intelligence has been crucial to law enforcement investigations and contributed substantially to their successes.

A. Terror Fundraising: Hamas Case

Hamas, which has been designated as a terrorist organization by the United States, the European Union, and Israel, has been fundraising in cryptocurrency since at least 2019. At first, Hamas used regular cryptocurrency wallets, but later moved to use non-custodial wallets. Most recently, Hamas has adopted advanced software that generates a unique address for each new donation.[42]

In 2021, intelligence indicated that Hamas launched fundraising campaign via social media asking for donations in cryptocurrency. In July 2021, the Israeli Minister of Defense designated crypto wallets related to this fundraising that were associated with Hamas' military wing.[43] The designation was made under Israel's Anti-Terrorism Law and certified that those funds were associated with terrorists, requiring their immediate seizure. The designation included over 20 different types of cryptocurrencies, including bitcoin, Ether, Tether, TRON, Cardano, XPR, Doge, and more.[44] This was probably the first terrorism financing-related cryptocurrency designation to include such a wide variety of cryptocurrencies.[45]

The designations were made public and also actively distributed by Israel's National Bureau for Counter Terror Financing (NBCTF) to VASPs around the globe. Shortly thereafter, many VASPs, regulated and nonregulated, identified connections to the designated wallets and shared this information with the NBCTF. Some sources communicated the information

---

[42] *See* Baydakova, *supra* note 7.
[43] *See* Administrative Seizure Order (ASO-44/21), MINISTRY OF DEFENSE (Isr.) https://nbctf.mod.gov.il/he/Announcements/Documents/%d7%a6%d7%aa%2044-21.pdf [https://perma.cc/UQ79-V5VR].
[44] *Hamas Cryptocurrency Donations Update | Seizures by Israel's National Bureau for Counter Terror Financing (NBCTF)*, CIPHERTRACE (July 16, 2021), https://ciphertrace.com/hamas-cryptocurrency-donations-update-seizures-by-israels-national-bureau-for-counter-terror-financing-nbctf [https://perma.cc/HKP6-UV38]; *Israeli Government Seizes Cryptocurrency Addresses Associated with Hamas Donation Campaigns*, CHAINALYSIS (July 8, 2021), https://blog.chainalysis.com/reports/israel-hamas-cryptocurrency-seizure-july-2021/ [https://perma.cc/5W68-WT4Z] [hereinafter CHAINALYSIS REPORT].
[45] *See id.*

directly to the NBCTF, while others informed the relevant LEAs in their respective jurisdictions or disseminated suspicious transaction reports to their own FIU, which in turn cooperated with the Israeli FIU and other relevant LEAs. The valuable information provided by VASPs around the globe included significant data they gathered by following their AML/CFT obligations, as well as through open-source information and blockchain analytics, and greatly assisted in tracing relevant wallets and seizing related funds.

Additionally, blockchain analytics companies conducted independent research regarding the designated wallets, revealing connections to additional wallets associated with the designation and with previous terror financing investigations.[46] Most findings became public when the companies published their investigations, which assisted in revealing new links to relevant suspected terrorism financing activities.

This case demonstrated that VASPs' cooperation can lead to important information sharing with LEAs. The information VASPs gathered as part of their AML/CFT obligations, in conjunction with blockchain analytics from the private sector, enabled Israel's NBCTF to seize and confiscate crypto wallets worth millions of dollars.

B. Crypto to Fiat Exchange Hints at the Identities of Ransomware Attackers

In a large, national cyberattack in Israel with national security implications, ransomware actors demanded payment in bitcoin. The attackers' identities were unknown and it was not clear whether they were common criminals or terrorists aiming to damage national infrastructures. The Israel Anti-Money Laundering and Terrorism Financing Prohibition Authority, Israel's FIU, was able to identify, based on transaction reports submitted to it by VASPs and other financial institutions (pursuant to their AML/CFT obligations) and open-source information, that the bitcoins transferred as part of the early negotiations with the hackers were redeemed into fiat currency at a currency exchange located in a particular jurisdiction. In the Israeli context, activity from that jurisdiction would most likely mean that the attack was geopolitically motivated and therefore the subsequent national response was designed accordingly. Having access to relevant data gathered by VASPs pursuant to their AML/CFT obligations can prove extremely valuable in analyzing national security incidents.

[46] *See, e.g.*, CHAINALYSIS REPORT, *supra* note 44.

C. Crypto to Fiat Exchange Helps Thwart Terrorist Plot

In a recent classified event, LEAs attempted to trace terror activists who were on their way to committing an act of terror. The terrorists were paid in cryptocurrency and cashed out in local fiat currency near the location of their planned mission. Based on the intelligence available to LEAs, which combined public open-source intelligence (OSINT) and blockchain analytics with due diligence information collected from VASPs, the LEAs were able to trace the terrorists and arrest them after they cashed out and before executing their plot.

IV. RECOMMENDATIONS

While the FATF should be praised for its global response to cryptocurrency's national security risks, the FATF Recommendations alone are insufficient to remedy the industry's pressing challenges. In order to further protect the financial system from the AML/CFT risks of cryptocurrency, while still promoting financial innovation, the following actions should be undertaken:

First, the FATF Recommendations must be implemented globally. The global standards must be implemented and enforced swiftly and effectively by all countries. A chain is only as strong as its weakest link. Without this step, the virtual nature of cryptocurrencies makes them ripe for jurisdictional arbitrage. All remaining governments must promptly adopt these requirements into their national legislation, especially the Travel Rule requirements given the large number of jurisdictions that have not yet done so.[47]

Second, the FATF should continue developing further standards and providing clarity on regulations affecting new financial technology products and emerging risks. Particularly important are higher-risk structures which eliminate intermediaries, such as decentralized finance (DeFi), decentralized governance structures (DAOs), peer-to-peer (P2P) transactions between unhosted wallets, and non-fungible tokens (NFTs). For example, with respect to DeFi applications, the FATF has already noted that even if such arrangements seem decentralized, the creators, owners or operators (or those maintaining other manners of control or sufficient influence) of these DeFi arrangements, may substantially fall under the current FATF definition of what constitutes a VASP.[48] The obligations for DeFi arrangements should be further refined.

---

[47] For current statistics on the implementation of the Travel Rule, see note 39 and accompanying text *supra*.

[48] FATF UPDATED GUIDANCE, *supra* note 24, at 27 (para. 67).

The continued development of the global FATF structure should be conducted in consultation with the private sector, which holds expertise and potential technological solutions to some of the hard problems in the field and which can also assist regulators in learning about new products and technologies as they develop. Regulatory experts should also be consulted to ensure that new regulations are harmonized with relevant additional regulation, both existing and new, relating to data protection, taxation, cybersecurity, investors and consumer protection, and financial stability.

Third, the private sector has an important role to play in developing technological solutions that ensure the integrity of the global financial ecosystem and enhance its legitimacy. It has a strong incentive to do so after it has become clear in recent years that, absent compliance with AML/CFT principles (to which other financial sector actors are bound), the cryptocurrency industry will continue facing regulatory difficulties, exclusion, and slower adoption. Until regulators master their understanding of the field and produce efficient solutions, the private sector should assume a leadership role and promote the design of *technological* solutions that implement AML/CFT principles (AML/CFT by design).

Technology developed by experts who understand the complex, and sometimes contradictory, financial regulations can help achieve the needed balance. Developers can design innovative technological solutions that solve current challenges in more sophisticated ways. For example, they can create financial services and products that ensure a high level of AML/CFT compliance and advance multiplayer information sharing mechanisms (between private-public or private-private counterparts) while ensuring a higher level of privacy than currently available (e.g., by using privacy-enhancing technologies such as zero-knowledge-proofs, homomorphic encryption, differential privacy, etc.).

In addition, the private sector, which has recently achieved significant progress in developing technological solutions for the FATF Travel Rule and in making those solutions widely available, should now undertake further efforts to strengthen *interoperability* across the different technological solutions. It should also ensure these solutions maintain flexibility to accommodate nuances in domestic regulatory requirements.

Moreover, the digital environment provides excellent opportunities for the Regulation Technology (RegTech) industry to lead a paradigm shift in the way financial transactions are monitored by financial intermediaries. For example, it allows for the promotion of a shift from the current focus on monitoring customers (the Know Your Customer approach) to a focus on monitoring transactional *patterns*. This can be facilitated by leveraging

artificial intelligence and machine learning technologies and applying them to public blockchain ledgers.

Fourth, law enforcement agencies must continue developing capabilities to monitor cryptocurrency transactions. They should endeavor to train investigators on illicit finance investigations involving cryptocurrencies, recruit experts in the field, and acquire advanced information technology systems, all of which will admittedly prove challenging. Information-sharing mechanisms should be revised to allow real-time analysis and swift data dissemination from VASPs. Seizure and confiscation mechanisms should be updated to confront the novel challenges associated with the digital environment. This will require updates to the way wallets are seized, maintained, and their value realized.

Fifth, international cooperation is critical in this virtual ecosystem. Strong international collaboration should be established among law enforcement officials across countries and between law enforcement officials and the private sector. In particular, law enforcement and financial institutions should cooperate in real-time. Existing collaborations, such as the Egmont Group, which connects FIUs globally, should be strengthened.[49]

Finally, moving forward, policy considerations underlying the fast development of the digital assets economy and Web3 should be afforded greater scrutiny. This should be done utilizing values-based decision-making. Consideration should be given to fundamental questions, such as which activities involving digital assets are desirable, which intermediaries should take part in these activities, and to what extent will their role alter current centers of power in the economy, increase decentralization, and encourage smaller new players to take larger part in the economy and become the new intermediaries.

[49] The Egmont Group of Financial Intelligence Units is an international organization that gathers all FIUs around the world. Each jurisdiction is required by the FATF Recommendations to establish an FIU and to exchange financial intelligence domestically and internationally with counterpart FIUs to combat money laundering, terrorist financing, and other predicate crimes. *See* FATF RECOMMENDATIONS, *supra* note 13, at 24 (Reccomendation 29), 104 (Interpretive Note to Recommendation 29), 113 (Interpretive Note to Recommendation 40). The Egmont Group provides its member FIUs with a platform for the secure exchange of financial intelligence, as well as for improving expertise. The organization is currently composed of 166 member FIUs. *About*, EGMONT GROUP, https://egmontgroup.org/about/ (last visited Oct. 22, 2022) [https://perma.cc/TQG3-MMJJ].