CONGRESSIONAL TESTIMONY: FOUNDATION FOR DEFENSE OF DEMOCRACIES

House Financial Services Committee
Subcommittee on Terrorism and Illicit Finance

Survey of Terrorist Groups and Their Means of Financing

YAYA FANUSIE

Director of Analysis
FDD's Center on Sanctions and Illicit Finance

Washington, DC
September 7, 2018

Center on Sanctions & Illicit Finance
FOUNDATION FOR DEFENSE OF DEMOCRACIES

www.defenddemocracy.org

Chairman Pearce, Vice Chairman Pittenger, and Ranking Member Perlmutter, on behalf of the Foundation for Defense of Democracies and its Center on Sanctions and Illicit Finance, thank you for the opportunity to testify today about a crucial technology that provides virtually unlimited opportunities but also certain threats.

Cryptocurrencies may become the way we transact in the future. But they are also becoming part of the illicit financing toolkit available to terrorists.[1] FDD's Center on Sanctions and Illicit Finance (CSIF) has now documented cryptocurrency fundraising campaigns run by social media entities associated with the Islamic State and al-Qaeda. Although public evidence indicates that terrorist groups have had only limited success so far with cryptocurrency fundraising efforts, the rising profile of digital currency has been accompanied by jihadist networks[2] experimenting with them more frequently. By preparing now for terrorists' increasing usage of cryptocurrencies, the U.S. can limit the ability to turn digital currency markets into a sanctuary for illicit finance. I will conclude my testimony today with specific recommendations for how the federal government and the private sector can address this challenge.

Terrorists Diversifying Their Portfolios

Terrorist groups regularly adapt their methods to their available resources, skill levels, and the opportunities presented in their target areas of operations. This is as true for financing as it is for plotting attacks. Terrorist organizations have a long history of exploiting banks and other traditional financial institutions, as well as semi-formal means of transferring funds, such as the *hawala* exchange system. But emerging financial technologies offer new channels to raise and move funds. Law enforcement officials and regulators have flagged cryptocurrencies for enabling illicit activity because of their pseudonymity and suitability for cyber crime and darknet marketplace transactions.[3]

The good news is that most terrorists, particularly those operating on jihadist battlefields, inhabit environments that are not currently conducive to cryptocurrency use. They usually need to purchase goods with cash (which is the most anonymous funding method), often in areas with unreliable technology infrastructure.[4] In addition, cryptocurrencies are based on distributed ledger (blockchain) technology, where users' pseudonymous transactions are recorded for public viewing.[5] This leaves a trail that unsophisticated users may find difficult to obfuscate. However, as digital currency usage grows, such barriers may fall away.

---

[1] This testimony mostly uses "cryptocurrencies" to refer to digital assets like Bitcoin that are based on a decentralized ledger blockchain system, but it is interchangeable with the terms "virtual currencies" and "digital currencies."

[2] This testimony focuses on terrorist organizations comprised of Salafi jihadist groups and networks.

[3] Rachel Rose O'Leary, "Europol Warns Zcash, Monero and Ether Playing Growing Role in Cybercrime," *CoinDesk*, October 3, 2017. (https://www.coindesk.com/europol-warns-zcash-monero-and-ether-playing-growing-role-in-cybercrime/)

[4] Zachary K. Goldman, Ellie Maruyama, Elizabeth Rosenberg, Edoardo Saravalle, and Julia Soloman-Strauss, "Terrorist Use of Virtual Currencies," *Center for a New American Security*, May 3, 2017. (https://www.cnas.org/publications/reports/terrorist-use-of-virtual-currencies)

[5] Generally speaking, each of the most popular cryptocurrencies have their own blockchain. For example, you can only view Bitcoin transactions on the Bitcoin blockchain and Ethereum transactions on the Ethereum blockchain.

For the moment, terrorist groups may lack the necessary skills to employ digital currencies more frequently and effectively. User friendliness is a challenge for this technology, whereas everyone knows how to use cash. Managing large amounts of cryptocurrency requires being extremely savvy in cyber security. For instance, to manage a cryptocurrency wallet, users must keep secure their digital private keys, which differ from regular passwords because they can never be replaced if forgotten.[6] If hackers acquire your private key and steal your digital currency, there is little one can do to retrieve the funds. Cryptocurrency prices are also volatile, and the broader public buys tokens more for speculation than purchasing real-world goods and services. Thus, operating financially with digital currencies remains a fringe activity both among the general public and within the population of global jihadists.

However, the minimal traction that cryptocurrencies have among jihadists should not be viewed as a steady-state condition. In recent years, I have observed multiple instances of jihadist groups trying to raise funds through cryptocurrencies. Although these networks have not raised much digital cash, I have watched them adapt and grow more sophisticated in their attempts to leverage financial technology. For example, some groups are moving beyond Bitcoin, the most popular cryptocurrency, to alternatives such as Monero that provide greater anonymity. There are only a few publicly verifiable cases of terrorists pursuing cryptocurrency financing, but these instances show that elements within jihadist networks are keenly aware of the technology's potential for secretive peer-to-peer and cross-border payments.

In 2014, Virginian teenager Ali Shukri Amin published a blog article explaining how supporters of the Islamic State could help fund the group by sending bitcoins through anonymous software wallets.[7] Amin was clearly an early technology adopter. He was an honor student who posted online advice about cyber security and encryption[8] and was accepted into a top college engineering program before his arrest.[9] He had thousands of Twitter followers, including jihadists in Iraq and Syria.[10] It is unclear how much Amin's Bitcoin tutorial directly impacted donations to the Islamic State, but it is one of the earliest signs of jihadists exploring how to exploit cryptocurrencies' pseudonymity.

Jahezona: First Terrorist Funding Campaign Publicly Visible on the Blockchain

In 2016, media reports surfaced that a consortium of jihadists in the Gaza Strip called the Mujahideen Shura Council (MSC) in the Environs of Jerusalem[11] began soliciting bitcoins for its

[6] Christine Masters, "Cryptocurrencies: Not User-Friendly Enough?" *Cryptovest*, August 23, 2017. (https://cryptovest.com/features/cryptocurrencies-not-user-friendly-enough/)
[7] U.S. Department of Justice, Press Release, "Virginia Teen Pleads Guilty to Providing Material Support to ISIL," June 11, 2015. (https://www.justice.gov/opa/pr/virginia-teen-pleads-guilty-providing-material-support-isil)
[8] Yasmeen Abutaleb and Kristina Cooke, "A teen's turn to radicalism and the U.S. safety net that failed to stop it," *Reuters*, June 6, 2016. (https://www.reuters.com/investigates/special-report/usa-extremists-teen/)
[9] Warren Richey, "One Virginia teen's journey from ISIS rock star to incarceration," *The Christian Science Monitor*, September 29, 2015. (https://www.csmonitor.com/USA/Justice/2015/0929/One-Virginia-teen-s-journey-from-ISIS-rock-star-to-incarceration)
[10] Warren Richey, "One Virginia teen's journey from ISIS rock star to incarceration," *The Christian Science Monitor,* September 29, 2015. (https://www.csmonitor.com/USA/Justice/2015/0929/One-Virginia-teen-s-journey-from-ISIS-rock-star-to-incarceration)
[11] David Barnett, "Ibn Taymiyyah Media Center returns to Facebook," *FDD's Long War Journal*, April 28, 2013. (https://www.longwarjournal.org/archives/2013/04/ibn_taymiyyah_media_center_ret.php)

weapons fundraising campaign known as *Jahezona*, (Arabic for "Equip Us").[12] The U.S. State Department designated the MSC as a foreign terrorist organization in 2014.[13] In 2016, the U.S. Treasury Department designated one of MSC's leaders for facilitating funding on behalf of the Islamic State.[14]

The MSC's media outlet posted infographics for the Jahezona campaign on Twitter and Telegram, listing the prices for rockets, rifles, grenades, and other gear for militants.[15] One effort sought to raise $2,500 per fighter. Some of the Twitter infographics gave an option to pay in Bitcoin, providing a QR code linked to the campaign's Bitcoin address.[16]

Because the QR code was visible on the Twitter posts, we were able to pull up the address and monitor its transactions on the Bitcoin blockchain. We discovered that after a few weeks of soliciting on social media, the address received only two deposits, totaling a little over $500 in Bitcoin. The *Jahezona* cryptocurrency crowdfunding campaign fell far short of its aim of raising $2,500 per fighter. Still, the *Jahezona* case is significant because it was the first time a Bitcoin funding campaign was definitively associated with a terrorist group, with a Bitcoin address publicly verified and observable during the campaign.[17]

By analyzing the *Jahezona* transactions on the Bitcoin blockchain,[18] CSIF was able to identify the cryptocurrency exchange where the deposits originated: a European exchange website named BTC-e known for facilitating money laundering. A joint U.S. law enforcement operation shut down BTC-e a year later for multiple illicit financing crimes.[19] Typically, media attention on terrorist funding campaigns would cause banks to close the associated accounts and scare off donors. But unlike money service businesses and bank accounts, cryptocurrency addresses operate by open-source software and cannot be shut down by a third party. Cryptocurrency wallets are managed by whoever controls the private digital key passcode. Even if law enforcement is aware

[12] "Fundraising Campaign to Arm Jihadis in Gaza Solicits Donations Via Bitcoin," *MEMRI Cyber and Jihad Lab*, July 8, 2016. (http://cjlab.memri.org/lab-projects/tracking-jihadi-terrorist-use-of-social-media/fundraising-campaign-to-arm-jihadis-in-gaza-solicits-donations-via-bitcoin/)
[13] U.S. Department of State, Press Release, "Terrorist Designation of the Mujahidin Shura Council in the Environs of Jerusalem (MSC)," August 19, 2014. (https://www.state.gov/j/ct/rls/other/des/266549.htm)
[14] U.S. Department of the Treasury, Press Release, "Treasury Sanctions Key ISIL Leaders and Facilitators Including a Senior Oil Official," February 11, 2016. (https://www.treasury.gov/press-center/press-releases/Pages/jl0351.aspx)
[15] "Salafi-Jihadis Conduct Online 'Equip Us' Campaign to Raise Funds for Jihad in Gaza," *MEMRI Cyber and Jihad Lab*, December 16, 2015. (http://cjlab.memri.org/lab-projects/monitoring-jihadi-and-hacktivist-activity/salafi-jihadis-conduct-online-equip-us-campaign-to-raise-funds-for-jihad-in-gaza/)
[16] Yaya Fanusie, "The New Frontier in Terror Fundraising: Bitcoin," *The Cipher Brief*, August 24, 2016. (https://www.thecipherbrief.com/column_article/the-new-frontier-in-terror-fundraising-bitcoin)
[17] Prior to the *Jahezona* campaign, there were media reports about the Islamic State using Bitcoin, but these claims could not be independently corroborated. It is quite common for scammers to create fake jihadist campaigns as moneymaking schemes. For our analysis, we considered a terrorist cryptocurrency campaign to be real if an established jihadist media channel promoted it.
[18] Yaya Fanusie, "The New Frontier in Terror Fundraising: Bitcoin," *The Cipher Brief*, August 24, 2016. (https://www.thecipherbrief.com/column_article/the-new-frontier-in-terror-fundraising-bitcoin)
[19] U.S. Department of Justice, Press Release, "Russian National And Bitcoin Exchange Charged In 21-Count Indictment For Operating Alleged International Money Laundering Scheme And Allegedly Laundering Funds From Hack Of Mt. Gox," July 26, 2017. (https://www.justice.gov/usao-ndca/pr/russian-national-and-bitcoin-exchange-charged-21-count-indictment-operating-alleged)

of an illicit address, authorities cannot freeze the account and cannot move funds without the private key.

Although the Mujahideen Shura Council has not recently published the *Jahezona* address on social media channels, it continues to receive deposits every month or so, usually in the low hundreds of dollars. It is unclear if the group still controls this address, but as of early September 2018, it contained over $1,000 in Bitcoin.

Jihadist Networks Crowdfunding Cryptocurrencies in Syria

The price of Bitcoin began to skyrocket in late 2017, with the price of one bitcoin hitting $10,000 for the first time last November.[20] Rising prices generated media attention, which in turn fed higher prices and greater hype.[21] This appeared to have the attention of jihadist networks.

Late last year, CSIF was notified by cryptocurrency analytics firm Elliptic (with whom we were collaborating on a research project on Bitcoin laundering) that some jihadist social media channels recently posted requests for Bitcoin funding. Our team looked into these postings[22] and initially saw little activity in the addresses, especially after social media platforms deleted their posts and accounts. However, one campaign associated with al-Qaeda[23] stood out because of its frequent posting of slick photo graphics and videos on Telegram. Calling itself *al-Sadaqa* (Arabic for "the Charitable Giving"), the group claimed to be raising funds for fighters in Syria. It transmitted its messages in English. It even posted quotes from now-deceased American al-Qaeda propagandist Anwar al-Awlaki.

CSIF monitored *al-Sadaqa's* social media channels (its initial Telegram channel was deleted, but it resurfaced within days under a new username). We also monitored and analyzed the group's Bitcoin address, which it highlighted regularly, asking followers to "donate anonymously with Bitcoin." In its initial campaigning, *al-Sadaqah* sought $750 for camp reinforcements. Within weeks, we noticed the address received about $685 worth of Bitcoin, which it soon sent to another address.

The *al-Sadaqah* group continued requesting funding for a variety of logistical supplies, sometimes publishing videos claiming to show fighters' encampments in the mountains. But it only received a handful of Bitcoin transactions, none as large as the $685 early in its campaign.

[20] Evelyn Cheng, "Bitcoin surpasses $10,000 for the first time," *CNBC*, November 29, 2017. (https://www.cnbc.com/2017/11/28/bitcoin-surpasses-10000-for-the-first-time.html)
[21] Nathaniel Popper, "Bitcoin's Price Has Soared. What comes Next?" *The New York Times*, December 7, 2017. (https://www.nytimes.com/2017/12/07/technology/bitcoin-price-rise.html)
[22] Michael del Castillo, "Think Tank Links rising Bitcoin Price to Terrorist Use," *CoinDesk*, December 21, 2017. (https://www.coindesk.com/u-s-think-tank-finds-rising-bitcoin-price-linked-terrorist-interest/)
[23] "Online Campaign in English Raising Funds for the Jihad in Syria in Bitcoin," *MEMRI Cyber and Jihad Lab*, November 13, 2017. (http://cjlab.memri.org/latest-reports/online-campaign-in-english-raising-funds-for-the-jihad-in-syria-in-bitcoin/)

Jihadists Adjusting Their Cryptocurrency Crowdsourcing Methods

Although the *al-Sadaqah* case may have been as unsuccessful as the *Jahezona* campaign a year prior, it demonstrated how jihadists may adjust when their cryptocurrency campaigns are unsuccessful. In monitoring *al-Sadaqah's* activity, we noticed that as its Bitcoin address lagged in receiving donations, the group introduced new techniques for supporters to give funds. Since Bitcoin blockchain transactions are public, most supporters – especially newcomers to cryptocurrency use – probably were hesitant to donate for fear of being detected by law enforcement or intelligence agencies.

It appears that *al-Sadaqah* tried to address this concern. At one point, the group encouraged followers to purchase Bitcoin vouchers for a gaming website that took payment in euros. Instead of sending Bitcoin directly, supporters could purchase the voucher and share with *al-Sadaqah*, which would use it to access the Bitcoin funds. The group also posted sites where supporters could locate Bitcoin ATMs to buy cryptocurrencies. Clearly, the campaign organizers were trying to make the Bitcoin-buying process easier for novices.

Al-Sadaqah's most significant adaptation was eventually branching out beyond Bitcoin. By early 2018, the group posted on Telegram that it was also accepting other cryptocurrencies like Monero, Verge, and Dash. These other tokens use varying types of anonymization techniques that make their transactions less traceable than Bitcoin.[24] However, *al-Sadaqah* kept the Bitcoin address on their infographics. An exception was a rare post of the group's Monero address. However, the Monero blockchain allows no views into its transactions. Even with the address, we could not determine how much it had received.

Also, *al-Sadaqah* did not just stick to cryptocurrency. With donations scarce, it soon announced ways to receive cash and money service transfers. To access those methods, supporters would have to communicate with the *al-Sadaqah* Telegram administrator via encrypted messaging. Thus, with more anonymous cryptocurrencies and other transmission methods in play, it is very difficult to assess *al-Sadaqah's* true funding level.

Another militant group in Syria appears to be following in *al-Sadaqah's* cryptocurrency footsteps. In mid-2018, CSIF noticed an organization called Malhama Tactical soliciting donations on Twitter.[25] Malhama Tactical is a private military contractor that caters to jihadists in Syria.[26] It was founded in 2016 by an Uzbek who served in the Russian military before leaving to join rebels in Syria in 2013.[27] The group has trained various al-Qaeda-affiliated fighters. Though it initially

[24] Kai Sedgwick, "Everything You Ever Wanted to Know About Privacy Coins," *Bitcoin News*, December 30, 2017. (https://news.bitcoin.com/everything-ever-wanted-know-privacy-coins/)
[25] Miles, "Revival of Insurgent Training Team Malhama Tactical," *The Firearm Blog*, July 2, 2018. (https://www.thefirearmblog.com/blog/2018/07/02/revival-of-insurgent-training-team-malhama-tactical/)
[26] Jonathan Rugman, "The firm that serves a jihadist clientele," *Channel 4 News*, April 3, 2017. (https://www.channel4.com/news/the-firm-that-serves-a-jihadist-clientele)
[27] Rao Komar, Christian Borys, and Eric Woods, "The Blackwater of Jihad," *Foreign Affairs*, February 10, 2017. (https://foreignpolicy.com/2017/02/10/the-world-first-jihadi-private-military-contractor-syria-russia-malhama-tactical/)

relied on contracts to train and support militants, the group started asking for donations amidst a financial crunch in 2017.[28]

The group's founder reportedly was killed in 2017, but it is now led by someone calling himself Abu Salman Belarus whom we discovered is one of *al-Sadaqah's* social media followers. Abu Salman gives updates about Malhama Tactical through his Twitter account, often in Russian. In June 2018, Abu Salman tweeted a Bitcoin address for Malhama Tactical donations, but it was later deleted. We reviewed the address and found it had received only a few transactions and had less than $100 worth of Bitcoin. We last saw the Twitter account seek Bitcoin donations in early August, but instead of listing the actual address, this time Abu Salman asked supporters to contact him via direct message for details.

Jihadist Media Outlets Tapping Cryptocurrency Technology

It is not just fighters that terrorist networks seek to support with cryptocurrencies. Salafi jihadist media sites are integrating Bitcoin campaigns into their platforms. In late November 2017, the pro-Islamic State Arabic website *Akhbar al-Muslimeen* (Arabic for "News of the Muslims") published a link for Bitcoin donations, according to an Israeli research institute.[29] *Akhbar al-Muslimeen* frequently publishes videos of Islamic State attacks and other jihadist propaganda. The donation link was connected to a page at a mainstream Bitcoin payment processor site. The link was soon removed, probably after the payment processor became aware that one of its customers was a terrorist media outlet.

However, the *Akhbar al-Muslimeen* administrators adjusted by keeping hyperlinks on the site reading, "Donate to site, servers are costly" above many articles. These links led readers to a page generating multiple Bitcoin addresses. Supporters could then copy these addresses and donate to them directly, away from the page. This showed some technical sophistication on the part of site administrators who eliminated their dependence on a Bitcoin payment processing site. In addition, generating many different Bitcoin addresses was likely designed to make it harder for outsiders to monitor donations. We identified a few dozen addresses created by the site, but most of them had no donations.

In December 2017, a jihadist website monitoring group reported that a separate Islamic State-affiliated website called *Isdarat* was requesting bitcoins.[30] The *Isdarat* website can only be viewed on the dark web via a Tor browser.[31] The site also uses multiple Telegram channels to disseminate

[28] Jonathan Rugman, "The firm that serves a jihadist clientele," *Channel 4 News*, April 3, 2017. (https://www.channel4.com/news/the-firm-that-serves-a-jihadist-clientele)
[29] "Drive for Bitcoin donations on an Isis-affiliated website," *The Meir Amir Intelligence and Terrorism Information Center*, December 6, 2017. (https://www.terrorism-info.org.il/app/uploads/2017/12/E_235_17.pdf)
[30] New Jersey Office of Homeland Security and Preparedness, "Female HVEs Likely to Play Supportive Role for ISIS," July 10, 2018. (https://www.waterisac.org/system/files/articles/Female%2BHVEs%2BSupport%2Bof%2BISIS%2B%287.23.2018%29.pdf)
[31] Anthony Cuthbertson, "Hackers replaced ISIS propaganda on the dark web with advertisements for an online pharmacy," *Business Insider*, November 5, 2015. (http://www.businessinsider.com/hackers-replaced-isis-propaganda-on-the-dark-web-with-advertisements-for-an-online-pharmacy-2015-11)

Islamic State videos and other propaganda.[32] Media sources did not publish the Bitcoin address, so it is unclear how much, if any, Bitcoin *Isdarat* raised.

Detection Does Not Necessarily Stop Cryptocurrency Campaigning

As mentioned above, a challenge with cryptocurrency addresses for counterterrorist financing is that digital wallets cannot be shut down by an outside party without acquiring private keys. Although *al-Sadaqah* was exposed by my published research[33] and in major outlets like the *Wall Street Journal*,[34] it continues to seek funds for its Bitcoin address on social media, showing that the group probably controls its private key.

This response differs from the terror funding activity discovered in the early years after the September 11 attacks. Previously, when they worked exclusively through the conventional banking system, terrorist-supporting charities that were detected by law enforcement or exposed in the press often had their funding channels quickly neutralized.[35]

Mixing Cryptocurrencies with Conventional Illicit Financing Schemes

Cryptocurrencies can be part of a mix of deceptive financial tools to obscure donors' intentions of terrorist funding. Last year, a Long Island, NY woman tried to send money to the Islamic State by acquiring fraudulent loans and credit cards.[36] She used the credit cards to purchase $62,000 worth of cryptocurrencies that she laundered into fiat money and sent as wire transfers to contacts in Pakistan, China, and Turkey. The fact that she sent funds through a banking infrastructure to her contacts instead of directly via cryptocurrencies shows that jihadist groups, while experimenting with digital currency, remain more comfortable with conventional financial tools.

Illicit finance investigators should also keep in mind that the cryptocurrency space is replete with scams. Sometimes, cyber criminals impersonate terrorists as a ploy to gain funding from extremists. In late August 2018, an independent researcher uncovered a site on the darknet called Sadaqa Coins claiming to be a marketplace for crowdfunding jihadist projects.[37] The site sought donations in Bitcoin, Ethereum, and Monero and claimed that funds would pay for weapons, sniper gear, vehicles, and computer equipment. However, one darknet technical expert reviewing the site

[32] Riyadh Mohammed, "ISIS Has a New Favorite Social media Network," *The Fiscal Times*, November 5, 2015. (http://www.thefiscaltimes.com/2015/11/03/ISIS-Has-New-Favorite-Social-Media-Network)
[33] Yaya Fanusie, "Terrorist Networks Eye Bitcoin as Cryptocurrency's Price Rises," *The Cipher Brief*, December 21, 2017. (https://www.thecipherbrief.com/article/exclusive/international/terrorist-networks-eye-bitcoin-cryptocurrencys-price-rises)
[34] Brett Forrest and Justin Scheck, "Jihadists See a Funding Boon in Bitcoin," *The Wall Street Journal*, February 20, 2018. (https://www.wsj.com/articles/jihadists-see-a-funding-boon-in-bitcoin-1519131601)
[35] U.S. Department of the Treasury, Press Release, "Fact Sheet: Designations of Somalia and Bosnia-Herzegovina Branches of Al-Haramain Islamic Foundation," March 11, 2002. (https://fas.org/irp/news/2002/03/dot031102fact.html)
[36] U.S. Department of Justice, Press Release, "Long Island Woman Indicted for Bank Fraud and Money Laundering to Support Terrorists," December 14, 2017. (https://www.justice.gov/usao-edny/pr/long-island-woman-indicted-bank-fraud-and-money-laundering-support-terrorists)
[37] Benjamin Strick, "Meet The World's First Jihadi Cryptocurrency Crowdsource Site On The Dark Web: SadaqaCoins," *Medium*, August 23, 2018. (https://medium.com/@benjamindbrown/first-jihadi-cryptocurrency-crowdsource-platform-on-dark-web-263edf8885b7)

assessed that it was most likely a scam and unrelated to real jihadist groups.[38] As scams increase, it will be crucial for investigators to determine if cryptocurrency campaigns are truly linked to known jihadist networks.

Recommendations

The above cases make a few things clear. One, terrorist organizations are looking to add cryptocurrency donations to their funding streams. Two, their efforts thus far have not be very fruitful, probably because cryptocurrencies' technical complexities, extremists' preference for cash, and the traceability of most blockchain protocols deter wider usage.

This is to be expected. Although cryptocurrencies have grown the past few years as a speculative asset class,[39] their daily use for purchasing goods and services is minimal.[40] Terrorist adoption of cryptocurrencies simply mirrors that of the general public. This also means that if public cryptocurrency adoption increases, terrorist groups will probably begin to transact more in digital tokens.

But cryptocurrencies and blockchain technology are not innately illicit and should not be feared. Like most technological innovations, they can be utilized for good or ill, depending on the user. Our adversaries, both state[41] and non-state actors, are building blockchain-based tools to advance their interests. The U.S. must keep up with this technology and address new risks emerging from an evolving financial ecosystem. Below are some actions that policymakers and the tech industry should take to mitigate risk.

Counter-Threat Financing Units Must Learn Blockchain Analysis. All units in U.S. government agencies that investigate terrorist funding should become proficient in analyzing cryptocurrency transactions. Public blockchain transactions can usually be viewed on "block explorer" websites.[42] Although cryptocurrency users operate pseudonymously, investigators can review the flows recorded on the blockchain for insight into suspects' behavior and their financial relationships.

While cryptocurrencies are not expected to displace conventional means of terror financing anytime soon, terrorists will likely use them if they grow more accepted for real-world goods and services. Therefore, all agencies with counter-threat financing groups should have dedicated analysts who specialize in blockchain analysis. Today, investigators have at their disposal not only free block explorer websites, but also various blockchain forensics firms they can leverage for

[38] Chris Monteiro, "There are still no credible dark web jihadi sites," *Pirate dot London*, August 25, 2018. (https://pirate.london/there-are-still-no-credible-dark-web-jihadi-sites-b2bcf1fbf22d)
[39] Nathaniel Popper, "Here's Some Cryptocurrency. Now Please Use It," *The New York Times*, July 1, 2018. (https://www.nytimes.com/2018/07/01/technology/cryptocurrency-ripple.html)
[40] Kenny Li, "Today's Big Problem with Cryptocurrency Adoption," *Hackernoon*, July 21, 2018. (https://hackernoon.com/todays-big-problem-with-cryptocurrency-adoption-7c9ab96a7779)
[41] Yaya Fanusie, "Blockchain Authoritarianism: The Regime In Iran Goes Crypto," *Forbes*, August 15, 2015. (https://www.forbes.com/sites/yayafanusie/2018/08/15/blockchain-authoritarianism-the-regime-in-iran-goes-crypto/#605c8f0e3dc6)
[42] Ofir Beigel, "A list of 8 Block explorers and what are they exactly?" *99 Bitcoins*, July 3, 2018. (https://99bitcoins.com/block-explorer-blockchain-browser/)

analysis. To mitigate any terrorist use of cryptocurrencies, the U.S. and its partners must get smart on the world of the blockchain.

Financial Authorities Should Engage More Cryptocurrency Exchanges. U.S. financial regulators and law enforcement must increase their engagement with cryptocurrency exchanges, which are where most people purchase digital currency. Many exchanges have ramped up their anti-money laundering compliance the past few years,[43] but many smaller exchanges trade in a greater variety of alternative tokens, including so-called "privacy coins."[44] Many of these newer exchanges also use more experimental software allowing fully decentralized, peer-to-peer trading[45] that lacks customer identification verification.[46] These decentralized exchanges currently have very little volume and some experts say they may not become widely used in the cryptocurrency space for quite a few years.[47] However, if decentralized exchanges flourish as fully anonymous platforms, they will be more attractive to those seeking to use cryptocurrency for illicit purposes. Thus, the cryptocurrency space appears to be evolving into two ecosystems: one growing more AML-compliant and one going more underground, developing less transparency.[48]

At FDD's Center on Sanctions and Illicit Finance, we have been facilitating conversations between government policymakers and blockchain technology leaders on illicit finance risks and national security threats. Many within the industry want to keep terrorists and other bad actors off their platforms. Financial authorities should work with those firms to protect citizens from terrorism without stifling technological innovation.

Cryptocurrency Enthusiasts Should Flag Illicit Wallets. Cryptocurrency addresses are easily and randomly software-generated, making them too numerous for a single investigative team to identify all suspect transactions. Law-abiding cryptocurrency exchanges are incentivized to prevent illegal transactions on their platforms, but do not have the capacity to identify all illicit addresses on every blockchain. And while blockchain forensics firms offer tools for exchanges to flag illicit activity, these tools are usually proprietary, focusing on just a handful of blockchain systems. Moreover, known illicit addresses operating on different blockchains are not shared freely among all exchanges and law enforcement agencies.

---

[43] Yaya Fanusie and Tom Robinson, "Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services," *Foundation for Defense of Democracies and Elliptic*, January 12, 2018. (http://www.defenddemocracy.org/content/uploads/documents/MEMO_Bitcoin_Laundering.pdf)

[44] Yaya Fanusie, "Good Crypto, Bad Crypto: Blockchain Projects Gaining Legitimacy While Spawning an Underground," *Forbes*, July 12, 2018. (https://www.forbes.com/sites/yayafanusie/2018/07/12/good-crypto-bad-crypto-blockchain-projects-gaining-legitimacy-while-spawning-an-underground/#3813ca4b1078)

[45] Nathan Sexer, "State of Decentralized Exchanges, 2018," *Consensys*, January 31, 2018. (https://media.consensys.net/state-of-decentralized-exchanges-2018-276dad340c79)

[46] Gary Basin, "The State of Decentralized Exchanges," *Hackernoon*, June 21, 2018. (https://hackernoon.com/the-state-of-decentralized-exchanges-235064446ab0)

[47] Gary Basin, "Decentralized Exchanges-FinCEN, Payment Channels, and Custody, Oh My!" *Hackernoon*, July 4, 2018. (https://hackernoon.com/decentralized-exchanges-fincen-payment-channels-and-custody-oh-my-1ae3d83bc42a)

[48] Yaya Fanusie, "Good Crytpo, Bad Crypto: Blockchain Projects Gaining Legitimacy While Spawning an Underground," *Forbes*, July 12, 2018. (https://www.forbes.com/sites/yayafanusie/2018/07/12/good-crypto-bad-crypto-blockchain-projects-gaining-legitimacy-while-spawning-an-underground/#2579dbc41078)

To address this gap, enthusiasts who care about the integrity of the cryptocurrency industry should flag activity associated with terrorists and other illicit actors. There should be one repository, perhaps developed by entrepreneurs in the private sector, where everyday users can flag illicit addresses from various blockchain systems. Of course, such a site should be built with protocols that review and vet submissions for credibility before publishing them. Such a resource would make it easier for investigators to find illegal activity and help everyday cryptocurrency users stay clear of problematic wallets. In fact, such a resource could be built as a blockchain-based platform, where registered users who credibly report illicit activity are rewarded with a cryptocurrency token. This could be applied not only to flag terrorist transactions, but also to hinder coins associated with ransomware and cyber criminals from moving throughout the blockchain.

Conclusion

Cold hard cash is still king, but jihadist groups are building diverse portfolios. Illicit actors adopt new technologies earlier than the broader public. When paper checks, credit cards, and PayPal each emerged, criminals exploited them early on. There are enough case studies of jihadist groups experimenting with cryptocurrencies to suggest that law enforcement and the intelligence community must prepare for terrorists to try to exploit digital tokens as the technology spreads.

On behalf of the Foundation for Defense of Democracies and its Center on Sanctions and Illicit Finance, thank you for the opportunity to testify. I look forward to your questions.