Hamas crypto funding, the WSJ, and the Warren Letter

An assessment of the facts surrounding Hamas' alleged use of crypto

Nic Carter
11/02/23

Executive summary

- The claim that Hamas "raised over $130m in crypto" is not supported by the available evidence (although better estimates have yet to emerge)
- The Israeli seizure orders, where all of the address data derives from, likely include affiliated brokers who account for the majority of transaction volume that third parties are counting as "funds raised". The major chain analysis firms are agreed on this point
- Even if all addresses were solely controlled by terror groups, Elliptic's summation of funds raised is still erroneous, and appears to be inflated by ~15%
- Elliptic – the major source for the WSJ, which was the sole source for the Warren letter – has revised their assessment of the data credibility and no longer supports the claim made by the WSJ and the Warren letter that Hamas raised "millions" in crypto
- The crypto crowdfunding campaigns for Hamas that have been identified have been extremely small scale, and have been interrupted by exchanges and stablecoins seizing funds
- Both Binance, Tether and other intermediaries are active in identifying and interrupting suspected terrorist finance activity
- Hamas itself ceased soliciting crypto donations in April 2023 after Israeli seizures
- While some amount of terrorist financing with crypto is unavoidable, we lack sufficient evidence to support the claim that Hamas "raised millions of dollars in crypto"
- The Warren letter makes aggressive claims that aren't supported by the evidence, and both of the letter's ultimate sources (Elliptic and the WSJ) have issued subsequent corrections
- Because Israeli intelligence have not shared further data, we still lack a precise estimate of the crypto funds that Hamas or Hamas affiliates actually control(led).

Introduction:

On October 10, following the attacks by Hamas on Israeli civilians, Angus Berwick and Ian Talley of the WSJ published the article "Hamas Militants Behind Israel Attack Raised Millions in Crypto". The WSJ followed up with "Why Hamas Uses Crypto to Raise Money" and then published an op-ed from Sen. Elizabeth Warren entitled "Cryptocurrency Feeds Hamas's Terrorism". Sen. Warren then wrote a letter to the White House and Treasury signed by over 100 members of Congress, reliant entirely on the WSJ claim that Hamas and affiliates had raised "over $130m in crypto" to fund their operations since 2021. Warren is now leading a campaign to aggressively marginalize the crypto industry in the US based on her provocative claim. Yet subsequent evidence has thrown her entire empirical basis into question.

The WSJ initially refused to update or retract their story, but subsequently issued a correction on October 27, after Elliptic released a blog post saying that the WSJ had misinterpreted their data.

On October 26, fearful that the WSJ would not do their jobs and would refuse to investigate the actual number regarding Hamas' crypto fundraising, I created a bounty program designed to solicit blockchain analysis from the crypto community. I had initially earmarked $10k for the bounty, but I received third party contributions and the pot swelled to $50k (with much of it still outstanding). The objective wasn't simply to rebut the WSJ's reporting; but to dig into the data and get to the bottom of the story — whatever the answer was. If my analysts discovered that Hamas had genuinely raised $130m in crypto, as Sen. Warren claimed, I wouldn't have concealed that.

As it has now been a week since the bounty was created, and I have reviewed over a hundred submissions, I wanted to take stock, summarize the state of our knowledge around this question, and showcase some of the better answers I've received.

Unfortunately, I don't have a concrete anwer to give you as to the extent of Hamas fundraising with crypto. I'm not sure any entity aside from Hamas itself knows. I doubt even that the Israeli intelligence have a perfect estimate. (Although I would encourage firms like Chainalysis and TRM to further weigh in with their own specific estimates.) What we can say confidently however is that the $130m figure so confidently declared by Senator Warren is not supported by the evidence we have at our disposal. In the remainder of this article, I'll explain why I think this is the case.

Timeline of events:

- July 2022: Israel's National Bureau for Counter Terror Financing (henceforth NBCTF) issues ASO 15/22 (link), targeting 47 addresses associated with "Dubai co for exchange" (datasource used by BitOK)
- April 2023: NBCTF issues ASO 19/23 (link), targeting 5 addresses and 77 Binance client accounts associated with "Dubai co for exchange, Al Matahadun for exchange, and Al Wefaq co for exchange" (datasource used by BitOK)
- April 2023: NBCTF issues ASO 34/23 (link), targeting 26 addresses and 67 Binance client accounts associated with Palestine Islamic Jihad (PIJ) (datasource used by Elliptic)
- April 2023: Al Qassam (Hamas affiliate) stops soliciting donations in Bitcoin, citing safety risks to their donors
- July 2023: Elliptic claims that PIJ had received $93m based on addresses disclosed in ASO 34/23
- August 2023: BitOK releases an analysis of addresses found in ASO 29/23 and 34/23
- Oct 7, 2023: Hamas attack on Israel
- Oct 9, 2023: Hamas-affiliated Gaza Now starts a crypto crowdfund, raising only $21k, of which 2k is frozen at Binance and 9k is frozen by Tether

- Oct 10, 2023: TRM releases an analysis finding <$1m raised by Hamas in crypto-based crowdfunding. They do not make an estimate based on the Israeli orders
- Oct 10, 2023: WSJ releases their first article on the topic citing both Elliptic ($91m) and BitOK ($41m)
- Oct 17, 2023: Senator Warren writes a letter which is signed by >100 members of congress, citing the WSJ article exclusively
- Oct 18, 2023: Chainalysis released a blog questioning the methodology without referencing either provider directly
- Oct 25, 2023: Elliptic releases a follow up disputing the WSJ's approach and the Warren letter
- Oct 25, 2023: BitOK releases clarification on their own methodology
- Oct 27, 2023: Initially defiant, the WSJ ultimately corrects their article, softening their claims, while still refusing to issue a full retraction
- In the Senate hearing on Oct 26, numerous Senators and witnesses continued to question the WSJ/Warren claim that crypto had funded "over $130m" in donations to Hamas or affiliates
- Oct 31, 2023: in a Twitter space, Elliptic CEO Tom Robinson says that he "wants to see the WSJ go further with their retractions" and that he "doesn't believe that the WSJ has provided evidence to support the title of the article"
- Oct 31, 2023: Sen. Warren doubles down on her claim, aware that the WSJ issued a correct, stating "it's not about one report" (even though her letter cites only one report)

On the ambiguity of blockchain data

Ever since I cofounded Coin Metrics in 2016, I've been looking at on-chain data almost every day. My number one challenge with this type of data is its ambiguity. The essential premise of on-chain data analysis, whether it's used for risk assessment (as with Chainalysis or Elliptic), or for capital markets (as with Coin Metrics, Nansen, or Dune), is to try and connect real-world identities to on-chain transactions. I understand how difficult this can be. Ultimately, blockchain data is ambiguous, and concrete numbers are few and far between. Many mistakes are made when people attach excessive levels of certainty to on-chain numbers that are inherently vague and complex to interpret.

Because of idiosyncrasies in how blockchain wallets work, and the ease of gaming or inflating on-chain data, it's very common for third party observers who aren't deeply familiar with on-chain data to make critical mistakes when looking at it. Occasionally, these reverberate in the press and create persistent myths. For instance, take the example of the infamous Griffin and Shams paper from 2020 published in the Journal of Finance (the most prestigious financial journal) that claimed that a "single large entity" was manipulating Bitcoin markets with fake Tethers, by looking at a lot of blockchain data and finding perceived relationships there. As it turns out, this was not the case, and they were probably looking at the activity of a market maker arbitraging the Tether peg. Subsequent developments showed that their claimed Bitcoin-Tether relationship did not hold.

But people believed the academics, because they backed their faulty analysis with a large amount of inscrutable blockchain data – and a story that many wanted to believe ("the price of Bitcoin is fake, and is propped up by unbacked manipulation relating to Tether").

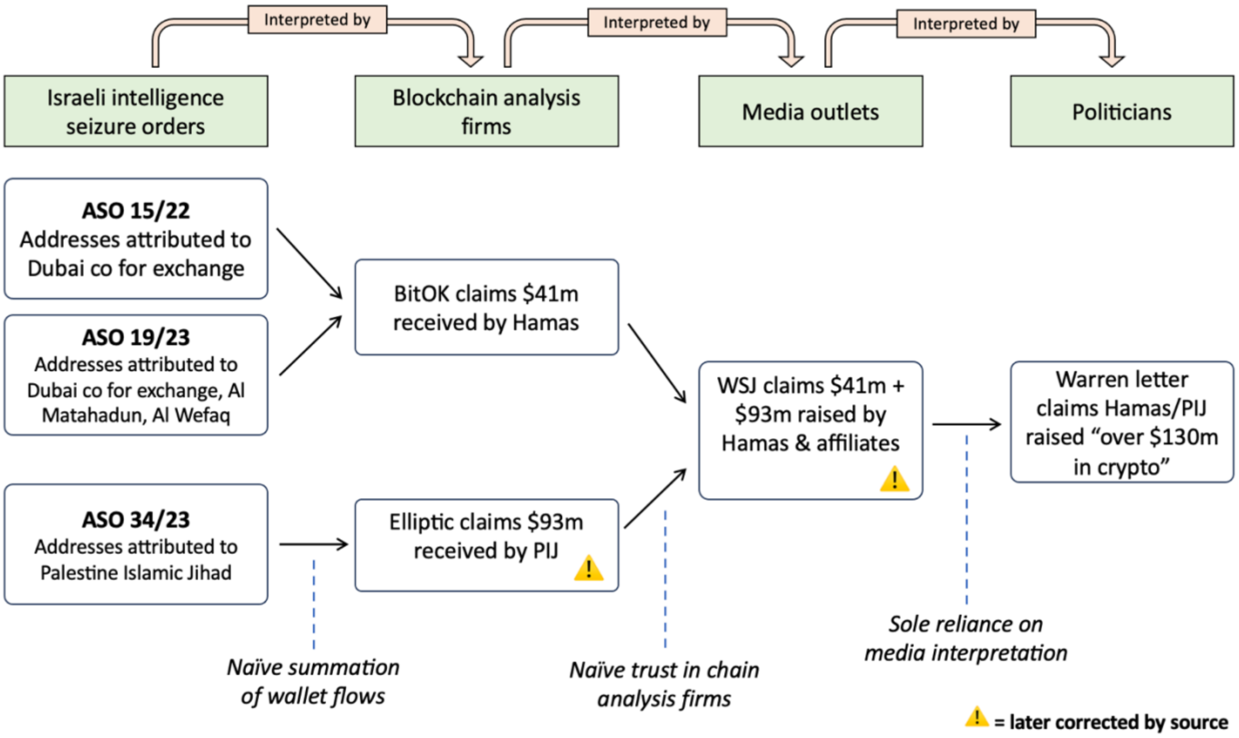
In the last few weeks, the same thing has happened with Hamas and alleged crypto funding. The idea of crypto powering the terrorist attacks on Israel was a convenient one for crypto-critical members of Congress, and a narrative blaming crypto for the attacks was quickly contrived. Israeli intelligence did identify clusters of addresses that they felt had some relationship to terrorist financing, but third parties over-interpreted that data and drew conclusions that weren't supported by the evidence.

Key issues

Having contemplated the totality of the story and the data for weeks now, I feel that there's a few ways the epistemic pipeline starting with "Israeli NBCTF issues seizure order for specific wallet addresses" and ending with "terrorist groups raised over $130m in crypto" could have been polluted. Specifically, the issues are as follows:

- Israeli intel is not focused on precision, but on freezing addresses that are terror-affiliated. This is a dragnet that can catch unrelated, or only semi-related third party addresses. Analysts need to be mindful of the difference
- It is very likely that the addresses in the Israeli intel dataset included third-party brokers that had plenty of non-terror related flows. Elliptic (initially), the WSJ (before their correction), and Sen. Warren in her letter conflate these numbers
- A "gross flow" methodology on a per-address basis artificially inflates flow data. My analysts have shown that the Elliptic numbers are inflated in this manner (although only by about 12-18%)
- Wallet flows are not equivalent to "funds raised"

We will dig into each in turn. To clarify the setting, I'm attaching a diagram of how action by Israeli intelligence was ultimately warped into a (now known to be exaggerated) claim by Sen. Warren in her letter that was signed by over 100 members of Congress.


Interpreted by
Interpreted by
Interpreted by
Israeli intelligence seizure orders
Blockchain analysis firms
Media outlets
Politicians
ASO 15/22 Addresses attributed to Dubai co for exchange
ASO 19/23 Addresses attributed to Dubai co for exchange, Al Matahadun, Al Wefaq
ASO 34/23 Addresses attributed to Palestine Islamic Jihad
BitOK claims $41m received by Hamas
Elliptic claims $93m received by PIJ ⚠
WSJ claims $41m + $93m raised by Hamas & affiliates ⚠
Warren letter claims Hamas/PIJ raised “over $130m in crypto”
Naïve summation of wallet flows
Naïve trust in chain analysis firms
Sole reliance on media interpretation
⚠ = later corrected by source

To briefly summarize, a game of telephone took place, starting with Israeli intelligence issuing seizure orders for Tron and Binance addresses, and ending in the halls of Congress. At each step the data became less concrete and the claims more extravagant. Blockchain analytics firms took addresses listed by Israeli intelligence and made aggressive inferences from the data, which were then repeated and extended by journalists, particularly at the WSJ. The press coverage was then once again reinterpreted by Sen. Warren in her letter. By the time it reached Congress, buried under three layers of interpretation, the claims bore little resemblance to the original data, and were presented without ambiguity, hedging, or an acknowledgement of the inherent uncertainty. Elliptic later significantly revised their level of confidence in the data, and the WSJ also issued a substantial correction, thus undermining the major claim made in the Warren letter.

The NBCTF’s Precision versus Comprehensiveness Tradeoff

First, and most importantly, the NBCTF is not an academic organization. They are not focused on specifically singling out wallet addresses which belong to Hamas or affiliates, but rather stopping terror in its tracks. I am speculating here, but I would posit that to them, a false negative is much worse than a false positive. As in, if they determine that terrorists have some on-chain identity, and they fail to designate the entire set of addresses, that’s a much worse outcome than if they tag the terrorist wallets as well as a few unrelated ones. They are presumably focused on minimizing type II error (false negatives), not type I error (false positives).

Their objective is to eliminate terror financing. This means that they are more willing to accept false positives rather than risking missing a few while trying to be surgical. This is really the crux of the matter: NBCTF may not care that they are tagging an affiliate or payment processor or brokerage/exchange that has a history of transacting with Hamas and others, rather than Hamas itself. From their perspective, they're still intercepting funds earmarked for terror, even if there is some collateral damage. And from a national security perspective, this makes total sense. It's just that when you strip this information out of that context, and declare that all activity associated with those wallets is specifically dedicated for funding terrorism, you start to introduce errors. It's Elliptic and BitOK that are making the key mistake, by blindly looking at a list of addresses published by Israeli Intel and deciding that 100% of those flows specifically pertain to funds raised by Hamas.

The NBCTF address listing likely includes data from third party brokers

The crux of the matter is that some of the addresses claimed to be owned by Hamas or affiliates may not have belonged not to PIJ, Hamas or their affiliates directly, but rather third parties, with only a fraction of their volume attributable to terrorist financing. For instance, the two orders the BitOK number of $41m was based on activity not by Hamas or PIJ, but rather "AL Mutahadun for Exchange, Dubai Company for Exchange, and AL Wefaq Co. for Exchange", which Binance describes as "currency exchange outfits." This can also be inferred from their names. In Reuters reporting, Al Mutahadun describes itself as "a money exchange company". This is not to say that they're *not* involved in funding Hamas – of course, the reason Israel sought to freeze their funds is because of that specific allegation. But because they operate currency exchange businesses, they may well maintain flows that are non-Hamas related.

So what we're dealing with here is an artifact of the nature of chain analysis itself. It's entirely valid for Chainalysis, Elliptic, or Israeli law enforcement to label addresses as terror-finance-affiliated, but this doesn't mean that all funds flowing through these addresses are specifically funds *being raised directly for Hamas*. I'm attaching commentary from each of the major chain analysis providers on this specific question. Chainalysis's entire blog post is focused on cautioning against this *specific conflation.* They are very careful to point out that wallets that are vaguely terror-affiliated may well be payment processors, OTC brokers, hawalas, or other types of service providers. They actually list 20 such service providers that have interacted with known-terrorist financing wallets, knowingly or unknowingly. As Chainalysis states, "it is often not productive to continue following funds once they've been deposited at a service [like one of these money transmitters]". Here are the key extracts from blog posts by Chainalysis, TRM, and Elliptic (in my opinion, the three most "blue chip" blockchain analysis firms) on this issue:

Chainalysis: *We have seen recent estimates related to the attacks on Israel that appear to include all flows to certain service providers that received some funds associated with terrorism financing. In other words, those totals include funds not explicitly related to terrorism financing. Of course, these service providers are supporting terrorism by acting as facilitators, and cutting off terrorist access to them through sanctions or other offensive operations is an important* *component to disrupting terrorist finance. But it would be incorrect to assume all of the transaction activity conducted by those service providers is related to terrorism.*

Translation: Chainalysis is taking aim at Elliptic, and pointing out that they are wrongly bundling in service providers with specifically PIJ-related wallets, and assuming that the entirety of those flows are terror-related.

TRM: According to Israeli authorities, the key address [in ASO 34/23] was controlled by Tawfiq Muhammad al-Law, a Syria-based hawala operator who worked with key Hezbollah and IRGC financiers. TRM identified on-chain links between the seized addresses and entities and exchanges located in Iran, Syria, Iraq and the Gaza strip, all of which have ties to the IRGC and Hezbollah.

Translation: TRM is pointing out that one of the main entities tagged by Israel in the order ended up composing the BitOK estimate was a hawala operator. Hawala refers to a kind of remittance process that works outside of the formal banking system. It's reasonable to assume that some of their flows were licit or non-terror related. At the very least, we specifically have an example of the kind of service provider Chainalysis is referring to that might be cofounding the analysis.

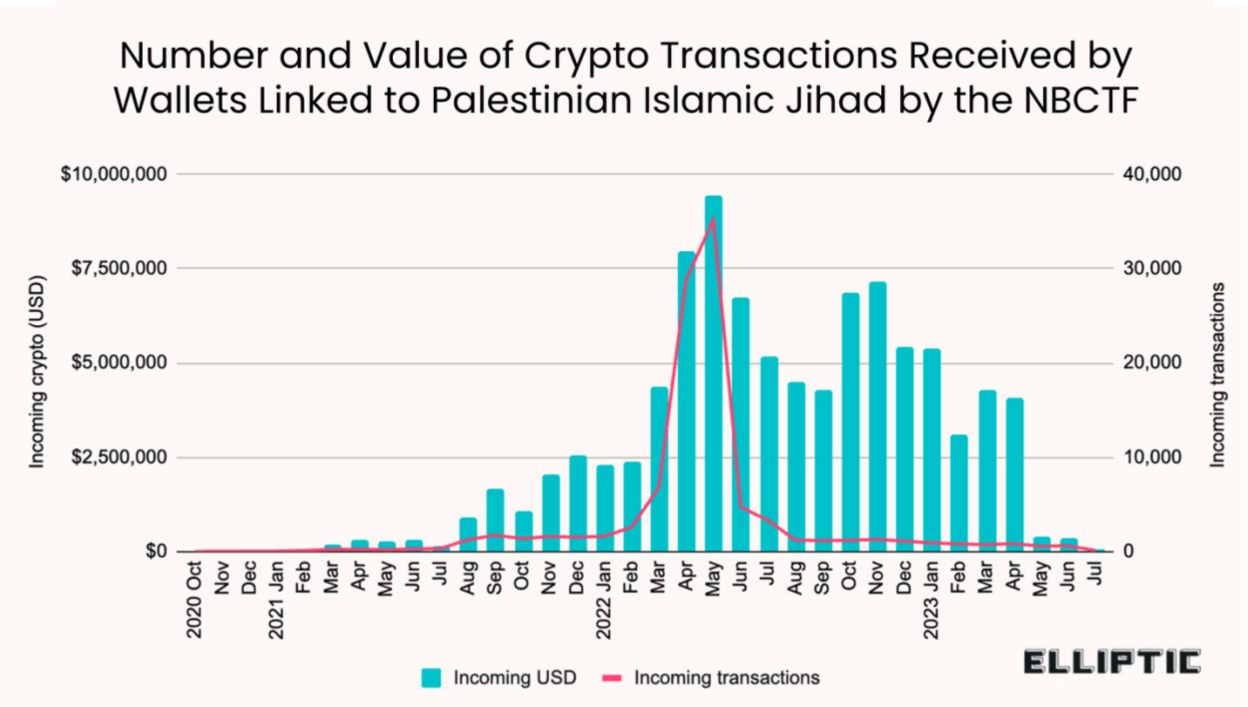
Elliptic: In July this year, the NBCTF issued a seizure order for crypto wallets linked to Palestinian Islamic Jihad […]. Elliptic analysis of the wallets seized by the NBCTF shows that these wallets received transactions totalling just over $93 million between 2020 and 2023. As we made clear in our research, in no way does this mean that PIJ had "raised" all of these funds or that they even all belonged to PIJ. It is not known what proportion of the funds received by those wallets are directly attributable to PIJ or other terrorist groups. It is likely that some of the wallets listed by the NBCTF belonged to small service providers such as brokers that were used by PIJ.

Translation: Elliptic is pointing out here a difference between *tagged addresses showing flows of $93m in the aggregate* and PIJ "raising" that amount of money. They align with the view of Chainalysis and TRM that some of the wallets were likely related to service providers. Elliptic was extremely direct in their language and the CEO has stated (on a subsequent Twitter space) that he "does not believe that the WSJ correction went far enough" and that he "doesn't believe that the WSJ has provided evidence to support the title of the article."

On-chain fund flows are net, not gross

Another mistake that researchers have made is grossing up incoming funds to wallets and taking their nominal value at face value. This can lead to inflated estimates of how much a cluster of wallets really has. One respondent to my challenge, Mrfti_plus, explained it well in this thread.

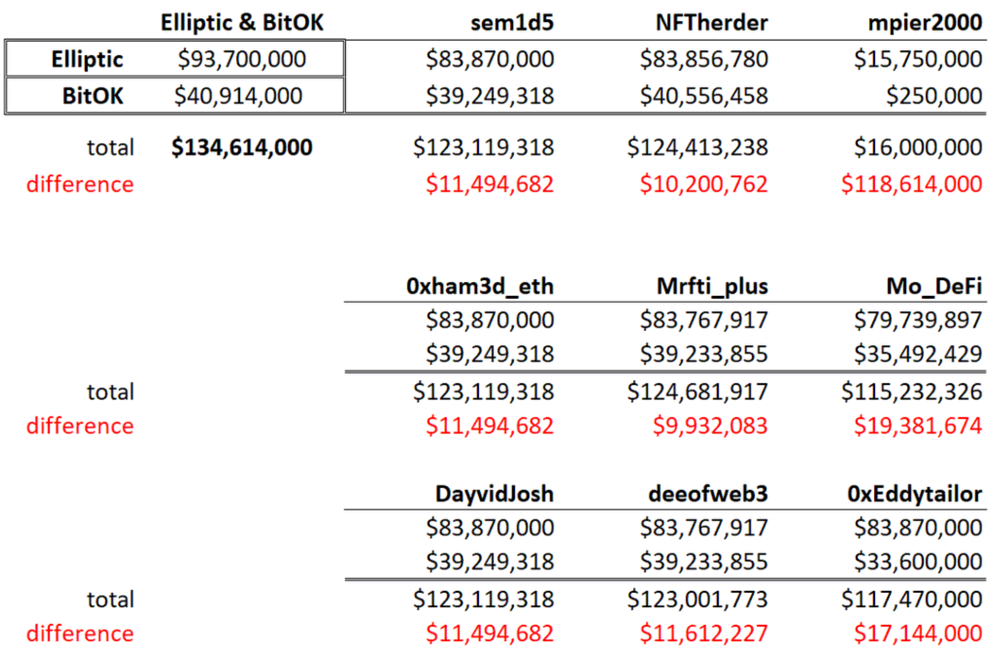
If I receive $100 and send it to Bob, and he sends $50 to Alice, and you naively add up all of the inflows at the wallet level, you get a *gross inflow* figure of $250 (my first $100, Bob's $100 inbound transaction, and Alice's $50), even though the total amount of money between us three is only $100. This is an easy way to inflate figures when aggregating on-chain data at the wallet level without considering the relationships between those wallets. If you look at the Elliptic chart (note: the heading to the chart was edited without comment after the WSJ article was published), you can see that it refers to "incoming USD" in the legend.



Elliptic's methodology involves adding up the flows received by all of the addresses tagged by Israeli intelligence as being Hamas affiliated. But some of these addresses also transacted between each other, driving up the numbers. Once you net out the double-counting, you get a lower figure.

The participants in my Bounty Program contributed a lot of different datapoints to my study, but the most important finding is the following: **Elliptic over-counted the flows, *even assuming that all NBCTF-tagged wallets were 100% terror-related*, by ~$11m**.

Here's a summary of findings by a few participants in my bounty program, compiled by @NFTherder:



	Elliptic & BitOK	sem1d5	NFTherder	mpier2000
Elliptic	$93,700,000	$83,870,000	$83,856,780	$15,750,000
BitOK	$40,914,000	$39,249,318	$40,556,458	$250,000
total	**$134,614,000**	$123,119,318	$124,413,238	$16,000,000
difference		$11,494,682	$10,200,762	$118,614,000

	0xham3d_eth	Mrfti_plus	Mo_DeFi
	$83,870,000	$83,767,917	$79,739,897
	$39,249,318	$39,233,855	$35,492,429
total	$123,119,318	$124,681,917	$115,232,326
difference	$11,494,682	$9,932,083	$19,381,674

	DayvidJosh	deeofweb3	0xEddytailor
	$83,870,000	$83,767,917	$83,870,000
	$39,249,318	$39,233,855	$33,600,000
total	$123,119,318	$123,001,773	$117,470,000
difference	$11,494,682	$11,612,227	$17,144,000

Importantly, I asked that the data and analysis be posted publicly. Here's four Flipside dashboards demonstrating this same finding that anyone can replicate and evaluate:

- MoDeFi
- Sam
- Dayvidjosh
- Deeofweb3

Each of these analyses finds roughly the same thing: Elliptic over-counted in their initial estimate. Moreover, some analysts, like Lamoka, also felt that BitOK overstated their findings (by 10% in their case). Notwithstanding the points made in the prior section about the addresses themselves not being fully attributable, we still find a consistent overstatement of the data. It is therefore clear to us at this point that the "over $130m" claim made by Sen. Warren in her letter is unsupported by the data.

Flows are not equivalent to "funds raised"

Ultimately, flows between wallets on the blockchain are not necessarily indicative of actual "funds raised". Lacking evidence of actual crowdfunding campaigns, it's not enough to look at flows in a cluster of wallets tagged by Israeli intelligence and determine that those transaction volumes represent new funds raised. The few crowdfunding campaigns we have actually witnessed were relatively meager and have been interrupted. GazaNow, a Hamas affiliate, has raised only $800,000 in crypto in the last two years, and some of these funds have been seized via Binance or Tether.

The WSJ coverage and the Warren letter nevertheless conflates *on chain flows* with *funds raised.* Here's some example of language used by the WSJ and Sen. Warren in her letter:

- *WSJ headline: "Hamas Militants Behind Israel Attack Raised Millions in Crypto"*

My view: this headline doesn't comport with the reality. We do not know that Hamas "raised money" in crypto. Indeed, both Elliptic and TRM point out that public crowdfunding campaigns by Hamas and affiliates raised less than $1m. Elliptic specifically states in their blog post: "there is no evidence to suggest that crypto fundraising has *raised* anything close to this amount [$91m], and data provided by Elliptic and others has been misinterpreted." My verdict: it's wrong to use the term "raised" here. A more accurate claim would have been "wallets targeted by Israeli authorities as potentially being linked to Hamas showed *flows* of ~$83m."

- *(Title of chart in WSJ article): "Crypto funds received by PIJ"*

My view: we know now that Elliptic overstated fund flows via double-counting (see the prior section). We also know that not all of the funds were attributable to PIJ directly. My verdict: this language is not supported by the evidence.

- *WSJ body text: "Digital-currency wallets that Israeli authorities linked to the PIJ received as much as $93 million in crypto between August 2021 and June this year"*

My view: the WSJ moderates their language slightly by noting that the wallets were "linked to the PIJ" by Israel authorities. They do not caveat or hedge sufficiently. My verdict: this claim is not supported by evidence.

- *Warren letter: "In the months leading up to their brutal and horrific October 7th attack on Israel, Hamas and Palestinian Islamic Jihad raised millions of dollars in crypto – evading U.S. sanctions and funding their operations […] between August 2021 and this past June, the two groups raised over $130 million in crypto"*

My view: we don't have the evidence to support this claim. The $130m claim is based on the gross flows to Israeli-tagged wallets, but as we have discussed, that figure was overestimated by methodological errors on the part of Elliptic, and likely further exaggerated by the presence of third-party brokers in the sample. While we don't currently have a better estimate, it's clear at this point that Warren's claim is not reliable. It's also a misrepresentation to characterize wallet flows as "funds raised". All we know is that funds are moving between addresses tagged by Israeli law enforcement as potentially having a Hamas connection; we don't know whether these were funds were "raised."

Further context

It’s true that Hamas has been active in trying to raise money in crypto; in fact, they’ve been one of the most active terror groups in trying to utilize the technology.

Nevertheless, crypto appears to be a relatively minor tool in the Hamas financing toolkit. Shlomit Wagman, formerly chair of the Israeli Money Laundering and Terrorism Financing Prohibition Authority lists in her congressional testimony the main sources of funding for Hamas as being state funding (transmitted via cash, hawala, and banks), business portfolios, fundraising (of which a portion is crypto), and stolen humanitarian aid.

Indeed, Hamas’ enthusiasm for crypto seems to be trending downwards, given the effectiveness of law enforcement in interrupting their crypto flows. Hamas’ journey with crypto began around 2019 when they started soliciting crypto donations, and seems to have trailed off in April 2023 when they announced a halt to their crypto fundraising activities (right after an Israeli seizure order went out). The problem with raising funds in crypto is that exchanges very actively seek to freeze suspected accounts; stablecoin issuers themselves routinely freeze funds suspected to be held by terror organizations; and donors can be deanonymized and identified (and perhaps even prosecuted). Transacting with crypto leaves a permanent paper trail, and even if a donor believes that either they or their recipient are pseudonymous at the time, if those addresses are ever subsequently connected to real-world identities, the pseudonymity is broken and the participants can be identified and prosecuted. This is an improvement over the banking system or conventional remittance or hawala channels, where records and databases are not strictly public, as they are with crypto.

Of course, it’s worth noting that physical cash cannot be seized remotely like a stablecoin can, and this is a significant improvement over cash from a law enforcement perspective. Crypto exchanges can be duped into servicing terror organizations (for instance, if they lie on their KYC, which Binance frequently points out), but this is the same for banks. It’s not just crypto exchanges which are exploited for this purpose but banks as well.

If I were a member of law enforcement, it would be my preference that terror organizations solely utilize crypto, rather than cash or banks. This leaves an indelible paper trail, and creates abundant opportunities to seize or interrupt financial flows, which law enforcement have become quite adept at doing. Yes, there is a period of latency while illicit actors achieve a level of sophistication before governments do and are able to transact relatively unencumbered. However, governments today are quite sophisticated at blockchain analysis, and have closed the skill gap. It’s for this reason that we see organizations like Hamas apparently moving away from crypto financing, as opposed to growing their on-chain footprint. This reality cannot be ignored when we consider illicit uses of crypto.