Testimony of Jonathan Levin

Chief Strategy Officer & Cofounder, Chainalysis

House Financial Services Committee

Digital Assets, Financial Technology and Inclusion Subcommittee

Crypto Crime in Context: Breaking Down the Illicit Activity in Digital Assets

November 15, 2023

Chairman Hill, Ranking Member Lynch, and members of the subcommittee:
My name is Jonathan Levin, one of the co-founders of Chainalysis, the leading blockchain analysis company. I am grateful for the opportunity to testify to this committee, on this topic, at this important time as the current issue at hand is particularly close to my heart.

The tragic events beginning on October 7, 2023 have shined a light on our core focus at Chainalysis: detecting and disrupting bad actors that use cryptocurrencies for terrorism financing and other illicit activity. We have spent almost a decade working with law enforcement and intelligence agencies in the US, Israel, and allied countries around the world to maximize disruption of these networks. After many joint successes, this has marked the dawn of a new era of financial intelligence for governments around the world.

On-Chain Detection of Illicit Activity

Financial intelligence has historically been composed of government collections and reporting from financial institutions. This is typically not real-time and highly dependent on domestic institutions to report on suspicious activity. Insight into finances of foreign governments is often mired in complex international collaboration and information sharing. Cryptocurrencies mark a departure from this where all governments can have access to every transaction that has occurred and sharing of information allows for full networks to be uncovered.

Chainalysis

Cryptocurrency transactions are inherently public and the data from those transactions is preserved on a transparent, immutable ledger. At Chainalysis, we analyze the transaction data from blockchain networks in conjunction with open source intelligence information and proprietary data to map the ecosystem of participants in these networks. We then provide software solutions and investigative support to allow investigators to trace the flow of transactions and identify potential illicit activity.

The process of identifying illicit activity on the blockchain involves two key components. The first is quantifying the funds directly in the hands of an illicit actor such as a terrorist organization, and the second is identifying the service providers that facilitate the movement of funds tied to that activity. When we look at known instances of terrorism financing, service providers such as money services businesses are often involved. One such service is the recently sanctioned "Buy Cash", a Gaza-based business that provides money transfer and virtual currency exchanges services. Some may do this in a way which is similar to an over-the-counter broker, while others may be more similar to street-level businesses like hawalas. Identifying whether these entities are service providers, or in fact controlling the terrorism-affiliated wallet is key, as is determining which portion of the funds passing through the service provider relate to terrorism financing.

Further details as to how these determinations are made, and the role of blockchain analytics, crypto exchanges and law enforcement, can be found in our recent blog post on this topic.[1]

Disruption of Terrorist Financing Activities Using Cryptocurrencies

To that end, I wanted to offer some additional context on the use of cryptocurrencies to finance Hamas and similar groups, and how that activity gets disrupted when law enforcement can draw on Chainalysis and work with the industry. There is evidence of terrorist organizations operating in Gaza attempting to raise funds using cryptocurrency

[1] Chainalysis, "Correcting the Record: Inaccurate Methodologies for Estimating Cryptocurrency's Role in Terrorism Financing," (Oct. 18, 2023), https://www.chainalysis.com/blog/cryptocurrency-terrorism-financing-accuracy-check/.

as early as 2016.[2] These involve both those directly involved in terrorist organizations as well as networks of enablers and facilitators who leverage otherwise legitimate businesses, such as hawala services and OTC brokers, to move funds for those organizations. Historically, this broader network of enablers has been particularly difficult to detect and disrupt.

However, many of these donation campaigns have been disrupted, due largely to the government's new ability to detect this type of terror financing and the supporting networks. For example, in August 2020, the DOJ announced that, with the aid of Chainalysis, it had dismantled terrorism financing campaigns by the military wing of Hamas, and by ISIS, and seized millions of dollars worth of funds.[3] Similarly, in the past two years, the Israeli government, again with support from Chainalysis, has undertaken multiple successful seizures of cryptocurrency funds intended for groups supporting Hamas, including Hezbollah and Iran's Quds Force.[4] In practice, this has meant working in collaboration with the private sector to freeze both the accounts at crypto exchanges and any other wallet addresses associated with terrorism financing. In each instance, international collaboration, as well as a trusted public-private partnership has been essential.

In April 2023, Hamas publicly announced that it was shutting down its campaign to accept cryptocurrency donations, citing successful government efforts to identify and prosecute donors.[5] Despite their own acknowledgement of the transparency and,

---

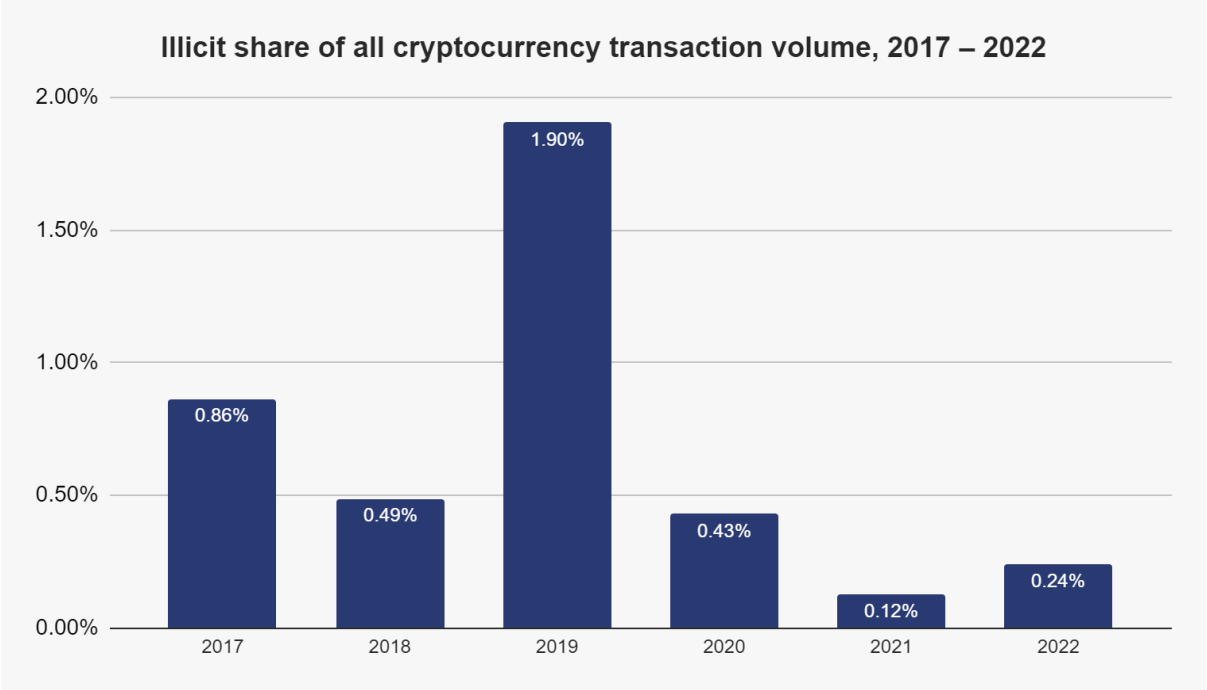
[2] Chainalysis, "Terrorism Financing in Early Stages with Cryptocurrency But Advancing Quickly," (Jan. 17, 2020), https://www.chainalysis.com/blog/terrorism-financing-cryptocurrency-2019/.
[3] Chainalysis, "Chainalysis in Action: Department of Justice Announces Takedown of Two Terrorism Financing Campaigns with Help from Blockchain Analysis," (Aug. 13, 2020), https://www.chainalysis.com/blog/cryptocurrency-terrorism-financing-al-qaeda-al-qassam-brigades-bitcointransfer/.
[4] Chainalysis, "Israeli Government Seizes Cryptocurrency Addresses Associated with Hamas Donation Campaigns," (July 8, 2021), https://www.chainalysis.com/blog/israel-hamas-cryptocurrency-seizure-july-2021/; Chainalysis, "Chainalysis In Action: Israeli Authorities Disrupt Hezbollah and Iran Quds Force Terrorism Financing Crypto Infrastructure, Seize $1.7 Million in First," (June 27, 2023), https://www.chainalysis.com/blog/israel-nbctf-hezbollah-iran-quds-crypto-seizure/.
[5] Chainalysis, "Hamas' Al-Qassam Brigades Announces End of Cryptocurrency Donation Efforts," (Apr. 27, 2023), https://www.chainalysis.com/blog/hamas-al-qassam-brigades-cryptocurrency-donations-shutdown/.

therefore, inherent ineffectiveness of using cryptocurrency for terrorism finance, we have refrained from taking a statement like that at face value and continue to work with law enforcement to detect and disrupt terrorists' use of cryptocurrency. Those investigations are ongoing, as we partner with law enforcement to understand the extent of different entities in their roles facilitating Hamas, their affiliates and enablers.

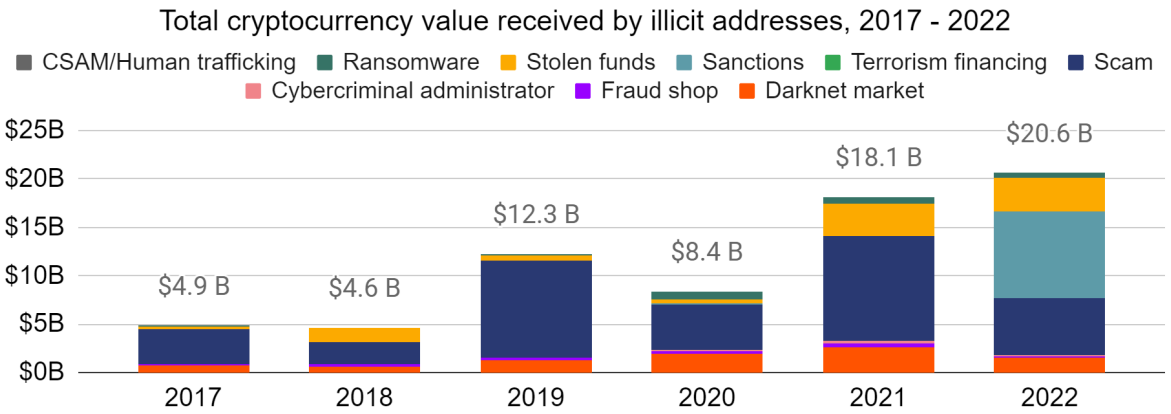
The Data on Illicit Activity

At Chainalysis, we regularly publish research based on our data to provide even more context about the types and amounts of illicit activity involving cryptocurrencies.

As a general matter, our data indicates that the amount of illicit activity constitutes only a small fraction of all cryptocurrency transaction activity.



In 2022, the amount of illicit activity involving cryptocurrencies was approximately $20.6 billion. The vast majority of that activity was attributable to ransomware, scams, and theft. Terrorism finance only made up a very small portion of the total volume of illicit activity.



Our annual Crypto Crime Report delves into each of these areas in more detail.[6]

Future Actions Necessary to Further Mitigate Illicit Activity

The reality is, though, that even more can be done.

First, the federal government should provide a path to compliance for the digital asset industry in the US in order to increase the number of domestic touchpoints for US law enforcement.[7] That requires legislation to be passed quickly that subjects cryptocurrency exchanges and stablecoin issuers to appropriate federal regulation.

Secondly, the ability to successfully conduct illicit transactions in cryptocurrency generally involves the exploitation of gaps and weak points in the global ecosystem. This is best exemplified by the use of non-compliant exchanges in foreign jurisdictions servicing bad actors. The US must continue to drive greater international collaboration to tackle those illicit actors effectively.

Finally and perhaps most importantly, the US should prioritize arming government agencies with sufficient resources and expertise to address the changing dynamics of how value is being transferred over blockchains. Disrupting terrorist financing and illicit

[6] Chainalysis, "The 2023 Crypto Crime Report," (Feb. 2023), https://go.chainalysis.com/rs/503-FAP-074/images/Crypto_Crime_Report_2023.pdf.
[7] Somensatto, Jason, "The U.S. Risks Its Position as a Stablecoin Leader," CoinDesk (Oct. 23, 2023), https://www.coindesk.com/consensus-magazine/2023/10/23/the-us-risks-its-position-as-a-stablecoin-leader/.

activity connected to cryptocurrency requires real time data, sophisticated technology and cutting-edge expertise to exploit it. The government should also consider building centers of expertise where data can be shared and closer public-private partnerships can be built.

Thank you again for this opportunity. I look forward to answering any questions you may have for me.