INCA DIGITAL

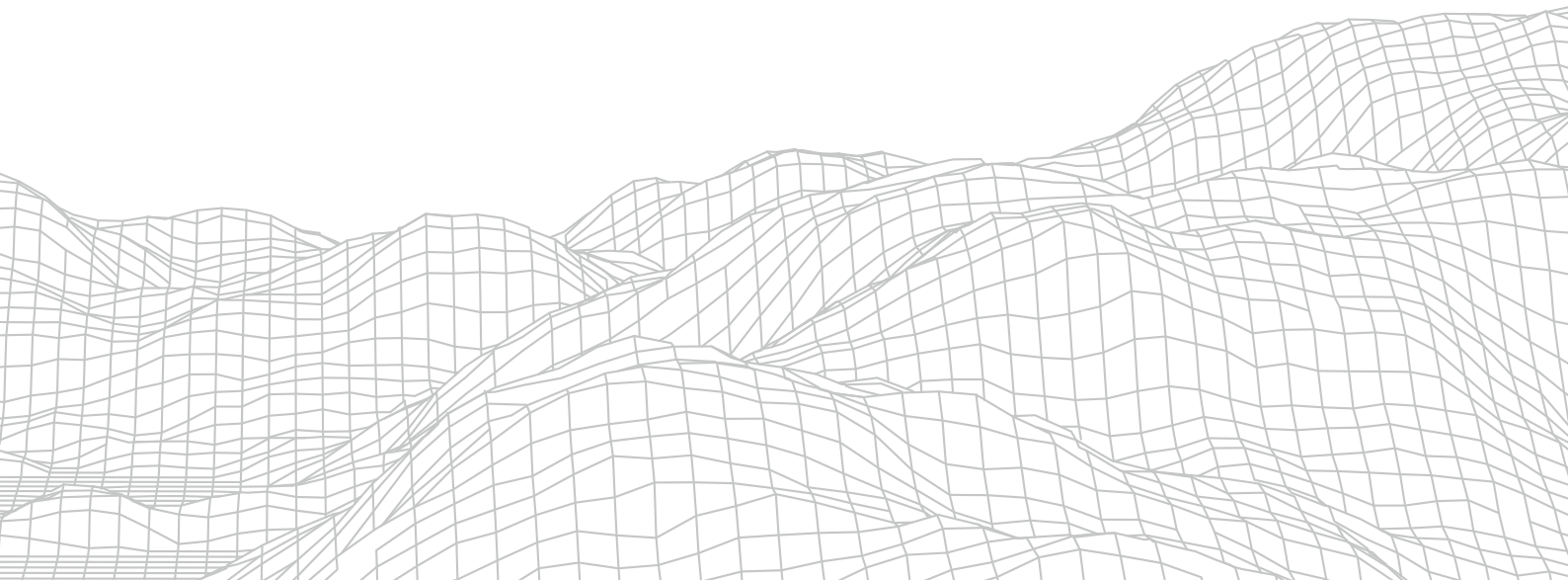
inca.digital

House Financial Services Committee

Subcommittee on National Security, Illicit Finance, and International Financial Institutions

How America and Its Allies Can Stop Hamas, Hezbollah, and Iran from Evading Sanctions and Financing Terror

Adam Zarazinski
CEO, Inca Digital



Honorable members of this committee,

Thank you very much for giving me the opportunity to testify here today.

My name is Adam Zarazinski. I am the CEO of Inca Digital, a data analytics and all-source intelligence company focused on cryptocurrency. I am also a Major in the United States Air Force Reserve JAG Corps. I spent 4 years active duty as well: two years as a prosecutor at Joint Base Andrews, and then two years in operations law, with a deployment in Afghanistan and then at an assignment to the Air Force District of Washington. I left active duty in 2018 to begin my tenure as CEO and founder of Inca Digital.

As you can see from my career, I don't like bad people who try to do bad things, and I've dedicated my career in part to stopping them. By utilizing the advantages of blockchains, when combined with other open source intelligence, we help financial institutions and the government identify and root out those who wish to do harm - both to consumers and to the United States and its allies. For example we work with partners within the Office of the Director of National Intelligence to support DA/Crypto. We also work with the Defense Advanced Research Projects Agency to develop tools and techniques for detailed data mapping of the intersection of traditional finance and crypto finance, ultimately in order to better understand illicit actor behavior.

It is an honor and a privilege to share my thoughts, and some of Inca Digital's data, on how America and its allies can stop Hamas, Hezbollah, and Iran from evading sanctions and financing terror, particularly as it relates to cryptocurrency and the tools we have to interdict bad actors in this space.

I would also like to provide the broader context for you on sanctions evasion and illicit finance in the region - focusing not just on cryptocurrency, but the myriad of ways these organizations move and launder illicit funds. And, finally, I will wrap my testimony with some broad recommendations on what you, our lawmakers, can do to help overcome this problem in the future.

The overall discussion on cryptocurrency and how it is used in illicit finance generally - from global frauds to funding terror organizations to assisting with sanctions evasion to challenging US dollar supremacy - is oftentimes chaotic, misconstrued, and taken out of context. As a result, we have multiple competing narratives, often at opposite sides of the spectrum.

On the one end of that spectrum, many paint broad brush strokes and argue that all crypto is related to crime and illicit finance, that it is an outsized and existential threat to our national security, poised to smash like a hurricane into our fragile infrastructure, and that therefore we should do away with cryptocurrency outright or restrict its use as much as possible here in the United States. On the other end of that spectrum, I am sure you are often told by lobbyists from large and well financed crypto companies that all crypto transactions are trackable and that there isn't anything to worry about; that every new case of theft, fraud, money laundering, or illicit activity in crypto is an aberration to be ignored, no more significant than a single grain of sand on a beach.

Both are wrong.

How Terrorist Financing Using Crypto Works

Typically, terrorist groups have leveraged cryptocurrency in two distinct manners: First, to solicit donations, and second, to procure goods or cyber infrastructure. These acquisitions are then utilized for recruitment and propaganda dissemination.

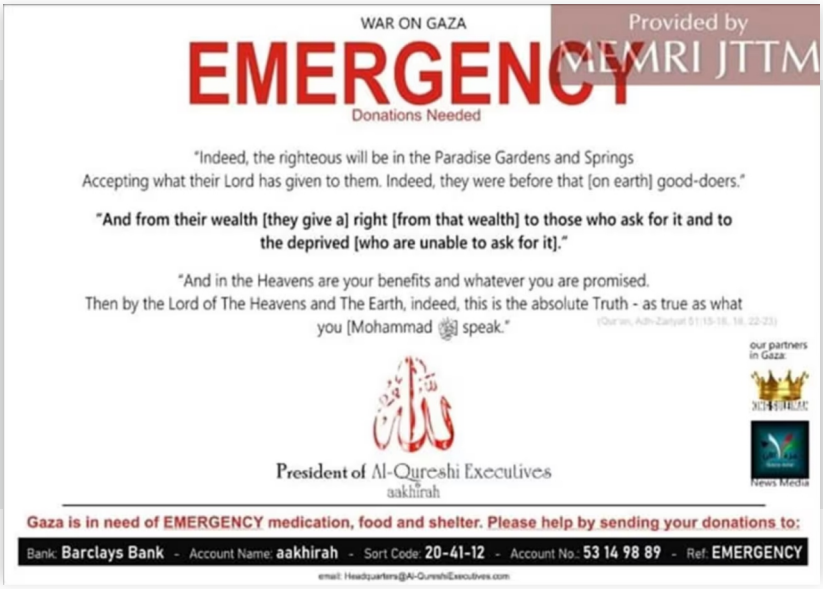
While both uses are concerning, Inca's observations indicate a greater inclination of these groups towards donation campaigns. The donors involved in these campaigns often display a lack of sophistication in obfuscating their tactics and transactions, which allows us to deploy our tools to identify where and how they are moving crypto.

For example, on January 29, 2019, the military wing of Hamas, known as the al-Qassam Brigades, called on supporters to send Bitcoin.

In their first version of the website, they offered a single Bitcoin address for all those willing to donate. This made it very easy to track their transactions. Later iterations of the website established by the Qassam Brigades allowed each visitor to be allocated an individual Bitcoin address, making it more difficult (but not impossible) for investigators to track the funds.

A screenshot from the video on the Qassam Brigades fundraising website

In August 2020, the Department of Justice dismantled the website,[1] but other donation campaigns appeared elsewhere. For example, recently various Gaza-based media outlets initiated campaigns promoting donations to Hamas as the attack on Israel began. On October 9, 2023, the outlet shared a post in English promoting a London-based company called Alqureshi Executives announcing an "emergency" donation campaign in support of the "war on Gaza."



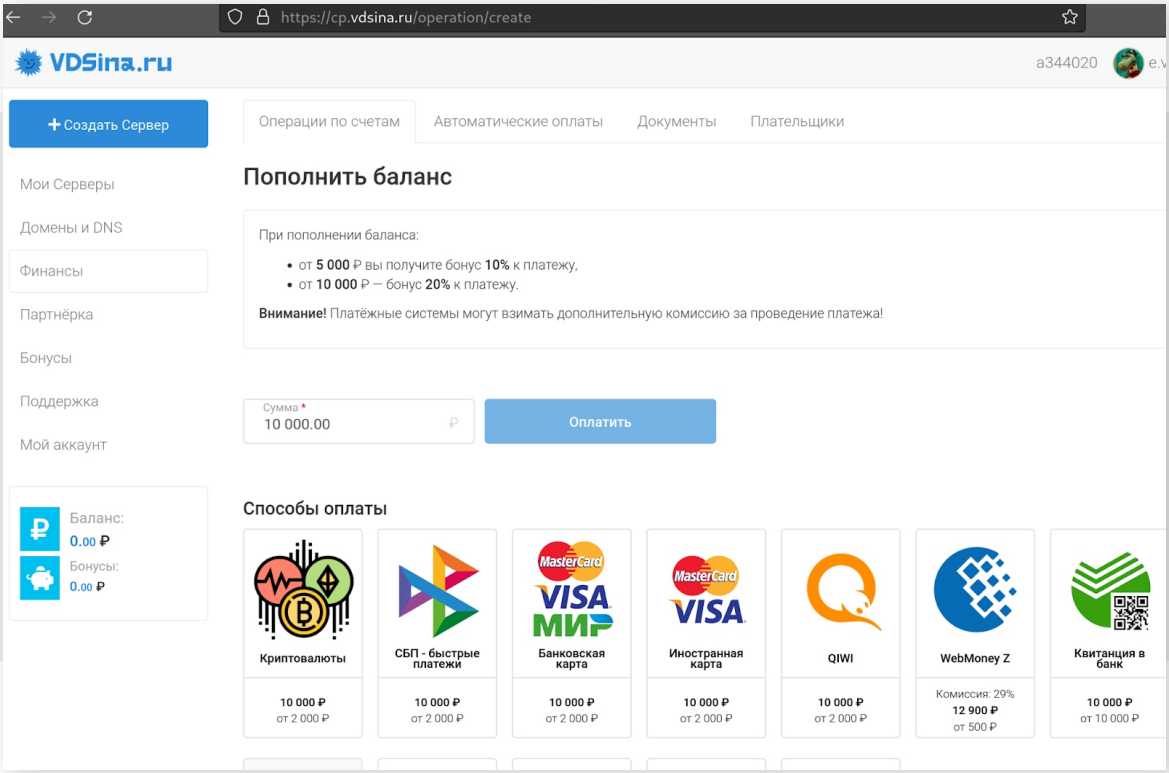
1 Office of Public Affairs. "Global Disruption of Three Terror Finance Cyber-Enabled Campaigns." Office of Public Affairs | Global Disruption of Three Terror Finance Cyber-Enabled Campaigns | United States Department of Justice, 13 Aug. 2020, www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns

Further, the "Gaza Now" Telegram channel[2] provided an email account for donations via various online financial service providers like PayPal, to a wallet to donate Tron and Tether (USDT), and a permalink to a fundraiser on Instagram. The post was later deleted. Inca Digital's data indicates most terrorist financing for Hamas and Hezbollah has now moved to Tether on Tron. Inca Digital is in the process of collecting more data on how this stablecoin is used.

A day earlier, October 8, the Gaza Now Telegram channel posted a link to a fundraising campaign on its Instagram account, however the Arabic description it provided to followers read: "All of our photos can be seen on our account on Instagram here: https://www.instagram.com/linking/fundraiser?fundraiser_id=243951224936346&source_name=SHARE_LINK."

2 "غزة الآن - Gaza Now." Telegram, telegram.me/gazaalannet. Accessed 24 Oct. 2023.

These fundraising websites must also be conscious of where they host. The Hamas military wing moved to a Russian IP address and VDSina hosting, from the Hosting Technologies company. Before this, alqassam.ps was from a Ukrainian IP address for more than two years. On October 15, the Hamas militant website also began simultaneously using the IP addresses of companies in Lebanon and Panama. In addition, a previously unknown network of domains believed to be associated with Hamas have been discovered. They all used the same Google Analytics code (UA-53251638) as the alqassam.ps website.



These public fundraising campaigns, albeit concerning, serve as a treasure trove of intelligence. Whenever names of companies, social media usernames, or cryptocurrency addresses are publicized, they offer an avenue to dissect the network, identifying not just the primary culprits but also affiliates and donors. Just from recent social media posts by supporters of Hamas, Inca Digital has been able to create a network map to identify user names, trading volumes, wallet addresses and more for Iran based crypto-exchanges such as Nobitex, Wallex, Excoino, Aban Tether, Bit24, TabDeal, Bitcoin, OK Exchange, Tether Land, Gaza based exchanges like quick4pay and Cash4ps, and Russian crypto OTC providers such as NiceChange, Payget, quickchange, Bitokk, btc24pro, Sunduk, and about 80 other providers in Russia.

Crypto Threat Finance for Hamas and Hezbollah in Context

Hamas, Hezbollah, and Iran have asked for donations via crypto wallets and do use cryptocurrency to move money - the examples above show this. But they also use local money changers, Hawalas, shell companies at banks, and even hand-carry cash to move to fund their operations.

I am sure you all saw the Wall Street Journal article that came about on October 10, 2023 about Hamas utilizing cryptocurrency to raise funds.[3] In that article, Elliptic and another forensics company estimated that a portion of $135 million had been received by Hamas and the Palestinian Islamic Jihad through crypto since 2020.[3,4] Elliptic noted that it was unclear what portion of those assets directly belonged to the group.[4] Chainalsysis, on the other hand, later released a report saying it has tracked funding in the hundreds of thousands of dollars to Hamas, but nothing more.[5] For argument's sake let us use the $135 million as the top line estimate - which amounts to approximately $45 million per year. To be clear, setting an upper bound with an overstatement of this magnitude, if Chainalysis is correct, is the equivalent of the precision of stating the House of Representatives has under 100,000 members.

Hamas traditionally has a budget of approximately $400 million to $550 million per year, and this has increased to approximately $700 million per year recently.[6,7,8,9] Iran provides the vast majority of this funding - over the last few years at approximately $350 million per year. Hamas also controls swaths of land and trade routes - and money comes from taxation, extortion, smuggling, kidnapping, and robbery, estimated between $300-$450 million/year.[8] Hamas also, of course, has access to non-recurring revenue as well.

---

3 Berwick, Angus, and Ian Talley. "Hamas Militants Behind Israel Attack Raised Millions in Crypto." The Wall Street Journal, Dow Jones & Company, 10 Oct. 2023, www.wsj.com/world/middle-east/militants-behind-israel-attack-raised-millions-in-crypto-b9134b7a?mod=livecoverage_web

4 Glover, Scott, et al. "'They're Opportunistic and Adaptive': How Hamas Is Using Cryptocurrency to Raise Funds." CNN, Cable News Network, 13 Oct. 2023, www.cnn.com/2023/10/12/us/hamas-funding-crypto-invs/index.html

5 Chainalysis Team. "Correcting Recent Claims on Crypto's Role in Terrorism Financing." Chainalysis, 19 Oct. 2023, www.chainalysis.com/blog/cryptocurrency-terrorism-financing-accuracy-check/

6 Glover, Scott, et al. "How Hamas Is Using Cryptocurrency to Raise Funds."

7 Sayegh, Hadeel, et al. "Who Funds Hamas? A Global Network of Crypto, Cash and Charities." Reuters, Thomson Reuters, 16 Oct. 2023, www.reuters.com/world/middle-east/hamas-cash-to-crypto-global-finance-maze-israels-sights-2023-10-16/

8 Tangalakis-Lippert, Katherine. "Who's Funding Hamas?" Business Insider, Business Insider, 21 Oct. 2023, www.businessinsider.com/how-does-a-militant-group-like-hamas-get-its-money-2023-10#:~:text=Experts%20estimate%20that%20Hamas%20has,for%20the%20Palestinian%20militant%20group

9 Jones, Rory, et al. "How the West-and Israel Itself-Inadvertently Funded Hamas." The Wall Street Journal, Dow Jones & Company, 20 Oct. 2023, www.wsj.com/world/middle-east/hamas-gaza-humanitarian-aid-diverted-cf356c48

For example, it is estimated that at least a portion of the Gaza Reconstruction Mechanism that received $3.5 billion from countries to rebuild after the 2014 attacks created a black market for materials sold in the strip that benefited Hamas,[7] and in 2022, the Department of Treasury estimated that Hamas has an investment portfolio valued at $500 million.[9]

When the full scope of Hamas' financing is taken into account, even if we take the most inflated number produced by the cryptocurrency industry, the portion of money moved through cryptocurrency only accounts for about 6% of all funds: $45 million per year laundered via cryptocurrency and $655 million gained by other means. Using the more conservative estimate of hundreds of thousands, which Inca believes is more likely accurate, cryptocurrency would be less than 1% of all funds for Hamas annually.

The same is true of Hezbollah.

US Agencies estimate that Hezbollah receives an annual fund of approximately $700 million per year from Iran.[10] They also receive hundreds of millions more in annual revenue through drug-trafficking, trafficking in art and diamonds, and money-laundering networks.[11] Here, too, a forensics company estimated that $12 million in cryptocurrency had been sent to Hezbollah since 2021.[12] This means approximately $4 million in cryptocurrency has been sent to Hezbollah for the past three years, with over a billion sent to the organization via other means.

The goal of providing the above context is not necessarily to simply minimize for the audience the role cryptocurrency plays in financing Hamas and Hezbollah. There is a more important narrative to disentangle and acknowledge. This is that the use and abuse of cryptocurrency is no different than the use and abuse of other methods of transferring value. Cryptocurrency is not something separate from the other ways Hamas and Hezbollah move and launder money globally.

Organizations like these are like planets with a gravitational pull for illicit funds - and they will try to drag money in through whatever vector they can - whether that is Hawala, bank transfers, or running through underground tunnels with backpacks full of cash.

---

10 The Department of the Treasury. "Under Secretary Sigal Mandelker Speech before the Foundation for the Defense of Democracies." U.S. Department of the Treasury, 5 June 2018, home.treasury.gov/news/press-releases/sm0406

11 "OFAC-Designated Hezbollah Financier and Eight Associates Charged with Multiple Crimes Arising Out of Scheme to Evade Terrorism-Related Sanctions." Office of Public Affairs | OFAC-Designated Hezbollah Financier and Eight Associates Charged with Multiple Crimes Arising Out of Scheme to Evade Terrorism-Related Sanctions | United States Department of Justice, 18 Apr. 2023, www.justice.gov/opa/pr/ofac-designated-hezbollah-financier-and-eight-associates-charged-multiple-crimes-arising-out

12 Berwick, Angus, and Ian Talley. "Hamas Militants Behind Israel Attack Raised Millions in Crypto."

They are now adding new technologies as they become available - crypto is one of those new technologies, and so are a myriad of other non-crypto alternative payments ecosystems - AliPay, WeChat Pay, Webmoney, Korona Pay, and more. The key is interdicting the bad guys across all vectors, and integrating new data analytics to create intelligence as operational realities on the ground change. This is what Inca Digital does best. To focus exclusively on cryptocurrency misses the bigger point: we need to stop the bad guys from getting money - wherever and however they do so.

There is a plethora of data and analysis available for the United States and our allies to identify illicit actors using these services to move money, and while the extent of terrorist financing through cryptocurrency might sometimes be amplified, it remains an undeniable concern. And, there are plenty of other national security challenges where cryptocurrency is now part of illicit operations: billions of dollars have been stolen from unwitting Americans in a scam known as Pig Butchering that now utilizes cryptocurrency, North Korean hackers have stolen over $3B in digital assets over the past five years, and there is a growing intersection of great power competition and digital assets, where China, Russia, Iran, and Venezuela are exploring ways to utilize blockchain technology and crypto-finance to further distance themselves from the Western-based financial system. All of these are national security challenges that must be addressed.

What We Can Do

Even with the above challenges, though, we do not have the capacity to hammer crypto out of existence. No amount of sanctions, no amount of actions from the Department of Treasury or stringent policies against crypto here at home will stop Iranian or Russian crypto OTC providers from laundering money. The problem is not primarily on shore in the United States. The problem is the list of companies I provided above - these organizations are completely outside of our jurisdiction. These companies will exist outside of our reach and whatever solution we opt for must acknowledge this fact. Eradicating crypto is simply not possible, and likely has not been possible for at least a decade, if not more.

Second, we cannot ignore the problem and expect it to go away. To return to the previous statement about how Hamas as an organization is the problem, not the specific type of technology used for moving money, they will attempt to exploit any weak spot in order to bring in funds. In order to interdict this sort of activity, what we must do is continue to develop technology to identify and stop bad actors, and build a strong, robust, and functional crypto ecosystem here in the US.

The recent revelations concerning certain groups utilizing cryptocurrency as a mechanism for funding underscores the adaptability and versatility of this innovative technology. It's crucial to remember that like any other technological advancement, cryptocurrency itself is neutral. Throughout history, every groundbreaking innovation, from the printing press to the internet, has been harnessed for both commendable and malicious intents. In the same way, while cryptocurrency can be employed in activities that challenge our security and values, it also holds the potential to democratize finance, spur economic growth, and foster financial inclusion globally.

Bringing crypto on-shore is ultimately the best way to control these activities, because it will exist offshore whether we like it or not, and the more of the market we get here to monitor and regulate safely the better. Crypto, if we set good rules and regulations, can be better for transparency and interdicting bad actors than traditional finance. Acknowledging it is not there yet, part of the goal of the work of our lawmakers should be to draft bills such that it can and does get there, and gets there onshore in a healthy way that balances privacy and law enforcement.

In other words, one of the best ways we can stymie cryptocurrency use in terrorist financing is to do what we always have - to what is fundamental to America: allow for an open society with bold thinkers and entrepreneurs pushing the limits of the system with technological innovation. Foster innovation and grow markets in decentralized finance. Our national security depends on it.