Written Testimony of Jonathan Levin
Co-Founder and Chief Strategy Officer
Chainalysis Inc.

Before the
House Homeland Security Committee
Subcommittee on Intelligence & Counterterrorism

Hearing on
Terrorism and Cryptocurrency: Industry Perspectives

June 9, 2022

Chairwoman Slotkin, Ranking Member Pfluger, and distinguished members of the Committee. Thank you for inviting me to testify before you today on this important topic. I appreciate that this Committee is looking into the nexus between cryptocurrency and terrorist financing. While terrorist financing comprises an extremely small fraction of the total activity we see in the cryptocurrency ecosystem, it is vital that it be addressed and that government agencies have the training and tools they need to investigate these incidents.

My name is Jonathan Levin and I co-founded Chainalysis Inc. with Michael Gronager, CEO of Chainalysis. I currently serve as Chief Strategy Officer. I began studying cryptocurrencies ten years ago through my research as an economist. I was interested in the way that the Internet could create brand new markets and impact developing economies. While the Internet brought citizens of the world closer together in terms of global connectivity, it did not give people the economic opportunities that were promised.

The cryptocurrency industry provides a new way to conduct global commerce, providing economic opportunities for people across the world. As with any new technology, cryptocurrency can be used by both good and bad actors. As such, preventing cryptocurrency from being abused for terrorist financing and other national security risks is intricately linked in our continued ability to project prosperity around the world. Helping this industry stay on top of the emerging threats of terrorist financing while ensuring the vibrant economic output that will be built on these new rails is the task at hand.

Cryptocurrency and blockchain technology are some of the best available tools in the toolkit that the United States has to compete with potential national security threats, like ransomware attacks and North Korean hackers. The entrepreneurial dynamism that cryptocurrencies present allows for innovators and builders to create universal access to financial products and re-engineer web2 business models to serve individuals and their data in a way that protects privacy and helps our communities. This technology is consistent with our American values and has the potential to be strategically more important in great power competition over the next few decades. Of course, we understand concerns about risk and abuse and that is why we are here today. At Chainalysis we share concerns about the illicit use of cryptocurrency, but we know that the inherent open nature of this

technology can be leveraged to mitigate the risks associated with it and bring bad actors to justice.

If there is one point I want to make to the members of this Committee, it is that the transparency of cryptocurrency blockchains enhances the ability of policymakers and government agencies to detect, disrupt and, ultimately, deter illicit activity. By mapping a single illicit actor to a cryptocurrency wallet address, for example from a transaction made in a terrorist financing campaign, law enforcement unlocks immediate insight into the network of wallet addresses and services (e.g., exchanges, mixers, etc.) that facilitate the illicit actor. In contrast, in a traditional finance investigation, a similar tip, linking an illicit actor to a bank account, is just the beginning of a long, extensive process to request and subpoena records that are manually reviewed and reconciled to generate a comparable amount of insight. Even with this insight, it comes with a significant time delay that creates opportunities for illicit actors to evade justice vs. the real-time monitoring capabilities of blockchain intelligence.

In my testimony, I provide background on Chainalysis, outline how blockchain analysis can be leveraged in investigations, explain how terrorists have used cryptocurrency in their fundraising efforts, and provide several case studies demonstrating how government agencies are rooting out terrorist financing using cryptocurrency. I also provide recommendations for improving the government's response to this threat.

Background on Chainalysis

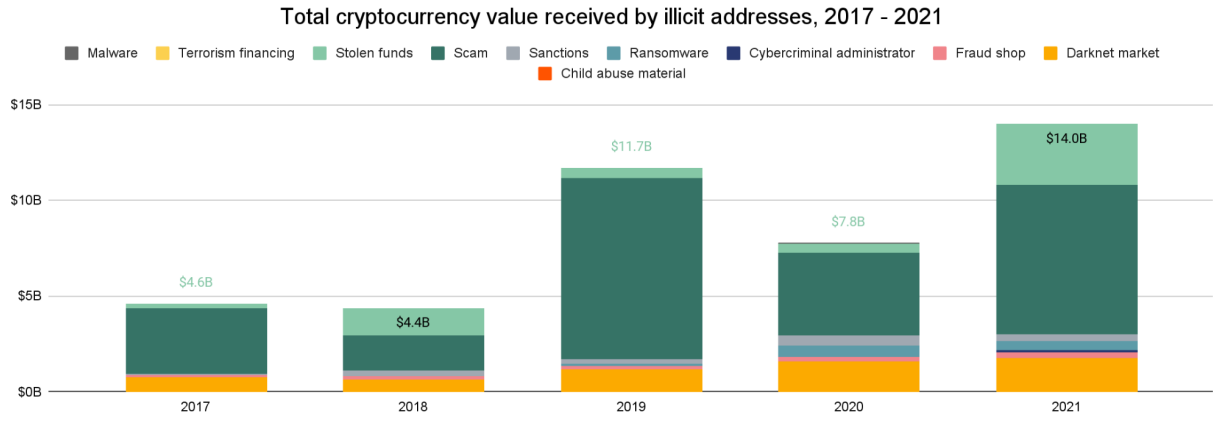
Chainalysis is the blockchain data platform. We provide data, software, services, and research to government agencies, exchanges, financial institutions, and insurance and cybersecurity companies. Chainalysis currently has over 750 customers in 70 countries. Our data platform powers investigations, compliance, and risk-management tools that have been used to solve many of the world's most high-profile cyber-crime cases and grow consumer access to cryptocurrency safely. We have worked closely with law enforcement and regulators as they have worked to disrupt and deter illicit uses of cryptocurrency.

Chainalysis's partnerships with law enforcement and regulators are consistent with our corporate mission: to build trust in blockchains. Fundamentally, we believe in the potential of open, decentralized blockchain networks to drive new efficiencies, reduce barriers for innovators to create new financial and commercial products, encourage innovation, enhance financial inclusion, and unlock competitive forces across financial services and other markets. Our goal is to contribute our data, tools and expertise to drive illicit finance and other risks out of the cryptocurrency ecosystem, enabling the realization of the technology's potential.

Chainalysis's data powers both investigative and compliance tools. Our investigative tool, Reactor, enables government agencies and investigative teams to trace the illicit uses of cryptocurrency, including money laundering, theft, scams, and other criminal activities. Our compliance tool, KYT (Know Your Transaction), provides cryptocurrency businesses and

financial institutions the ability to screen their clients transactions and ensure that they are not attempting to interact with illicit entities. This transaction monitoring tool provides ongoing insights for cryptocurrency businesses so that they can protect their businesses and clients and ensure regulatory compliance.

Chainalysis also leverages our data to conduct research into the cryptocurrency ecosystem, including the illicit use of cryptocurrency. We publish a number of reports, including our annual Crypto Crime Report. Based on this research, we reported in our 2022 Crypto Crime Report that cryptocurrency-based crime hit a new all-time high in 2021, with illicit addresses receiving $14 billion over the course of the year, up from $7.8 billion in 2020. Top categories include scams, stolen funds, darknet markets, and – pertinent to this hearing – ransomware.



Despite this large increase in illicit transaction volume, illicit activity as a percentage of total volume has actually fallen dramatically since 2019. In 2019, the illicit share was about 3%, in 2020 it was just over 0.5%, and in 2021 it was 0.15%. The reason for this is that cryptocurrency usage is growing faster than ever before, so while cryptocurrency-related crime is definitely increasing, the legitimate use of cryptocurrency is far outpacing its use by illicit actors. This is good news for the cryptocurrency ecosystem, but government and industry must still put in place and implement the appropriate controls to mitigate risks in the system.

Terrorist financing through cryptocurrency remains extremely low; however, we have identified terrorist organizations that have attempted to finance their operations with cryptocurrency. For example, in 2019 and 2020, al-Qaeda raised cryptocurrency through Telegram channels and Facebook groups. Thanks to the Federal Bureau of Investigation, Homeland Security Investigations, and Internal Revenue Service-Criminal Investigation, more than $1 million was seized from a money service business (MSB) operator who facilitated some of these transactions. Additionally, in early spring of 2021, the 'Izz al-Din al-Qassam Brigades, Hamas' military wing, collected more than $100,000 in donations in cryptocurrency. In July 2021, the Israeli Government seized much of these funds from associated MSBs. According to our own analysis, Hamas raised at least $160,000 across

three campaigns from 2019-2021 and from October 2021 through March 2022, an ISIS-related campaign (the Forgotten Ones) raised $36,000, but terrorists appear to have pivoted away from public-facing cryptocurrency donation campaigns.

How Blockchain Analysis Can Be Leveraged in Investigations

It is a common misconception that cryptocurrency is completely anonymous and untraceable. In fact, the transparency provided by many cryptocurrencies' public ledgers is much greater than that of other traditional forms of value transfer. Cryptocurrencies like Bitcoin operate on public, immutable ledgers known as blockchains. Anyone with an Internet connection can look up the entire history of transactions on these blockchains. The ledger shows a string of numbers and letters that transact with another string of numbers and letters. Chainalysis maps these numbers and letters – cryptocurrency addresses – to their real-world services. For example, in Chainalysis products, we are able to see that a given transaction was between a customer at a specific exchange, with a customer at another exchange, between a customer at an exchange and a sanctioned entity, or any other illicit or legitimate service using cryptocurrency. Our data set and investigative tools are invaluable in empowering government and private sector investigators to trace cryptocurrency transactions, identify patterns, and, crucially, see where cryptocurrency users are exchanging cryptocurrency for fiat currency.

Using blockchain analysis tools, law enforcement can trace cryptocurrency addresses to identify the origination and/or cash-out points at cryptocurrency exchanges. Law enforcement can serve subpoenas to these cryptocurrency exchanges, which are required to register as MSBs here in the United States and collect Know Your Customer (KYC) information from their customers. In response to a subpoena, the exchange will provide law enforcement with any identifying information that it has related to the cryptocurrency transaction(s) in question, such as name, address, and government identification documentation, allowing the authorities to further their investigation.

Background on Terrorist Financing and Cryptocurrency

As noted above, terrorist financing represents a small fraction of the 0.15% of the entire crypto market occupied by illicit activity. Terrorist organizations use an array of methods to raise, store, and transfer funds on the blockchain. Although terrorist organizations' use of encrypted communications and cyber platforms limits visibility into their financing activity, the transparent nature of cryptocurrency and blockchain analytics provides an invaluable forensic tool that empowers governments to identify, trace, and disrupt the flow of funds. In addition, the blockchain's public, unclassified nature plays a critical role in fostering robust international collaboration among governments, given terrorist organizations' transnational networks and ability to inspire lone actors worldwide.

Financing Method/Platform	Description
Compliant exchanges	While these platforms are sometimes used by terrorists in their financing campaigns, because they have robust anti-money laundering/countering the financing of terrorism (AML/CFT) policies and procedures in place, law enforcement can serve legal process to these exchanges and receive information about the account holder and their transactions, which can help authorities build a more complete picture of on-chain terrorist financial facilitation networks and disrupt these financial flows.
High-risk exchanges	Terrorists also use high-risk exchanges, which do not collect KYC information and are frequently located in jurisdictions with strategic AML/CFT deficiencies. These platforms tend to ignore law enforcement requests.
Social Media	Terrorist organizations have leveraged social media platforms not only to disseminate propaganda, but also to raise funds on the blockchain. For example, in 2019 and 2020, al-Qaeda raised digital assets through Telegram channels and Facebook groups. The increasing use of encrypted communications platforms across a range of threat actors, including terrorist organizations, complicates the efforts of counterterrorism practitioners in identifying terrorist financing trends and preferences.

Terrorists have used cryptocurrency for a variety of purposes, such as to purchase military equipment and procure computer infrastructure. For example, in 2016, the pro-ISIS, Gaza-based Ibn Taymiyya Media Center (ITMC) hosted the *Jahezona* ("Equip Us") cryptocurrency donation campaign - the first of its kind - and posted a graphic on Telegram depicting the type of weaponry different dollar-equivalent donation amounts could purchase. The Jahezona campaign, which the ITMC also advertised on YouTube and Twitter, ran from 2016 to 2018 and raised thousands of dollars worth of cryptocurrency. Although this may not seem like a large sum over a two-year period, we must keep in mind that terrorist attacks are not expensive to carry out, especially when the attackers are acting alone.

Graphic published by the ITMC during its Jahezona campaign with QR code and dollar-equivalents for different weapons

In 2020, the Department of Justice (DOJ) seized bitcoin addresses of an al-Qaeda money laundering network. In this campaign, organizations purporting to act as charities were actually soliciting donations that would equip Syria-based terrorists with weapons. Blockchain analytics revealed a likely administrator for the network who paid for encrypted cloud storage from a provider who accepts Bitcoin. This demonstrates that terrorist groups see utility in cryptocurrency to fund their procurement of secure technology platforms, well beyond the scope of funding attacks.

In addition to Sunni terrorist networks in conflict zones, such as Gaza and Syria, Iran stands out for its embrace of cryptocurrency. Many key sectors of Iran's economy remain under U.S. and international sanctions, and a body of press reporting has pointed to Iran's creation of parallel trade and financial systems to help it evade these sanctions. Several generals in the Islamic Revolutionary Guard Corps (IRGC) — which plays an outsize role in Iran's politics and economy and is designated as a Foreign Terrorist Organization — have publicly endorsed the use of cryptocurrency, including the launch of a central bank digital currency, to circumvent sanctions. Iran has encouraged cryptocurrency mining projects to establish operations in the country, which subsidizes electricity and other power utilities. Iran has granted over 1,000 licenses to mining operations, and nearly 17% of funds moving to local Iranian cryptocurrency services come from mining entities, compared to 5% in the Middle East overall. While we haven't identified any of these links to date, we continue to monitor for any on-chain indicators that the IRGC's expeditionary force, the Qods Force, is using the blockchain to further destabilize international security by funding its regional proxies, such as the militias in Iraq, Hizballah in Lebanon, and the Huthis in Yemen.

Press reporting has emphasized the potential for cryptocurrency adoption to continue rising in Afghanistan given the country's political isolation, economic volatility, instability at Afghanistan's central bank, and a run on banks following the Taliban takeover in August 2021. In 2021, Afghanistan ranked 20th in global crypto adoption, according to the Chainalysis Global Crypto Adoption Index. Afghanistan ranks this high because we weight the metrics that feed the index by countries' purchasing power and Internet using population, where Afghanistan ranks among the lowest. Some Afghans have turned to crypto as a safe place to store value amid economic uncertainty and the challenges of broad

adoption in the country and the country has a nascent cryptocurrency economy driven by modest P2P exchange trading. It remains to be seen how their cryptocurrency economy will develop under the Taliban, but this is something we will continue to monitor. In addition to the Taliban takeover, the local affiliate of the Islamic State in Iraq and ash-Sham, ISIS-Khorasan, remains active in Afghanistan, raising the risk that it and affiliated networks could abuse cryptocurrency services in this strategically situated, high-risk jurisdiction.

As the nature of the terrorist threat itself continues to evolve, we are also monitoring the use of cryptocurrency by racially and ethnically-motivated violent extremists (REMVE) in the United States and worldwide. According to the Intelligence Community's 2022 Annual Threat Assessment, "individuals and small cells inspired by a variety of ideologies and personal motivations—including Sunni violent extremism, racially or ethnically motivated violent extremism, and violent militia extremism—probably present the greatest terrorist threat to the United States." Therefore, governments and industry alike should continue to rigorously and uniformly apply AML/CFT frameworks across all potential violent extremist funding mechanisms.

Al-Qaeda, ISIS, and Hamas Among Terrorist Groups Fundraising in Cryptocurrency—With Government Seizures Close Behind

I will outline several case studies from 2021—one in June, one in July, and another in December. I would like to clarify that these case studies represent outlier examples - these are the largest terrorist financing cases involving cryptocurrency that we know of and are therefore likely not representative of the overall trends. However, what these cases do show are governments' recent successes in the fight against cryptocurrency-financed terrorism, underscoring the importance of properly training, tooling, and resourcing the government agencies charged with combatting this threat.

Case 1: Israeli Government Seizes Cryptocurrency Addresses Associated with Hamas Donation Campaigns

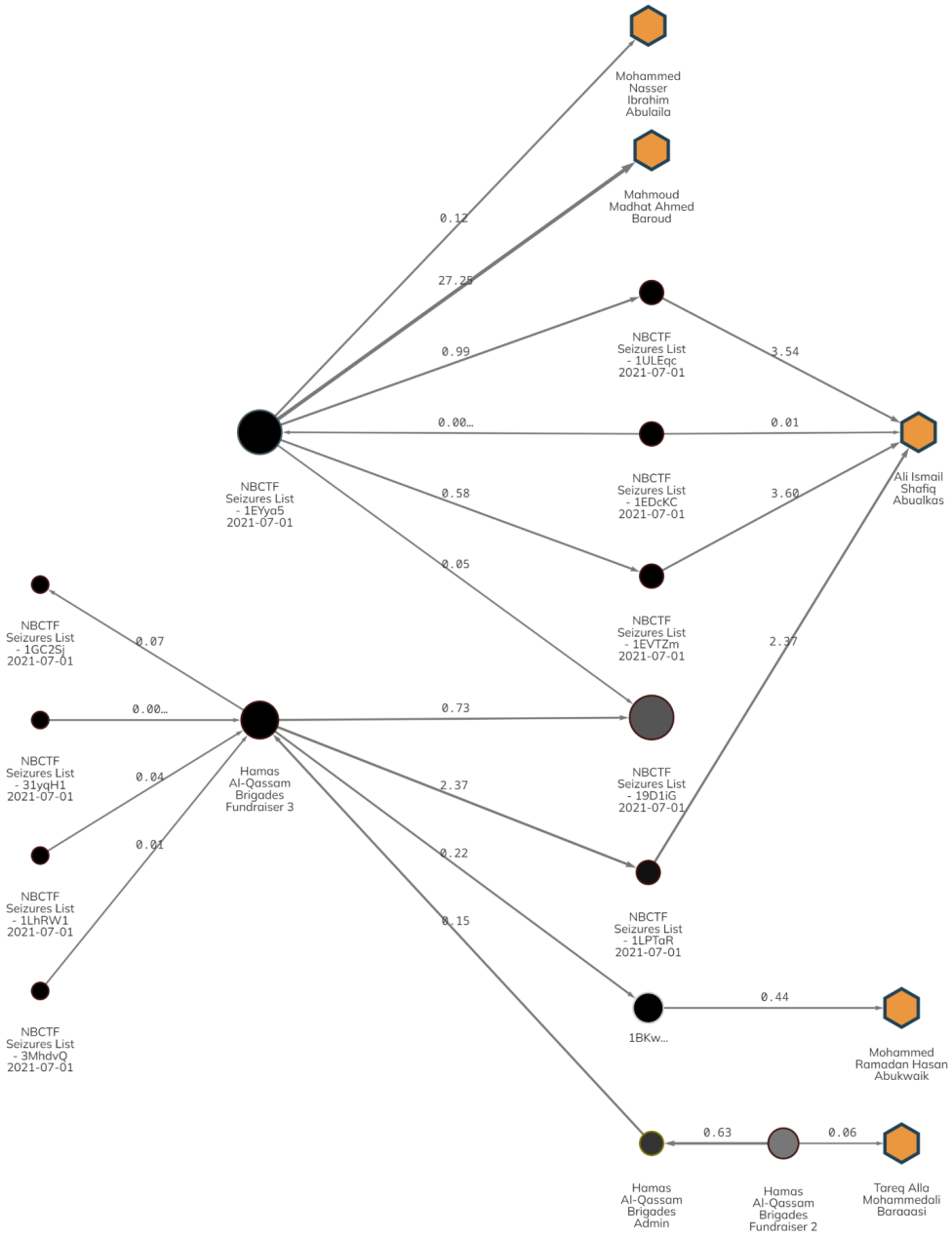
On June 30, 2021, Israel's National Bureau for Counter Terror Financing (NBCTF) announced the seizure of cryptocurrency held by several wallets associated with donation campaigns carried out by Hamas. The action came after a sizable growth in cryptocurrency donations to al-Qassam Brigades in May following increased fighting between the group and Israeli forces.

Notably, this is the first terrorism financing-related cryptocurrency seizure to include such a wide variety of cryptocurrencies. Israeli authorities seized not only Bitcoin, but also Ether, Tether, Ripple, and more. The seizure was made possible through an investigation of open-source intelligence (OSINT) and blockchain data, as well as cooperation from the compliance team at a global cryptocurrency exchange.

Below, we examine how the second of these—the analysis of blockchain data—contributed to the case.

How funds moved from donation addresses to exchanges

The Chainalysis Reactor graph below shows the Bitcoin portion of the transactions carried out by many of the addresses listed in the NBCTF seizure announcement. Many of these addresses have been attributed to individuals connected to the donation campaigns.



The orange hexagons represent deposit addresses hosted at large, mainstream cryptocurrency exchanges that are controlled by individuals named in the NBCTF announcement. As we can see, the funds often passed through intermediary wallets, high-risk cryptocurrency exchanges, and MSBs before reaching the exchanges from which the named individuals likely hoped to cash out into fiat currency.

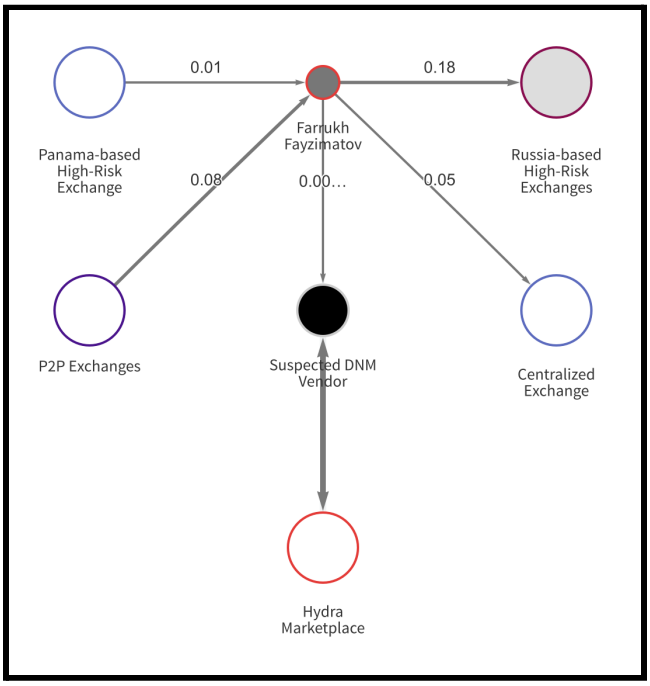
Interestingly, we can see that two donation addresses named in the announcement received funds from addresses associated with the Idlib, Syria office of BitcoinTransfer (top right of the graph), a Syrian cryptocurrency exchange connected to previous terrorism financing cases. Another exchange received funds from a Middle East-based MSB that had previously received funds from the ITMC (directly beneath the BitcoinTransfer cluster), an organization that has also been associated with terrorism financing in the past.

This investigation is a perfect example of the value of blockchain analysis, especially when used in conjunction with other open-source data. Israeli authorities analyzed and leveraged OSINT to find Hamas' donation addresses and, with blockchain analysis tools, were able to follow the funds to find consolidation addresses and uncover the names of individuals associated with the campaigns. Up-to-date transaction data across several blockchains was crucial in this case as agents tracked and seized funds denominated in several different cryptocurrencies. We applaud the Israeli authorities for a successful operation and look forward to providing valuable tools that facilitate more such successes for government customers around the world.

Case 2: Terrorist Financier designated by the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC)

On July 28, 2021, the US Department of the Treasury's Office of Foreign Assets Control (OFAC) sanctioned Syria-based Tajikistani national Farrukh Furkatovitch Fayzimatov for materially assisting and supporting Hay'at Tahrir al-Sham (HTS), a Sunni militant group involved in the Syrian Civil War. Fayzimatov utilized social media to post propaganda, recruit new members, and solicit donations to purchase equipment for the benefit of HTS.

His fundraising efforts have been linked to an address tracked by Chainalysis, the details of which are depicted in the graph below.



On the left side of the graph, we find that Fayzimatov received funds directly from centralized and peer-to-peer (P2P) exchanges that did not collect know-your-customer information. This indicates that the individuals sending bitcoin to Fayzimatov intended to keep their activity anonymous. On the right, we observe that Fayzimatov sent funds to Russia-based high-risk exchanges, a centralized exchange that did collect KYC information, and a suspected vendor at Hydra Marketplace (a Russian-language darknet market that was designated by OFAC on April 5, 2022). Following the OFAC designation, Fayzimatov's on-chain activity ceased.

Case 3: Wales-based convicted terrorist caught using darknet market 'Bypass Shop'

In December 2021, a 29-year-old man was sentenced to 16 months in jail for Bitcoin transactions made on the Bypass Shop, a darknet market for stolen credit card information.

The transactions were made from the man's wallet at an exchange, which prompted the company to issue a suspicious activity report. From there, the U.K. police identified the man as British citizen Khuram Iqbal of Cardiff, Wales, and arranged for his arrest.

This was not Iqbal's first run-in with the law. Iqbal had previously spent time in jail in 2014 for possessing terrorist information and disseminating terrorist publications under the pseudonym *Abu Irhaab*, Arabic for "father of terrorism." In total, Iqbal possessed nine copies of al-Qaeda's English-language *Inspire* magazine, and had published more than 800 links to extremist material on Facebook.

Before his arrest, Iqbal had twice attempted to join the jihadi cause by flying to Kenya and Turkey in 2011 and 2012, respectively. He was deported on both occasions.

Recommendations

Ensure adequate funding, resources, and training for government agencies charged with investigating the illicit use of cryptocurrency, including terrorist financing.

As terrorist organizations adopt blockchain technologies and cryptocurrency fundraising techniques, governments must keep up with adversaries' latest techniques, tactics, and procedures. Governments that have already embraced blockchain analysis have seized millions of dollars in cryptocurrency and stopped a number of terrorist financiers—further evidence that with the proper tools, investigators can cut off terrorist organizations the funds they need to survive, operate, procure weapons, and carry out attacks. Many government agencies have limited or inconsistent personnel dedicated to investigating the illicit use of cryptocurrency because of a lack of training resources and a lack of funding for new personnel, tools, and training. Allocating appropriate financial and personnel resources to these efforts would ensure that investigators can trace illicit transactions, seize funds, and help bring criminals to justice when criminals exploit cryptocurrency.

Improve coordination and collaboration within and between governments.

The illicit use of cryptocurrency, including for terrorist financing, is a global issue and investigations often cross borders. We must improve information sharing and coordination between US government agencies and their counterparts in other countries. It is important that countries work together and with private industry to enable cross-border investigations of ransomware threats. Establishing and improving upon coordination and collaboration mechanisms between countries can help to streamline investigations and enable law enforcement to bring bad actors to justice.

Provide assistance to countries to support their implementation of robust AML/CFT laws for cryptocurrency businesses.

The US should work with other countries to support their efforts to implement comprehensive Anti-Money Laundering/Countering the Financing of Terrorism (AML/CFT) laws for cryptocurrency businesses to limit illicit actors opportunities for jurisdictional arbitrage. By requiring cryptocurrency exchanges, cryptocurrency kiosks, peer-to-peer exchangers, over-the-counter (OTC) trading "desks", and other cryptocurrency businesses to implement robust AML/CFT laws, including Know Your Customer (KYC) laws, illicit actors will have fewer cashout opportunities to convert their ill-gotten cryptocurrency into fiat currency.

The US government should provide assistance through the US Department of State and other mechanisms to other countries to assist in the development and implementation of these laws, as well as capacity building to enforce them. This will help to limit the regulatory arbitrage opportunities available to bad actors and make it even more difficult for terrorists

to fund themselves with cryptocurrency at scale because they will more frequently encounter regulated, compliant exchanges that implement AML/CFT standards and work with law enforcement. Although cryptocurrency can be abused by terrorist organizations and other threat actors, it is also a powerful tool with the potential to provide meaningful economic opportunity in conflict zones or jurisdictions with weak institutions. The US government should encourage private and public initiatives that leverage blockchain technology to minimize sanctions exposure and greatly improve the traceability of funds in difficult or high-risk jurisdictions.

Encourage OFAC to include cryptocurrency-related information in SDN List designations.

Through blockchain analysis, we have seen the effectiveness of cutting off the flow of funds to illicit wallets when OFAC has included cryptocurrency-related information in SDN List designations. OFAC should continue to include as much relevant cryptocurrency information in their designations as possible, and update designations when they receive pertinent information after the fact. This will help law enforcement and the intelligence community, as well as our global partners in combatting terrorist financing. This will also help to combat evasion of US and international sanctions and will also help to cut threat actors off from unregulated cashout venues. Finally, it will help to erode the pseudonymity of threat actors on the blockchain and map out connections to other high-risk and illicit services.

Conclusion

While terrorist financing comprises an extremely small fraction of the total activity we see in the cryptocurrency ecosystem, terrorist attacks can be carried out with small amounts of funding. It is imperative that government agencies be equipped to address this constantly changing threat. Cryptocurrency's transparency allows for not only the disruption of terrorist financing campaigns, but also the identification, arrest, and prosecution of terrorist financers. By providing the resources necessary to understand this threat, law enforcement and the US government as a whole will be better equipped to mitigate risks and investigate and disrupt terrorist financing when it does occur using cryptocurrency.