DRAFT – NOT FOR CITATION

14 HARV. NAT'L SEC. J. (forthcoming Dec. 2022)

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

Shlomit Wagman[*]

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 designed relevant countermeasures. The countermeasures were implemented into the binding global standards that all jurisdictions must adopt, and FATF has been leading coordinated implementation efforts around the world. FATF's response was the first global, coordinated regulatory response to cryptocurrencies; dozens of countries have already adopted FATF's cryptocurrency measures. It is imperative that the remaining countries follow suit, and that FATF holds them accountable for doing so.

This paper will review the anti-money laundering and counter-financing of terrorism (AML/CFT) framework and its application to cryptocurrencies. Then, it will present case studies demonstrating the important contributions that the AML/CFT toolkit has made to financial systems' global integrity and security. The case studies include the seizing of crypto used by terrorists for fundraising, revealing the identity of attackers in a ransomware cyberattack, and arresting terrorists who were paid through crypto and traced before completing their planned attack. This paper will also highlight unaddressed cryptocurrency challenges, including decentralized systems and un-hosted wallets. Finally, the paper will recommend potential actions that the global community, individual countries, and the private sector can take.

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 USD 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

[*] 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 and 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 would like to thank Mrs. Katherine Ford, an MPA candidate at the Harvard Kennedy School, for her valuable input and comments.

[1] As of June 2022, the market value of crypto assets is estimated at around USD 1 trillion, which is actually a dramatic decrease from their market value in November 2021 of around USD 2.9 trillion. https://coinmarketcap.com/charts/.

international commerce and cross-border financial activities and decrease transaction costs and barriers.

However, cryptocurrencies pose challenges to national security and financial systems' integrity. Cryptocurrencies have unique characteristics that make them appealing for 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 unbound to 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.

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 as a payment method 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 receiving payment in cryptocurrency.[4] Terrorist organizations are also raising funds in cryptocurrency. For example, ISIL called for crypto donations in this memorable poster[5]:

In their attempts to avoid tracing, illegal actors have adopted even more sophisticated cryptocurrency technologies, such as using cryptocurrencies that operate over private ledgers

[2] https://www.theguardian.com/technology/2017/aug/03/wannacry-hackers-withdraw-108000-pounds-bitcoin-ransom; https://www.justice.gov/usao-ndca/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists.

[3] https://www.justice.gov/opa/pr/member-irans-islamic-revolutionary-guard-corps-irgc-charged-plot-murder-former-national.

[4] See, e.g., https://www.justice.gov/usao-wdmi/pr/2015_0811_BCance; https://www.gao.gov/blog/virtual-currency-use-human-and-drug-trafficking-increases-so-do-challenges-federal-law-enforcement; https://www.coindesk.com/markets/2020/04/21/crypto-payments-for-child-porn-grew-32-in-2019-report/.

[5] https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns.

(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 by virtual assets is low, especially when compared with that of other "traditional" financial crimes.[9] However, as cryptocurrency is 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 cryptocurrency may be abused and encourage the development of both technological and regulatory measures in the early stages of innovation. Unless risks of cryptocurrency abuse are properly mitigated, the field's development will suffer. Regulators could even outlaw cryptocurrency, as countries such as China have attempted to do.[10]

II. Designing a Unified Global Response

The international community identified the risks that cryptocurrencies pose to the integrity of the entire global financial system relatively early. It then developed a comprehensive response.

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

---

[6] https://cointelegraph.com/news/isis-affiliated-news-website-to-collect-donations-with-monero.

[7] https://www.coindesk.com/policy/2021/06/08/hamas-tapped-binance-to-launder-bitcoin-donations-blockchain-data-suggests/.

[8] https://home.treasury.gov/news/press-releases/jy0916. 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. 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.

[9] FATF's 12-Month Review of Revised FATF Standards on Virtual Assets and VASPs [*June 2020*] provides an overview of the estimated illicit use of VAs, based on data provided by seven blockchain analytic companies. See https://www.fatf-gafi.org/publications/fatfrecommendations/documents/12-month-review-virtual-assets-vasps.html.

[10] https://www.reuters.com/world/china/china-central-bank-vows-crackdown-cryptocurrency-trading-2021-09-24/.

[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, as a main strategy for the combat against criminality and organized crime via financial tools. Subsequent to the terror events of September 11, its mandate was expanded to combat terrorism financing as well. For additional background on 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.

FATF enumerated FATF Standards, which are mandatory measures for all countries and jurisdictions to implement into their national legal systems.[13] All jurisdictions, regardless of their membership status, must adopt FATF Standards into their legal framework and implement them in an efficient manner or risk being cut off from the global financial system. FATF and FSRBs conduct ongoing monitoring to review and evaluate the level of compliance of countries with these Standards.[14] When 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.

The "grey list" refers to the list of jurisdictions under increased monitoring. Those are jurisdictions are actively working with FATF to address strategic deficiencies in their regimes to counter money laundering, terrorist financing, and proliferation financing. When FATF places a jurisdiction under increased monitoring, it means the country has committed to resolve swiftly the identified strategic deficiencies within agreed timeframes and is subject to increased monitoring.[15] The "blacklist" refers to the list of high-risk jurisdictions that have significant strategic deficiencies to counter money laundering, terrorist financing, and proliferation financing. For all countries identified as high-risk, FATF calls on all members 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 emanating from the country.[16]

Those lists are powerful signaling tools that put severe pressure on the listed jurisdictions to quickly meet FATF Standards. 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.[17] A place on the blacklist practically abolishes financial activities within the jurisdiction.[18]

---

[13] FATF standards are articulated in its 40 Recommendations, and in the Interpretive Notes and Methodology. The Standards include, among others, 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, include the establishment of a national Financial Intelligence Unit (FIU), cooperate with international counterparts, etc. See *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation*, FATF (2012), https://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html (updated March 2022).

[14] FATF is assessing these requirements and how well countries are implementing these measures as part of its mutual evaluation process. It evaluates the legal and institutional framework of a country, as well as whether that framework produces expected results. Countries that have already undergone their mutual evaluation in the past years will be required to report back during their follow-up process on the actions they have taken in this area. https://www.fatf-gafi.org/publications/virtualassets/documents/virtual-assets.html?hf=10&b=0&s=desc(fatf_releasedate).

[15] http://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/increased-monitoring-june-2022.html.

[16] http://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/call-for-action-february-2020.html. As of September 2022, North Korea and Iran are the only countries listed on FATF's blacklist.

[17] Zarate & Watson, supra note 11, 405–08. The philosophy behind FATF's mandate rest on the notion that financial enforcement has the capability to supplement and ensure effective 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 the global economies, and the global regime is as strong as its weakest link, global compliance is monitored closely.

[18] See id.

FATF was the first international organization to develop a holistic strategic response to cryptocurrency's security risks. As compared to other regulators, FATF acted relatively early in assessing the significant risks that cryptocurrency poses to the AML/CFT regime. This astute assessment, along with the organization's dynamic and proactive nature, allowed FATF to quickly bring the relevant experts together to design a holistic solution to the risks that cryptocurrency poses to the AML/CFT field.

In 2014-2015, FATF published mapping and risk analysis exercises.[19] By 2018, it amended the mandatory standards to apply cryptocurrencies to its rules, which all jurisdictions must promulgate through their own legal systems.[20] FATF has continued to be responsive to impending challenges by publishing clarifications and updates on applying its standards to the field and implementing a risk-based approach when considering updates.[21]

III. The Essence of the AML/CFT Global Regime Regarding Crypto

FATF's regulatory approach to cryptocurrencies is similar to the approach it has taken to regulate all other traditional financial activities. It requires countries to impose the full

[19] In June 2014, FATF issued a document which sets key definitions and maps potential AML/CFT risks regarding virtual assets (http://www.fatf-gafi.org/publications/methodsandtrends/documents/virtual-currency-definitions-aml-cft-risk.html), in response to the emergence of virtual currencies and their associated payment mechanisms for providing new methods of transmitting value over the Internet. In June 2015, FATF issued the Guidance for a Risk-Based Approach to Virtual Currencies, as part of a staged approach to addressing the money laundering and terrorist financing (ML/TF) risks associated with virtual currency payment products and services. https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf.

[20] In October 2018, FATF adopted changes to Recommendation 15 ("New technologies") to explicitly clarify that it applies to financial activities involving virtual assets, and also added two new definitions in the Glossary, "virtual asset" (VA) and "virtual asset service provider" (VASP). https://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets.html. The amended FATF Recommendation 15 requires that VASPs be regulated for anti-money laundering and combating the financing of terrorism (AML/CFT) purposes, licensed or registered, and subject to effective systems for monitoring or supervision. FATF Recommendations, supra note 13, at 17. In June 2019, FATF adopted an Interpretive Note to Recommendation 15 to further clarify how FATF requirements should apply in relation to VAs and VASPs, in particular with regard to the application of the risk-based approach (RBA) to VA activities or operations and VASPs; supervision or monitoring of VASPs for AML/CFT purposes; licensing or registration; preventive measures, such as customer due diligence, recordkeeping, and suspicious transaction reporting, among others; sanctions and other enforcement measures; and international co-operation. https://www.fatf-gafi.org/publications/fatfrecommendations/documents/public-statement-virtual-assets.html; FATF Recommendations, supra note 13, at 76–77.

[21] In June 2019, FATF also published Guidance on the application of the RBA to VAs and VASPs. https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html. This guidance was updated in October 2021. https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets-2021.html. In June 2020, FATF published a report to the Financial Ministers of the G20 on the "So-Called Stablecoins": https://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-FATF-Report-G20-So-Called-Stablecoins.pdf.
In addition, it published in June 2020 a 12-Month Review of Revised FATF Standards on Virtual Assets and VASPs, and in July 2021 the 2nd 12-Month Review of Revised FATF Standards on Virtual Assets and VASPs. In June 2022, it published the Targeted Update on Implementation of FATF's Standards on VAs and VASPs. https://www.fatf-gafi.org/media/fatf/documents/recommendations/Targeted-Update-Implementation-FATF%20Standards-Virtual%20Assets-VASPs.pdf.

AML/CFT framework, albeit with relevant modifications pertinent to cryptocurrencies' unique technological characteristics.

In order to ensure that the regulations are as effective as possible, and to avoid circumvention of the global standards, FATF defined crypto 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, transferred, or used for payment."[22] It does not include the digital representation of fiat currencies.[23] VA was also defined broadly to capture any relevant financial services.[24]

As it has done when regulating other financial activities, FATF identified cryptocurrency 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 any relevant financial services, such as virtual currency exchanges, certain types of wallet providers, and financial services providers.[25]

All jurisdictions must establish licensing or registration requirements for VASPs.[26] At a minimum, VASPS must list where they were created.[27] Some jurisdictions may also require licensing or registration as a condition for conducting business.[28] VASPs should be subject to the full range of preventative measures and AML/CFT obligations, similar to other financial intermediaries. These obligations include 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 designation lists.[29] In order to conduct the needed examinations as part of the consumer due diligence and licensing process, FATF recommends using blockchain analytic tools.[30]

[22] The term Virtual Asset is defined as: "a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in FATF Recommendations." See FATF Recommendations, supra note 13, at 132.
[23] Id.
[24] In October 2021, FATF further clarified that the definitions of VA and VASP to make clear that these definitions are expansive and there should not be a case where a relevant financial asset is not covered by FATF Standards (either as a VA or as another financial asset). See Updated Guidance, supra note 21.
[25] The definition of "Virtual Asset Service Provider" was also designed to be very broad in nature, and includes: "any natural or legal person who is not covered elsewhere under the Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person: i) exchange between virtual assets and fiat currencies; ii) exchange between one or more forms of virtual assets; iii) transfer of virtual assets; iv) safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and v.) participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset". FATF Recommendations, supra note 13, at 133.
[26] Updated Guidance, supra note 21.
[27] Id.
[28] Id.
[29] Id.
[30] Id.

Given the cross-border nature of VASPs' activities, FATF Recommendations require them to impose additional preventive measures.[31] In 2019, FATF adopted a low USD/EUR 1,000 threshold for VA transfers that trigger FATF obligations.[32] Some countries, such as the United Kingdom, have implemented zero-dollar thresholds for transactions conducted in VA.

Most importantly, FATF has applied its "Travel Rule" requirements to VASPs. The "Travel Rule," codified in FATF Recommendation 16, requires VASPs to obtain, hold, and transmit required originator and beneficiary information, immediately and securely, when conducting VA transfers.[33] These are the same obligations traditional financial intermediaries are required to undertake when they transmit transaction information via SWIFT.[34] Countries should ensure that their implementation of this rule is compatible with national data protection and privacy rules.[35]

Dozens of jurisdictions already adopted FATF regime on VA, but many others still need to follow suit. As of June 2021, 52 jurisdictions reported to FATF that they have implemented the Standards into their local legislation, and 26 additional jurisdictions reported that they are in the process of introducing the Standards as legislation.[36] With respect to the Travel Rule implementation, as of March 2022, only 29 jurisdictions reported to FATF they have implemented Travel Rule in their domestic legislation and only 11 reported having begun enforcement.[37] This lack of uniform implementation enables jurisdictional arbitrage by criminals. When a criminal finds that one country implemented FAFT standards, the criminal can locate their transactions in another jurisdiction with lax standards.

IV. Law Enforcement and Cryptocurrency

Aside from the risks associated with virtual assets, their digital environment provides ample opportunities for law enforcement agencies (LEAs) to conduct financial investigations.

Analysis of public blockchain ledgers allow both VASPs 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.[38] The public

[31] See FATF Recommendations, supra note 13, at 14–19 (Recommendations 10–21).
[32] FATF Recommendations, supra note 13, at 177. In other words, all VASPs around the globe should conduct the exact same procedures of Know Your Customer, identify them, monitor their activities, keep those records for several years, etc. for any transaction above the threshold of USD/EUR 1,000. Since those interactions are usually conducted remotely, the KYC information is usually verified against governmental identification, and by cross-referencing that with biometric data, which is usually more reliable than current face-to-face human verification.
[33] FATF Recommendations, supra note 13, at 17–18.
[34] Id.
[35] Updated Guidance, supra note 21, at 5.
[36] https://www.fatf-gafi.org/media/fatf/documents/recommendations/Second-12-Month-Review-Revised-FATF-Standards-Virtual-Assets-VASPS.pdf (paras. 27–28).
[37] Targeted Update, supra note 21 (para. 12). 98 jurisdictions responded to FATF's March 2022 survey. Around a quarter of those that responded reported to be in in the process of passing the relevant legislation. Around a third (36 out of 98) have not yet started implementing the Travel Rule into domestic legislation. "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.
[38] See, e.g., https://www.science.org/content/article/why-criminals-cant-hide-behind-bitcoin.

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.[39]

When VASPs collect data pursuant to their AML/CFT obligations, the data can provide the linkage between pseudonymous wallets to identifiable entities, especially when cryptocurrency holders cash in or out virtual assets to fiat currency. The information collected by VASPs as part of their customer due diligence (CDD) obligations include a vast repository of information including government-issued identification (many times crossed with biometric data), geographical location, IP addresses, statements regarding the source of funds, and red flags which were identified by VASPs based on their understanding of the transaction or identity of the customer.

When combined with open-source intelligence, signals intelligence, and human intelligence, financial intelligence empowers LEAs to trace suspicious financial activities and unmask the lawbreakers.

V. Case Studies

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

1. Terror Fundraising by Hamas

Hamas, which has been designated as a terrorist organization by the United States, the European Union, and Israel, has been fundraising in Bitcoin since 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.[40]

In 2021, Israel discovered a Hamas fundraising campaign that was advertised online via social media. In July 2021, the Israeli Minister of Defense designated crypto wallets that were

[39] These limitations pose tremendous challenges to LEAs in tracing such activities. This is among the reason for the growing adoption of private ledgers cryptocurrencies by illicit actors (see, for example, ISIS's campaign, https://cointelegraph.com/news/isis-affiliated-news-website-to-collect-donations-with-monero). However, the use of such coins also has many downsides, including the limited capability to convert them into Fiat, hence their limited use.

[40] https://www.coindesk.com/policy/2021/06/08/hamas-tapped-binance-to-launder-bitcoin-donations-blockchain-data-suggests/.

associated with Hamas' military wing.[41] The designation was made under Israel's Anti-Terrorism Law and certified that those funds were associated with terrorists, requiring their immediate seizure.[42] The designation included over 20 different types of cryptocurrencies, including Bitcoin, Tether, Ether, TRON, Cardano, XPR, Doge, and more.[43] This was probably the first terrorism financing-related cryptocurrency designation to include such a wide variety of cryptocurrencies.[44]

The designations were actively distributed by Israel's National Bureau for Counter Terror Financing (NBCTF) to VASPs around the globe. Though never publicized, shortly thereafter, a large number of VASPs, regulated and nonregulated, identified connections to the designated wallets and shared this information with the NBCTF. Some sources communicated the information directly to the NBCTF, while others informed the relevant law enforcement authorities in their respective jurisdictions or disseminated suspicious transaction reports to their own Financial Intelligence Units (FIUs), which in turn cooperated with Israeli law enforcement authorities.

The valuable information gathered through open-source and data provided by VASPs around the globe assisted in tracing relevant wallets and seizing related funds.

Additionally, blockchain analysis companies conducted independent research regarding the designated wallets, revealing connections to additional wallets associated with the designation and with previous terror financing investigations.[45] 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 use of blockchain analytics from the private sector in conjunction with info obtained from VASPs enabled the NBCTF to confiscate crypto wallets worth millions of USD.

2. Crypto to Fiat Exchange Hints at Identity 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. The Israel Anti Money Laundering and Terrorism Financing Prohibition Authority, Israel's FIU, was able to identify, based on open-

[41] See https://nbctf.mod.gov.il/he/Announcements/Documents/%d7%a6%d7%aa%2044-21.pdf.
[42] Id. The Anti-Terrorism Law was passed in 2016 and permits the Minister of Defense to seize property of terrorist organizations. https://www.gov.il/BlobFolder/dynamiccollectorresultitem/counter-terrorism-law-2016-english/he/legal-docs_counter_terrorism_law_2016_english.pdf, §§ 56(b)(1), (b)(2).
[43] https://blog.chainalysis.com/reports/israel-hamas-cryptocurrency-seizure-july-2021/; https://ciphertrace.com/hamas-cryptocurrency-donations-update-seizures-by-israels-national-bureau-for-counter-terror-financing-nbctf.
[44] See https://blog.chainalysis.com/reports/israel-hamas-cryptocurrency-seizure-july-2021/.
[45] See, for example, the reports made by Chainalysis on July 8, 2021, https://blog.chainalysis.com/reports/israel-hamas-cryptocurrency-seizure-july-2021/, and by Ciphertrace on July 16, 2021: https://ciphertrace.com/hamas-cryptocurrency-donations-update-seizures-by-israels-national-bureau-for-counter-terror-financing-nbctf.

source information and data collected from VASPs, that the Bitcoins transferred as part of the early negotiations were redeemed into fiat currency at a currency exchange located in Iran. In the Israeli context, this meant the attack was almost certainly geopolitically motivated. Having access to VASPs' data can prove extremely valuable in resolving national security incidents.

3. 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 crypto 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.

VI. Recommendations

While FATF should be praised for its global response to cryptocurrency's national security risks, FATF Standards alone are far from sufficient. In order to further guard the financial system from the AML/CFT risks of cryptocurrency while promoting financial innovation, actions should be taken by several counterparts.

First, FATF Standards must be implemented globally. A chain is only as strong as its weakest link. The global standards must be implemented and enforced swiftly and effectively by all countries.[46] Otherwise, cryptocurrencies' virtual nature makes them ripe for jurisdictional arbitrage.

Second, FATF should continue developing its standards and provide clarity on regulations affecting new financial technology products and emerging risks. Particularly important are higher-risk structures which eliminate intermediaries, such as decentralized governance structures (DeFi), peer-to-peer (P2P) transactions between unhosted wallets, and NFTs. For example, with respect to DeFi applications, FATF already noted that even if those 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 a VASP where they are providing or actively facilitating VASP services.[47] The standards applicable to this situation should be further refined.[48]

[46] See Targeted Update, supra note 21.

[47] See Updated Guidance, supra note 21, at 67. Moreover, FATF clarifies that this approach applies even if other parties play a role in the service or portions of the process are automated. Owners/operators can often be distinguished by their relationship to the activities being undertaken. For example, there may be control or sufficient influence over assets or over aspects of the service's protocol, and the existence of an ongoing business relationship between themselves and users, even if this is exercised through a smart contract or voting protocols, or in cases where any party profits from the service, or has the ability to set or change parameters to identify the owner/operator of a DeFi arrangement.

[48] Interestingly enough, some experts suggest that although considered a decentralized platform, current DeFi market is pretty centralized de-facto, as only a limited number of platforms are being used by the vast majority of customers.

Moreover, the continued development of the global regime 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 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 other existing ones that involve data protection, tax, cyber security, consumer protection, and financial stability.

Third, the private sector has an important role in developing technological solutions that ensure the integrity of the global financial ecosystem and enhance its legitimacy. They have a strong incentive to do so after it has become clear in recent years that without compliance with the AML/CFT principles (to which other financial sectors are bound), the cryptocurrency industry will continue facing difficulties and financial exclusion. Therefore, and until regulators master their understanding of the field and produce efficient solutions, the private industry 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 sometime contradicting) legal requirements under financial regulation can sophistically achieve the needed alchemic balance. For example, technological experts can develop solutions that ensure substantial compliance with AML/CFT requirement and collection and analyzing customers data, advanced information sharing mechanisms between multiple actors and law enforcement authorities, in a manner that protects customers' privacy while ensuring the needed transparency to law enforcement authorities and compliance with relevant domestic legislation (e.g., tax, privacy and data protection, records keeping, cyber security etc.). This can be achieved by developing innovative technological solutions, e.g., using zero-knowledge proof techniques, allow access to unencrypted private data only if permission was granted by the mandatory combination of several keys held by different counterparts (some of them may be granted only with a court order/ official FIU request for information) etc.[49]

In addition, the digital environment provides excellent opportunities for the Regulation Technology (RegTech) industry to lead a paradigm shift in the way financial transactions currently are being monitored by financial intermediaries. It allows adoption of more extensive landscape by moving from the current focus on customer(s) (the Know Your Customer approach) to focus on *patterns* by reviewing big-data of transactions conducted by multi-players over an extended timeline and typologies (the Know Your Transaction approach). This is facilitated by using artificial intelligence and machine learning technologies over the public blockchain ledgers.

[49] Technology may provide creative solutions, such as KYC attached to blockchain transactions with private data encrypted and accessible only under certain conditions set in smart contracts or requires the combination of a few keys (some may function only by court order/FIU request for additional information).

Fourth, the Travel Rule should be further promoted and its implementation should be expedited. All remaining governments must promptly adopt this requirement into their national legislation, especially given the large number of jurisdictions that have not done so.[50]

In addition, the private sector, which has recently achieved significant progress in developing Travel Rule technological solutions and in making them widely available, should now make further efforts to strengthen *interoperability* across the different technological solutions developed. It should also ensure flexibility to accommodate for nuances in domestic requirements, including compliance with domestic privacy and data protection laws, records keeping obligations, differences in thresholds that intrigues the travel rule application, etc. Meanwhile, VASPs should ensure their prompt implementation of the Travel Rule in practice.[51]

Fifth, law enforcement authorities must continue developing their capabilities in the field. They should train investigators on illicit finance investigations involving virtual currency, recruit designated experts, acquire advanced IT systems and obtain sufficient budgets, actions which may prove very challenging. Information-sharing mechanisms should be revised to allow swift dissemination of data from VASPs and real-time analysis. In addition, seizure and confiscation mechanisms should be updated to face the new challenges associated with the digital environment. This will require updates to the way wallets are seized, maintained, and their value realized. LEAs should also develop tools and approaches focused on advanced monitoring ex-ante rather than ex-post enforcement.

Sixth, international cooperation is critical in this virtual ecosystem. Strong international collaboration should be established among LEAs and between LEAs and the private sector. In particular, LEAs and financial institutions should cooperate in real-time. Existing collaborations, such as the Egmont channel which connects FIUs globally, should be strengthened.[52]

Finally, moving forward, broader consideration should be given to the policy considerations underlying the fast development of the digital assets economy and decentralized web 3.0 processed. This should be done by taking into account value-based decisions, such as the desirable type of activities and intermediaries that should take part in these activities, which control they gain, to what extend that may alter current centers of power in the economy, increase decentralization, encourage smaller new players to take larger part in the economy and become new intermediaries, and more.

[50] See supra text accompanying notes 37–38.

[51] See Targeted Update, supra note 21.

[52] The Egmont Group of Financial Intelligence Units is an international organization that gathers all FIUs around the world. Each jurisdiction is required by FATF Standards to establish an FIU (recommendation 29) and to exchange financial intelligence domestically and internationally with counterpart FIUs to combat money laundering, terrorist financing, and other predicate crimes. The Egmont group provides its member FIUs with a platform for the secure exchange of financial intelligence as well as improving expertise. The organization is currently composed of 167 members FIUs. For more information, see https://egmontgroup.org/about/.