Center on Law, Ethics and National Security

Essay Series
Number 21
October 23, 2023

Financial Jihad: Combating the Use of Virtual Assets in Terrorist Financing

By Madison Cash

DUKE LAW

FINANCIAL JIHAD: COMBATING THE USE OF VIRTUAL ASSETS IN TERRORIST FINANCING

MADISON CASH

ABSTRACT

Cryptocurrency has played an increasingly important role in the world of terrorist financing, inside the U.S. and abroad. Many foreign terrorist organizations use a combination of cryptocurrency and other informal money transfer channels to build an aura of anonymity, in turn incentivizing and protecting donations. Cryptocurrency is not as anonymous as it seems, and law enforcement can and has traced accounts and payments funneled through virtual asset transfer systems. However, cryptocurrency, in conjunction with informal systems of money transfer such as the hawala system, pose a particular threat to the effective investigation and prosecution of terrorist financing. These informal systems are often most powerful in areas controlled by uncooperative foreign powers. To address this gap, the author proposes that the U.S. should encourage effective multilateral collaboration within a unified regulatory scheme. In addition, it ought to aggressively penalize those who teach terrorist groups how to use cryptocurrency to raise funds as well as those intermediaries who facilitate illicit cryptocurrency transfers.

I. INTRODUCTION

Hamas's brutal attack on Israel on October 7, 2023 was the culmination of years of planning and fundraising, in which the use and exchange of cryptocurrency played a vital, if fraught, role.[1] In the aftermath of the attack, Senator Elizabeth Warren and others sent a letter to the White House on October 17, 2023, imploring it to provide "additional details on its plan to prevent the use of crypto for the financing of terrorism."[2]

In recent years, cryptocurrency has emerged as a new form of terrorist financing. According to foreign terrorist organization ("FTO") Hay'at Tahrir al-Sham ("HTS"), cryptocurrency is the "Currency of the Future Economy" and is being increasingly used by foreign militant groups to generate funds. The House of Representatives has acknowledged that donating funds, support, or training to foreign terrorist organizations ("FTOs") "helps defray the costs to the terrorist organization of running the ostensibly legitimate activities. This in turn frees an equal sum that can then be spent on terrorist activities."[3]

Terrorists use cryptocurrency to not only hide illicit transactions, but blackmail, hack, commit ransom attacks, compromise crypto-ATMs, and fund arms.[4] Coupled with the anonymity, speed, and scope of the dark web, trading and mixing cryptocurrency transactions are especially appealing for FTOs operating within "areas with internal turmoil" which lack financial infrastructure and rigorous oversight of currency transmission.[5] In addition, these groups actively train their new members and surrounding communities to securely trade in cryptocurrency and avoid sanctions checks by using VPNs and other

---

[1] The Wall Street Journal, "Hamas Militants Behind Israel Attack Raised Millions in Crypto," Angus Berwick and Ian Talley, October 10, 2023, https://www.wsj.com/world/middle-east/militants-behind-israel-attack-raisedmillions-in-crypto-b9134b7a.

[2] Letter from Elizabeth Warren, Senator, to The Honorable Brian E. Nelson, Under Secretary for Terrorism and Financial Intelligence, and Jake Sullivan, National Security Advisor, (Oct. 17, 2023).

[3] H.R. REP. NO. 104-383, at 81 (1995).

[4] Shacheng Wang & Xixi Zhu, *Evaluation of Potential Cryptocurrency Development Ability in Terrorist Financing*, 15 POLICING: A J. OF POL. & PRACTICE, 2329, 2330 (2021), https://doi.org/10.1093/police/paab059.

[5] *Id.* at 2331.

anonymizing tools, amplifying the spread of covert financing operations.[6] Amir Taaki, the lead developer of Dark Wallet, an underground Bitcoin transaction anonymity enhancer, has said: "Cryptocurrency's whole purpose is being able to move large quantities of money around without censorship . . . Terrorists are essentially non-state sanctioned political groups, so cryptocurrency is ideal for them."[7] As many sources have noted, however, cryptocurrency is not impenetrable. "Digital footprints left on the blockchain can be used by forensic experts to expose networks of financiers, provide evidence for law enforcement, and create an avenue for authorities to divert funds originally directed towards illicit causes."[8]

In response to the unique threat of international terrorist financing, Congress has created a web of regulatory and criminal statutes to effectively enforce U.S. national security priorities. For example, 18 U.S.C. § 2339B (2018) enables criminal prosecution of anyone who knowingly provides material support or resources to a designated FTO, including property, expert advice or assistance, personnel, or transportation. Additionally, any U.S. financial institution that has possession or control over funds in which a designated FTO has interest must hold the funds and report the possession to the Office of Foreign Assets Control of the U.S. Department of the Treasury ("OFAC").[9] The Bank Secrecy Act ("BSA")[10] requires qualifying financial institutions to maintain anti-money-laundering programs ("AML") and combat the financing of terrorism ("CFT").[11] This extra layer of regulation, applied to banks

---

[6] Rachel-Rose O'Leary, *The Bitcoin Terrorists of Idlib are Learning New Tricks*, WIRED (March 31, 2021), https://www.wired.co.uk/article/bitcoin-crypto-terrorism-syria.

[7] *Id.* This paper focuses on international use of cryptocurrency to fund FTOs, but it should be noted that in the U.S., domestic terrorist groups have now begun to use cryptocurrency to fund their goals.

[8] Sam Lyman, "How Hamas' Crypto Fundraising Backfired," FORBES, October 20, 2023, https://www.forbes.com/sites/digital-assets/2023/10/20/how-hamas-crypto-fundraising-backfired/?sh=3b8f45483a4d.

[9] U.S. DEP'T OF STATE, BUREAU OF COUNTERTERRORISM, FOREIGN TERRORIST ORGANIZATIONS, https://www.state.gov/foreign-terrorist-organizations/.

[10] 31 U.SC. §§ 5311-5336 (2018).

[11] RENA MILLER & LIANA ROSEN, CONG. RSCH. SERV., IF11064, U.S. EFFORTS TO COMBAT MONEY LAUNDERING, TERRORIST FINANCING, AND OTHER ILLICIT FINANCIAL THREATS: AN OVERVIEW 1 (2022), https://crsreports.congress.gov/product/pdf/IF/IF11064/6.

and covered financial entities filing reports with the Department of Treasury's Financial Crimes Enforcement Network ("FinCEN"), allows the U.S. government to be notified of suspicious financial activity that could trigger further investigation.[12]

This article will discuss the characteristics of cryptocurrency that make it uniquely suitable for terrorist financing, the regulatory loopholes that augment terrorist use of cryptocurrency, and the methods by which FTO affiliates often avoid detection of their fundraising efforts. It will also explain U.S. responses to FTOs' illicit uses of cryptocurrency, highlighting the vulnerabilities built into traditional exchange systems that assist in timely apprehension of terrorist financiers. It will discuss the difficulty of tracing cryptocurrency transfers in conjunction with informal systems of financing often located in areas controlled by uncooperative foreign powers. To address this challenge, the U.S. should encourage effective multilateral collaboration within a unified regulatory scheme. In addition, it ought to aggressively penalize those who teach terrorist groups how to use cryptocurrency to raise funds as well as those intermediaries who facilitate illicit cryptocurrency transfers.

II. THE RISKS IMPLICIT WITHIN VIRTUAL ASSET TRANSFER.

Cryptocurrency, since its emergence in 2009, has been touted as a generally anonymous, decentralized method of transferring assets, avoiding the risks of regulated banking or government overstep.[13] While it does have legitimate uses, cryptocurrency's highly private, decentralized system is attractive to criminals seeking an avenue for money laundering, theft, and financing of terrorist crimes, often simultaneously.[14] In addition, cryptocurrency's global reach necessitates international collaboration to effectively enforce global oversight that is currently missing in the patchwork of inconsistent AML regulatory efforts abroad.[15]

Pseudonymous cryptocurrency functions by providing a space for individual peer-to-peer transactions, accessible through private and

---

[12] *Id.* at 2; § 5318(g)(1); 31. C.F.R. § 1022.320 (a)(1-2) (2021).
[13] *Cryptocurrency*, BRITANNICA.COM, https://www.britannica.com/topic/cryptocurrency (last visited Apr. 23, 2023).
[14] U.S. DEP'T OF JUST. CYBER DIGITAL TASK FORCE, CRYPTOCURRENCY: ENF'T FRAMEWORK 5-6 (2020), https://www.justice.gov/archives/ag/page/file/1326061/download.
[15] *Id.* at ix.

public keys, otherwise known as pseudonyms.[16] After one individual creates a message recording both the origin of their coins and the public key of the intended recipient of their coins, they can sign the message with their private key.[17] This message is then broadcasted to other peers, who check for the validity of the signature.[18] To facilitate this process, every peer must have access to the transaction history of the virtual coins in question.[19] After the transactions are allowed to flood the network, they are recorded by the blockchain that functions as a distributed ledger.[20] The blocks that make up the blockchain are collections of multiple transactions attached to a coin generation transaction created by miners, special users who solve a complex algorithm in return for payment of cryptocurrency generated by the coin generation transaction.[21] Once the blocks have then been further verified by other blocks, they are added to the blockchain, "which [is] a consensus-defined set of rules rather than system requirements."[22]

Virtual currency can then be converted into fiat currencies and other virtual currencies through cryptocurrency exchanges, which also function as banks.[23] Wallet services have also been built to store cryptocurrency for users until they are ready to complete a transaction.[24] Often, those with criminal intent are drawn to mixing services, which can enhance cryptocurrency's laundering capabilities by receiving illicit virtual assets and mixing them with other customers' legitimate virtual assets to be sent to the intended destination.[25] Chain-hopping is another popular method of utilizing cryptocurrency's convertibility, as users transfer funds rapidly from one type of cryptocurrency to another to obfuscate the individual behind the multiple transactions. [26]

---

[16] Sarah Meiklejohn et al., *A Fistful of Bitcoins: Characterizing Payments Among Men with No Names*, 38 ;LOGIN: 10, 11 (2013), https://smeiklej.com/files/login13.pdf.
[17] *Id.*
[18] *Id.*
[19] *Id.*
[20] U.S. DEP'T OF JUST. CYBER DIGITAL TASK FORCE, *supra* note 14, at 4.
[21] *Id.*
[22] Meiklejohn, *supra* note 16.
[23] *Id.*
[24] *Id.* at 12.
[25] U.S. DEP'T OF JUST. CYBER DIGITAL TASK FORCE, *supra* note 14, at 41.
[26] *Id.* at 44.

III. TERRORIST FINANCING USING CRYPTOCURRENCY

Increasing the ease of terrorist financing is among the most serious and highly publicized implications of cryptocurrency, as addressed by the Report of the Attorney General's Cyber Digital Task Force.[27] Although the 2020 Report noted that "public data on terrorist use of cryptocurrency is limited," more individuals have since begun using cryptocurrency to fund FTOs covertly.[28] Assisted by the pandemonium of the COVID19 pandemic, "terrorist organizations have used this global crisis to make illegal profits by forging medical supplies, investing fraud, and abusing measures to stimulate the economy."[29] The United Nations' Senior Legal Officer at the Counter-Terrorism Committee Executive Directorate, Svetlana Martynova, asserted that in 2020, 5% of all terrorist attacks were linked to digital assets; in 2022, cryptocurrency could account for 20% of the financing of such terrorist initiatives, in combination with traditional financing options.[30]

A. FTO Evasion of the BSA's AML-CFT Regulations

Because of its potential for terrorist abuse, cryptocurrency has now been incorporated into the U.S. regulatory ecosystem. Recently, the Anti-Money Laundering Act of 2020 amended the BSA's definitions of monetary instrument and financial institutions to cover cryptocurrency exchanges.[31] Now, virtual currency exchanges "must collect identifying information of their customers and verify their clients' identities," alongside traditional financial institutions.[32]

Most questions of the BSA's application to assets related to cryptocurrency are answered by a fact-dependent analysis of whether an entity is acting in its private capacity to directly transact with

---

[27] *Id.* at viii.
[28] *Id.* at 7.
[29] Wang, *supra* note 4, at 2332.
[30] Sidhartha Shukla, *UN Says Crypto Use in Terror Financing Likely Soaring*, BLOOMBERG (Oct. 31, 2022), https://www.bloomberg.com/news/articles/2022-10-31/un-finding-more-cases-where-crypto-involved-in-terror-financing?leadSource=uverify%20wall&sref=zNmRQ0gk.
[31] MILLER, *supra* note 11, at 2; §§ 5312 (a)(2)(R), a(3)(D).
[32] Gebhart's Aff. ¶ 10 (relying on *United States v. E-Gold, Ltd.*, 550 F. Supp. 2d 82, 87-97 (D.D.C. 2008)) (*located at* Office of Pub. Affs., *Global Disruption of Three Terror Finance Cyber-Enabled Campaigns*, DEP'T OF JUST. (Aug. 13, 2020), https://www.justice.gov/opa/press-release/file/1304276/download.)

another entity, or whether it facilitates exchanges of assets.[33] According to FinCEN guidance, BSA regulations apply to any exchange operating functionally as a money transmitter ("MSB"), whether domestic or foreign, that has a nexus to the U.S.[34] Importantly, anonymizing services which exist to "mix" or "tumble" cryptocurrency transactions to prevent tracking are also subject to BSA requirements, because they are offering secure money transmission.[35] The problem in enforcing these regulations is detecting unregistered money transmitters and mixing services, which are often offered solely on the dark web and thus uninterested in complying with regulation.[36]

This difficulty is amplified by the insulation of private individuals from AML-CFT regulation under the BSA. The BSA does not cover peer-to-peer exchanges if a natural person is "engaging in such activity on an infrequent basis and not for profit or gain."[37] The BSA does not require individual transactions under a certain monetary cap to undergo BSA regulation.[38] Additionally, "unhosted" wallets, wallets

---

[33] FINCEN, *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies*, FIN-2019-G001 2 (May 19, 2019), https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf. ("Whether a person is a money transmitter under FinCEN's regulations is a matter of facts and circumstances.")

[34] *See* Bank Secrecy Act Regulations - Definitions and Other Regulations Relating to Money Services Businesses, 76 FR 43585 (July 21, 2011), https://www.federalregister.gov/documents/2011/07/21/2011-18309/bank-secrecy-act-regulations-definitions-and-other-regulations-relating-to-money-services-businesses. ("[T]he BSA rules apply to all persons engaging in covered activities within the United States, regardless of each person's physical location. . . . Foreign-located MSBs will be subject to the same civil and criminal penalties as MSBs with a physical presence in the United States, with respect to their failure to comply with regulatory requirements").

[35] FINCEN, *supra* note 33, at 19.

[36] *See, e.g.*, Off. of Strategic Commc'n, *First Bitcoin "Mixer" Penalized by FinCEN for Violating Anti-Money Laundering Laws*, FINCEN (Oct. 19, 2020), https://www.fincen.gov/news/news-releases/first-bitcoin-mixer-penalized-fincen-violating-anti-money-laundering-laws.

[37] 31 CFR § 1010.100(ff)(8)(iii) (2023)

[38] FATF, *Updated Guidance for a Risk-Based Approach for Virtual Assets and Virtual Asset Service Providers*, FATF 20 (28 Oct. 2021), https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html ("While P2P transactions are also used for licit activity, illicit actors can exploit the lack of obliged intermediary in P2P transactions to obscure the proceeds of crime because there is no obliged entity carrying out the core functions

that are completely controlled by an individual, are not regulated under the BSA, although individuals can transfer funds from an exchange into their unhosted wallets.[39] According to the Financial Action Task Force ("FATF") in 2021, "FATF is not aware of any technically proven means of identifying the person that manages or owns an unhosted wallet, precisely and accurately in all circumstances," further allowing terrorist financiers using unhosted wallets to escape detection.[40] This gap allowing unhosted wallets to continue unregulated has invited attempts by FinCEN to amend the BSA regulations to require cryptocurrency exchanges to collect personal data from individuals transferring funds over a certain amount to their private wallets.[41] Partially due to the pushback from the cryptocurrency industry, FinCEN has not yet explicitly included unhosted wallets under the BSA.[42]

The gaps in the BSA allow FTO affiliates to function as unregistered exchanges, often by transacting with donors over a cryptocurrency exchange or converting donors' fiat currency into virtual currency and then transmitting the cryptocurrency to a variety of different unhosted wallet addresses.[43] Failing multilateral implementation of a unified AML-CFT program also exposes the U.S to risks, as many virtual asset service providers ("VASPs") in countries with deficient reporting solutions and security regulations engage in regulatory arbitrage and instantaneous cross-border transaction transmission with U.S. users, undermining the BSA's

---

of the FATF Standards, such as CDD and filing suspicious transaction reports (STR). Conversely, visibility of P2P transactions on public ledgers might support financial analysis and law enforcement investigations, especially when combined with other information sources, unless there are anonymity-enhancing protocols and technologies associated with the VA.")

[39] *See id.*

[40] *Id.* at 53 n. 9.

[41] Off. of Strategic Commc'n, *FinCEN Extends Reopened Comment Period for Proposed Rulemaking on Certain Convertible Virtual Currency and Digital Asset Transactions*, FINCEN (Jan 26, 2021), https://www.fincen.gov/news/news-releases/fincen-extends-reopened-comment-period-proposed-rulemaking-certain-convertible.

[42] Alessio Evangelista, Associate Director of the Enforcement & Compliance Div., FinCEN, Remarks at Chainalysis Links Conference (May 19, 2022) (transcript available at https://www.fincen.gov/news/speeches/prepared-remarks-alessio-evangelista-associate-director-enforcement-and-compliance.)

[43] *See* Gebhart's Aff., *supra* note 32, at ¶ 30-31.

effectiveness.[44] There are a growing amount of virtual asset kiosks that convert cryptocurrency into fiat currency, even if the individuals are receiving assets from noncompliant entities, further circumventing the BSA's protections.[45] Savvy FTOs will continue to evolve and exploit the weaknesses in the U.S.'s current CFT program under the BSA.[46]

B. FTOs' Strategies to Avoid Detection

In addition to posing difficulties to regulators, cryptocurrency offers several benefits to FTOs interested in increasing anonymity in their movements. When using virtual currency, FTOs can encourage users to donate to unique addresses for every transaction to avoid tracing.[47] For instance, the al-Qassam Brigades' ("AQB") financing campaign in 2019 initially began by soliciting funds, funneling virtual assets into one address hosted by a U.S. based virtual currency exchange.[48] Hamas's military branch was the first FTO to use cryptocurrency to fundraise.[49] It later adapted to a more sophisticated avoidance of the BSA by creating a network of individual asset addresses available to each donor.[50] AQB provided video instruction explaining to donors how to contribute to its mission "anonymously" through this system of diversified wallets and addresses. [51] Allegedly, donors were encouraged to use public wifi while creating their private wallet to avoid disclosure of their IP address and were directed to make use of the hawala system, discussed at length below.[52]

Individualizing donor addresses to evade control by the authorities is "essentially impossible with traditional financial

---

[44] U.S. DEP'T OF TREASURY, 2022 NAT'L TERRORIST FINANCING RISK ASSESSMENT 23 (2022), https://home.treasury.gov/system/files/136/2022-National-Terrorist-Financing-Risk-Assessment.pdf.

[45] *Id.*

[46] Off. of Pub. Affs., *Global Disruption of Three Terror Finance Cyber-Enabled Campaigns*, DEP'T OF JUST. (Aug. 13, 2020), https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns.

[47] Gebhart's Aff., *supra* note 32, at ¶ 17.

[48] U.S. DEP'T OF TREASURY, *supra* note 44, at 22.

[49] Lyman, *supra* note 8.

[50] *Id.*

[51] *Id.*

[52] *Terrorism Financing in Early Stages with Cryptocurrency but Advancing Quickly*, CHAINALYSIS (Jan. 17, 2020), https://blog.chainalysis.com/reports/terrorism-financing-cryptocurrency-2019/ (last visited Apr. 23, 2023).

accounts."[53] A cryptocurrency user can also combine multiple addresses in a single transaction if they have a private key, further obfuscating investigative efforts.[54] AQB's adaptations led the Department of Treasury to conclude that "the evolution indicates terrorist groups can adapt to risk-mitigation efforts and exploit nuanced vulnerabilities within this emerging technology."[55]

It should be noted that although cryptocurrency has qualities that aid in money laundering and, subsequently, terrorist financing, most terrorist cells have not relied on cryptocurrency exclusively.[56] Instead, many terrorist groups elect a combination of currencies and methods of donation, creating a difficult path for law enforcement to follow.[57] In many FTO networks, this is accomplished by an informal money service provider, often known as a "hawala."[58] The hawala system is especially appealing for international terrorist financiers because using a hawala bypasses banks, exchanges, and regulation entirely, even evading OFAC's international sanctions.[59]

When using a hawala to convert cash to cryptocurrency to finance a FTO, donors hand over cash and provide the facilitator with the virtual asset addresses given by the FTO.[60] The facilitator, known as the hawaladar, then sends the equivalent cryptocurrency amount to the address provided, serving as an unofficial intermediary between the donor and the FTO.[61] This can occur repeatedly, lengthening the chain

---

[53] Nathaniel Popper, *Terrorists Turn to Bitcoin for Funding, and They're Learning Fast*, N.Y. TIMES, Aug. 18, 2019, https://www.nytimes.com/2019/08/18/technology/terrorists-bitcoin.html.
[54] Gebhart's Aff., *supra* note 32, at ¶ 18.
[55] U.S. DEP'T OF TREASURY, *supra* note 44, at 22.
[56] Wang, *supra* note 4, at 2335-2336. This is likely due to its instability and fluctuation in price.
[57] *Id.*
[58] John F. Wilson, Senior Economist, Middle Eastern Dep't, IMF, Remarks at Seminar on Current Developments in Monetary & Financial Law (May 16, 2002) (transcript available at https://www.imf.org/external/np/leg/sem/2002/cdmfl/eng/wilson.pdf.)
[59] Kailey Pickitt, *Hawalas' Role in the Financial War on Terrorism,* GEO. SECS. STUD. REV. ONLINE (2017), https://georgetownsecuritystudiesreview.org/2017/10/26/hawalas-role-in-the-financial-war-on-terrorism/.
[60] *Terrorism Financing in Early Stages with Cryptocurrency but Advancing Quickly*, CHAINALYSIS (Jan. 17, 2020), https://blog.chainalysis.com/reports/terrorism-financing-cryptocurrency-2019/ (last visited Apr. 23, 2023).
[61] *Id.*

of transmission between users. Once the currency is collected by its final recipient, it can be converted to fiat currency or exchanged for a gift card through intermediary accounts to further invest in materials to complement the mission of the FTO.[62] In doing so, the FTO donor and recipient can escape detection and liability.

IV. LAW ENFORCEMENT STRATEGIES TO DETECT TERRORIST FINANCING USING CRYPTOCURRENCY

Depending on the cryptocurrency used, law enforcement can overcome these hurdles. As one judge on the District Court for the District of Columbia has noted, "virtual currency is traceable . . . Yet like Jason Voorhees the myth of virtual currency's anonymity refuses to die." [63] For pseudonymous virtual currency, like Bitcoin, FTO donors and members can be identified by analyzing the blockchain for multiple transactions linked to the user or grouped addresses within a single exchange of the cryptocurrency for fiat currency.[64]

For instance, the safeguards taken by AQB in 2019 did not result in total anonymity because it used Bitcoin in its individualized transfers, which is a regulated exchange under the BSA.[65] Its use of a regulated exchange led to the massive investigation of hundreds of domestic donors and FTO facilitators.[66] To complete this investigation, law enforcement gathered identifying information from the exchange itself under Know Your Customer laws required under the BSA. [67] After the U.S. Department of Justice and Israel's National Bureau for Counter Terror Financing seized millions of dollars worth of crypto and almost 200 accounts from AQB, Hamas announced that it would no longer be using bitcoin due to "the intensification of prosecution and the redoubling of hostile efforts against anyone who tries to support the resistance through this currency."[68]

At times, U.S. agencies also contract with companies that specialize in blockchain analysis to group clusters of data, effectively identifying individuals behind similar transactions.[69] One 2013 study conducted by researchers at the University of California first

---

[62] *See* Gebhart's Aff., *supra* note 32, at ¶ 27.
[63] *In re: Criminal Complaint*, No. 22-mj-067-ZMF, 2022 WL 1573361, at *4 (D.D.C. May 13, 2022).
[64] Gebhart's Aff., *supra* note 32, at ¶ 17, 20.
[65] Off. of Pub. Affs., *supra* note 46.
[66] *Id.*
[67] Gebhart's Aff., *supra* note 32, at ¶ 21.
[68] Lyman, *supra* note 8.
[69] *Id.* ¶ 20.

conceptualized blockchain analysis by discovering that if two addresses were used to source funds within the same transaction, the addresses are often controlled by the same user, since individuals tend to pool resources held in multiple accounts.[70] Another clustering technique employed by the researchers found that generally, if an address that can be used to receive the change from a transaction is attached as an output to a message, then it belongs to the sender of the funds.[71] The study found that "Although [these clusters do] not de-anonymize the individual participating in the transaction . . . [they do] serve to de-anonymize the flow of bitcoins into and out of the service."[72]

In combination with blockchain analysis, agencies can use typical law enforcement tools to further de-anonymize the transaction. For instance, agents can trace IP addresses used to log into different accounts, ultimately determining the identity of cryptocurrency users.[73] In some investigations, conventional "sting operation" strategy can be useful. The successful dismantling of AQB's cryptocurrency campaign involved government communication with terrorist facilitators.[74] After confirming that the incoming proceeds would be used to fund weapons for terror organizations, agents took over the campaign website to further track who had and continued to donate to the campaign.[75]

Even when some FTOs have used mixing techniques to diversify funds, traditional investigative techniques, along with agencies' subpoena power, can still result in locating the owner of illicit accounts. One study found that even when mixing is involved, "for the most part tracking the bitcoins was quite straightforward, and we ultimately saw large quantities of bitcoins flow to a variety of exchanges directly from the point of [withdrawal.]" [76] An FTO might also attempt to use privacy coins, which are created by services advertising anonymity enhanced cryptocurrency (such as Monero and

---

[70] Meiklejohn, *supra* note 16, at 13.
[71] *Id.* at 14.
[72] *Id.*
[73] Gebhart's Aff., *supra* note 32, at ¶ 41.
[74] *Chainalysis in Action: Dep't of Just. Announces Takedown of Two Terrorism Financing Campaigns with Help from Blockchain Analysis,* CHAINALYSIS (Aug. 13, 2020), https://blog.chainalysis.com/reports/cryptocurrency-terrorism-financing-al-qaeda-al-qassam-brigades-bitcointransfer/ (last visited Apr. 23, 2023).
[75] *Id.*
[76] Meiklejohn, *supra* note 16, at 14.

Zcash).[77] For all of the coverage in popular media referencing the terrorist financing potential of such privacy coins,[78] it is uncertain whether they will gain traction in their current form. Monero, according to some recent disclosures, can be traced by IRS criminal investigators in conjunction with civilian partners:[79] "leaked Chainalysis documents . . . show that Chainalysis says to its law enforcement customers that it can trace Monero in the majority of cases."[80] Similarly, Zcash might not realistically achieve anonymity in shielding transactions, especially because most third parties that transact with Zcash require transparent transactions.[81]

Finally, even if agencies have difficulty tracing the entity who is packaging and mixing the funds in suspicious ways, it is difficult to convert virtual assets into fiat currency without using an exchange, which then leads to detection. One commentator has noted that "because [cryptocurrency exchanges are] all so transparent and traceable, it's going to be very difficult for whoever took that money to cash it out or spend it or get away with this crime in a way where they won't be identified."[82]

V. RECOMMENDATIONS AND CONCLUSION

By employing innovative investigative tools such as blockchain analysis and more traditional law enforcement strategies, such as infiltration of terrorist modes of communication, U.S. agencies can successfully identify virtual asset accountholders behind FTO financing campaigns. Individuals involved in creating and executing FTO fundraising campaigns have recently been indicted under state and federal material support statutes.[83] The U.S. could further combat

---

[77] U.S. DEP'T OF JUST. CYBER DIGITAL TASK FORCE, *supra* note 14, at 4.
[78] Gadget Lab, *Cryptocurrency's Myth of Anonymity*, WIRED (Feb 9, 2023), https://www.wired.com/story/gadget-lab-podcast-585/.
[79] Gebhart's Aff., *supra* note 32, at ¶8.
[80] Gadget Lab, *supra* note 78.
[81] Claire Ye, et al., *Alt Coin Traceability* 8 (Carnegie Mellon Univ., Working Paper No. 593, 2020), https://eprint.iacr.org/2020/593.pdf.
[82] Gadget Lab, *supra* note 78.
[83] *D.A. Bragg, NYPD Commissioner Sewell Announce Indictment of Upper East Side Woman for Using Cryptocurrency to Fund Syrian-Based Terrorist Groups; Launder Supporters' Contribution*, MANHATTAN DIST. ATT'Y'S OFF. (Jan. 31, 2023), https://manhattanda.org/d-a-bragg-nypd-commissioner-sewell-announce-indictment-of-upper-east-side-woman-for-using-cryptocurrency-to-fund-syrian-based-terrorist-groups-launder-supporters-contributions/; *Four Defendants Charged With Conspiring to Provide Cryptocurrency to ISIS*, U.S. ATT'YS OFF.,

the spreading use of informal virtual asset transfers by exercising statutory and regulatory tools to their full extent.

For instance, the growth of terrorist financing using cryptocurrency could be slowed by penalizing those who are teaching FTO members and donors how to transmit funds anonymously, which is a component of many terrorist financing schemes.[84] Federal material support statutes, such as § 2332B, penalize actors who provide expert assistance and support to FTOs, even those operating outside of the U.S. [85] Because internal FTO training initiatives are well-documented and often conducted online, law enforcement can use its surveillance and enforcement powers to identify the experts providing assistance and dismantle the furtherance of illicit transfer of virtual assets.[86]

In addition, mixing and anonymizing services might also be captured under the scope of material support statutes, in addition to traditional conspiracy or fraud statutes. Several mixing services have been sanctioned by OFAC recently for materially supporting the laundering of funds derived from an illegal foreign cyber-activity (hacking) that posed a threat to U.S. national security. While sanctions are effective for halting use of the mixing service and redirecting illicit funds back to the U.S., the individual creators and facilitators of such programs could also be held accountable for their actions by criminal prosecution for sanctions violations and material support to FTOs. These entities often informally advertise their services to FTOs, in addition to cybercriminals, and do not comply with BSA regulation requiring screening and reporting of suspicious transactions.[87] Thus,

---

E.D.N.Y. (Dec.14, 2022), https://www.justice.gov/usao-edny/pr/four-defendants-charged-conspiring-provide-cryptocurrency-isis.

[84] *See* U.S. DEP'T OF JUST. CYBER DIGITAL TASK FORCE, *supra* note 14, at 7.

[85] *See United States v. Al Kassar*, 660 F.3d 108, 118 (2d Cir. 2011).

[86] Off. of Pub. Affs., *supra* note 46.

[87] *See, e.g.*, U.S. DEP'T OF TREASURY, *U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash*, U.S. DEP'T OF TREASURY (Aug. 8, 2022), https://home.treasury.gov/news/press-releases/jy0916 (discussing sanctions imposed on Tornado Cash, a mixing service that allowed various entities, including a Democratic People's Republic of Korea-sponsored group, to launder nearly 7 billion in U.S funds using virtual currency.) As of August 30, 2023, the founders of Tornado Cash had been indicted on charges of conspiracy to commit money laundering, conspiracy to commit sanctions violations, and conspiracy to operate an unlicensed money transmitting business., U.S. ATTY'S OFFICE, SOUTHERN DISTRICT OF NEW YORK, *Tornado Cash Founders Charged with Money Laundering and Sanctions Violations*, DEP'T OF JUST. (Aug. 23, 2023), https://www.justice.gov/usao-sdny/pr/tornado-cash-founders-charged-money-laundering-and-sanctions-violations.

prosecution of these intermediary actors that intentionally advertise their capacity to facilitate illicit virtual asset transfers to FTOs would effectively deter continued FTO reliance on these systems. The scope of the under-utilized federal material support statutes can encompass these actors, as they penalize any actors who knowingly provide assistance or expert advice to such designated terrorist organizations.[88]

Finally, FTO use of cryptocurrency functions most effectively in combination with the widespread, informal network of diversified money transmitters, making it challenging to link the numerous individuals involved with the virtual assets transmitted and establish the criminal intent required to successfully prosecute under federal material support laws. The power of the hawala network, which operates on trust, is not one to be underestimated,[89] and aids the evasion of regulation by entities acting as informal money transmitters. In the realm of terrorist financing, moving small, diversified amounts of virtual assets through covert, unregulated money transfer programs are arguably the ideal way to avoid U.S. regulation and sanction.

To this end, FATF has recommended requiring licenses to be issued to hawaladars, which Pakistan has adopted as part of developing UN regulation and multilateral collaboration with American authorities.[90] In a testament to the power of requiring licenses for informal money transmitters, many individuals, such as the facilitators of the previously discussed AQB campaign, have been successfully penalized for operating informal, unlicensed money transmitters that funnel virtual assets to FTOs under existing U.S. regulation.[91] With more countries creating a licensing system specifically covering these informal money transmitters, U.S. regulation of FTOs' use of cryptocurrency could be more effective.

Combating more dispersed forms of virtual asset transfer pose unique difficulties to law enforcement but can be addressed with multilateral compliance, monitoring, and enforcement of regulations against hawaladars engaged in terrorist financing. With a more focused, expansive use of its available regulatory and criminal enforcement tools, the U.S. can effectively address the threat of terrorist use of cryptocurrency, even as the hawala system makes illicit

---

[88] § 2332B.

[89] *See* Raza MS, Fayyaz M, Ijaz H. *The Hawala System In Pakistan: A Catalyst For Money Laundering & Terrorist Financing.* 5 FORENSIC RES CRIMINOL. INT J. 367, 367 (2017), doi10.15406/frcij.2017.05.00167/.

[90] *Id.* at 386.

[91] Off. of Pub. Affs., *supra* note 46.

virtual asset financing a more potent risk.