Project craaft

Collaboration, Research & Analysis Against the Financing of Terrorism

NATO OTAN

This publication is supported by: The NATO Science for Peace and Security Programme

Assessing Terrorist Use of Virtual Asset Intermediaries

Allison Owen

Research Briefing No. 2

About Project CRAAFT

Project CRAAFT is a research and community-building initiative aimed at strengthening global counter-terrorist financing (CTF) efforts. The initiative began with CRAAFT I and continues with CRAAFT II – Collaborative Responses to the Role of New Technologies in Terrorist Financing – launched in 2025. This new phase focuses on how emerging technologies impact terrorist financing and is led by the Centre for Finance and Security (CFS) at RUSI, in partnership with RUSI Europe and the Regional Institute for Security Studies (RISS) in Tbilisi. The project is supported by the NATO Science for Peace and Security (SPS) Programme. Learn more at <projectcraaft.eu>

Data Provider Statement

The Royal United Services Institute partnered with Crystal Intelligence to receive blockchain analytic data.

Crystal Intelligence

Published in 2025 by the Royal United Services Institute for Defence and Security Studies.

Acknowledgements

The author would like to thank Nicholas Smart and the Research and Investigation Team at Crystal Intelligence for providing data from internal investigations and analysis for this research brief.

Setting Parameters

Terrorist groups' experimentation with virtual assets highlights the need to understand integrated intermediary services for converting such funds to fiat currency. Although virtual assets are not replacing conventional methods, evidence shows that some groups are attempting to integrate virtual assets into existing financial operations for receiving and moving funds.[1]

It is important to temper concerns about terrorist groups' use of virtual assets by considering the larger context. Grey literature suggests that terrorist groups prefer using traditional financial assets to using virtual assets. The United Nations Security Council, for example, emphasises that transactions for Islamic State and its affiliates predominately link to cash couriers and informal value transfer systems (hawala). Nonetheless, there is an increased use of virtual assets by terrorist groups.[2] As such, traditional methods for moving funds continue to be used, but virtual asset integration may simplify – and in some cases obfuscate – operations.

Reluctance by terrorist groups to shift fully to receiving and moving funds via virtual assets is probably due to factors including price volatility, with some virtual asset types and the risk of confiscation due to transaction transparency for most major tokens. According to the US National Risk Assessment, another reason may be a lack of virtual asset-to-fiat currency conversion options in jurisdictions where terrorist groups operate.[3]

This research brief examines intermediary services that convert virtual assets to fiat currency in cases related to three groups: Hamas, Hezbollah and ISIS.[4] This research brief is based, in part, on data provided by blockchain analytics company Crystal Intelligence, which was gathered through its internal investigations.

To further analyse these intermediary service providers, the author conducted interviews with representatives of the public and private sector familiar with the intersection of virtual assets and terrorism financing. In addition, the research brief considers grey literature, including multilateral and government documents, private sector reports and academic research.

This brief does not provide historical background on such groups. Instead, its aim is to provide context to the operational movement of funds, with an emphasis on intermediary services, enabling authorities to identify key areas for data collection during investigations. By understanding the movement of virtual assets and fiat currency in these operations, law enforcement can further disrupt terrorist activities.

Conversion Services

Intermediary services that convert virtual assets to fiat currency and vice versa may, whether wittingly or unwittingly, facilitate transfers for illicit actors. This can stem from a variety of factors; for instance, the intermediary may not implement anti-financial crime checks or may not be required to do so by authorities in the jurisdiction where they operate. This section focuses on terrorism finance links to small-scale conversion services and over-the-counter (OTC) brokers using virtual assets.

Case Study: Hamas

One example of a terrorist organisation using intermediary services arose from an investigation into Hamas. A Crystal Intelligence investigation identified the 'Shadow Unit', a cyber group under the umbrella of Hamas' Cyber Unit. According to Crystal's analysis, the Shadow Unit has requested donations on a Telegram channel to financially support the military efforts of Al Qassem Brigades, Hamas'

1. US Department of the Treasury, 'Action Plan to Address Illicit Financing Risks of Digital Assets', 16 September 2022, <https://home.treasury.gov/system/files/136/Digital-Asset-Action-Plan.pdf>, accessed 9 April; FinCEN, 'FinCEN Alert to Financial Institutions to Counter Financing to Hamas and its Terrorist Activities', 20 October 2023, <https://www.fincen.gov/sites/default/files/2023-10/FinCEN_Alert_Terrorist_Financing_FINAL508.pdf>, accessed 14 April 2025.
2. United Nations Security Council, 'Eighteenth Report of the Secretary-General on the Threat Posed by ISIL (Da'esh) to International Peace and Security and the Range of United Nations Efforts in Support of Member States in Countering the Threat', S/2024/117, 31 January 2024, <https://documents.un.org/doc/undoc/gen/n24/017/61/pdf/n2401761.pdf>, accessed 19 March 2025.
3. US Treasury, '2024 National Terrorist Financing Risk Assessment', p. 23, February 2024, <https://home.treasury.gov/system/files/136/2024-National-Terrorist-Financing-Risk-Assessment.pdf>, accessed 11 April 2025.
4. According to a 2024 article by Jessica Davis: 'Not all Islamic State theaters have adopted cryptocurrency use'. See Jessica Davis, 'The Financial Future of the Islamic State', *CTC Sentinel* (vol. 17, no. 7, July/August 2024), <https://ctc.westpoint.edu/the-financial-future-of-the-islamic-state/>, accessed 28 May 2025.

military arm. Two Telegram posts requested donations in virtual assets – the first including specific wallet addresses for donations and the second instructing users to email for more information. The second post, according to the blockchain analytics company, stated 'To fulfil the duty of support and assistance to your jihadi brothers, communicate through our private email to support Al Qassem Brigades'.

Figure. 1: Screenshot of Second Post in Telegram Channel

Source: Image manually collected from Telegram

After anonymously inquiring about the procedure, the investigative team received a response with the following information.

> 'If you have no experience dealing with digital currencies, you can ask for help from a trusted friend inside or outside your country or visit a money transfer office or exchange service in your country that offers digital currency transactions. You should only show the wallet details from this message for the transfer to be completed. Do not disclose your identity to the entity handling the transfer on your behalf to ensure your security.'

The email displays a TRON virtual asset address soliciting donation in a USDT token on the TRON network.[5] USDT on the TRON network is a version of the stablecoin that runs on the TRON blockchain, known for faster transactions and lower fees. Further, stablecoins are tokens pegged to an asset, often fiat currency or a physical commodity such as gold, and they have lower price volatility risks that are often associated with other types of virtual assets.

Another aspect of the investigation conducted into the Shadow Unit involves attempts to disrupt investigations by authorities into donations sent via virtual assets. For example, the virtual asset address listed in the email received by Crystal Intelligence is allegedly changed periodically for security and is valid for one transfer only. As such, the Shadow Unit states that it is necessary for the user to contact it through the same email address for any new transfer. A March 2025 US Department of Justice document highlights a similar procedure of reaching out to the same email address, and noted that, during its investigation into a different virtual asset address, its email responses listed 'received 34 deposits on or about February 11, 2025 and February 21, 2025, totalling 25,211 USDT'.[6] Furthermore, the document noted that while tracing funds tied to the Al Qassem Brigades, they found an unattributed virtual asset address that had 'patterns of transactional behaviour consistent' with OTC cash-to-crypto (and vice versa) businesses.[7]

5. USDT is a stablecoin issued by Tether. Tether has assisted law enforcement in a number of terrorist finance seizures of USDT. For a recent example, see Chainalysis, 'United States DOJ and FBI Seize Cryptocurrency in Major Disruption of Hamas Terrorist Financing Scheme', 28 March 2025, <https://www.chainalysis.com/blog/doj-fbi-seize-cryptocurrency-disrupt-hamas-terrorist-financing-scheme-march-2025/>, accessed 28 May 2025.
6. US Department of Justice, 'Application for a Warrant to Seize Property Subject to Forfeiture', 25 March 2025, p. 23, <https://www.justice.gov/usao-dc/media/1394711/dl?inline>, accessed 28 May 2025.
7. US Department of Justice, 'Application for a Warrant to Seize Property Subject to Forfeiture', p. 30.

The use of service providers that appear to be either OTC brokers or small money businesses to facilitate the movement of funds for terrorism finance is a typology identified as early as 2023.[8] When analysing these intermediaries, blockchain analytics company Chainalysis emphasised that even if funds are traced to such a service provider, it may have facilitated that activity unknowingly.[9] This point highlights the need to ensure that compliance checks are implemented by these services.

Case study: Lebanon

OTC brokers and small-scale services can support customers with the conversion of virtual assets to other asset types or fiat currency. It should be noted that not all OTC brokers and small-scale services are tied to high-risk activity. These businesses can offer customers access to virtual assets as an alternative means of safeguarding personal wealth, as well as provide liquidity for startup virtual asset service providers.

This subsection analyses two appearances of OTC brokers in terrorism financing cases to provide context of operations. Authorities should use this information to understand where to collect further data when investigating cases. Research for this subsection, based on information from two Israeli seizure orders, provides further details on two services in Lebanon that may be affiliated with terrorist finance activity.

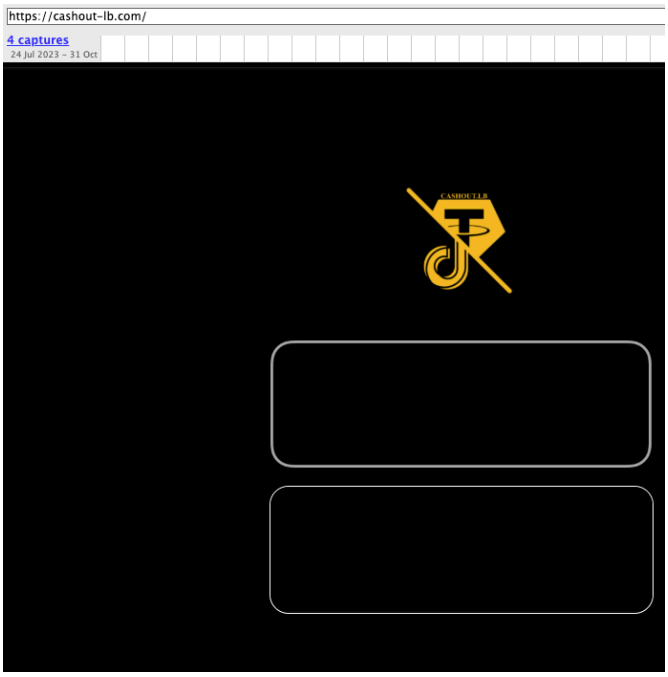
Before analysing these cases, it is important to understand how virtual assets are treated in Lebanon. The country limits the presence of virtual asset activity and requires financial institutions to report activity when customer transactions indicate ties to virtual assets.[10] Despite initial estimates of virtual asset use being relatively low in the area, Lebanon has seen increased adoption of virtual assets as citizens seek alternative means to safeguard personal wealth due to economic instability.[11] Meanwhile, the country is increasingly moving towards a dollarised, cash-based economy.[12] The need for financial stability, coupled with a cash-based economy, may account for the increased presence of OTC cash-to-crypto (and vice versa) brokers or similar small conversion businesses in the country, which operate out of kiosks around major cities.

The presence in the country of such services that do not implement proper compliance checks has resulted in two cases of exploitation, identified through analysis of two Israeli seizure orders.

A 2023 Israeli seizure warrant listed a virtual asset wallet held by the owner of exchange service 'Cashout', with the seizure warrant providing a Lebanese-based address. Although full details are not available, the warrant notes that the law enforcement action is intended to thwart Hezbollah activity.[13] The listed website on the seizure order, cashout-lb.com, is no longer live, but an archived version of the site (Figure 2) shows that the service offered applications on popular marketplaces. The logo on the archived website, which appears to be unique based on a Google Image search to determine similar designs, matches the logo of an application listed on a popular online store (see Figure 3).

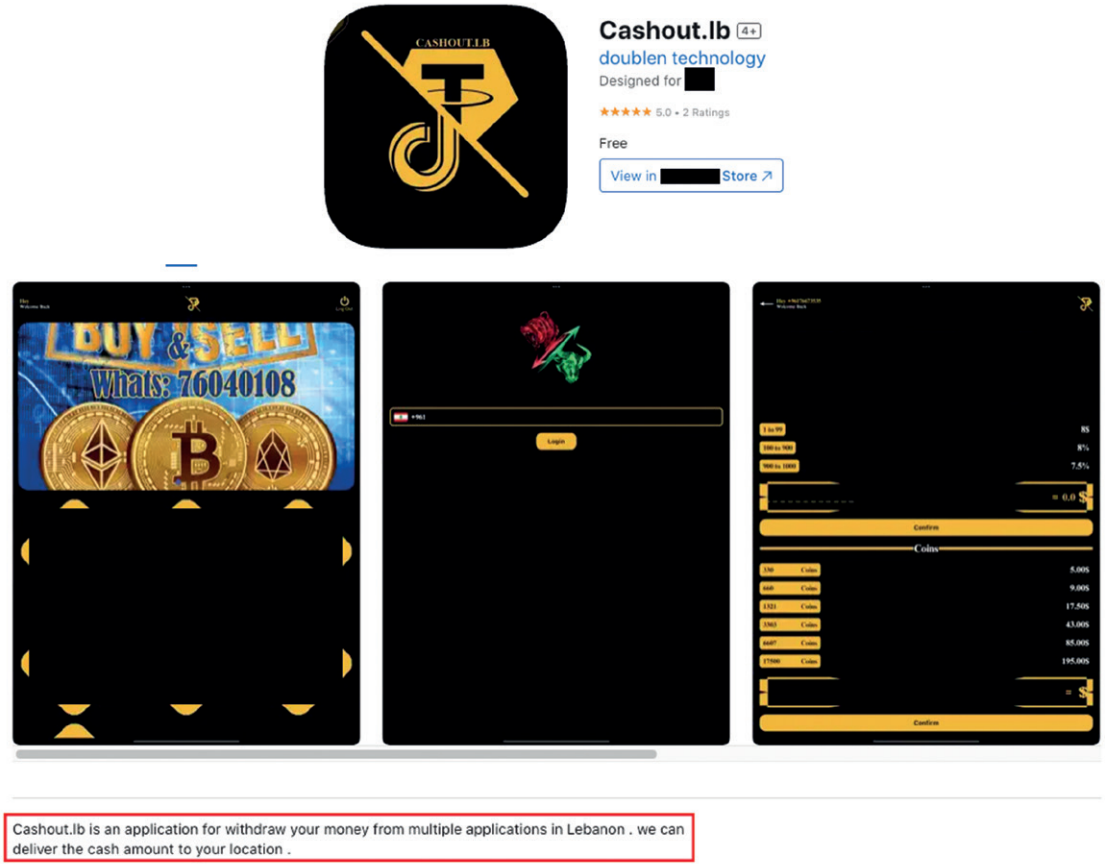
8. Chainalysis, 'Correcting the Record: Inaccurate Methodologies for Estimating Cryptocurrency's Role in Terrorism Financing', 18 October 2023, <https://www.chainalysis.com/blog/cryptocurrency-terrorism-financing-accuracy-check/>, accessed 27 May 2025.
9. *Ibid*.
10. Author interview with CTF expert D, online, 5 May 2025.
11. Author interview with CTF expert D, online, 5 May 2025.
12. *Ibid*; The World Bank, 'Lebanon: Poverty and Equity Assessment 2024: Weathering a Protracted Crisis', p. 10, <https://documents1.worldbank.org/curated/en/099052224104516741/pdf/P176651-325da1d8-f439-48a7-ab6b-ae97816dd20c.pdf>, accessed 8 May 2025.
13. Israeli Ministry of Defense, 'Administrative Seizure Order (ASO – 60/23)', 21 December 2023, <https://nbctf.mod.gov.il/he/PropertyPerceptions/Documents/%d7%a6%d7%aa%2060-23.pdf>, accessed 11 April 2025.

Figure 2: Archived website of Cashout-lb.com



Source: Wayback Machine (<https://web.archive.org/web/20230724022936/https:/cashout-lb.com/>), archived 24 July 2023.

Figure 3: Screenshot of Application on a Popular Online Store



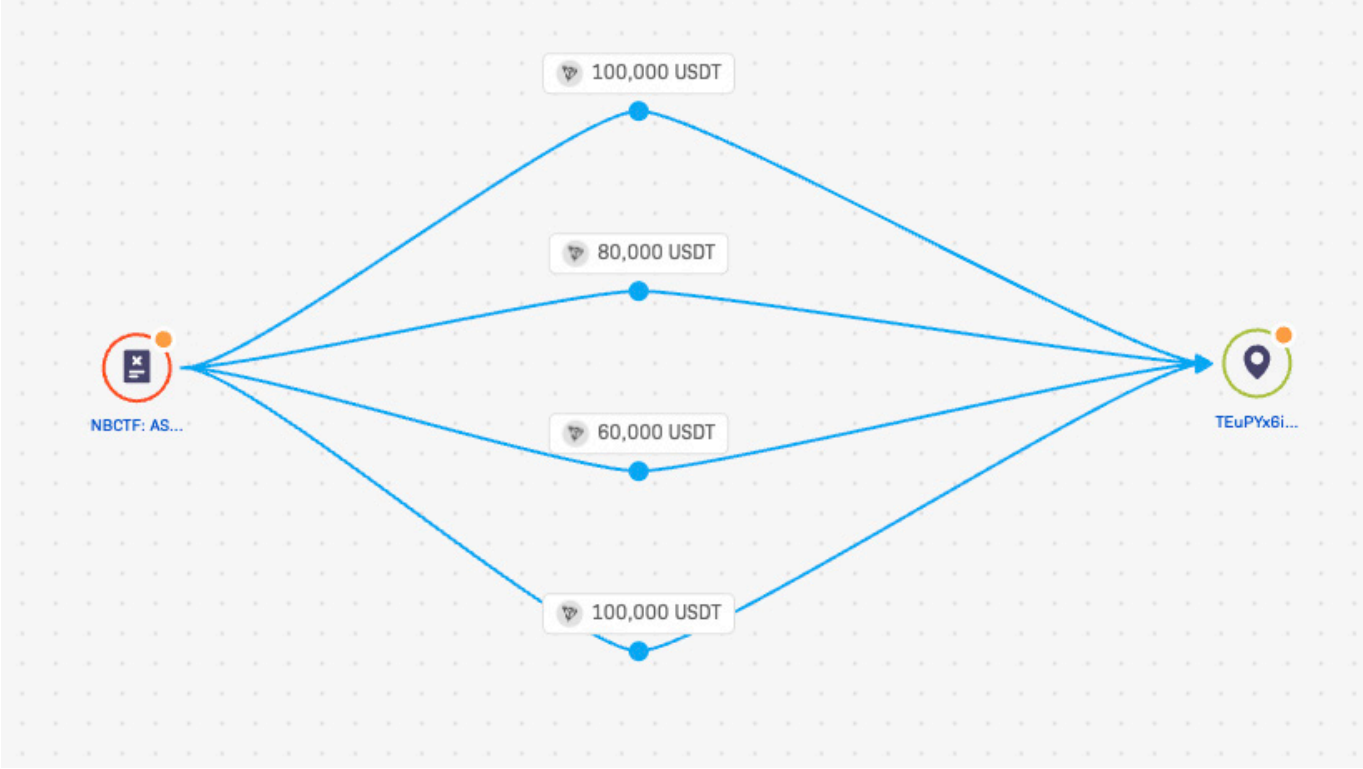
Source: Application Store.

The overview states: 'Cashout.lb is an application [to] withdraw your money from multiple applications in Lebanon. We can deliver the cash amount to your location' (see Figure 3).

Access to liquidity needs to be considered in this case – particularly, the service provider's capability to convert virtual assets to fiat currency, as well as gain access to cash for customers. Smaller virtual asset-to-fiat conversion services may hold personal or business accounts at high-volume exchanges. With accounts at high-volume exchanges, the smaller service can operate on behalf of their customers. The process of smaller services operating through high-volume exchanges is common practice, but the larger exchange needs to ensure that smaller conversion services are compliant during both client onboarding and ongoing monitoring.[14]

Another case that reflects the use of such conversion services stems from a different 2023 Israeli seizure order, which details cryptocurrency wallets identified as the property of 'a designated terrorist organization or property used for the perpetration of a severe terror crime'.[15] One of the addresses listed in the seizure order can be traced to 'Virtual Asset Address 1' (see Figure 4), which reflected transaction patterns that indicate a small service provider: according to Tronscan.org, this address had received 3,026 incoming transactions from a mix of virtual asset addresses and made 668 outgoing transactions, primarily to a high-volume exchange.[16]

Figure 4: Screenshot of Trace from Israeli Seizure to OTC Address



Source: Crystal Intelligence

14. Noémi També and Allison Owen, 'Institutional Virtual Asset Service Providers and Virtual Assets Risk Assessment Guide', p. 17, RUSI, 7 August 2023, <https://www.rusi.org/explore-our-research/publications/special-resources/institutional-virtual-asset-service-providers-and-virtual-assets-risk-assessment-guide>, accessed 23 April 2025.
15. Israeli Ministry of Defense, 'Administrative Seizure Order (ASO- 53/23)', 22 October 2023, <https://nbctf.mod.gov.il/he/Announcements/Documents/%d7%a6%d7%95%20%d7%aa%d7%a4%d7%99%d7%a1%d7%94%20%d7%9e%d7%99%d7%a0%d7%94%d7%9c%d7%99%2053-23.pdf>, accessed 11 April 2025.
16. Tronscan, <https://tronscan.org/>, accessed 3 July 2025. Tronscan is a blockchain explorer that allows users to track transactions on the TRON blockchain. Notably, the transaction volume should not be considered as a threshold for all activity. The transaction flows are only listed to depict an indication of a small-volume business.

This virtual asset address is displayed as a QR code on a desk in a photo of a small conversion service in Lebanon (see Figure 5), suggesting that it offered virtual asset conversion services to the individual or entity linked to the address listed in the seizure order. Notably, the social media account tied to the service was suspended.

These case studies underscore the need for authorities to assess the scope of small-scale services and OTC brokers operating in their jurisdiction and ensure that appropriate regulation is in place for requiring compliance checks. Second, authorities responsible for investigating financial crime should consider training on how to identify such businesses. By understanding indicators, investigators can ensure that they do not accidentally trace through such businesses, which can result in following a false trail.

Authorities can also consider business practices for gaining access to liquidity within the jurisdiction. Crystal Intelligence analysed 32 OTC brokers based in Lebanon. By monitoring addresses attributed to the brokers, they identified the total value of virtual assets in US dollars sent to virtual asset exchanges. This data is shown in Table 1. As noted before, not all OTC brokers are tied to high-risk activity. Instead of flagging all activity by OTC brokers as high-risk, authorities should require such services to implement anti-financial crime checks. Nevertheless, assessing the OTC broker industry in the country as a whole can provide context to the movement of funds so authorities investigating activity can have a more thorough understanding of the cross-over from virtual assets to fiat currency.

Figure 5: Screenshot of Image Listed for a Small Conversion Service in Lebanon

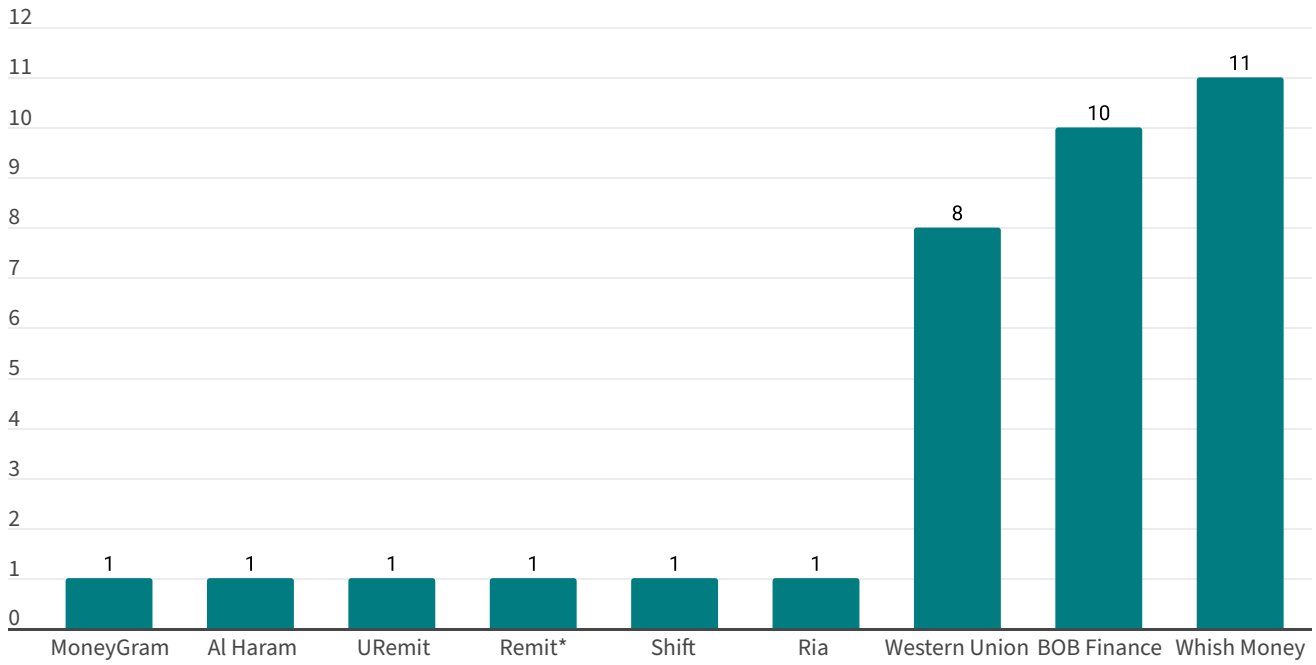
Source: Google Maps.

Table 1: Incoming Funds from Addresses Attributed to OTC Brokers in Lebanon to Exchanges*

Year	Incoming Funds from OTCs to Accounts at Exchanges
2021	$2,445,304.49
2022	$6,072,984.82
2023	$5,776,754.77
2024	$12,883,441.42
2025	$1,283,192.84

Source: Crystal Intelligence
*The value of the virtual assets in US Dollars was calculated by Crystal Intelligence on 20 April 2025.

Figure 6: Data on Money Transfer Services Used by Lebanese P2P and OTC Services, June 2024



Source: Crystal Intelligence.
*Remit refers to international remittance as a catch-all term.

The conversion service gaining access to fiat currency when operating with virtual assets, however, is another feat to overcome. Crystal Intelligence data notes that customers may use established third-party money transfer services to transfer funds to accounts potentially owned by the OTC broker, and in return receive virtual assets to their allocated wallet. As such, authorities should consider the connection between the use of money transfer services and OTC brokers when investigating terrorist finance cases. The money transfer services used by OTC and peer-to-peer (P2P) services in Lebanon are shown in Figure 6.

A private sector representative suggested that if larger transaction volumes of fiat currency were received and sent by OTC services, the transaction would likely require a bank transfer and, therefore, undergo more comprehensive compliance checks.[17] Further, institutions in Lebanon that deal with electric money transfers must adhere to anti-money laundering and counter terrorism financing obligations.[18]

With larger transaction amounts sent to OTC broker services, authorities need to assess if a broader network is involved in providing the necessary liquidity through access to fiat currency either via financial institutions or physical cash.

Diversification of Funds

One private sector representative identified that within the virtual asset industry, facilitators operating wittingly or unwittingly with terrorist groups tend to diversify their income streams.[19] For example, it may appear that an individual linked to the movement of terrorist funds may also be involved in other fraudulent virtual asset-associated activity, such as 'pump and dump' schemes.[20] When looking at service providers that received funds tied to terrorist financing activity, blockchain analytic company Chainalysis reported in 2023 that '8 out of 20 suspected service providers that [were] counterparties to [a] known terror-affiliated wallet [had] also transacted with Garantex', a service provider that had online infrastructure taken down by US, German and Finnish authorities in March 2025.[21]

This highlights the importance of compliance officers at virtual asset service providers investigating alerts and comprehensively analysing cases which may not initially appear to be tied to urgent matters, to identify links to higher risk activities. For example, a case may initially appear to be connected with only one type of illicit activity, but further investigation may reveal ties to terrorist activity, requiring urgent action.

This challenge is not unique to the virtual asset industry. According to a private sector anti-money laundering expert, traditional financial institutions commonly report terrorist finance cases as money laundering unless there is strong evidence of a connection to a sanctioned terrorist group.[22] The challenge with detection of terrorist activity by the private sector in the traditional finance space is that transactions are in small denominations and the source of funds can be clean – that is, not tied to illicit activity.[23] In the virtual asset industry, however, the level of transparency linked to the underlying technology for most assets, combined with thorough investigations by blockchain analytics companies, improves the likelihood of detecting terrorism financing exposure.

Areas to Monitor

A slight change in financial flow operations for terrorist groups may occur as more virtual asset-to-fiat currency conversion options materialise in jurisdictions commonly exploited by terrorist groups. This threat will be amplified if those jurisdictions do not monitor and restrict illicit activity conducted by intermediaries offering cashout services. As noted by an interviewee, regulating the industry can provide more data on activity occurring in the country, whereas prohibiting it pushes it underground.[24] Other avenues for the movement of funds also need to be considered by authorities monitoring financial flows tied to terrorist groups.

Crystal Intelligence data shows the movement of assets attributed to the Islamic State transferred through a Syria-based peer-to-peer service that is nested in a high-liquidity exchange. Its investigations note that the service claims to be domiciled in Turkey and operates under a Luxembourg-based phone number, but operations of the company

17. Author interview with private sector expert G, online, 23 April 2025.
18. Banque du Liban, '٢/١١/٢٠١٥ تاريخ ٤٤ قانون رقم' ['Law No. 44 of 24 November of 2015 Combating Money Laundering and Terrorist Financing'], <https://www.bdl.gov.lb/CB%20Com/Laws%20And%20Regulations/Laws/Law_44_AR.pdf>, accessed 20 May 2025.
19. Author interview with private sector expert G, online, 23 April 2025.
20. A 'pump and dump' scheme involves a user artificially inflating an asset's price through false claims to attract investment from other customers. After customers invest their money, the initial user sells their funds, resulting in the late investors losing funds.
21. Chainalysis, 'Correcting the Record'; US Department of Justice, 'Garantex Cryptocurrency Exchange Disrupted in International Operation', 7 March 2025, <https://www.justice.gov/opa/pr/garantex-cryptocurrency-exchange-disrupted-international-operation>, accessed 27 May 2025.
22. Author interview with CTF expert B, online, 2 May 2025.
23. Author interview with CTF expert D, online, 5 May 2025.
24. Author interview with CTF expert D, online, 5 May 2025.

extend beyond these jurisdictions. To access fiat currency, in a similar manner to the previously mentioned OTC brokers, the company leverages third-party money transfer services. One development that could alter the landscape of fund movements is that the platform announced plans to integrate Mastercard payments in the future, emphasising the need for authorities to identify integrated financial institutions. Further investigations continue.

Finally, reports of virtual asset integration into hawala date to as early as 2022.[25] A counterterrorism financing expert emphasised this point, stating that hawala, which is deeply rooted in the country, often involved the use of stablecoins for reconciliation.[26] As with all informal value transfer systems, such fragmentation can make an investigation by authorities more complex.[27] Notably, this trend is not specific to Lebanon. According to a report by Jessica Davis, hawaladars in Afghanistan were 'relatively quick to adopt cryptocurrency as a service'.[28] This integration should be further monitored and data collected due to the risk of this procedure being abused by terrorist groups. For example, Islamic State, according to a 2022 US Treasury report, received donations for refugee camps via virtual assets, which are subsequently converted into cash via hawaladars.[29] In addition, a 2023 ICSR report highlights how Hamas moves virtual assets using either official exchanges or informal exchanges that 'are essentially hawalas or money services businesses that also have cryptocurrency capabilities'.[30] Authorities should consider identifying the scale of this activity in their jurisdiction and associated risks.

Conclusion

Terrorist groups continue to rely on traditional financial networks, but there is still a degree of interest in the use of virtual assets to simplify operations. This research brief provides examples of how small-scale services are used to facilitate the movement of funds tied to terrorism finance. While traditional methods of terrorist financing still dominate, the integration of virtual assets into terrorist financing activity – and related investigations – can provide insight into financial flows conducted by terrorist groups. Understanding the convergence of traditional financial flows with modern technology – and gathering appropriate data – is essential to detecting and disrupting the evolution of terrorist activities.

About the Author

Allison Owen is an Associate Fellow at RUSI's Centre for Finance and Security and an independent financial crime consultant, published author, researcher and trainer.

25. Jessica Davis, 'Cryptocurrency Meets Hawala', Insight Monitor, 10 February 2022, <https://newsletter.insightthreatintel.com/p/cryptocurrency-meets-hawala>, accessed 20 May 2025. Hawalas 'arrange for transfer and receipt of funds or equivalent value and settle through trade, cash, and net settlement over a long period of time'. For more information, please see FATF, 'Role of Hawala and Other Similar Service Providers in Money Laundering and Terrorist Financing', October 2013, <https://www.fatf-gafi.org/en/publications/Methodsandtrends/Role-hawalas-in-ml-tf.html>, accessed 26 June 2025.
26. Author interview with CTF expert D, online, 5 May 2025.
27. *Ibid.*
28. Jessica Davis, 'The Financial Future of the Islamic State'. Hawaladars are 'money transmitters that provide hawala services'. For more information, please see FATF, 'The Role of Hawala and Other Similar Service Providers in Money Laundering and Terrorist Financing'.
29. US Department of Treasury, 'Action Plan to Address Illicit Financing Risks of Digital Assets', p. 4. For more information on this topic, please see Jessica Davis, 'The Financial Future of the Islamic State'.
30. Marc-André Argentino, Jessica Davis and Tore Refslund Hamming, 'Financing Violent Extremism: An Examination of Maligned Creativity in the Use of Financial Technologies', ICSR, 12 April 2023, p. 16, <https://icsr.info/wp-content/uploads/2023/04/ICSR-Report_Financing-Violent-Extremism-An-Examination-of-Maligned-Creativity-in-the-Use-of-Financial-Technologies.pdf >, accessed 4 June 2025.