September 28, 2026

TETHERED TO TERRORISM:

Crypto & Iran's Shadow Banking Network

United States Senate | Permanent Subcommittee on Investigations

Ranking Member Richard Blumenthal & Minority Staff

Table of Contents

EXECUTIVE SUMMARY

Tether's role in Iranian shadow banking is unprecedented and pervasive—providing what appears to be a primary and preferred cryptocurrency for the Islamic Republic's schemes to prop up the regime and sustain its regional security threats. Recent media and industry reporting have illustrated the role of Tether's stablecoin in Iranian and Russian money laundering schemes, including sanctioned Iranian oil sales and military procurement. Given Tether's significant nexus to the United States, these recurring reports call into question whether the firm has taken sufficient action to investigate, prevent, and deter foreign adversaries from using its cryptocurrency in a manner that is directly adverse to American national security. Further, given Tether's deep connections with the Trump Administration, its continuing use by the Iranian regime raises questions as to whether Tether has received lax enforcement and lenient oversight over its anti-money laundering obligations from relevant federal authorities.

As part of its ongoing inquiry into the role of cryptocurrencies in illicit finance, the Permanent Subcommittee on Investigation (PSI or the Subcommittee) conducted a forensic analysis of blockchain transaction data from 846 unique cryptocurrency wallets that have been sanctioned or targeted for seizure due to their association with Iran and its regional proxies. This analysis of Iran's shadow banking network found:

- **Finding 1: Tether has become a primary illicit international payment system for Iran, allowing it to circumvent international sanctions on its banks.** Tether, and its U.S. dollar-pegged stablecoin (USDT), has become a primary cryptocurrency connected to the Islamic Republic's money laundering schemes. Of the 846 wallets sanctioned for their association with Iran and its terrorist proxies, 84% have transacted exclusively, or nearly exclusively, in USDT. These activities include efforts by the Iranian government to move funds into, and out of, Iran and to prop up the country's currency in the face of U.S. sanctions, including through the Central Bank of Iran.

- **Finding 2: Tether serves as a central payment mechanism that interlinks Iran and its terrorist proxy organizations, undermining U.S. security interests in** the region. Iran's cryptocurrency-based shadow banking network has processed significant volumes of funds and implicates various Iranian interests. For example, two sanctioned Iranian oil smugglers, Alireza Derakhshan and Arash Estaki Alivand, were able to move more than $603 million in USDT over a four-year period from 2021-2025 in a network that connected to Hizballah, the Houthis, and Iranian financial institutions. These payments occur either through money launderers like Derakhshan and Alivand or through unregulated exchanges or intermediaries that routinely move hundreds of millions of dollars. These are effectively digital versions of hawala networks that have long concerned national security officials.[1]

[1] *See, e.g.*, *Financial War on Terrorism: New Money Trails Present Fresh Challenges Hearing Before the S. Comm. on Fin.*, 107th Cong. (2002).

In addition to supporting terrorist organizations, there is evidence that this shadow banking network is used for the procurement and sales of drones and other military equipment.

- **Finding 3: Tether's repeated failure to freeze illicit wallets and prevent abuse created the permissive environment under which Iranian shadowing** banking has flourished. Tether repeatedly failed to block wallets associated with Iranian exchanges, suspicious brokers, and terrorist organizations. Prior to 2024, Tether did not comprehensively and consistently freeze wallets designated by counter-terrorism agencies and continues to fail to proactively block clearly illicit wallets. This absence of deterrence invited abuse: terrorist organizations such as Hamas shifted from transacting in Bitcoin and a mix of cryptocurrencies to promoting USDT. Even where it has responded, Tether has at times taken weeks, or even failed, to blacklist illicit wallets altogether. The Subcommittee's analysis shows that in one case, $34.6 million continued to move through sanctioned wallets *after* they had been designated. Indeed, late last year the most notorious money launderer in Iran posted a Central Bank of Iran wallet address on Twitter/X. Based on the Subcommittee's review of blockchain records, Tether has yet to blacklist that and similarly attributed addresses.

Iran's embrace of Tether should be a chilling warning. Cryptocurrencies are actively undermining the attempts of the United States and its allies to prevent the Islamic Republic's regional terrorism, nuclear enrichment, hostile drone and missile programs, and human rights abuses through international sanctions and counterterrorism financing measures. The Subcommittee's analysis demonstrates Tether has in effect provided Iran access to a high-liquidity, widely accepted, and pseudonymous international payment system that the United States has assiduously sought to deny it. This channel for money laundering is significant enough that in May 2026, during the ongoing war with Iran, the Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) issued an alert that called out cryptocurrencies as "one leg of Iran's shadow banking network," naming stablecoins and "large volume stablecoin issuers" (of which Tether is the largest) as being of particular concern.[2]

The Subcommittee's analysis demonstrates that USDT has become a significant financial lifeline within Iran's shadow banking network. Warnings from FinCEN, media investigations, and industry reporting reinforce the Subcommittee's analysis. The Subcommittee's preliminary findings raise grave questions about whether Tether, which has a substantial nexus to the United States through its founding in California, relationship with Cantor Fitzgerald, and U.S. Treasury holdings, is taking sufficient action to prevent USDT from being used to threaten American national security. These findings emphasize the need to ensure that cryptocurrency issuers, particularly those that transact in dollar-pegged tokens or maintain a relationship with the United States, are fully and

[2] U.S. Dep't of the Treasury, Fin. Crimes Enf't Network, FIN-2026-Alert002, FinCEN Alert on the Use of Front Companies, Financial Facilitators, and Digital Asset Infrastructure by Iran's Islamic Revolutionary Guard Corps to Evade Sanctions and Launder Proceeds 6 (May 11, 2026), https://www.fincen.gov/system/files/2026-05/FinCEN-Alert-IRGC.pdf.

directly required to comply with U.S. sanctions and banking laws. Similarly, these findings highlight the dangers to public safety and national security of recent decisions by the Trump Administration to drop investigations, settle cases, and otherwise provide undue leniency for cryptocurrency firms.

METHODOLOGY

The Subcommittee analyzed blockchain transactions for cryptocurrency wallets attributed to Iranian government entities and those of its regional proxies, namely Hamas, Hizballah, and the Houthis (Ansarallah). Blockchain wallet ownership is pseudonymous, providing a digital address but no direct attribution of the actual name or location of the owner. Thus, outside researchers and industry rely on government attribution, investigative techniques (such as depositing money through a storefront), or analytical assessments (such as creating social graphs linked based on transactions) to identify their owners. One of the most prolific sources of reliable, public attribution of wallets used for illicit finance are the sanctions and seizure designations of U.S. Treasury Department's Office of Foreign Assets Control (OFAC) and Israel's National Bureau for Counter Terror Financing (NBCTF).[3] When OFAC and the NBCTF identify wallets, that attribution can help investigations into other suspicious wallets and expand public knowledge of the volume and breadth of illicit finance.

The Subcommittee collected the transactions of cryptocurrency wallets identified by OFAC and NBCTF as controlled or associated with Iran and its regional proxies, totaling 846 wallets from more than five years of orders (starting June 2021[4] until August 2026).[5] Illicit actors frequently rotate wallet addresses to avoid detection and blacklisting, so the Subcommittee supplemented the government-sourced list with its own custom-built forensic tools and third-party platforms for additional attribution, such as to identify cryptocurrency exchanges (which can have millions of wallets). The Subcommittee's analysis identified dozens of additional suspicious wallets beyond those listed by government sources but kept overall aggregate statistics to those externally confirmed as illicit. Lastly, the Subcommittee's analysis included wallet addresses leaked on social media from Iranian officials, media reports on transactions, fundraising campaigns, and other public information.

---

[3] In line with the intended scope, the Subcommittee focused on wallets associated with the Iranian government and the IRGC, as well as Hamas, Hizballah, and the Houthis. Wallets clearly associated with ISIS and cybercrime that were otherwise not associated with the Iranian government were excluded, such as OFAC's designation of the Nemesis darknet drug market that is allegedly run by a resident of Iran. *See, e.g.*, *OFAC Designates Iranian-Linked Crypto Exchanges in First-Ever Action Targeting Digital Asset Firms in Iran's Financial Sector*, CHAINALYSIS (Jan. 30, 2026), https://www.chainalysis.com/blog/ofac-designates-iranian-crypto-exchanges-january-2026/.

[4] Administrative Seizure Order (ASO) 44/21, Anti-Terrorism Law 5776-2016 (June 30, 2021) (Isr.), https://nbctf.mod.gov.il/he/Announcements/Documents/%25D7%25A6%25D7%25AA%252044-21.pdf.

[5] Press Release, U.S. Dep't of the Treasury, Off. of Foreign Assets Control, Treasury Launches Unprecedented Campaign Against Iranian Regime on Economic D-Day (Aug. 24, 2026), https://home.treasury.gov/news/press-releases/sb0613.

INVESTIGATION BACKGROUND

This report represents the continuation of multiple inquiries PSI has made into sanctions evasion in recent years. In December 2024, PSI released a report entitled "Examining the Bureau of Industry and Security's Enforcement of Semiconductor Export Controls," following an investigation into the distribution networks Russia uses to smuggle semiconductors into the country and evade U.S. sanctions.[6]

On February 24, 2026, the Subcommittee initiated an inquiry into Binance following reporting that the exchange had allowed nearly $2 billion in money laundering to Iranian proxies and Russia's shadow fleet.[7] On March 6, Binance replied to the Subcommittee's letter to deny reports that its platform had been used for sanctions evasion, claiming those media reports contained "significant inaccuracies and defamatory claims."[8] On April 1, the Subcommittee wrote again to Binance regarding discrepancies in its reply following further reporting that confirmed the company's platform had been used to launder money for Iran.[9] On April 17, the Subcommittee wrote to the Department of Justice and the Treasury Department questioning whether the company was in compliance with consent orders it had entered with both regulators in 2023.[10]

Finally, the Subcommittee wrote to Tether on June 4, 2026, requesting information and documents related to USDT's use in Iranian shadow banking and its compliance with American sanctions and banking law.[11] In particular, the Subcommittee sought information on Tether's handling of transactions with Iranian entities and sanctioned cryptocurrency exchanges, such as whether the company had ever failed to freeze wallets associated with terrorist organizations or the Iranian

---

[6] Press Release, Office of Sen. Richard Blumenthal, New Senate Permanent Subcommittee on Investigations Majority Staff Report Exposes Failure to Stop U.S. Technology from Fueling Russia's War Machine and China's AI Arms Race (Dec. 18, 2024), https://www.blumenthal.senate.gov/newsroom/press/release/new-senate-permanent-subcommittee-on-investigations-majority-staff-report-exposes-failure-to-stop-us-technology-from-fueling-russias-war-machine-and-chinas-ai-arms-race.

[7] Press Release, Office of Sen. Richard Blumenthal, Blumenthal Opens Inquiry After New Reporting Reveals Binance Allowed $1.7 Billion in Money Laundering to Iran Proxies & Russia's Shadow Fleet (Feb. 24, 2026), https://www.blumenthal.senate.gov/newsroom/press/release/blumenthal-opens-inquiry-after-new-reporting-reveals-binance-allowed-17-billion-in-money-laundering-to-iran-proxies-and-russias-shadow-fleet.

[8] *Binance's Formal Response to Recent Congressional Inquiry*, BINANCE (Mar. 3, 2026), https://www.binance.com/en/blog/compliance/6264258296613630636.

[9] Press Release, Office of Sen. Richard Blumenthal, Blumenthal Presses Binance on Potential Misrepresentations Regarding Money Laundering & Terrorist Financing (Apr. 1, 2026), https://www.blumenthal.senate.gov/newsroom/press/release/blumenthal-presses-binance-on-potential-misrepresentations-regarding-money-laundering-and-terrorist-financing.

[10] Press Release, Office of Sen. Richard Blumenthal, Blumenthal Presses Trump DOJ & Treasury Department on Binance's Lax Anti-Money Laundering Compliance (Apr. 17, 2026), https://www.blumenthal.senate.gov/newsroom/press/release/blumenthal-presses-trump-doj-and-treasury-department-on-binances-lax-anti-money-laundering-compliance.

[11] Press Release, Office of Sen. Richard Blumenthal, Blumenthal Probes Tether On Its Role in Iranian Shadow Banking (June 4, 2026), https://www.blumenthal.senate.gov/newsroom/press/release/blumenthal-probes-tether-on-its-role-in-iranian-shadow-banking.

government, as raised in this investigation. While Tether confirmed receipt of the Subcommittee's letter, the company has not provided a response as of the publication of this report.

BACKGROUND

Tether and USDT

Tether is the largest stablecoin issuer in the world, representing approximately 60% of all stablecoins by market capitalization as of September 2026.[12] Tether began operating in 2014 as a startup based out of Santa Monica, CA, launching its signature U.S. dollar-pegged token, USDT, later that year.[13] Tether's rise has been marked by persistent opacity, with investors and regulators seeking to determine whether every USDT token was fully backed by fiat currencies or assets, and where its reserves are held.[14] Tether's management and operations have been similarly opaque, characterized by hidden ownership information[15] and past allegations that the company used falsified documents and shell companies to gain access to bank accounts.[16] This opacity reinforces legal concerns about its management and financial standing: in 2021, the Attorney General for the State of New York found that Tether had secretly lent at least $625 million to Bitfinex, a trading platform owned by the same investors.[17]

While Tether is inextricably intertwined with American financial infrastructure and overseen by U.S. companies, it nominally operates from El Salvador—seemingly to evade U.S. legal responsibilities and to take advantage of the Salvadoran president's zeal for cryptocurrency. Tether's primary custodial relationship for its treasuries runs through Cantor Fitzgerald, the New York-based financial services firm formerly led by Secretary of Commerce Howard Lutnick and now run by his children. Cantor Fitzgerald has a stake in Tether worth billions. Tether reportedly provided Secretary Lutnick's children with a loan to enable them to buy out his stake in Cantor

---

[12] *Stablecoins*, DEFILLAMA, https://defillama.com/stablecoins?chartType=volume (last visited Sep. 23, 2026).

[13] Zeke Faux, *Anyone Seen Tether's Billions?*, BLOOMBERG (Oct. 7, 2021, at 14:25 ET), https://www.bloomberg.com/news/features/2021-10-07/crypto-mystery-where-s-the-69-billion-backing-the-stablecoin-tether.

[14] Press Release, Commodity Futures Trading Comm'n, CFTC Orders Tether and Bitfinex to Pay Fines Totaling $42.5 Million (Oct. 15, 2021), https://www.cftc.gov/PressRoom/PressReleases/8450-21.

[15] Ben Foldy, Ada Hui & Peter Rudegeair, *The Unusual Crew Behind Tether, Crypto's Pre-Eminent Stablecoin*, WALL ST. J. (Feb. 2, 2023, at 13:42 ET), https://www.wsj.com/articles/tether-ownership-and-company-weaknesses-revealed-in-documents-11675363340.

[16] Ben Foldy & Ada Hui, *Crypto Companies Behind Tether Used Falsified Documents and Shell Companies to Get Bank Accounts*, WALL ST. J. (Mar. 3, 2023, at 15:19 ET), https://www.wsj.com/finance/banking/crypto-companies-behind-tether-used-falsified-documents-and-shell-companies-to-get-bank-accounts-f798b0a5.

[17] Press Release, N.Y. Att'y Gen. Letitia James, Attorney General James Ends Virtual Currency Trading Platform Bitfinex's Illegal Activities in New York (Feb. 23, 2021), https://ag.ny.gov/press-release/2021/attorney-general-james-ends-virtual-currency-trading-platform-bitfinexs-illegal; James v. iFinex Inc., Settlement Agreement at 8-9 (N.Y. Att'y Gen. Investor Prot. Bureau Feb. 17, 2021), https://ag.ny.gov/sites/default/files/2021.02.17_-_settlement_agreement_-_execution_version.b-t_signed-c2_oag_signed.pdf.

Fitzgerald when he divested assets after his nomination.[18] USDT is widely available on American exchanges and Tether has recently announced that it would expand its operations in the United States. The company launched another dollar-pegged stablecoin and hired Bo Hines, a former White House official, weeks after he had left his role as the lead crypto policy staffer for the Trump Administration.[19] Moreover, the dollar that backs every USDT is, according to Tether's own attestations, held overwhelmingly in U.S. Treasury bills. This makes Tether one of the largest holders of U.S. government debt, holding more U.S. Treasury bonds than Israel or the United Arab Emirates.[20]

Iranian Shadow Banking and Cryptocurrencies

From its earliest days, cryptocurrency has been tied to illicit activities, as demonstrated by the early use of Bitcoin in ransomware, the online black market Silk Road, and the funding of the Islamic State.[21] Tether's prevalence in illicit finance in particular, such as North Korean military sales and cartel drug trafficking, is well documented.[22]

Around 2018, Iran made its first strategically-notable adoption of cryptocurrency with the embrace of Bitcoin mining, using cheap or subsidized electricity to generate Bitcoin that could be sold for fiat currencies abroad.[23] At the same time, Iranian cybercrime groups took advantage of the

---

[18] David Kocieniewski, Anthony Cormier & Todd Gillespie, *As Lutnick Sold Cantor to His Children, Tether Gave Them a Loan*, BLOOMBERG NEWS (Mar. 18, 2026, at 15:25 ET), https://www.bloomberg.com/news/features/2026-03-18/tether-made-loan-to-lutnick-s-children-as-they-bought-his-assets.

[19] *Tether Announces the Launch of USA₮, the Federally Regulated, Dollar-Backed Stablecoin, Made in America*, TETHER (Jan. 27, 2026), https://tether.io/news/tether-announces-the-launch-of-usat-the-federally-regulated-dollar-backed-stablecoin-made-in-america/; *Tether Appoints Former White House Crypto Council Executive Director Bo Hines as Strategic Advisor for Digital Assets and U.S. Strategy*, TETHER (Aug 19, 2025), https://tether.io/news/tether-appoints-former-white-house-crypto-council-executive-director-bo-hines-as-strategic-advisor-for-digital-assets-and-u-s-strategy/.

[20] *Compare Transparency*, TETHER, https://tether.to/en/transparency/?tab=reports (last visited Sep. 15, 2026) (showing Tether holds approximately $114.9 billion in U.S. Treasuries), *with Major Foreign Holders of Treasury Securities*, U.S. DEP'T OF THE TREASURY, https://ticdata.treasury.gov/resource-center/data-chart-center/tic/Documents/slt_table5.html (last visited Sep. 15, 2026) (valuing the United Arab Emirates and Israel's holdings at $114.8 billion and $110.9 billion at the end of June 2026, respectively).

[21] Press Release, U.S. Immigr. & Customs Enf't, HSI Seizes Biggest Anonymous Drug Black Market Website and Assists in Arrest of Operator and Overseas Co-Conspirators (Oct. 1, 2013), https://www.ice.gov/news/releases/hsi-seizes-biggest-anonymous-drug-black-market-website-and-assists-arrest-operator; Press Release, U.S. Dep't of Just., Virginia Man Sentenced to More Than 11 Years for Providing Material Support to ISIL (Aug. 28, 2015), https://www.justice.gov/archives/opa/pr/virginia-man-sentenced-more-11-years-providing-material-support-isil.

[22] FIN. ACTION TASK FORCE, TARGETED REPORT ON STABLECOINS AND UNHOSTED WALLETS: PEER-TO-PEER TRANSACTIONS 12–14 (2026), https://www.fatf-gafi.org/content/dam/fatf-gafi/publications/targeted-report-on-stablecoins-and-unhosted-wallets.pdf.coredownload.inline.pdf; *2026 Crypto Crime Report*, TRM LABS (Jan. 28, 2026), https://www.trmlabs.com/reports-and-whitepapers/2026-crypto-crime-report.

[23] Thomas Erdbrink, *How Bitcoin Could Help Iran Undermine U.S. Sanctions*, N.Y. TIMES (Jan. 29, 2019), https://www.nytimes.com/2019/01/29/world/middleeast/bitcoin-iran-sanctions.html; Colin Harper, *Inside Iran's Thriving, Underground Bitcoin Mining Scene*, BLOCKSPACE (May 14, 2025), https://blockspace.media/insight/inside-irans-thriving-underground-bitcoin-mining-scene/.

borderless, decentralized payment system that Bitcoin provides as the financial rails for ransomware campaigns that have disrupted schools, hospitals, and state governments across the United States.[24]

That same year, the Iranian government started building a digital version of its shadow banking system that could launder money and bypass international sanctions.[25] Iran's exclusion from the international financial system—such as having its banks cut off from the SWIFT network due to sanctions—made conventional cross-border banking increasingly difficult. Cryptocurrencies could bridge that gap.

Iran eagerly fostered the creation of domestically-controlled cryptocurrency exchanges, such as Nobitex, that could hide and facilitate payments on behalf of the regime in addition to serving retail consumers in Iran.[26] When the Department of Justice and FinCEN announced a settlement against Binance for violations of sanctions and banking laws in November 2023, it alleged that Binance had already been used to transfer $898 million in illicit payments to Iran between January 2018 and May 2022.[27] These included transfers to those new Iranian exchanges and sanctioned entities, such as individuals associated with the Islamic Revolutionary Guard Corp (IRGC). The Binance charges would be a preview of money laundering tools that cryptocurrencies would continue to provide to the Islamic Republic.

The Iranian government has further embraced and institutionalized the use of cryptocurrencies alongside traditional money-laundering tools of gold, cash smuggling, and foreign shell companies. Between 2024 and 2025, two Chinese partners of Binance (Blessed Trust and Hexa Whale) were able to launder at least $1.5 billion—nearly twice the amount cited in the Binance case—to Iran and the Houthis mainly using Tether.[28] The Blessed Trust and Hexa Whale examples

[24] Press Release, U.S. Dep't of Just., Two Iranian Men Indicted for Deploying Ransomware to Extort Hospitals, Municipalities, and Public Institutions, Causing Over $30 Million in Losses (Nov. 28, 2018), https://www.justice.gov/archives/opa/pr/two-iranian-men-indicted-deploying-ransomware-extort-hospitals-municipalities-and-public.

[25] Angus Berwick & Tom Wilson, *Crypto Exchange Binance Helped Iranian Firms Trade $8 Billion Despite Sanctions*, REUTERS (Nov. 7, 2022, at 09:08 ET), https://www.reuters.com/business/finance/exclusive-crypto-exchange-binance-helped-iranian-firms-trade-8-billion-despite-2022-11-04/.

[26] Sune Engel Rasmussen, *How Iran's Chief Sanctions Buster Went from Death Row to Crypto*, WALL ST. J. (May 3, 2026, at 22:00 ET), https://www.wsj.com/world/middle-east/how-irans-chief-sanctions-buster-went-from-death-row-to-crypto-51424fe7; Gavin Finch et al., *One of Iran's Most Powerful Families Founded its Largest Crypto Exchange. It's Used By the IRGC to Move Millions*, REUTERS (May 1, 2026, at 08:13 ET), https://www.reuters.com/investigations/one-irans-most-powerful-families-founded-its-largest-crypto-exchange-its-used-by-2026-05-01/.

[27] Press, Release, U.S. Dep't of Just., Binance and CEO Plead Guilty to Federal Charges in $4B Resolution (Nov. 21, 2023), https://www.justice.gov/archives/opa/pr/binance-and-ceo-plead-guilty-federal-charges-4b-resolution; Binance Holdings Ltd., FinCEN Consent Order No. 2023-04 (Nov. 11, 2023), https://www.fincen.gov/system/files/enforcement_action/2023-11-21/FinCEN_Consent_Order_2023-04_FINAL508.pdf.

[28] David Yaffe-Bellany & Michael Forsythe, *Binance Employees Find $1.7 Billion in Crypto Was Sent to Iranian Entities*, N.Y. TIMES (Feb. 23, 2026), https://www.nytimes.com/2026/02/23/technology/binance-employees-iran-firings.html; Patricia Kowsmann, Angus Berwick & Ben Foldy, *Binance Fired Staff Who Flagged $1 Billion Moving to Sanctioned Iran Entities*, WALL ST. J. (Feb. 23, 2026, at 16:14 ET),

reinforce industry reports that the use of cryptocurrencies to evade sanctions increased 694% in 2025 alone,[29] accounting for an estimated minimum of $2 billion in illicit Iranian cryptocurrency transactions last year.[30]

FINDINGS

Finding 1: Tether has become a primary illicit international payment system for Iran, allowing it to circumvent international sanctions on its banks.

The Subcommittee's analysis demonstrates how singularly Iran's digital shadow banking network relies on Tether's USDT. The Subcommittee found that, of the wallets identified for seizure by Israel's NBCTF, 87% of 757 wallets implicated in Iranian terrorism financing had predominantly transacted in USDT (for both the Tron and Ethereum blockchain).[31] Similarly, for wallets designated by OFAC in relation to Iran or Iran-linked terrorist organizations, the Subcommittee found 57% of 101 wallets had predominantly transacted in USDT (see Attachment I). Moreover, most of the additional wallets labeled as "Mixed" mainly transacted in USDT, meaning that in practice Tether represents the vast majority of cryptocurrency activity under OFAC designations, particularly when considering the amount of funds laundered. Bitcoin followed far behind in second place, at 7% for NBCTF and 19% for OFAC respectively, more commonly occurring in either the earliest designations or on wallets associated with ransomware operators or large exchanges (which would naturally be handling a broader portfolio on behalf of retail customers).

---

https://www.wsj.com/finance/currencies/binance-iran-sanctions-financing-staff-b1648133; Leo Schwartz & Ben Weiss, *Inside the Binance Accounts Internal Investigators Say Helped Transfer More Than $1 Billion to Iran-Linked Entities: A 79-Year-Old VIP Chinese Trader and a Suspected Iranian Gold Smuggler*, FORTUNE (Mar. 12, 2026, at 13:14 ET), https://fortune.com/2026/03/12/binance-accounts-iranian-entities-sanctions-chinese-vips-gold-smuggler/.

[29] *2026 Crypto Crime Report*, TRM LABS (Jan. 28, 2026), https://www.trmlabs.com/reports-and-whitepapers/2026-crypto-crime-report; *Crypto Crime Reaches Record High in 2025 as Nation-State Sanctions Evasion Moves On-Chain at Scale*, CHAINALYSIS (Jan. 8, 2026), https://www.chainalysis.com/blog/2026-crypto-crime-report-introduction/.

[30] *Crypto Crime in 2025 Was Primarily Driven by 694% Surge in State-Driven Sanctions Evasion Volume*, CHAINALYSIS (Mar. 25, 2026), https://www.chainalysis.com/blog/2026-crypto-crime-report-introduction/; Osman Sonmez, *Iran's USDT and Stablecoin-Based Sanctions Evasion: An Empirical Analysis of Digital Dollar Exploitation for International Trade Finance* (July 9, 2026), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=6362678.

[31] For purpose of analysis, we define "predominantly" as greater than 80% of the U.S. dollar value of aggregate transactions, using the current market rate as a rough benchmark. Different approaches to thresholds, evaluation of market rates, and assessing activity may make a slight difference in the prevalence of certain tokens (namely Ethereum), the top token would overwhelmingly remain USDT followed far behind by Bitcoin.

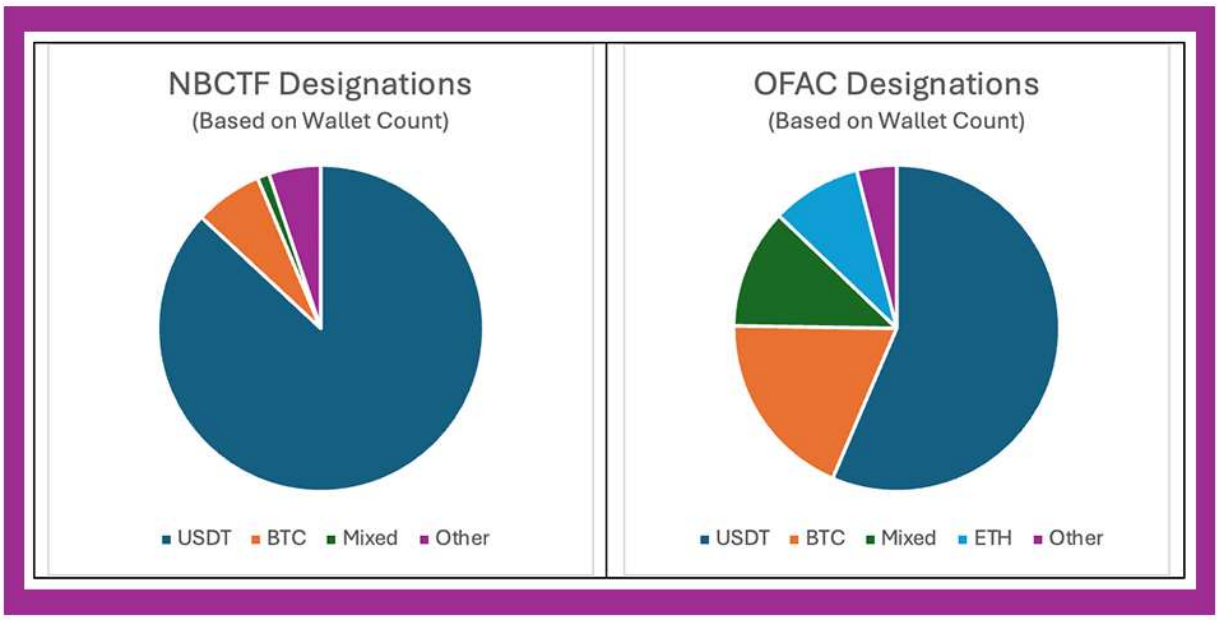


Figure 1: Share of Analyzed Wallets That Transact Primarily in USDT

Only the native Ethereum (ETH) and TRON (TRX) tokens had meaningful (but still limited) use by sanctioned Iran-linked wallets, in terms of being held by multiple groups and in an aggregate volume above a million dollars. Indeed, most Ethereum blockchain designations generally still transacted in USDT. USDT's largest competitor, USDC—the dollar-pegged stablecoin issued by the second largest stablecoin issuer Circle—was extremely limited in the Subcommittee's analysis, appearing only in a few transactions by the sanctioned Iranian exchange Shelbit. Binance's USDT-pegged stablecoin does appear in volumes above a million dollars with Nobitex, Shelbit, and a sanctioned Iranian hacker. Other tokens and meme coins, such as Solana, Dogecoin (DOGE), Shiba Inu Coin (SHIB), and Ripple (XPR), appear at a negligible number and volume—again, generally in older designations.

That Iran would be interested in a stablecoin like Tether's USDT is unsurprising. USDT is readily accessible on Chinese-founded and unregulated cryptocurrency exchanges—often referred to as "no-know-your-customer" (KYC) exchanges, over-the-counter (OTC) trading desks, or "cashdesks."[32] USDT also has a stable value compared to the rapid inflation of the Iranian Rial, or the wild fluctuations—including the risk of the loss of value—with Bitcoin and other non-stablecoin tokens. The widespread, international acceptance and stability of USDT provides easy on- and off-ramps between cryptocurrencies and fiat currency across borders. Tether also has a significant official presence and adoption in the Middle East, making it easier for Iran to purchase

[32] *See Tether Token,* TETHER, https://web.archive.org/web/20260908233236/https://tether.to/en/ (last visited Sep. 11, 2026) (noting Tether's "widespread adoption" across Chinese-originated exchanges such as Gate.io, HTX, KuCoin, and OKX).

USDT in countries like the United Arab Emirates or Türkiye, and then transfer those funds to entities inside of Iran, its proxies, or to purchase items abroad.[33]

Iranian cryptocurrency exchanges, such as the IRGC-linked Nobitex, have dealt substantially in Tether, including exchanging USDT for Iranian Rials even in the middle of war with the United States and advising their customers how to evade OFAC sanctions with Tether.[34] While some Iranian exchanges essentially serve as a bank to hold (or custody) cryptocurrencies for customers, such as Nobitex, others such as the OFAC-designated Shelbit and Zedpay[35] act more as a payment settlement mechanism, moving billions in USDT between Iran and international counterparties (including sanctioned Russian exchanges) without holding onto funds for long periods of time.[36] Exchanges not only provide a mechanism and market for Iranian government actors to buy and sell USDT and other cryptocurrencies, but also a place to co-mingle illicit finance with the savings of ordinary Iranians, who may be using stablecoins for remittances or to hedge against the country's hyperinflation.

The Subcommittee used wallet designations and associated transactions as a benchmark to determine that USDT emerged as a preferred cryptocurrency of Iranian shadow banking and those of its proxies between 2023 and 2024. Bitcoin and a diverse set of other cryptocurrencies were predominant in earlier designations of wallets. For example, Israel's first designation in June 2021 targeted a public Hamas fundraising campaign that had raised over a hundred million dollars in mainly Bitcoin, as well as a few million in USDT, ETH, and TRX.[37] Similarly, when OFAC sanctioned Iranian ransomware operators in 2022, a group that OFAC alleged were affiliated to the IRGC, only Bitcoin addresses were disclosed.[38]

---

[33] *Tether Trade Finance Completes Funding of First Middle Eastern Crude Oil Transaction*, TETHER (Nov. 8, 2026), https://tether.io/news/tether-trade-finance-completes-funding-of-first-middle-eastern-crude-oil-transaction/.

[34] Chart of Live Tether to Iranian Toman Exchange Rate, NOBITEX (Iran), https://nobitex.ir/panel/exchange/usdt-irt/ (last visited Sep. 15, 2026); Maryam Azarfar, فریز شدن تتر چیست و چگونه از آن پیشگیری کنیم؟ [*What is Tether Freeze and How to Prevent It?*], NOBITEX (Iran) (July 19, 2026), https://nobitex.ir/mag/what-is-usdt-freezing/.

[35] Press Release, U.S. Dep't of the Treasury, Treasury Further Dismantles Iranian Financier Zanjani's Network (July 24, 2026), https://home.treasury.gov/news/press-releases/sb0576.

[36] *How Shelbit Became a USD 6.3 Billion Settlement Layer for Iran's Illicit Economy*, TRM LABS (Aug. 7, 2026), https://www.trmlabs.com/resources/blog/how-shelbit-became-a-usd-6-3-billion-settlement-layer-for-irans-illicit-economy.

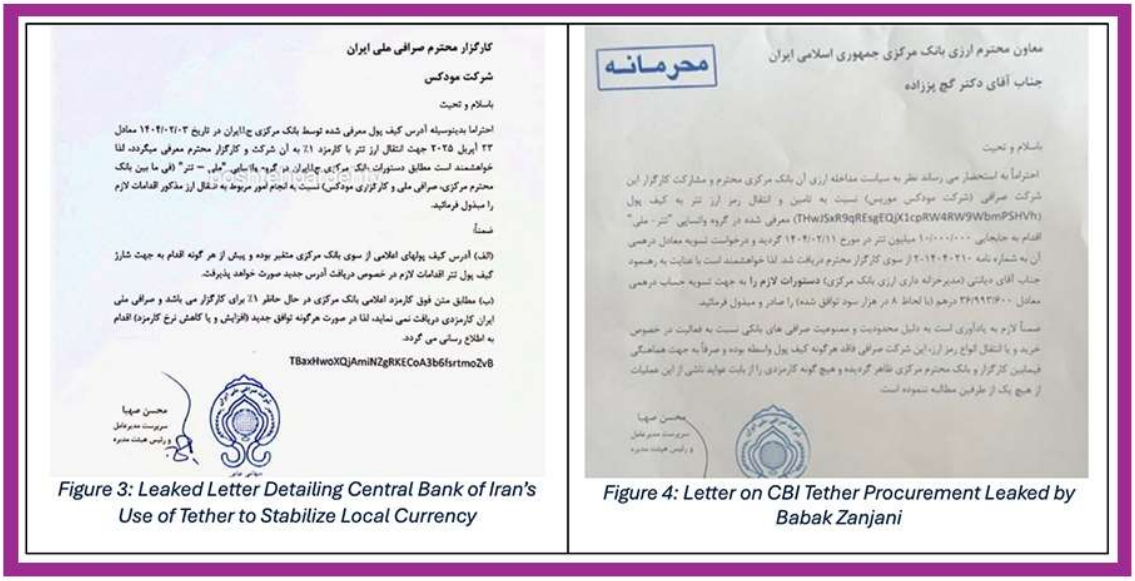
[37] *Minister of Defense Benny Gantz Signs an Administrative Order to Seize Electronic Wallets Used by Hamas to Trade Different Types of Cryptocurrency*, NAT'L BUREAU FOR COUNTER TERROR FIN. OF ISRAEL (July 12, 2021), https://nbctf.mod.gov.il/en/Pages/CryptoSeizureEN072021.aspx (calculation of prevalence by the Subcommittee for ASO 44/21); Angus Berwick & Ian Talley, *Hamas Militants Behind Israel Attack Raised Millions in Crypto*, WALL ST. J. (Oct. 10, 2023, at 15:34 ET), https://www.wsj.com/world/middle-east/militants-behind-israel-attack-raised-millions-in-crypto-b9134b7a.

[38] Press Release, U.S. Dep't of the Treasury, *Treasury Sanctions IRGC-Affiliated Cyber Actors for Roles in Ransomware Activity* (Sep. 14, 2022), https://home.treasury.gov/news/press-releases/jy0948.

Figure 2: Hamas-associated groups shift from fundraising Bitcoin to multiple cryptocurrencies, including USDT

By 2024, Tether became the overwhelmingly most common cryptocurrency used by wallets designated for Iranian and regional illicit financing. For example, when OFAC designated Gaza Now for fundraising, nearly all the $4.5 million dollars of cryptocurrencies received by the eight wallets designated were in USDT. This shift is illustrated by Hamas public fundraising requests placing greater emphasis on USDT in posts collected from Telegram by the Subcommittee (as illustrated in Figure 2. At the time, media reports also noted the change, attributing the transition to increased seizures by Binance (which at that time was negotiating a settlement with the DOJ over the same issues) and a perception that Tether was less monitored.[39]

[39] Leo Schwartz, *What's the Deal with Hamas and Crypto?*, FORTUNE (Nov. 15, 2023, at 09:35 ET), https://fortune.com/crypto/2023/11/15/hamas-crypto-tether-bitcoin-israel-illicit-finance/.



کارگزار محترم صرافی ملی ایران

شرکت مودکس

باسلام و تحیت

احتراماً بدینوسیله آدرس کیف پول معرفی شده توسط بانک مرکزی ج.ا.ایران در تاریخ ۱۴۰۴/۰۲/۰۳ معادل ۲۳ آپریل ۲۰۲۵ جهت انتقال ارز تتر با کارمزد ۰٫۱ به آن شرکت و کارگزار محترم معرفی میگردد، لذا خواهشمند است مطابق دستورات بانک مرکزی ج.ا.ایران در گروه «آسیایی "ملی" – تتر» (فی ما بین بانک محترم مرکزی، صرافی ملی و کارگزاری مودکس) نسبت به انجام امور مربوط به انتقال ارز مذکور اقدامات لازم را مبذول فرمائید.

ضمناً

(الف) آدرس کیف پولهای اعلامی از سوی بانک مرکزی متغیر بوده و پیش از هر گونه اقدام به جهت شارژ کیف پول تتر اقدامات لازم در خصوص دریافت آدرس جدید صورت خواهد پذیرفت.

(ب) مطابق متن فوق کارمزد اعلامی بانک مرکزی در حال حاضر ۰٫۱ برای کارگزار می باشد و صرافی ملی ایران کارمزدی دریافت نمی نماید، لذا در صورت هرگونه توافق جدید (افزایش و یا کاهش نرخ کارمزد) اقدام به اطلاع رسانی می گردد.

TBaxHwoXQjAmiN2gRKECoA3b6fsrtmo2v8

محسن صهبا

معاون محترم ارزی بانک مرکزی جمهوری اسلامی ایران

جناب آقای دکتر گچ پزداده

محرمانه

باسلام و تحیت

احتراماً به استحضار می رساند نظر به سیاست مداخله ارزی آن بانک مرکزی محترم و مشارکت کارگزار این شرکت صرافی (شرکت مودکس موریس) نسبت به تامین و انتقال رمز ارز تتر به کیف پول (THwJSxR9qREsgEQjX1cpRW4RW9WbmPSHVh) معرفی شده در گروه واتسایی "تتر- ملی" اقدام به جابجایی ۱،۰۰۰،۰۰۰ میلیون تتر در مورخ ۱۴۰۴/۰۲/۱۱ گردید و درخواست تسویه معادل درهمی آن به شماره نامه ۱۴۰۴-۲۱۰-۲ از سوی کارگزار محترم دریافت شد لذا خواهشمند است با عنایت به رهنمود جناب آقای دیانتی (مدیرحزانه داری ارزی بانک مرکزی) **دستورات لازم را** به جهت تسویه حساب درهمی معادل ۳۶/۹۹۳/۶۰۰ درهم (با لحاظ ۸ در هزار سود توافق شده) را صادر و مبذول فرمائید.

ضمناً لازم به یادآوری است به دلیل محدودیت و ممنوعیت صرافی های بانکی نسبت به فعالیت در خصوص خرید و یا انتقال انواع رمز ارز، این شرکت صرافی فاقد هرگونه کیف پول واسطه بوده و صرفاً به جهت هماهنگی فیمابین کارگزار و بانک محترم مرکزی ظاهر گردیده و هیچ گونه کارمزدی را از بابت عواید ناشی از این عملیات از هیچ یک از طرفین مطالبه ننموده است.

محسن صهبا

Figure 3: Leaked Letter Detailing Central Bank of Iran's Use of Tether to Stabilize Local Currency

Figure 4: Letter on CBI Tether Procurement Leaked by Babak Zanjani

Leaks from the Central Bank of Iran (CBI) shed further light into the shadow banking network. In October 2025, a confidential letter from the CBI was published by an Iranian reporter describing the use of USDT in a scheme to prop up the value of the Iranian Rial and facilitate oil sales to counter American economic pressure. The letter was addressed to a brokerage referred to as the Modex Exchange Company, which is reportedly run by Iranians, for a transaction orchestrated in a WhatsApp group call "National – Tether." Two months later, another letter describing the purchase of USDT abroad for the CBI was leaked on Twitter by Babak Zanjani, the nation's primary money laundering operative, out of apparent frustration over allegations he mishandled state funds.[40]

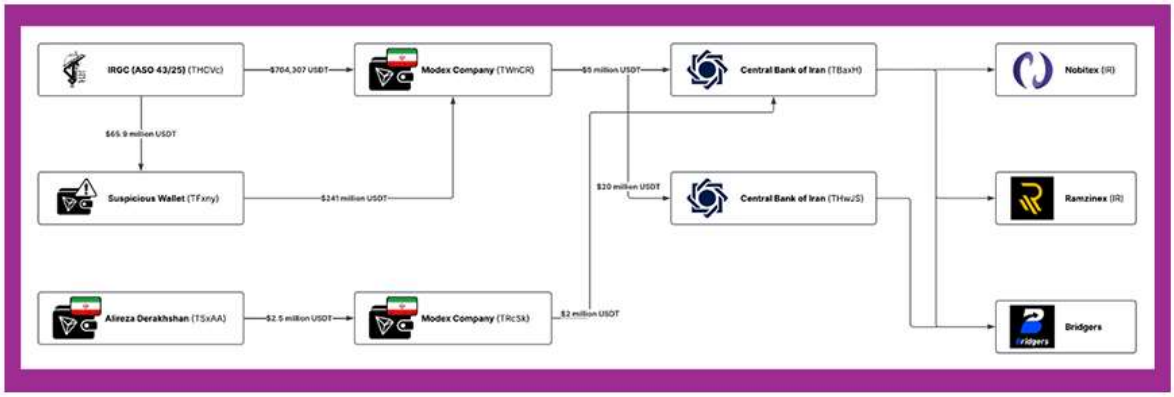


Figure 5: USDT Moving into the Central Bank of Iran from Regional Exchanges and IRGC-Linked Accounts, and then Onward to Iranian Exchanges and Mixers (April-May 2025)

[40] Image posted by Poshteh Pardeh, Telegram (t.me/poshtehpardehtv/11145) (Oct. 1, 2025, at 03:35 ET), https://t.me/poshtehpardehtv/11145; Image posted by Babak Zanjani (@babakzanjani_ch), X (Dec. 21, 2025, at 15:58 ET), https://x.com/babakzanjani_ch/status/2002846070846423212/photo/1.

The Subcommittee analyzed the two wallets referenced by the letters. According to blockchain transactions, the two CBI wallets received nearly $50 million, exclusively in USDT in April and May 2025. Within days of each transfer, the CBI sent the funds to Iranian exchanges, such as Nobitex and Ramzinex, or to a mixer (essentially, an automated money laundering service)—reinforcing the theory that the Iranian government uses domestic exchanges as a safe harbor.

Matching the timing of transfers and amounts also identified three wallets that were used by the Modex Exchange Company to fund the CBI. These wallets, over the limited, several months period of their use, received nearly $600 million in USDT, including from known Iranian money launderers. This suggests that, even if the Modex associated wallets were not Iranian controlled, those behind them dealt broadly with illicit finance. It is also notable that, according to the letters, Modex was used to purchase USDT with Emirati Dirham, suggesting some presence in the United Arab Emirates. The brief window into the CBI's National-Tether operation was likely the tip of the iceberg. Indeed, when OFAC sanctioned two other wallet addresses linked to the CBI in April 2026, those two wallets contained $344.2 million in Tether. [41]

Finding 2: Tether serves as a central payment mechanism that interlinks Iran and its terrorist proxy organizations, undermining U.S. security interests in the region.

While the CBI's network illustrates Iran's use of Tether to move hundreds of millions in U.S. dollars through its shadow banking system, other examples demonstrate that USDT provides the rails for a settlement and transfer mechanism between the Islamic Republic and its regional terrorist proxies.

[41] Press Release, U.S. Dep't of the Treasury, Off. of Foreign Assets Control, Iran-related Designations; Counter Terrorism and Iran-related Designation Update; Issuance of Iran-related General License (Apr. 24, 2026), https://ofac.treasury.gov/recent-actions/20260424.

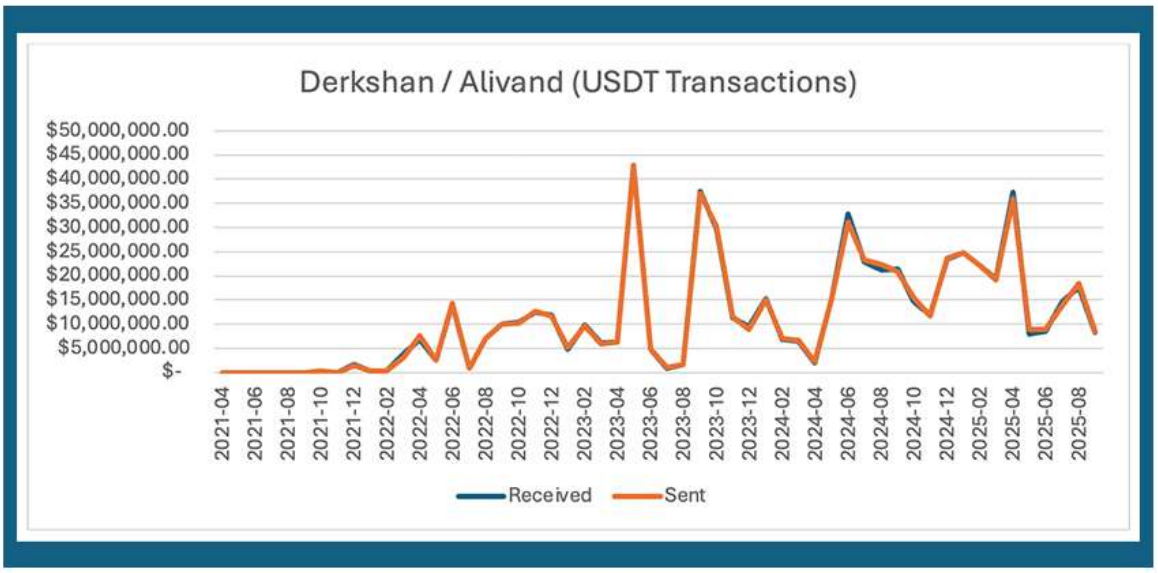


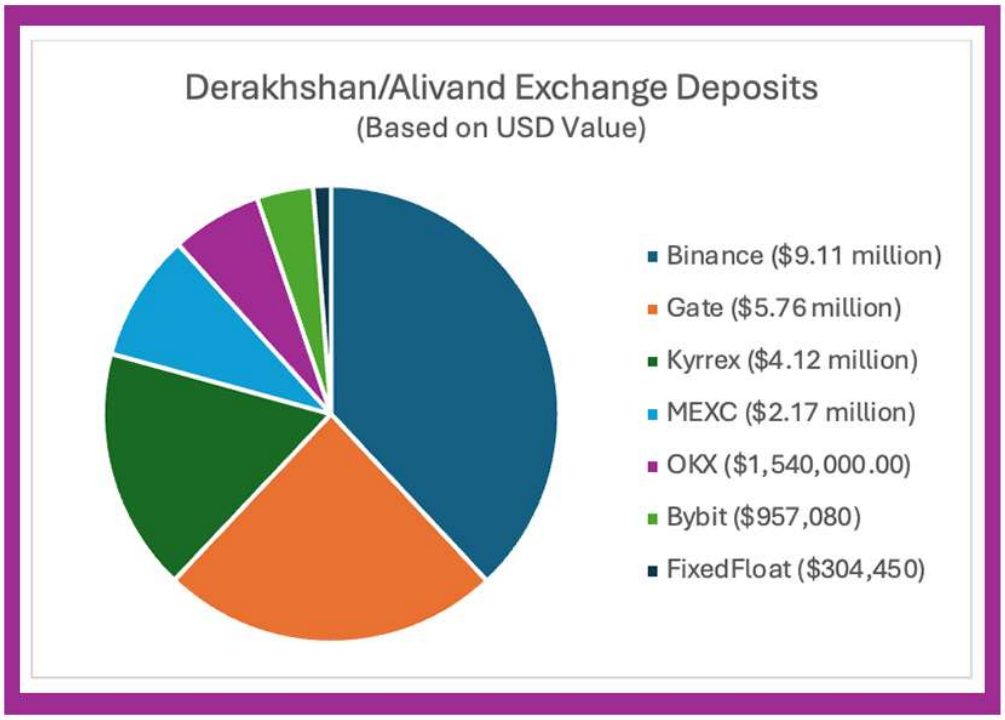
Figure 6: Alireza Derakhshan and Arash Estaki Alivand's USDT Transaction History

In September 2025, OFAC designated the Iranian nationals Alireza Derakhshan and Arash Estaki Alivand for running an international network of front companies to facilitate Iranian oil sales and military procurement.[42] From the wallet addresses sanctioned by OFAC, the Subcommittee's forensic analysis found that, over four years, Derakhshan and Alivand had received $603 million in USDT in these operations, operating nearly exclusively in Tether.[43] Funds entered the network generally either through prominent exchanges based outside of the United States, such as Bybit, Kyrrex,[44] OKX, Gate, and Binance, or through repeated multi-million dollar USDT transfers from unattributed wallets (potentially belonging to cashdesks or hawala networks).

[42] Press Release, U.S. Dep't of the Treasury, Treasury Targets Financial Network Supporting Iran's Military (Sep. 16, 2025), https://home.treasury.gov/news/press-releases/sb0248.

[43] Outside of USDT, the two transacted 200,000 in USDC and 65 ETH, well less than one percent of the total volume.

[44] Scilla Alecci, *Hunt for Missing Millions Unmasks One Crypto Exchange Hidden Inside Another*, INT'L CONSORTIUM OF INVESTIGATIVE JOURNALISTS (Nov. 20, 2025), https://www.icij.org/investigations/coin-laundry/hunt-for-missing-millions-unmasks-one-crypto-exchange-hidden-inside-another/.



Figures 7: Exchange Usage by Alireza Derakhshan and Arash Estaki Alivand[45]

Importantly, the Derakhshan/Alivand network demonstrates the existence of a network of unidentified entities moving billions of dollars between illicit regional actors using Tether, as well as the breadth of their activities. As noted in Figure 5, Alivand funded one of the wallets behind Modex Company's "National-Tether" scheme to support the CBI, sending $2.5 million in USDT the day after the transaction with the CBI. However, Alivand also sent millions of USDT to other unattributed wallets that also sent funds to Modex. These transfers were likely either unattributed Iranian money laundering operations or unregulated regional brokers (also shown in Figure 5).

[45] Subcommittee staff generated this figure using data extracted from sanctioned wallets and complemented with data generated in Arkham Intelligence.

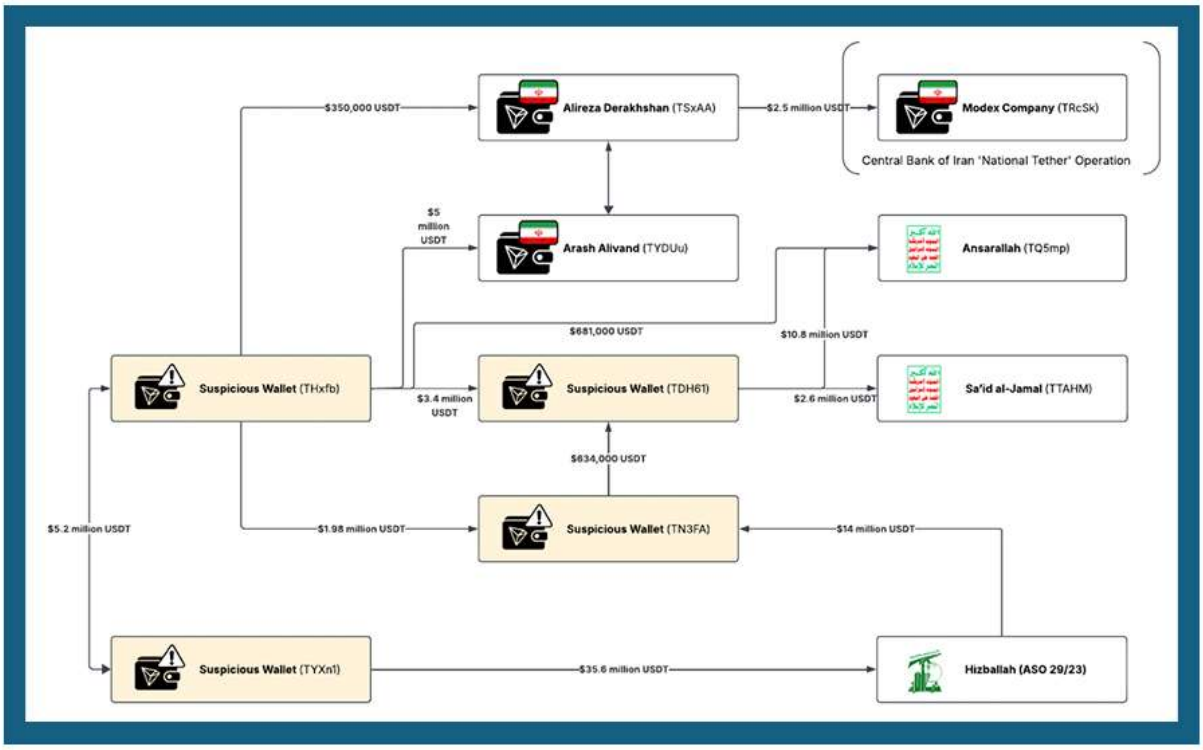


Figure 8: Derakhshan and Alivand Illustrate the Deep Web of Iranian Shadow Banking (Transactions Between 2023-2025)

Figure 8 demonstrates how Alivand and Derakhshan are linked to networks of suspicious wallets that funneled tens of millions to known Hizballah, Houthi financiers, and other IRGC attributed wallets.[46]

The Subcommittee's analysis of sanctioned wallets found that the four wallets labeled "suspicious" in Figure 8 alone received over $2.7 billion during April 2023 to October 2024. Each wallet was generally only active for several months, but at that time engaged in notable suspicious behavior like receiving funds and immediately forwarding the same amount elsewhere.[47] Moreover, while different Middle Eastern terrorist groups are recurringly linked to this set of wallets, other sanctioned entities outside the region, such as cybercrime groups, do not appear. Regardless of ultimate ownership, this web of transactions suggests that Iranian shadow banking can take advantage of a large, well-connected regional distribution network—a network built on Tether.

The Subcommittee's analysis raises serious concerns about how this payment network could be used for the procurement of drone and missile parts. Iranian drones, namely the "Shahed" series and their Russian "Geran" counterparts, have been an instrument of terror against Ukrainian

[46] *OFAC Targets $600 Million Iranian Shadow Banking Network Using Cryptocurrency to Evade Sanctions*, CHAINALYSIS (Sep. 16, 2025), https://www.chainalysis.com/blog/ofac-sanctions-iranian-shadow-crypto-banking-network-september-2025/.

[47] Such as repeatedly relaying $2 million USDT payments from Modex and another IRGC wallet elsewhere.

infrastructure and civilians, and have killed American service members in Iranian attacks against U.S. bases in the Middle East. Iran's deadly innovation was building drones at low-cost using commercial off-the-shelf parts, enabling overwhelming swarms. The Subcommittee has previously published findings regarding the role of Chinese suppliers and diverted Western technologies in these drones.[48]

There is emerging evidence that Iran and its proxies have used cryptocurrencies to market drones and procure components for their manufacture. In September 2025, the United States Attorney's Office for the District of Massachusetts filed a civil forfeiture to freeze and recover $584,741 in USDT from Mohammad Abedini, the founder of an Iranian firm that produces navigation systems.[49] According to the order, Abedini sought to procure foreign semiconductors and sensors for end use in its Sepehr Navigation System, which has been found in recovered Shahed drones that targeted Americans. When OFAC sanctioned a network of Houthi financial facilitators and operatives involved in procuring weapons from Russia, TRM Labs disclosed that those operatives had sent money to a "Russian broker selling unmanned aerial vehicles (UAVs) and anti-UAV equipment, among other military gear on behalf of Chinese manufacturers."[50] Similarly, Chainalysis has found indirect links between designated Iranian wallets and a "Hong Kong-based drone manufacturer."[51]

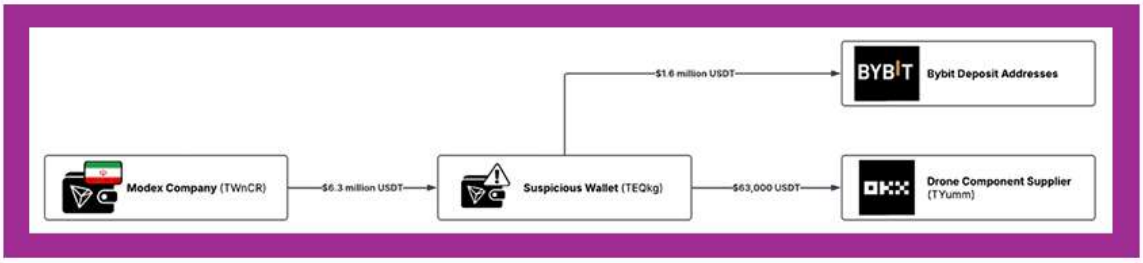


Figure 9: Tether transferred from a Modex-associated wallet to an OKX deposit address for a Chinese supplier of drone components. It is also notable that the wallet was also making deposits into other Chinese exchanges as it transacted with the Chinese suppler.

[48] Press Release, Office of Sen. Richard Blumenthal, Senate Permanent Subcommittee on Investigations Releases Majority Staff Report Revealing Semiconductor Manufacturers' Deficient Compliance with Export Controls (Sep. 10, 2024), https://www.blumenthal.senate.gov/newsroom/press/release/senate-permanent-subcommittee-on-investigations-releases-majority-staff-report-revealing-semiconductor-manufacturers-deficient-compliance-with-export-controls.

[49] Press Release, U.S. Dep't of Just., United States Seeks Civil Forfeiture of Cryptocurrency Associated with Iranian National Mohammed Abedini (Sep. 11, 2025), https://www.justice.gov/usao-ma/pr/united-states-seeks-civil-forfeiture-cryptocurrency-associated-iranian-national-mohammad; United States v. 584,741 USDT associated with the cryptocurrency wallet with address TTyRaPB6TQT9MEpwwRux4naX31Rov8e648, No.1:25-cv-12539 (D. Mass. Sep. 11, 2025).

[50] Press Release, U.S. Dep't of the Treasury, Treasury Sanctions Houthi Network Procuring Weapons and Commodities from Russia (Apr. 2, 2025), https://home.treasury.gov/news/press-releases/sb0068; *From UAVs to Sanctions Evasion: How the Houthis Use Crypto*, TRM LABS (Apr. 17, 2025), https://www.trmlabs.com/resources/blog/from-uavs-to-sanctions-evasion-how-the-houthis-use-crypto.

[51] *From the Battlefield to the Blockchain: How Cryptocurrency Is Helping Finance the Drone Revolution*, CHAINALYSIS (Mar. 30, 2026), https://www.chainalysis.com/blog/cryptocurrency-drones-research/.

In the course of its inquiry, the Subcommittee had the opportunity to view data prepared by a third-party investigator demonstrating how Iranian and Russian entities purchase drone components using USDT. This data included transcripts of Chinese suppliers offering to accept cryptocurrencies for dual use components and providing wallet addresses to receive potential payments. The Subcommittee confirmed that one of the identified wallets had, in January 2026, been sent USDT by a wallet exclusively funded by the Iran-linked Modex Exchange Company (Figure 9). That Chinese electronics supplier advertises "drone supplies," including the class of semiconductors found in Shahed and Geran drones. Although only $64,000 in USDT was sent, the semiconductors of concern only cost $1-$3 dollars per unit, which would still be a large procurement. Ultimately, while these transactions do not demonstrate the end-recipient or the purchased components, they and previous reports demonstrate the risk posed by cryptocurrencies for procuring components and equipment for Iranian military purposes.

Finding 3: Tether's repeated failure to freeze illicit wallets and prevent abuse created the permissive environment under which Iranian shadowing banking has flourished.

The Subcommittee's analysis raises concerns about Tether's efforts to find and block illicit wallets—and its timeliness and comprehensiveness in doing so. Despite its founding in the United States and deep reliance on American financial infrastructure, Tether has stated that its compliance with OFAC sanctions is "voluntary" and that it follows "OFAC *guidelines*" (emphasis added).[52] It has issued press releases lauding itself for measures to block sanctioned accounts after OFAC's designation, which any bank or commercial interest would do as a simple matter of business and compliance with the law.[53] Based on the Subcommittee's analysis of blockchain activity, Tether appears to conduct inconsistent or inadequate de-risking and regularly partners with exchanges with histories of compliance failures.

As the issuer of USDT, Tether has the technical means to freeze and block wallets from withdrawing funds through a "blacklist" function built into the stablecoin's "contract" (its technical implementation on the blockchain). It can also "destroy" the funds in a wallet. Tether additionally can review whether its direct clients (typically the cryptocurrency exchanges that purchase USDT to sell to their own customers) are engaging in "know-your-customer" screening of their users and monitoring transactions for illicit use. In principle, Tether should be engaged in its own monitoring of USDT transactions for partners' compliance and impose accountability for

[52] *Tether Introduces New Policy to Strengthen Ecosystem Security*, TETHER (Dec. 9, 2023), https://tether.io/news/tether-introduces-new-policy-to-strengthen-ecosystem-security/; *Tether Supports Freeze of More Than $344 Million in USD₮ in Coordination with OFAC and U.S. Law Enforcement*, TETHER (Apr. 23, 2026), https://tether.io/news/tether-supports-freeze-of-more-than-344-million-in-usdt-in-coordination-with-ofac-and-u-s-law-enforcement/.

[53] *Tether Supports Freeze of More Than $344 Million in USD₮ in Coordination with OFAC and U.S. Law Enforcement*, TETHER (Apr. 23, 2026), https://tether.io/news/tether-supports-freeze-of-more-than-344-million-in-usdt-in-coordination-with-ofac-and-u-s-law-enforcement/.

breaches—including the termination of business relationships and the blacklisting of accounts. Indeed, these expectations are included in Tether's own terms of service.[54]

> *Tether is committed to providing safe, compliant, and reputable Services and to identify, detect, prevent, and report on money laundering, terrorist financing, and other improper activities under applicable AML Laws, CTF Laws, Anti-Corruption Laws, and Economic Sanctions Laws. Accordingly, Tether insists on a comprehensive and thorough user due diligence process and ongoing analysis and reporting.*[55]

The Subcommittee's analysis of blockchain records raises questions regarding the adequacy, or indeed even the existence, of Tether's efforts to proactively investigate clear signs of Iranian shadow banking using USDT. The Subcommittee's analysis further raises questions about the extent to which Tether acts on such clear indicators of illicit finance by its business partners, including Binance and Chinese-founded exchanges.

The Subcommittee's analysis pinpointed specific dates when wallets were frozen by Tether. This analysis revealed cases of significant delays by Tether in blacklisting wallets, even when a government attributed them to sanctioned entities or terrorist organizations. From 2021 to May 2023, Tether did not appear to freeze any wallets designated by the NBCTF, despite multiple orders specifying addresses controlled by Hamas.[56] Indeed, Tether appears to have become regularly responsive to NBCTF only after the Hamas attacks on October 7, 2023.

While Tether now appears to respond to sanctions and designations orders in some instances, these efforts still appear uneven and inconsistent. Delays by Tether have allowed terrorist organizations to continue laundering illicit funds through wallets after they were targeted for seizure. When the NBCTF designated 39 wallets in June 2023 (ASO 29/23)[57] as associated with the Hizballah money launderer Tawfiq Muhammad Sa'id Al-Law—wallets that had been active since 2021—Tether failed to blacklist all but five of them for months, waiting until March 2024 to freeze the remaining 34 addresses, notably shortly before OFAC sanctioned Al-Law as well. The Subcommittee's forensic analysis found that this delay by Tether allowed the sanctioned wallets to move out more than $34.6 million in USDT after the NBCTF seizure notice was published, including withdrawals and deposits in exchanges like Binance, Paribu, and BTCTurk (the latter two being Turkish exchanges). Similarly, wallets attributed by the NBCTF in March 2022 (ASO 15/22) as belonging to a Hamas-

---

[54] *Legal*, TETHER, https://tether.to/en/legal/ (last visited Sep. 15, 2026).

[55] *Id.*

[56] While NBCTF orders carry a signature date, the actual orders have in some cases not become public for weeks or months, so we also note dates where the orders appear to have been made public.

[57] *The Defense Establishment Thwarted Terrorist Infrastructure Belonging to Hezbollah and the Iranian Quds Force, Which Operated to Transfer Funds through Digital Currencies for Quds Force and Hezbollah*, NAT'L BUREAU FOR COUNTER TERROR FIN. OF ISRAEL, https://nbctf.mod.gov.il/en/Pages/28062023EN.aspx (last visited Sep. 19, 2026).

affiliated money laundering operation were never frozen and continued to engage in transfers after their designation.[58]

Outside of sanctions or seizure notices, Tether has also failed to act on wallets that bear strong indicators of illicit finance, despite ample information about their ties to Iranian entities or terrorist organizations being in the public domain.

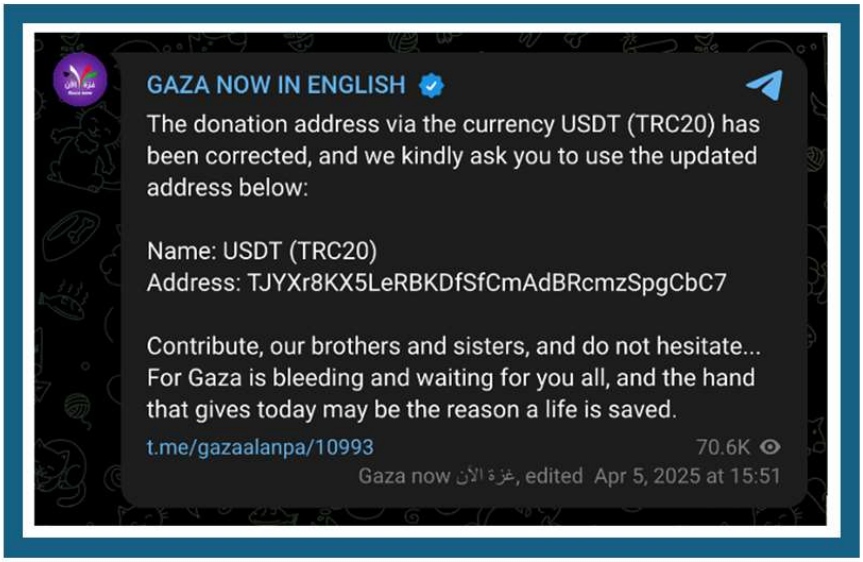


Figure 10: Gaza Now Crowdfunding Through Tether in April 2025

As described earlier, by 2023, terrorist organizations were openly soliciting donations in USDT, while authorities in the United States and elsewhere were warning about (and sanctioning) Tether-based money laundering. The Subcommittee scraped posts from Telegram channels of Palestinian militant groups, and found wallets openly fundraising for sanctioned entities or violence were not frozen. For example, Gaza Now, sanctioned by OFAC in March 2024 for supporting Hamas, continued to fundraise openly through Tether after being sanctioned, posting wallet addresses publicly on Telegram in 2025 that received contributions and were not frozen (Figure 10).

This is also clear with the wallets leaked by Babak Zanjani, who is widely notorious for money laundering and being sanctioned by the United States. Mr. Zanjani is not a secretive figure: he maintains a prolific public presence, with half a million followers on Twitter/X and Instagram, where he posted the CBI's wallets. These leaked wallets had observable prior ties to Iranian money launderers and exchanges, as described previously. Even though the most famous Iranian money launderer posted these wallet addresses on Twitter in December 2025, based on the Subcommittee's review of blockchain records, Tether has not yet blacklisted them as of September

[58] *Perceptions of Digital Currencies*, NAT'L BUREAU FOR COUNTER TERROR FIN. OF ISRAEL, https://web.archive.org/web/20220830112612/https:/nbctf.mod.gov.il/he/PropertyPerceptions/Pages/Blockchain.aspx (last visited Sep. 11, 2026).

2026. Additionally, as covered previously, the Subcommittee uncovered significant transfers of funds from the Modex Exchange Company to both the CBI and, through an intermediary wallet, the IRGC. In total, the three Modex-associated wallets took in $575 million in USDT over the course of three months (April to June 2025). Yet, Tether did not blacklist those wallets either.

CONCLUSION

The Subcommittee's investigation has found that Tether's USDT became a primary cryptocurrency for Iran, Hamas, Hizballah, and the Houthis beginning in 2023 and has expanded in scale since. This rise coincides with apparent failures and delays by Tether to freeze wallets associated with money laundering, including counter-terrorism orders, public fundraising for terrorist organizations, and leaks from within the Iranian regime. The broader set of intermediaries seen with the Modex Exchange Company and the Derakhshan /Alivand network demonstrates that these networks can move billions of dollars in transactions on an annual basis. The Subcommittee's analysis, backed by recent seizures and media reporting, shows that Iran remains undeterred in its continued use of Tether. The prevalence of USDT in Iran's shadow banking system and the company's unhurried approach to blacklisting sanctioned wallets raises grave questions about the adequacy of the company's oversight and anti-money laundering measures.

Like anyone seeking to move illicit funds, Iranian shadow banking networks and other illicit actors naturally gravitate to stablecoin issuers and exchanges that are slow to blacklist, freeze, or trace funds. It is notable that the Subcommittee's investigation found that USDT was the only stablecoin significantly present in the sample evaluated. Conversely, there are ample cryptocurrencies like Bitcoin and Ethereum (or decentralized finance tools) that do not have built-in, centralized capabilities for freezing wallets or provide greater privacy assurances. Those cryptocurrencies should be especially appealing to Iran if it was concerned about the actual threat of asset seizures, and countries like North Korea have shown themselves more adept in their use. While Iran has discussed, and potentially used, Bitcoin to collect toll fees for the Strait of Hormuz, the wallet designated in connection to Iran's shadow fleet of oil tankers had received millions in USDT during the current war.[59] The fact that Iran and its allies or business partners continue to use USDT and have not fully migrated back to Bitcoin would suggest that Tether has failed to deter or chill its money laundering operations through the stablecoin firm's current, seemingly limited and reactive approach.

The Subcommittee is particularly concerned about Tether's apparently inconsistent response, and failure to be proactive, to specific allegations and public evidence of terrorist financing using USDT. As noted, terrorist organizations have successfully moved tens of millions of dollars of USDT when Tether failed to freeze accounts after designations. The Subcommittee also found examples of millions of dollars leaving targeted wallets in the days or hours before the wallet was

[59] Press Release, U.S. Dep't of the Treasury, Off. of Foreign Assets Control, Treasury Launches Unprecedented Campaign Against Iranian Regime on Economic D-Day (Aug. 24, 2026), https://home.treasury.gov/news/press-releases/sb0613.

blacklisted or identified in sanctions. Unlike traditional banking, the instantaneous nature of cryptocurrencies means that once funds leave a wallet, they cannot be clawed back, and illicit actors have ample tools to conceal their movement. Solely relying on the reactive freezing of wallets after designations will not work.

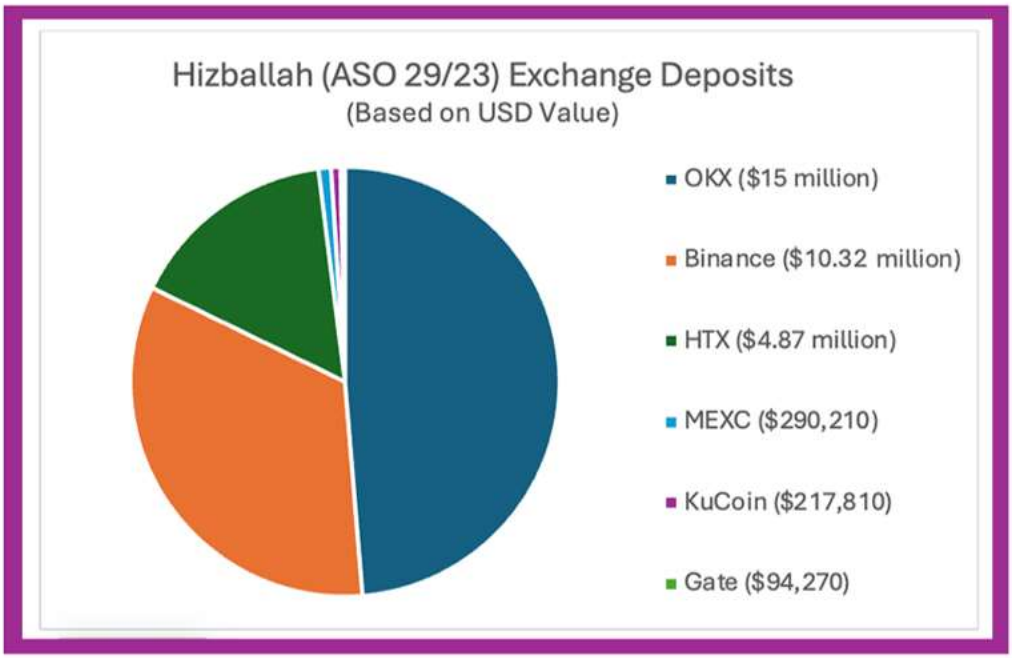


Figure 11: Exchange Usage for Hizballah Wallets under ASO 29/23, showing Tether partners being used to move funds into and out of the network.[60]

These concerns are heightened given that Tether has a direct client relationship with entities like Binance, Gate, OKX, and HTX,[61] which media reports and government orders have demonstrated are regularly used for illicit finance. As with the examples of Iranian money launderers (Figure 5) and Hizballah (Figure 11), those same Tether exchange partners continue to play a significant role in Iranian shadow banking. These findings raise questions about what due diligence Tether and its partners perform regarding the ownership of client accounts, what information was sought from clients and exchange customers after clear breaches of U.S. law, and what notice was proactively provided to law enforcement about such suspicious activities.

Congress must take seriously the pattern and gravity of cryptocurrency's role in Iranian shadow banking as it regulates the adoption of digital assets. The Subcommittee's findings heighten concerns that cryptocurrencies can supercharge illicit finance in ways that fundamentally undermine American national security and public safety. Furthermore, federal enforcement

[60] Subcommittee staff generated this figure using data extracted from sanctioned wallets and complemented with data generated in Arkham Intelligence.

[61] *UK Sanctions List: Huobi Global S.A.*, GOV.UK (May 26, 2026), https://search-uk-sanctions-list.service.gov.uk/designations/RUS3619/Entity.

agencies must be vigilant in holding Tether, and any other similarly situated issuer, accountable for any negligence or malfeasance. Stablecoin issuers with a significant nexus to the United States, particularly those that offer dollar-denominated stablecoins, should be subject to American sanctions law rather than being allowed to hide behind foreign jurisdictions. Issuers should proactively monitor their partners and their partners' clients for high-risk activities, such as transactions with terrorists and sanctioned entities. Exchanges with a pattern of repeat compliance failures and disregard for American law, like exchanges in the Middle East, Russia, and China, should be subject to heightened scrutiny by stablecoin issuers and American regulators. Federal law enforcement, such as the Department of Justice, the U.S. Securities and Exchange Commission, and OFAC must hold stablecoin issuers accountable for repeated failures to prevent illicit finance and sanctions violations.

ATTACHMENT I: SANCTIONED WALLETS USED IN PSI ANALYSIS

Government	ID	Affiliation	Sanction Date	Currencies
U.S. (OFAC)	SDN 38419	Ahmad Khatibi Aghada	Sep 2022	BTC (3)
U.S. (OFAC)	SDN 38420	Amir Hossein Nikaeen Ravari	Sep 2022	BTC (4)
U.S. (OFAC)	SDN 45678	Buy Cash Money and Money Transfer Company	Oct 2023	BTC (1)
U.S. (OFAC)	SDN 48302	Tawfiq Muhammad Sa'id Al-Law	Mar 2024	USDT (1)
U.S. (OFAC)	SDN 47635	Gaza Now	Mar 2024	USDT (6), ETH (3), BTC (1)
U.S. (OFAC)	SDN 32171	Sa'id Ahmad Muhammad Al-Jamal	Dec 2024	USDT (5)
U.S. (OFAC)	SDN 47664	Ansarallah	Apr 2025	USDT (8)
U.S. (OFAC)	SDN 55484	Alireza Derakhshan	Sep 2025	USDT (2)
U.S. (OFAC)	SDN 55502	Arash Estaki Alivand	Sep 2025	USDT (5)
U.S. (OFAC)	SDN 56865	Zedcex Exchange Ltd	Jan 2026	USDT (7)
U.S. (OFAC)	SDN 4632	Central Bank of Iran	Apr & Jul 2026	USDT (6)
U.S. (OFAC)	SDN 58199	Zaid Issam Ahmed Al-Jebouri	Jul 2026	USDT (7)
U.S. (OFAC)	SDN 58258	Crypto Home DMCC	Aug 2026	USDT (2), BNB (1), BTC (1)
U.S. (OFAC)	SDN 58287	SHPS Shelbit	Aug 2026	USDT (3), BTC (2), SOL (1)
U.S. (OFAC)	SDN 58284	Siavash Kayvanpour	Aug 2026	BTC (2), USDT (2)
U.S. (OFAC)	SDN 58409	Almpertos Tsoris	Aug 2026	USDT (1)
U.S. (OFAC)	SDN 57065	Arman Kahzadian	Aug 2026	ETH (2), BTC (1)
U.S. (OFAC)	SDN 24003	Behzad Mesri	Aug 2026	ETH (11), USDT (7), USDT (bsc) (2), BTC (1), USDC (1), WETH (1)
U.S. (OFAC)	SDN 57061	Keyvan Fayyaz Gareh Blagh	Aug 2026	ETH (4), USDT (4), BTC (3), USDT (bsc) (3), SHIB (2)
U.S. (OFAC)	SDN 57064	Mojtaba Ghal'eh-Kuhi	Aug 2026	BTC (1), ETH (1), USDT (bsc) (1)

Israel (NBCTF)	ASO 44/21	Hamas	Jul 2021	BTC (36), USDT (18), DOGE (7), LTC (4), LSK (3), SC (3), ETH (2), ADA (1), ALGO (1), BNB (1), DGB (1), IOST (1), KMD (1), STRAT (1), TRX (1), XLM (1), XRP (1), XVG (1), ZEC (1)
Israel (NBCTF)	ASO 15/22	Hamas	Mar 2022	USDT (43), TRON* (4), TRX (1)
Israel (NBCTF)	ASO 19/23	Hamas	Apr 2023	USDT (4), EVM* (1), TRON* (1)
Israel (NBCTF)	ASO 29/23	Hizballah	Jun 2023	USDT (39)
Israel (NBCTF)	ASO 34/23	Palestinian Islamic Jihad	Jul 2023	USDT (25), TRX (1)
Israel (NBCTF)	ASO 53/23		Oct 2023	USDT (17)
Israel (NBCTF)	ASO 60/23	Hizballah	Dec 2023	USDT (bsc) (1)
Israel (NBCTF)	ASO 5/24		Mar 2024	USDT (42)
Israel (NBCTF)	ASO 2/24	Hamas	Apr 2024	ETH (2), USDT (2)
Israel (NBCTF)	ASO 26/24		Dec 2024	BTC (16), USDT (1)
Israel (NBCTF)	ASO 34/24		Dec 2024	USDT (5)
Israel (NBCTF)	ASO 1/25	Hamas	Feb 2025	USDT (58)
Israel (NBCTF)	ASO 33/24	Hamas	Mar 2025	USDT (5)
Israel (NBCTF)	ASO 16/25	Hamas	Apr 2025	USDT (3)
Israel (NBCTF)	ASO 20/25	Hamas	Jun 2025	USDT (4)
Israel (NBCTF)	ASO 22/25	IRGC	Jun 2025	ETH (2), USDT (bsc) (2), USDT (1)
Israel (NBCTF)	ASO 41/25	Hamas	Aug 2025	USDT (2)
Israel (NBCTF)	ASO 43/25	IRGC	Sep 2025	USDT (187), TRX (3)
Israel (NBCTF)	ASO 19/25	Hamas	Sep 2025	USDT (95), TRX (1)

Israel (NBCTF)	ASO 49/25	Hamas	Oct 2025	USDT (10)
Israel (NBCTF)	ASO 50/25	Hamas	Oct 2025	USDT (1)
Israel (NBCTF)	ASO 51/25	Hamas	Nov 2025	USDT (9)
Israel (NBCTF)	ASO 53/25	Hamas	Nov 2025	USDT (21)
Israel (NBCTF)	ASO 1/26	Hamas	Feb 2026	USDT (14)
Israel (NBCTF)	ASO 2/26	Hamas	Feb 2026	USDT (8)
Israel (NBCTF)	ASO 6/26	Hamas	Mar 2026	USDT (3)
Israel (NBCTF)	ASO 13/26	Hamas	Apr 2026	USDT (5)
Israel (NBCTF)	ASO 7/26	Hamas	Apr 2026	USDT (8)
Israel (NBCTF)	ASO 8/26	Hamas	Apr 2026	USDT (6)
Israel (NBCTF)	ASO 18/26	Hizballah; IRGC	Jul 2026	USDT (37)