TERRORISM AND CRYPTOCURRENCY: INDUSTRY PERSPECTIVES

HEARING

BEFORE THE

SUBCOMMITTEE ON INTELLIGENCE AND COUNTERTERRORISM

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTEENTH CONGRESS

SECOND SESSION

JUNE 9, 2022

Serial No. 117–59

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE

48–616 PDF WASHINGTON : 2022

COMMITTEE ON HOMELAND SECURITY

BENNIE G. THOMPSON, Mississippi, *Chairman*

SHEILA JACKSON LEE, Texas
JAMES R. LANGEVIN, Rhode Island
DONALD M. PAYNE, JR., New Jersey
J. LUIS CORREA, California
ELISSA SLOTKIN, Michigan
EMANUEL CLEAVER, Missouri
AL GREEN, Texas
YVETTE D. CLARKE, New York
ERIC SWALWELL, California
DINA TITUS, Nevada
BONNIE WATSON COLEMAN, New Jersey
KATHLEEN M. RICE, New York
VAL BUTLER DEMINGS, Florida
NANETTE DIAZ BARRAGÁN, California
JOSH GOTTHEIMER, New Jersey
ELAINE G. LURIA, Virginia
TOM MALINOWSKI, New Jersey
RITCHIE TORRES, New York
JOHN KATKO, New York
MICHAEL T. MCCAUL, Texas
CLAY HIGGINS, Louisiana
MICHAEL GUEST, Mississippi
DAN BISHOP, North Carolina
JEFFERSON VAN DREW, New Jersey
MARIANNETTE MILLER-MEEKS, Iowa
DIANA HARSHBARGER, Tennessee
ANDREW S. CLYDE, Georgia
CARLOS A. GIMENEZ, Florida
JAKE LATURNER, Kansas
PETER MEIJER, Michigan
KAT CAMMACK, Florida
AUGUST PFLUGER, Texas
ANDREW R. GARBARINO, New York
VACANCY

HOPE GOINS, *Staff Director*
DANIEL KROESE, *Minority Staff Director*
NATALIE NIXON, *Committee Clerk*

SUBCOMMITTEE ON INTELLIGENCE AND COUNTERTERRORISM

ELISSA SLOTKIN, Michigan, *Chairwoman*

SHEILA JACKSON LEE, Texas
JAMES R. LANGEVIN, Rhode Island
ERIC SWALWELL, California
JOSH GOTTHEIMER, New Jersey
TOM MALINOWSKI, New Jersey
BENNIE G. THOMPSON, Mississippi *(ex officio)*
AUGUST PFLUGER, Texas, *Ranking Member*
MICHAEL GUEST, Mississippi
JEFFERSON VAN DREW, New Jersey
JAKE LATURNER, Kansas
PETER MEIJER, Michigan
JOHN KATKO, New York *(ex officio)*

BRITTANY CARR, *Subcommittee Staff Director*
ADRIENNE SPERO, *Minority Subcommittee Staff Director*
JOY ZIEH, *Subcommittee Clerk*

CONTENTS

TERRORISM AND CRYPTOCURRENCY: INDUSTRY PERSPECTIVES

Thursday, June 9, 2022

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON INTELLIGENCE
AND COUNTERTERRORISM,
Washington, DC.

The subcommittee met, pursuant to notice, at 9:01 a.m., in room 310 Cannon House Office Building, Hon. Elissa Slotkin [Chairwoman of the committee] presiding.

Present: Representatives Slotkin, Langevin, Gottheimer, Pfluger, Van Drew, LaTurner, and Meijer.

Chairwoman SLOTKIN. OK. Lovely to see you all. Good morning. The Subcommittee on Intelligence and Counterterrorism is meeting today on a hearing entitled, "Terrorism and Cryptocurrency: Industry Perspectives". Nearly a year ago this subcommittee received testimony from the Department of Homeland Security on how they are addressing this important issue. Today I am glad to welcome the Blockchain Association, Chainalysis, and Coinbase to share a couple of things with us.

First, what trends the cryptocurrency and blockchain industry have observed regarding terrorist and illicit use, how the industry works to prevent such use, and how it partners with the Government in this endeavor.

In full transparency, last week I introduced the Cryptocurrency Accountability Act. This was to ensure that as the investment in cryptocurrency grows Members of Congress are required to disclose all holdings and trades, similarly, to the way we are required to disclose normal stock trades. The goal is just to improve transparency and help stop corruption that erodes confidence in our Government.

Now, while this is a separate issue from what we are discussing today, I think it speaks to the bigger sort-of context for our hearing today, which is the issue of cryptocurrency and blockchain technology is really a new space, certainly for Members of Congress. You know, I like to joke that sometimes our committee Chairs are from the flip phone generation. We are just kind-of catching up on the left and right limits that we should put down on social media is new, let alone things like cryptocurrencies and blockchain technology. Because it really is such a new field, there is a lack of frankly understanding of oversight of regulation. I think what we are all concerned about is what is the right space for the U.S. Congress to provide oversight, what is the right approach. I don't think

there is any unanimity on the answer to that. As I have expressed to some of you, I think that on any given day up on Capitol Hill, you can hear how cryptocurrencies and blockchain analysis are going to change the world and they are going to be bigger than the internet and it is going to revolutionize everything we know. Then on the same day you can hear people truly dismissive cryptocurrencies and saying that it is, you know, a Ponzi scheme. So there is really not a consensus view and a baseline understanding to begin with.

So because of that, this committee's purview is making sure bad actors don't have new avenues to exploit to carry out activities that affect the U.S. homeland, U.S. allies, and U.S. partners.

I am a former CIA officer. My Ranking Member here is a former military officer. So we both have strong interest in making sure bad guys don't have new ways to threaten us and to fund their bad activity. So for the purposes of this hearing, that is really our focus. Trying to hear directly from the industry, in addition to others that we will and have heard from, what the space looks like in terms of terrorists and other bad actors, criminals, seeking to exploit this technology.

The sort-of breadcrumbs of cryptocurrency are showing up everywhere in our districts. As I have expressed to some of you, you can drive through some of the smaller cities of Michigan where I am from and see bitcoin ATMs at all kinds of gas stations. I think a lot of people don't totally understand what those are. Even as recently as this week, the Michigan legislature had passed a bill requiring that Michigan students take a financial literacy course as part of their education because: (a) That is just a good thing to do, but (b) it has never been easier for a young person to trade stock and to invest in things like cryptocurrency. It was listed by name in that way. So it is very much kind-of seeping into the average person's life.

According to the analysis of the U.S. Federal Trade Commission, consumers reported losing more than $1 billion to fraud involving cryptocurrencies from January 2021 through March 2022. As related to illicit or illegal use, Chainalysis, most recent crypto crime trends report found that illicit or illegal use of cryptocurrencies made up a mere .15 percent of all crypto activity in 2021, although I understand that others in the Federal Government may have slightly different number. Nevertheless, according to the report, even at that low percentage point, the raw value of the illicit transaction volume has reached its highest level ever at $14 billion, up from $7.8 billion just in 2020. So the trend is certainly going up.

Regarding terrorism, specifically in 2020 U.S. authorities seized millions of dollars over 300 cryptocurrency accounts connected to groups like Hamas, al-Qaeda, and ISIS. So here you understand our concern. This is not small potatoes to us for providing oversight issues related to terrorism.

At our hearing last year this subcommittee heard how DHS is in particular investigating terrorists and illicit use of cryptocurrency and provide State, local, Tribal, territorial, and private-sector partners with information necessary to try and combat the use, but nothing is more helpful to us and important to us than to hear directly from you all in the industry to tell us what you are seeing,

to hopefully be transparent about what you are monitoring, what you are seeing are the trends in crypto and blockchain technology, and maybe the novel ways you are countering some of these potential exploitation routes.

Our committee wants to be a partner. I think I told all of you before the hearing that I personally—and I don't—I think I can speak for my Ranking Member, we don't have an agenda, we are not for, we are not against, we are—this is new territory and part of this hearing is to publicly have the conversation about this. Since it is so new, I think it is partly just to educate and hear from voices.

So we are ready to partner with you to help educate us up here, but also educate the public on how we can crack down on any and all illicit use of cryptocurrencies.

[The statement of Chairwoman Slotkin follows:]

STATEMENT OF CHAIRWOMAN ELISSA SLOTKIN

JUNE 9, 2022

The Subcommittee on Intelligence and Counterterrorism will be in order. The subcommittee is meeting today on "Terrorism and Cryptocurrency: Industry Perspectives."

Without objection, the Chair is authorized to declare the subcommittee in recess at any point.

Good morning.

Nearly a year ago, the subcommittee received testimony from Department of Homeland Security officials on how they are addressing this important issue.

Today, I am glad to welcome The Blockchain Association, Chainalysis, and Coinbase, to share with us:

- what trends the cryptocurrency and blockchain industry has observed regarding terrorist and illicit use;
- how the industry works to prevent such use; and
- how it partners with Government in this endeavor.

Last week, I introduced the "Cryptocurrency Accountability Act" to ensure that as the use of cryptocurrency grows, Members of Congress are required to disclose all holdings and trades. The goal is to improve transparency and help stop corruption that erodes confidence in our Government.

Now, while this is a related but separate issue from what we are discussing today, it speaks to the fact that the laws and regulations that govern traditional financial institutions do not always apply to cryptocurrency exchanges and the crypto industry.

Because of the lack of regulation and the idea that cryptocurrency and blockchain technology provide a level of anonymity, bad actors, terrorists, criminals seek to exploit the technology.

In my home State of Michigan, there are Bitcoin ATMs, which as I understand it, are simply kiosks through which you can make Bitcoin purchases and sales. Unlike bank ATMs, Bitcoin ATMs do not require users to have an account to use them.

I am curious to know if these ATMs are really offering legitimate alternatives to financially manage day-to-day life or if they are just another way for illicit financial actors to take advantage of people.

According to analysis by the U.S. Federal Trade Commission, consumers reported losing more than $1 billion to fraud involving cryptocurrencies from January 2021 through March 2022.

As related to illicit or illegal use, Chainalysis' most recent Crypto Crime Trends report found that illicit or illegal use of cryptocurrency made up a mere 0.15 percent of all cryptocurrency activity in 2021. Although, I understand that some in the Federal Government believe the percentage could be a bit higher.

Nevertheless, according to the Chainalysis report, even at that low percentage point, the raw value of illicit transaction volume has reached its highest level ever at $14 billion—up from $7.8 billion in 2020.

Regarding terrorism specifically, in 2020 U.S. authorities seized millions of dollars, over 300 cryptocurrency accounts, connected to Hamas's military wing, al-Qaeda, and ISIS.

That's not small potatoes.

At the subcommittee's hearing last year, my colleagues and I heard how DHS, in particular, investigates terrorist and illicit use of cryptocurrency and provides State, local, Tribal, territorial, and private-sector partners with information necessary to combat such use.

Today, I look forward to hearing from our witnesses about how you are monitoring and investigating exploitation of crypto and blockchain and the novel ways in which you are countering misuse.

Our subcommittee stands ready to partner with you to take on this challenge.

The Chair now recognizes the Ranking Member of the subcommittee, the gentleman from Texas, Mr. Pfluger, for an opening statement.

Chairwoman SLOTKIN. With that, I now recognize the Ranking Member, Mr. Pfluger, from Texas, for his opening remarks.

Mr. PFLUGER. Thank you, Madam Chair. I appreciate you holding this hearing today. I would also like to thank our witnesses from Chainalysis, the Blockchain Association, and Coinbase. Thank you for your time.

Totally support the comments made by the Chair on making sure that we understand, fully have a good transparent conversation, and don't rush into policy without knowing the facts first. I think that today should be a productive conversation on innovative solutions and that we can use the ideas heard today to provide safeguards against terrorists and other adversaries' use of crypto as a tool to evade the current law.

The battle against terror financing and illicit activity is not a new one. We all know that. But the creation of cryptocurrency has introduced additional complications to that fight and cryptocurrency can provide both security and anonymity in financial transactions, making it an alluring tool for the nefarious actors around the world.

Chainalysis reported that in 2021 illicit addresses received $14 billion through cryptocurrency—an all-time high. Between ransomware payments, the dark net market, sanctions evasion, and terrorism financing, we are combatting bad actors from a variety of multiple angles. Congress is notorious for being one step behind when it comes to new technologies, but we cannot afford to play catch up when it comes to any of these issues, and especially the pace and the speed at which they are accelerating and changing. That is why we are meeting with industry leaders today, to fully understand the scope of the problem and the challenges and then also to find innovative solutions to close that gap in the illicit activities involving digital assets.

At the end of this hearing, like the Chair mentioned, I hope to understand what we should expect going forward, what trends we are seeing in terms of terrorist use of digital assets and how the public and private sectors can better work together and collaborate on stopping those bad actors.

Given the global threat picture, we also cannot overlook the foreign nation-states who are attempting to use crypto to line their own pockets, essentially evading sanctions as well.

I would like to hear more from the panel about Iranian efforts to utilize crypto mining and understand what the outlook is for Russia's use of similar methods. What steps are being taken in the private sector already to ensure that crypto isn't a back door to America's use of soft power at a time when sanctions enforcement is an important tool in our foreign policy?

With that said, it is imperative that we remember regulation should not be implemented hastily. I think that is the purpose of today's conversation. I applaud the efforts of colleagues like Senator Lummis, who has long worked on industry regulation. As legislators it is incumbent upon us to protect our constituents in the American way of life while supporting private-sector growth and the U.S. economy. We must pursue the least burdensome regulatory path while also ensuring safety and security.

I look forward to our discussion today. I hope that the committee can support the private-public partnerships necessary to combat terrorists and other illicit financing via cryptocurrency. Our witnesses are not only leaders in the private sector, but many of you also have Government experience to draw upon, which will be helpful to craft common-sense reform if needed with our committee.

This is a new frontier for the security of our homeland and it is vital that we are working hand-in-glove between the public and the private industries and the sectors.

The last thing I will say before we get into the questions is, in your testimony, is the United States needs to lead here. If we don't and if there is a vacancy, China, Russia, Iran, and other actors around the world will lead and that really is the purpose of today's hearing.

I would like to thank our witnesses for appearing before the subcommittee today. I look forward to a robust conversation.

Madam Chair, I yield back.

[The statement of Ranking Member Pfluger follows:]

STATEMENT OF RANKING MEMBER AUGUST PFLUGER

Thank you, Madam Chair. I appreciate you holding this hearing today and would like to thank our witnesses from Chainalysis, the Blockchain Association, and Coinbase. I look forward to a productive conversation on innovative solutions that we can use to safeguard against terrorists and other adversaries' use of crypto as a tool to evade the rule of law.

The battle against terrorist financing and illicit activity is not a new one, but the creation of cryptocurrency has introduced additional complications to that fight. Cryptocurrency can provide security and anonymity in financial transactions, making it an alluring tool for nefarious actors. Chainalysis reported that in 2021, illicit addresses received $14 billion through cryptocurrency—an all-time high. Between ransomware payments, the darknet market, sanctions evasion, and terrorism financing, we are combatting bad actors from multiple angles.

Congress is notorious for being one step behind when it comes to new technologies, but we cannot afford to play catch-up when it comes to any of these issues. That is why we are meeting with industry leaders today—to understand the full scope of the challenges and find innovative solutions that will close the small, but profitable gap in cryptocurrency that is being used for illicit activity. At the end of this hearing, I hope to understand what we should expect going forward—what trends are we seeing in terms of terrorist use of cryptocurrency and how can we crack down on the billion-dollar profits nefarious actors are making from illicit cyber activity.

Given the global threat picture, we also cannot overlook the foreign nation-states who are attempting to use crypto as a way to line their own pockets—essentially evading sanctions. I'd like to hear more from the panel about Iranian efforts to utilize crypto mining and understand what the outlook is for Russian's use of similar methods. What steps are being taken in the private sector to ensure that crypto isn't a back door to America's use of soft power at a time when sanctions enforcement is an important tool to our foreign policy?

With that said, it is imperative that we remember—regulation should not be implemented hastily. As legislators it's incumbent upon us to protect our constituents and the American way of life while supporting private-sector growth and the U.S. economy. We must pursue the least burdensome path while ensuring the Nation's safety and security.

I look forward to our discussion today and hope that this committee can support the public-private partnerships necessary to combat terrorist and other illicit financing via cryptocurrency. Our witnesses are not only leaders in the private sector, but they also have Government backgrounds that will give them the experience to craft common-sense reforms with our committee. This is a new frontier for the security of our homeland, and it is vital that we are working hand-in-glove to understand the threat and mitigate against it.

I thank our witnesses for appearing before the subcommittee today, and I look forward to a robust conversation. Madame Chairwoman, I yield back the balance of my time.

Chairwoman SLOTKIN. Great. I thank the Ranking Member for his comments. Other Members may submit statements for the record.

[The statement of Chairman Thompson follows:]

STATEMENT OF CHAIRMAN BENNIE G. THOMPSON

JUNE 9, 2022

Good morning.

Today, the subcommittee will hear from the cryptocurrency industry about how terrorists and other criminals may try to exploit cryptocurrency and the blockchain—and how the industry is responding.

This committee was formed after 9/11, as part of the effort to better protect the homeland from terrorism and other threats.

Over the past two decades, technology has changed drastically.

Digital finance technologies built on the blockchain, including cryptocurrency, and the digital marketplaces that make use of them have revolutionized the American economy and global markets.

Unfortunately, terrorists' tactics have followed suit.

Terrorists today not only use the internet to connect and recruit supporters, but also to seek funding to further their extremist activities.

Over recent years, ISIS supporters have launched campaigns to teach people how to use Bitcoin to obscure financial support to the terrorist group.

And when they believed that Bitcoin no longer provided the level of anonymity they sought, ISIS supporters began asking people to send money via a different cryptocurrency, Monero, citing its features that conceal transactions.

The issue is not exclusive to foreign terrorism.

In 2020, at least a dozen far-right groups and their leaders, including an American far-right commentator, received approximately $522,000 worth of Bitcoin from a French supporter.

One year ago, this subcommittee held a hearing with Department of Homeland Security (DHS) officials to examine terrorists' use of digital currency and how it is changing the threat landscape.

The subcommittee has also had Classified briefings with the Treasury Department and others on this issue, and I thank Chairwoman Slotkin for her steadfast leadership and for convening this hearing.

Today, we have leaders from the cryptocurrency industry here to share their perspectives.

The private sector and cryptocurrency industry are the first line of defense for protecting homeland security from terrorists and criminals who may seek to use cryptocurrencies to finance their illicit acts.

As a Nation, we must continue to create and innovate. We cannot be stagnant or fearful of new technology.

But we also must ensure that those developing and leading on emerging technologies are at the forefront of building in safeguards to protect against terrorists' exploitation and the ensuing danger.

I look forward to a productive conversation on this topic and to working with the cryptocurrency and blockchain industries to ensure they have the tools and resources they need.

I thank the witnesses for joining us today and look forward to this important discussion.

Chairwoman SLOTKIN. I now welcome our panel of witnesses. We have two in person and one coming virtually.

Our first witness is Ms. Kristin Smith, executive director of the Blockchain Association. In that role Ms. Smith represents companies in the crypto industry leading the industry in strategy and public policy development. Before joining the Blockchain Association Ms. Smith served as a Congressional staffer in both House and Senate offices, as well as in the private sector where she advocated for companies in the telecommunications, internet, and other tech-focused industries. Welcome.

Our second witness is Mr. Jonathan Levin, co-founder and chief strategy officer Chainalysis, a blockchain data platform that helps organizations with cryptocurrency investigations, compliance, and market intelligence. Mr. Levin advises stakeholders on blockchain analysis capabilities and is responsible for designing long-term strategic initiatives that help Government agencies, cryptocurrency businesses, and financial institutions around the world manage and assess cryptocurrency-related risk.

Our final witness, who is joining us virtually from London, thank you very much, is Mr. John Kothanek, vice president of global intelligence at Coinbase, the largest U.S. cryptocurrency exchange. He is a former Marine who worked in intelligence operations and went on to start and run Paypal's criminal investigations team. As the vice president of global intelligence for Coinbase Mr. Kothanek is responsible for standing up, training, and managing teams around the world, and for providing the best-in-class service, training, and investigative support to law enforcement partners.

Without objection, the witnesses' full statements will be inserted in the record.

I now ask each witness to summarize his or her statements for 5 minutes, beginning with Ms. Smith.

Please go ahead.

STATEMENT OF KRISTIN SMITH, EXECUTIVE DIRECTOR, THE BLOCKCHAIN ASSOCIATION

Ms. SMITH. Thank you, Chairwoman Slotkin, Ranking Member Pfluger, and Members of the subcommittee for inviting me to testify today.

My name is Kristin Smith and I am the executive director of the Blockchain Association, a nonprofit trade association dedicated to advancing good policy so that crypt networks can flourish in the United States.

The Blockchain Association includes more than 90 leading companies who are committed to responsible innovation and strengthening the United States' strategic position in finance and technology. Our diverse membership includes this dynamic industry—reflects this dynamic industry and includes exchanges, developers, investors, and other participants in the crypto ecosystem. I am honored to be testifying today with professionals from Chainalysis and Coinbase who partner with law enforcement every day to stop bad actors from using crypto networks.

Today I will explain what crypto networks are, what problems they solve, and why they will be the source of the next wave of American innovation.

Bitcoin was the world's first cryptocurrency and the Bitcoin network is the world's first crypto network. Invented in 2009, Bitcoin

allows anyone anywhere in the world to send and receive value using nothing more than a computer with an internet connection. Before Bitcoin, if someone wanted to make a payment over the internet they had to rely on an intermediary, like a bank, to add an entry in its private ledger debiting them and crediting the person they want to pay. In other words, before Bitcoin all on-line payments depended on gatekeepers and middle men, who are slow and expensive under the best of circumstances. Under the worse of circumstances, they expose American's sensitive information to cyber attacks, discriminate against underserved communities, and exploit their own customers in pursuit of profit.

Bitcoin solves these problems by replacing centralized intermediaries with a decentralized ledger or database that allows anyone anywhere to send payments across the world almost instantly at almost no cost. Unlike the legacy banking system, which is dominated by large private financial institutions, the Bitcoin network is public payment infrastructure, it is digital cash for the digital age.

It is critical to note that crypto is more than currency. Digital cash was the first use for crypto networks, but far from the last. American innovators, entrepreneurs, and developers are now using that same technology crypto networks to build the next iteration of the internet, sometimes referred to as "Web 3". "Web 1" refers to the early internet of the 1990's when users could only do basic tasks, like read websites and send emails. "Web 2" refers to the internet we largely have today, with all its interactive applications and services. But just like the banking system, Web 2 is dominated by a few large companies, the tech giants, who wield outsized power and influence for their own benefit at the expense of the American public. Web 3, born from and built on crypto networks, is the solution to this imbalanced power. Web 3 brings property rights to the web. It not only allows individuals to own their own data and content, it also allows them to possess digital goods and property. Just like when the mainframe computer was replaced with personal computers and proprietary operating systems were replaced with web-based software, the opening up internet platforms and the ability to have digital ownership that comes along with it will unleash immense innovation and change how we live, work, and play.

For the United States to realize the full benefits of Web 3 and ensure we remain the global leader in this space, we must give American entrepreneurs the freedom to innovate.

Crypto networks present extraordinary opportunities, but also risks. The subject of today's hearing is an important one to address head on. Thankfully policy makers at the Treasury Department and across the Government have been doing just that for many years. FinCEN, under the Treasury Department, was the very first regulator to issue guidance related to crypto networks back in 2013. Since then the U.S. law enforcement and intelligence communities have proven highly effective in identifying and stopping bad actors from using crypto networks. The Blockchain Association and all of its member companies are strongly committed to protecting the integrity of the financial system, supporting U.S. National security, and advancing U.S. interest.

I greatly appreciate the chance to testify today and I look forward to your questions.

[The prepared statement of Ms. Smith follows:]

STATEMENT OF KRISTIN SMITH

JUNE 9, 2022

I. CRYPTO NETWORKS ARE ESSENTIAL TO THE INTERNET OF THE FUTURE

Thank you for inviting me to testify today. My name is Kristin Smith and I am the executive director of the Blockchain Association, a nonprofit trade association dedicated to advancing good policy so that crypto networks can flourish in the United States. The Blockchain Association includes more than 90 leading companies who are committed to responsible innovation and strengthening the United States' strategic position in global finance and technology. Our diverse membership reflects this dynamic industry, and includes exchanges, developers, investors, and other participants in the crypto ecosystem.

I'm honored to be testifying today with professionals from Chainalysis and Coinbase who partner with law enforcement every day to stop bad actors from using crypto networks. Today, I will explain what crypto networks are, what problems they solve, and why they will be the source of the next wave of American innovation.

Bitcoin is the world's first cryptocurrency—and the Bitcoin network is the world's first crypto network. Invented in 2009, Bitcoin allows anyone, anywhere in the world to send and receive value using nothing more than a computer with an internet connection. Before Bitcoin, if someone wanted to make a payment over the internet, they had to rely on an intermediary, like a bank, to add an entry to its private ledger debiting them and crediting the person they wanted to pay. In other words, before Bitcoin, all on-line payments depended on gatekeepers and middlemen, who are slow and expensive under the best of circumstances. Under the worst of circumstances, they expose Americans' sensitive information to cyber attacks, discriminate against underserved communities, and exploit their own customers in the pursuit of profit.

Bitcoin solves these problems by replacing centralized intermediaries with a decentralized ledger that allows anyone, anywhere, to send payments across the world, almost instantly at almost no cost. Unlike the legacy banking system, which is dominated by large, private financial institutions, the Bitcoin network is a public payments infrastructure: Digital cash for the digital era.

It's critical to note that crypto is more than currency. Digital cash was the first use case for crypto networks, but far from the last. American innovators, entrepreneurs, and developers are now using that same technology—crypto networks—to build the next iteration of the internet: Sometimes called "Web 3." Web 1 refers to the early internet of the 1990's, when users could only do basic tasks like read websites or send emails. Web 2 refers to the internet we have today, with all its interactive applications and services. But just like the banking system, Web 2 is dominated by a few large companies—the tech giants—who wield outsized power and influence for their own benefit at the expense of the American public.

Web 3—born from and built on crypto networks—is the solution to this imbalance of power. Web 3 brings property rights to the web. It not only allows individuals to own their own data and content, but it also allows them to possess digital goods and property. Just like when the mainframe computer was replaced with personal computers, and proprietary operating systems were replaced with web-based software, the opening of internet platforms—and the ability to have digital ownership that comes along with it—will unleash immense innovation and change how we live, work, and play. For the United States to realize the full benefits of Web 3—and ensure we remain the global leader in this space—we must ensure American entrepreneurs have the freedom to innovate.

Crypto networks present extraordinary opportunities, but also risks. The subject of today's hearing is an important one to address head-on, and thankfully, policy makers at the Treasury Department and across the Government have been doing just that for many years. FinCEN was the very first regulator to issue guidance related to crypto networks back in 2013. Since then, the U.S. law enforcement and intelligence communities have proven highly effective in identifying and stopping bad actors from using crypto networks. The Blockchain Association and all of its members are strongly committed to protecting the integrity of the financial system, supporting U.S. National security, and advancing U.S. interests.

II. CRYPTO NETWORKS ARE NOT VULNERABLE TO USE BY BAD ACTORS

In the United States, custodial crypto companies like exchanges, payment processors, and other "flat on-ramps and off-ramps" are regulated as money services businesses (MSBs) and are responsible for compliance with the Bank Secrecy Act (BSA). These companies have established highly effective anti-money laundering (AML) compliance programs and regularly coordinate with U.S. law enforcement authorities to detect and prevent illicit activity. Peer-to-peer transactions, on the other hand, are not subject to the BSA pursuant to long-standing guidance from FinCEN. Yet, for several reasons, these transactions pose little risk of money laundering and terrorist financing.

First, before cryptocurrencies are exchanged for goods or services, they typically have to be converted to a National currency, which requires that they be exchanged through a regulated financial institution where they will be subject to the same level of due diligence as transactions in the traditional financial system. In these cases, cryptocurrency transactions pose no greater risk of money laundering or terrorist financing than ACH payments or wire transfers.

Second, the transparent and immutable nature of public blockchains allows law enforcement to "follow the money" and establish attribution in cases involving cryptocurrencies. According to the Department of Justice, "armed only with the knowledge of a target's cryptocurrency address and this single—but highly valuable—data set, [the blockchain], law enforcement can learn a myriad of vital pieces of information about a target." Indeed, many of the individuals charged in recent high-profile "busts" involving cryptocurrencies were identified after sending their assets to custodial accounts at regulated financial institutions that law enforcement was able to subpoena to establish attribution for the relevant criminal activity. It is largely due to law enforcement's ability to leverage blockchain technology and coordinate with industry participants that the amount of illicit activity on crypto networks is so low.

Third, the reality is that nearly 14 years after the invention of Bitcoin, the vast majority of money laundering and terrorist financing continues to occur in the traditional financial system. According to the United Nations, "The best estimate for the amount available for laundering through the financial system, emerging from a meta-analysis of existing estimates, would be equivalent to 2.7 percent of global GDP (2.5 percent–4 percent) or US$1.6 trillion in 2009." From this statistic, it becomes clear that the value of illicit funds laundered each year through the traditional financial system is nearly greater than the value of all cryptocurrencies combined. For context, the largest cryptocurrency by market capitalization is bitcoin, which has a capitalization of about $568 billion, and the combined market capitalization of stablecoins that reference the U.S. dollar is about $144 billion. Additionally, the level of illicit activity in cryptocurrency markets, which according to blockchain analytics firm Chainalysis represented just 0.15 percent of cryptocurrency transaction volume in 2021, further proves that cryptocurrencies have not been widely adopted by illicit actors.

Despite the minimal amount of illicit activity, some observers have suggested that the risk of illicit activity in peer-to-peer transactions is substantial enough to justify restricting the ability of crypto users to transact outside the confines of regulated financial institutions. It is not. Restricting the right of individuals to engage in peer-to-peer transactions on crypto networks would be akin to banning paper cash, a disproportionate response that would cause broad and long-lasting harm to the ideals of privacy and economic freedom at the core of our society.

III. EXHIBITS AND FURTHER READING

For more information on the level and typology of illicit activity as well as a deeper dive into the importance of self-hosted wallets, I recommend the subcommittee read the following exhibits:

The Blockchain Association/Miller Whitehouse-Levine and Lindsey Kelleher/Self-Hosted Wallets and the Future of Free Societies/November 2020.—This report is divided into two sections that seek to offer policy makers a broad introduction to self-hosted wallets. The first section describes what self-hosted wallets are, their role in the digital asset ecosystem, and the current regulatory framework for managing digital asset transactions involving self-hosted wallets. The second section argues that imposing restrictions on individuals' ability to use self-hosted wallets would be misguided.

CoinCenter/Jerry Brito/The Case for Electronic Cash/February 2019.—This paper shows that a cashless economy is a surveillance economy, arguing that removing the option to freely transact without intermediation greatly limits economic self-determination and places economic lives in the hands of financial institutions and gov-

ernments. By presenting several case studies that demonstrate negative externalities associated with a completely intermediated payments system, the paper ultimately concludes that electronic cash, i.e. peer-to-peer transactions using self-hosted wallets, should be fostered and celebrated.

Consensys/James Beck/What is Web 3? Here Are Some Ways To Explain It To A Friend/January 12, 2022.—This article describes Web 3 and how it is different from the internet that we know and use today. Critically, this article describes the motivation behind the creation of Web 3 as "a reaction to social networks not keeping our data secure, and selling it for their own profit."

Chainalysis/The 2022 Crypto Crime Report/February 2022.—This report gives an overview of illicit activity within the cryptocurrency ecosystem. The author of this report is Chainalysis, one of the world's preeminent blockchain analytics firms. According to the report, "with the growth of legitimate cryptocurrency usage far outpacing the growth of criminal usage, illicit activity's share of cryptocurrency transaction volume has never been lower . . . Transactions involving illicit addresses represented just 0.15 percent of cryptocurrency transaction volume in 2021."

Unchained/Laura Shin, Zia Faruqui, and Jessi Brooks/How This DOJ Strike Force Hunts Down Cryptocurrency Criminals/October 20, 2020.—In this podcast, Laura Shin discusses how Zia Faruqui, Magistrate Judge, and Jessi Brooks, assistant U.S. attorney in the National Security Section at the United States Attorney's Office, prosecuted a number of Federal criminal and civil forfeiture cases involving cryptocurrency, including the Welcome to Video case, which led to the takedown of one of the web's largest child pornography sites, a case involving the North Korea affiliated Lazarus group, and another case involving Hamas and the Al Qassam Brigades. Interestingly, the success of each of these cases was contingent upon law enforcement's ability to leverage blockchain analytics to identify the perpetrators of these crimes.

Reuters/Brett Wolf/Recovery of Colonial Pipeline Ransom Funds Highlights Traceability of Cryptocurrency, Experts Say/June 23, 2021.—This article describes the Colonial Pipeline attack and the efforts of law enforcement to identify and return the stolen funds. According to one blockchain analytics expert who was quoted in the article, "the seizure of approximately 85 percent of the ransom paid by Colonial Pipeline highlights how successful U.S. law enforcement has been in developing the capacity to execute this sort of complex operation using blockchain analysis in real time."

LawFare/Andrew Mines and Devorah Margolin/Cryptocurrency and the Dismantling of Terrorism Financing Campaigns/August 26, 2020.—This article describes how several U.S.-designated terrorist organizations attempted to receive funding using cryptocurrency. Ultimately, these terrorists were thwarted by law enforcement, who partnered with members of the cryptocurrency ecosystem to identify the terrorists and trace the flow of funds. Of particular note is the article's assertion that "despite common assumptions that Bitcoin transactions are fully anonymous, U.S. officials used third-party blockchain analysis and personally identifying information from virtual exchanges to track 150 cryptocurrency accounts associated with al-Qassam, and to investigate U.S.-based individuals who donated to these campaigns."

Bloomberg/Matt Levine/Business Rapper Was Bad at Bitcoin Laundering/February 9, 2022.—This article describes the hack of the cryptocurrency exchange, Bitfinex, and law enformcent's efforts to identify and prosecute the culprits as well as recover about 80 percent of the 119,754 Bitcoin worth $3.6 billion that was stolen. One critical aspect of this article is Mr. Levine's comparison of money laundering with cash to money laundering with cryptocurrency: "If you come to a bank with a sack of cash and say, 'I, uh, inherited this from my grandmother, she kept cash in sacks,' that is somewhat hard for the authorities to check. If you come to a crypto exchange with a sack of Bitcoins and say 'I got these cheap in 2014,' that is easier to check. Permanent immutable public ledger on the blockchain!"

Chairwoman SLOTKIN. Thank you for your testimony.

I now recognize Mr. Levin to summarize his statement for 5 minutes.

STATEMENT OF JONATHAN LEVIN, CO-FOUNDER AND CHIEF STRATEGY OFFICER, CHAINALYSIS, INC.

Mr. LEVIN. Thank you, Chairwoman Slotkin, Ranking Member Pfluger, and distinguished Members of the committee. Thank you

for inviting me here today to testify before you on this important topic.

My name is Jonathan Levin and I co-founded Chainalysis with Michael Gronager, the CEO of Chainalysis. I currently serve as the chief strategy officer.

I began studying cryptocurrencies 10 years ago through my research as an economist. I was interested in the way that the internet could create both new markets and impact developing economies. While the internet brought about citizens of the world closer together in terms of global connectivity, it did not give people the economic opportunities that were promised. The cryptocurrency industry provides a new way to conduct global commerce, providing economic opportunities for people across the world. Economic development has always been a key force against global terror, and as such preventing cryptocurrency from being abused for terrorist financing and other National security risks is intricately linked to our continued ability to encourage prosperity around the world and enhance our National security.

Can the clerk cue visual one?

If there is one point I want to make to the Members of this committee, it is that the transparency of cryptocurrency enhances the ability of policy makers, Government agencies to detect, attribute, and ultimately disrupt illicit activity. In many instances it is easier to investigate cases involving the illicit use of cryptocurrency than other forms of payment, as demonstrated by the visual that is shown on the screen. By studying an illicit actor's cryptocurrency wallet in the center of the diagram, law enforcement can identify the cash-out destination and the full network of accomplices and malicious tools underpinning their campaign. In contrast, many terrorist financing investigations are predicated on difficult to trace cash payment networks or prepaid cards.

As previously mentioned, the overall percentage of illicit transactions in cryptocurrency is just 0.15 percent, indicating that the vast majority of cryptocurrency transactions are legitimate. While terrorist financing comprises an extremely small fraction of the total activity that we see in the ecosystem, it is nonetheless important that we address it.

Can the clerk cue visual two?

In my written testimony I provide background on Chainalysis outlining how blockchain analysis can be leveraged in investigations and explain how terrorists have used cryptocurrency in their fundraising efforts. I also provide several case studies like seen on this diagram demonstrating how Government agencies are rooting out terrorist financing using cryptocurrencies and actually seizing funds from their operations.

I also provide recommendations for improving the Government's response to this threat.

Can the clerk take down the visual?

First, it is critical that we ensure that there is adequate funding resources and training for Government agencies with the task at hand. As terrorist organizations and other illicit actors are innovating with their techniques, governments must keep up with our adversaries. Governments have already embraced blockchain analysis, have seized millions of dollars, as previously mentioned, in

cryptocurrency, and stopped several financiers that have tried to fund terrorist organizations. Further evidence that with the proper tools, investigators can cut off terrorist organizations from the funds they need to survive. This is increasingly important in the face of more and more communications going dark and the challenges that this creates for law enforcement.

Second, the illicit use of cryptocurrency, including for terrorist financing, is a global issue and investigations often cross borders. We must improve the information sharing in coordination between U.S. Government agencies and their counterparts on these investigations. Again, the transparency of cryptocurrencies and their public nature create unprecedented opportunities for such collaboration.

Finally, the United States should work with other countries around the world to assist them in the development and implementation of anti-money-laundering laws and regulations for cryptocurrency businesses to ensure that bad actors are cut off from cashing out their ill-gotten gains in unregulated jurisdictions.

With that, I thank you and look forward to your questions.

[The prepared statement of Mr. Levin follows:]

PREPARED STATEMENT OF JONATHAN LEVIN

JUNE 9, 2022

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

My name is Jonathan Levin and I co-founded Chainalysis Inc. with Michael Gronager, CEO of Chainalysis. I currently serve as chief strategy officer. I began studying cryptocurrencies 10 years ago through my research as an economist. I was interested in the way that the internet could create brand new markets and impact developing economies. While the internet brought citizens of the world closer together in terms of global connectivity, it did not give people the economic opportunities that were promised.

The cryptocurrency industry provides a new way to conduct global commerce, providing economic opportunities for people across the world. As with any new technology, cryptocurrency can be used by both good and bad actors. As such, preventing cryptocurrency from being abused for terrorist financing and other National security risks is intricately linked in our continued ability to project prosperity around the world.

Helping this industry stay on top of the emerging threats of terrorist financing while ensuring the vibrant economic output that will be built on these new rails is the task at hand.

Cryptocurrency and blockchain technology are some of the best available tools in the toolkit that the United States has to compete with potential National security threats, like ransomware attacks and North Korean hackers. The entrepreneurial dynamism that cryptocurrencies present allows for innovators and builders to create universal access to financial products and re-engineer Web 2 business models to serve individuals and their data in a way that protects privacy and helps our communities. This technology is consistent with our American values and has the potential to be strategically more important in great power competition over the next few decades. Of course, we understand concerns about risk and abuse and that is why we are here today. At Chainalysis we share concerns about the illicit use of cryptocurrency, but we know that the inherent open nature of this technology can be leveraged to mitigate the risks associated with it and bring bad actors to justice.

If there is one point I want to make to the Members of this committee, it is that the transparency of cryptocurrency blockchains enhances the ability of policy makers and Government agencies to detect, disrupt and, ultimately, deter illicit activity.

By mapping a single illicit actor to a cryptocurrency wallet address, for example from a transaction made in a terrorist financing campaign, law enforcement unlocks immediate insight into the network of wallet addresses and services (e.g., exchanges, mixers, etc.) that facilitate the illicit actor. In contrast, in a traditional finance investigation, a similar tip, linking an illicit actor to a bank account, is just the beginning of a long, extensive process to request and subpoena records that are manually reviewed and reconciled to generate a comparable amount of insight.

Even with this insight, it comes with a significant time delay that creates opportunities for illicit actors to evade justice vs. the real-time monitoring capabilities of blockchain intelligence.

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

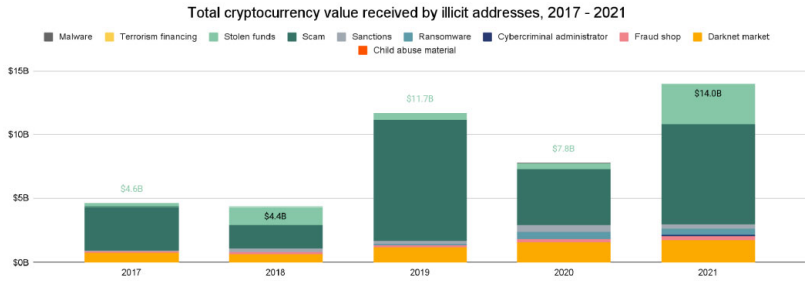
BACKGROUND ON CHAINALYSIS

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

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

Chainalysis's data powers both investigative and compliance tools. Our investigative tool, Reactor, enables government agencies and investigative teams to trace the illicit uses of cryptocurrency, including money laundering, theft, scams, and other criminal activities. Our compliance tool, KYT (Know Your Transaction), provides cryptocurrency businesses and financial institutions the ability to screen their clients transactions and ensure that they are not attempting to interact with illicit entities. This transaction monitoring tool provides on-going insights for cryptocurrency businesses so that they can protect their businesses and clients and ensure regulatory compliance.

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



Despite this large increase in illicit transaction volume, illicit activity as a percentage of total volume has actually fallen dramatically since 2019. In 2019, the il-

licit share was about 3 percent, in 2020 it was just over 0.5 percent, and in 2021 it was 0.15 percent. The reason for this is that cryptocurrency usage is growing faster than ever before, so while cryptocurrency-related crime is definitely increasing, the legitimate use of cryptocurrency is far outpacing its use by illicit actors. This is good news for the cryptocurrency ecosystem, but Government and industry must still put in place and implement the appropriate controls to mitigate risks in the system.

Terrorist financing through cryptocurrency remains extremely low; however, we have identified terrorist organizations that have attempted to finance their operations with cryptocurrency. For example, in 2019 and 2020, al-Qaeda raised cryptocurrency through Telegram channels and Facebook groups. Thanks to the Federal Bureau of Investigation, Homeland Security Investigations, and Internal Revenue Service-Criminal Investigation, more than $1 million was seized from a money service business (MSB) operator who facilitated some of these transactions. Additionally, in early spring of 2021, the 'Izz al-Din al-Qassam Brigades, Hamas' military wing, collected more than $100,000 in donations in cryptocurrency. In July 2021, the Israeli government seized much of these funds from associated MSBs. According to our own analysis, Hamas raised at least $160,000 across three campaigns from 2019–2021 and from October 2021 through March 2022, an ISIS-related campaign (the Forgotten Ones) raised $36,000, but terrorists appear to have pivoted away from public-facing cryptocurrency donation campaigns.

HOW BLOCKCHAIN ANALYSIS CAN BE LEVERAGED IN INVESTIGATIONS

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

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

BACKGROUND ON TERRORIST FINANCING AND CRYPTOCURRENCY

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

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

Terrorists have used cryptocurrency for a variety of purposes, such as to purchase military equipment and procure computer infrastructure. For example, in 2016, the pro-ISIS, Gaza-based Ibn Taymiyya Media Center (ITMC) hosted the Jahezona ("Equip Us") cryptocurrency donation campaign—the first of its kind—and posted a graphic on Telegram depicting the type of weaponry different dollar-equivalent donation amounts could purchase. The Jahezona campaign, which the ITMC also advertised on YouTube and Twitter, ran from 2016 to 2018 and raised thousands of dollars worth of cryptocurrency. Although this may not seem like a large sum over a 2-year period, we must keep in mind that terrorist attacks are not expensive to carry out, especially when the attackers are acting alone.

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

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

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

Press reporting has emphasized the potential for cryptocurrency adoption to continue rising in Afghanistan given the country's political isolation, economic volatility, instability at Afghanistan's central bank, and a run on banks following the Taliban takeover in August 2021. In 2021, Afghanistan ranked 20th in global crypto adoption, according to the Chainalysis Global Crypto Adoption Index. Afghanistan ranks this high because we weight the metrics that feed the index by countries' purchasing power and internet-using population, where Afghanistan ranks among the lowest. Some Afghans have turned to crypto as a safe place to store value amid economic uncertainty and the challenges of broad adoption in the country and the country has a nascent cryptocurrency economy driven by modest P2P exchange trading. It remains to be seen how their cryptocurrency economy will develop under the Taliban, but this is something we will continue to monitor. In addition to the Taliban takeover, the local affiliate of the Islamic State in Iraq and ash-Sham, ISIS-Khorasan, remains active in Afghanistan, raising the risk that it and affiliated networks could abuse cryptocurrency services in this strategically-situated, high-risk jurisdiction.

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

AL-QAEDA, ISIS, AND HAMAS AMONG TERRORIST GROUPS FUNDRAISING IN CRYPTOCURRENCY—WITH GOVERNMENT SEIZURES CLOSE BEHIND

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

CASE 1: ISRAELI GOVERNMENT SEIZES CRYPTOCURRENCY ADDRESSES ASSOCIATED WITH HAMAS DONATION CAMPAIGNS

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

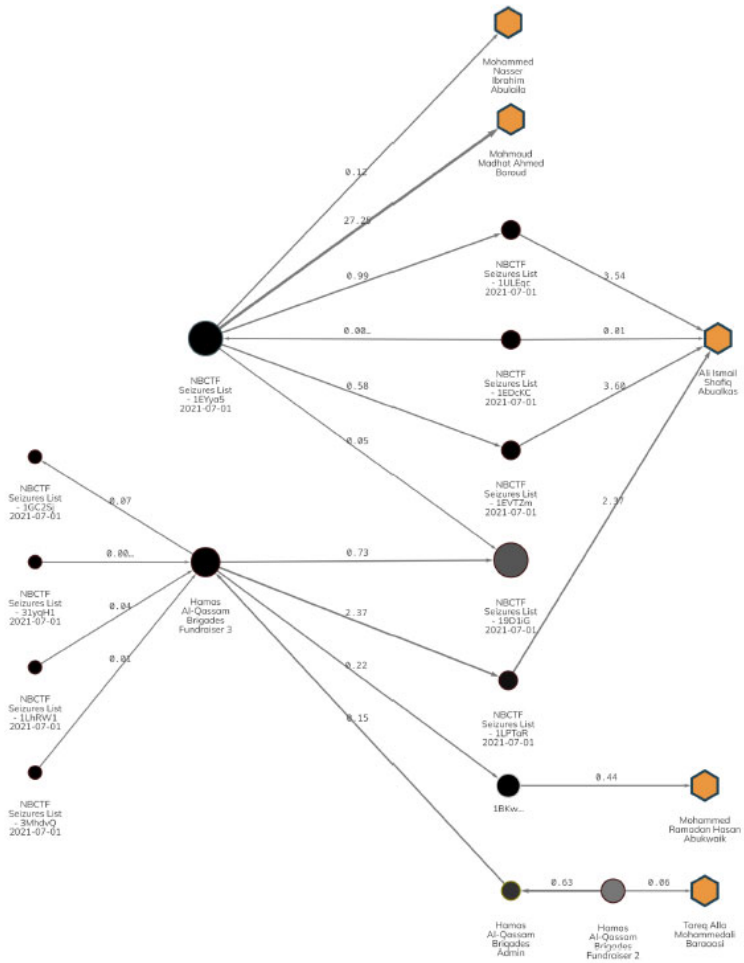
Notably, this is the first terrorism financing-related cryptocurrency seizure to include such a wide variety of cryptocurrencies. Israeli authorities seized not only Bitcoin, but also Ether, Tether, Ripple, and more. The seizure was made possible through an investigation of open-source intelligence (OSINT)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

as well as cooperation from the compliance team at a global cryptocurrency exchange.

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

How funds moved from donation addresses to exchanges

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



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

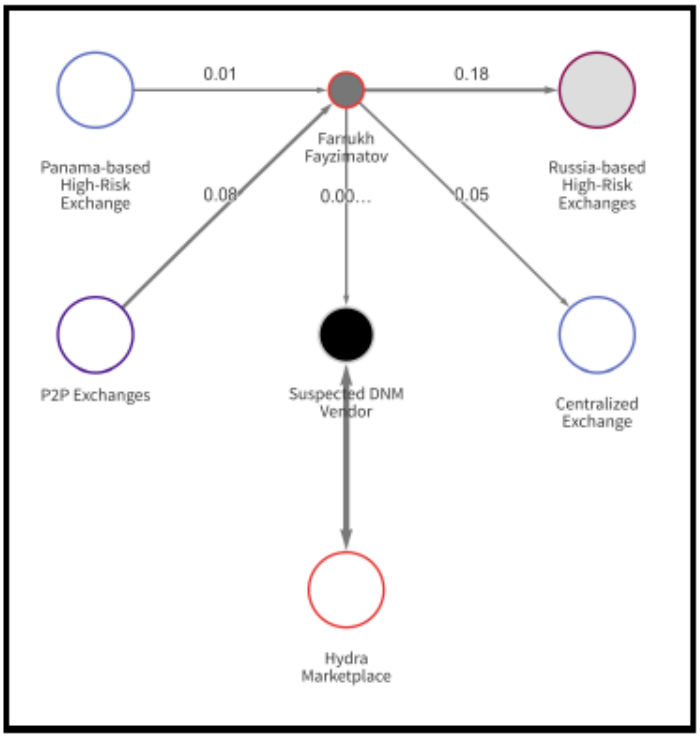
Interestingly, we can see that two donation addresses named in the announcement received funds from addresses associated with the Idlib, Syria office of BitcoinTransfer (top right of the graph), a Syrian cryptocurrency exchange connected to previous terrorism financing cases. Another exchange received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

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

CASE 2: TERRORIST FINANCIER DESIGNATED BY THE U.S. DEPARTMENT OF THE TREASURY'S OFFICE OF FOREIGN ASSETS CONTROL (OFAC)

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

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



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

CASE 3: WALES-BASED CONVICTED TERRORIST CAUGHT USING DARKNET MARKET 'BYPASS SHOP'

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

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

This was not Iqbal's first run-in with the law. Iqbal had previously spent time in jail in 2014 for possessing terrorist information and disseminating terrorist publications under the pseudonym Abu Irhaab, Arabic for "father of terrorism." In total, Iqbal possessed 9 copies of al-Qaeda's English-language *Inspire* magazine, and had published more than 800 links to extremist material on Facebook.

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

RECOMMENDATIONS

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

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

Improve coordination and collaboration within and between governments.

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

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

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

The U.S. Government should provide assistance through the U.S. Department of State and other mechanisms to other countries to assist in the development and implementation of these laws, as well as capacity building to enforce them. This will help to limit the regulatory arbitrage opportunities available to bad actors and make it even more difficult for terrorists to fund themselves with cryptocurrency at scale because they will more frequently encounter regulated, compliant exchanges that

implement AML/CFT standards and work with law enforcement. Although cryptocurrency can be abused by terrorist organizations and other threat actors, it is also a powerful tool with the potential to provide meaningful economic opportunity in confiict zones or jurisdictions with weak institutions. The U.S. Government should encourage private and public initiatives that leverage blockchain technology to minimize sanctions exposure and greatly improve the traceability of funds in difficult or high-risk jurisdictions.

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

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

CONCLUSION

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

Chairwoman SLOTKIN. Thank you for your testimony.

I now recognize Mr. Kothanek to summarize his statement for 5 minutes.

STATEMENT OF JOHN KOTHANEK, VICE PRESIDENT, GLOBAL INTELLIGENCE, COINBASE, INC.

Mr. KOTHANEK. Chairwoman Slotkin, Ranking Member Pfluger, and the Members of the subcommittee, thank you for this opportunity to testify on the role of crypto in combatting terrorism and criminal activity.

My name is John Kothanek and I am vice president for global intelligence at Coinbase. I am responsible for investigating and combatting crypto-related criminal activity on our platform and across the internet. My team works with law enforcement around the world to provide best-in-class training and investigative support to combat crypto-related crime.

I came to Coinbase in 2014 after meeting with our CEO, Brian Armstrong, and co-founder, Fred Ehrsam, to discuss their vision for the company and the future of crypto. They were laser-focused on becoming the most secure, trusted, and compliant on-ramp for buying, selling, and trading crypto. They knew they wanted to build a team that was part of the solution, not part of the problem. That is why I joined Coinbase and how I have built the global intelligence team.

Our mission is to protect our customers, crypto, and the country. As a former Marine and son of an Air Force pilot, I spent most of my life thinking about how to stop bad actors from hurting good people. I took my experience from the military to the private sector where I started Paypal's investigation team in 2000. We built a

program from the ground up that changed investigations for digital transactions and became the industry standard. We have done the same at Coinbase for crypto.

Coinbase is a global platform that enables millions of individuals, businesses, and developers in over 100 countries to participate in the crypto economy. Since our early days, Coinbase has strived to set the standard for legal and regulatory compliance for digital assets. Specific to the interest of this subcommittee, we are Federally registered as a money service business with FinCEN and serve on the Department of the Treasury's Bank Secrecy Act Advisory Group.

Coinbase attacks illicit activity from a variety of angles. My team works hand-in-hand with our financial crimes compliance team, which has developed both robust anti-money laundering and Know Your Customer programs and proprietary transaction monitoring systems to identify illegal activity. Our programs are further bolstered by something called unique to the crypto. Every blockchain has a public ledger of transactions. Our teams analyze publicly available blockchain data with the aid of sophisticated blockchain tools in order to trace criminal proceeds and attribute blockchain addresses to potential criminals.

Another key component of our strategy to combat crime is our relationship with law enforcement. We have built a collaborative partnership with law enforcement agencies in concert with our strict privacy commitments to our customers to pursue bad actors in the crypto space. We do this in several ways. We offer cryptocurrency investigations training free of charge to thousands of law enforcement officers around the world. We also help law enforcement interpret the blockchain information that we provide to them and direct officers to the tools and the resources they need to pursue their investigations.

Finally, we participate in public-sector working groups to share information that can help and investigate the effort.

We believe law enforcement that understands cryptocurrency and the ways in which our public blockchains could be analyzed to detect and investigate criminal activity can more effectively affect the public, including our customers.

While we are proud of our successes investigating criminal activity, there are several major challenges to stopping bad actors. Specifically, criminal actors tend to rely on a small group of non-compliant foreign exchanges to cash out their illicit gains because these foreign exchanges are not subjected to U.S. regulations. Criminal actors avoid exchanges like Coinbase because we have AML and KYC programs and investigative teams that freeze accounts or refer to law enforcement.

Despite the incredible growth of expertise across law enforcement agencies, we often run into situations where law enforcement, especially at the local level, lack the necessary tools and resources to pursue crypto-related crime. We would recommend that the U.S. Government develop tailored solutions in this space, including three recommendations.

We need to ensure law enforcement at the Federal level has resources necessary to target non-compliant offshore exchanges and mixing services that enable criminal actors to monetize their activ-

ity. We need to ensure the United States develops strong international partnerships with governments and overseas law enforcement to combat global organized crime activity. We would recommend to Congress to help direct and provide resources to develop local, State, and Federal task forces to share information to combat illegal activity.

In closing, thank you, Chairwoman Slotkin and Ranking Member Pfluger, and the Members of the subcommittee for holding this important hearing. Coinbase is committed to working with Congress and law enforcement to combat illegal activity while also protecting the privacy and security of our customers. Combatting illegal activity on our platform is core to our mission of enabling economic freedom in a trusted, secure, and compliant way.

Thank you. I look forward to answering your questions.

[The prepared statement of Mr. Kothanek follows:]

PREPARED STATEMENT OF JOHN KOTHANEK

JUNE 9, 2022

Chairwoman Slotkin, Ranking Member Pfluger, and Members of the subcommittee, thank you for this opportunity to testify on the role of crypto in combating terrorism and criminal activity.

My name is John Kothanek and I serve as the vice president for global intelligence at Coinbase. I am responsible for standing up, training, and managing our teams around the world in investigating and combating crypto-related criminal activity on our platform and across the internet. We work with all levels of United States and foreign law enforcement on large-scale cyber crime and criminal investigations, providing best-in-class service, training, and investigative support.

I came to Coinbase in 2014 after meeting with our CEO Brian Armstrong and cofounder Fred Ersham to discuss their vision for the company and the future of crypto. They were laser-focused on becoming the most secure, trusted, and compliant on-ramp for buying, selling, and trading crypto. That has always meant keeping bad actors off the platform. They knew they wanted to build a team that was part of the solution, not part of the problem. That's why I joined Coinbase, and how I've built the Global Intelligence team. Our mission is to protect our customers, crypto, and the country. As a former Marine and son of an Air Force pilot, I have spent most of my life thinking about how to stop bad actors from hurting Americans. I took my experience from the military to the private sector, when I joined Paypal's then-new anti-fraud team in 2000. My goal was to use new technological tools to find illicit transactions and distinguish them from legitimate ones. We built a program from the ground up that became the industry standard. We've done the same at Coinbase.

Our Global Intelligence team is one piece of the puzzle at Coinbase. Our company is a leading provider of end-to-end financial infrastructure and technology for the cryptoeconomy. We define the cryptoeconomy as a fair, accessible, efficient, and transparent financial system for the internet age that leverages digital assets built on blockchain technology. Coinbase Global, Inc. (COIN) became a public company registered with the SEC and listed on Nasdaq in May 2021. Our primary operating company, Coinbase, Inc., and our affiliates (collectively, "Coinbase") make up one of the largest digital asset financial infrastructure platforms in the world, including our exchange for digital assets.

Our global platform enables millions of individuals, businesses, and developers in over 100 countries to participate in the cryptoeconomy. More than 89 million individuals rely on Coinbase to provide a safe, trusted, and easy-to-use crypto account to buy, sell, store, spend, earn, and use crypto assets. We also offer a comprehensive solution that combines advanced trading, custody services, and financing for roughly 11,000 institutional customers. On top of our retail and institutional services, we provide technology and services, such as Coinbase Cloud, that enable more than 185,000 developers to build crypto-based applications and securely accept crypto assets as payment.

Coinbase is the largest U.S. digital asset exchange. We currently list 172 assets for trading and 212 assets for custody on our platform. Every asset listed on the Coinbase platform is subject to a rigorous legal, compliance, and security review.

With an early focus on regulatory requirements, Coinbase has strived to set the standard for legal and regulatory compliance in the digital asset industry. We are licensed as a money transmitter in 42 States, hold a "BitLicense" and a New York Trust Charter from the New York Department of Financial Services, and are authorized to engage in consumer lending in 15 States.

More specific to the interests of this subcommittee, we are Federally-registered as a money services business with FinCEN and we serve on the Department of the Treasury's Bank Secrecy Act Advisory Group. Additionally, our activities are subject to Federal oversight from the Internal Revenue Service, the Commodity Futures Trading Commission, the Securities and Exchange Commission, the Federal Trade Commission, and the Consumer Financial Protection Bureau.

Coinbase has worked to develop best-in-class criminal investigative methods. We have trained State, Federal, and international law enforcement agencies to identify and pursue illicit use of digital asset technologies, and we host law enforcement for in-house secondments to partner with my team on blockchain investigations. We have twice been recognized by FinCEN for providing essential intelligence to law enforcement authorities. In 2019, we received the Private/Public Partnership award from Homeland Security Investigations for our contribution to major law enforcement investigations.

Since Day 1, we have gone after the bad guys. We take a comprehensive approach to combating illegal activities, looking across not only the blockchain but the internet in general. Before we explore how we combat terrorism and other illicit activity, it is important to level set on a few key terms.

Blockchain technology is enabled by cryptography. At the core of all cryptocurrencies or digital assets are private keys—complex and secret numbers used by an individual transacting on the blockchain. A private key is mathematically linked to a public key, which is the address that others can use to transact with the owner of the private key. Put simply, a distributed ledger—a blockchain—is really just the history of transactions between public keys. A transaction occurs if the private key associated with the public key cryptographically signs off on the transaction.

Blockchain technology creates a ledger of transactions that are transparent and immutable. However, unlike traditional ledgers, there is no need for a central authority to maintain the database. Blockchain-based ledgers are public, distributed, and immutable: Anyone can download the ledger and see the entire history of every transaction that has ever occurred on a given blockchain and nobody can change it. That free public history is an essential feature of a blockchain because it ensures visibility into the counterparties involved in the transaction. It also enables more robust criminal investigations.

This is contrary to many of the narratives surrounding crypto, but the reality is that blockchain technology can help identify and prevent criminal activities. Cryptocurrency is easier to track than fiat currency because searchable databases (public blockchains) exist for most transactions. The information in these blockchains exists permanently, and provides law enforcement with details about crypto transactions that are not available with fiat currency. The Department of Justice discusses this utility as part of its investigation methods; the September 2019 edition of the Department of Justice Journal of Federal Law and Practice says:

"Cryptocurrency, despite the purported anonymity it grants criminals, provides law enforcement with an exceptional tracing tool: The blockchain. While the blockchain's historical ledger will not list the names of parties to transactions, it provides investigators with ample information about how, when, and how much cryptocurrency is being transferred."[1]

The public blockchains have helped advance law enforcement efforts with new tools that reveal the structure of organized ransomware crime rings and individual hackers in ways that are unavailable with fiat.

I would now like to describe in more detail Coinbase's efforts to fight crime and protect our customers. From the very early days of the company, we have been committed to preventing criminals from abusing our platform and our customers. We feel a strong obligation to protect our customers, our company, and the crypto ecosystem as a whole from bad actors. If this technology is going to succeed, ordinary people need to be able to trust and safely interact with the crypto-economy.

We attack illicit activity on our platform from a variety of angles. As one of the first regulated digital asset exchanges in the United States, we quickly developed robust Anti-Money Laundering (AML) and Know Your Customer (KYC) programs.

[1] 67 DOJ J. FED. L. & PRAC., No. 3 at 166 (2019).

Our Financial Crimes Compliance team uses a proprietary transaction monitoring system to identify potentially illegal activity so that we can file Suspicious Activity Reports with FinCEN and, if necessary, close those accounts.

Our Financial Crimes Compliance program incorporates all of the traditional components and controls you would expect from a financial institution, and it is further bolstered by a characteristic unique to cryptocurrency—the public ledger of transactions within the blockchain. By reviewing publicly available blockchain data, especially with the aid of sophisticated blockchain analysis tools like Coinbase Tracer, both our compliance and global investigations teams are able to trace the proceeds of crime and attribute blockchain addresses to known entities, including criminal entities. Once we confirm that an address is associated with crime—for example, an address used to receive stolen funds or an alleged terrorism financing address—we are able to block other customers from sending to that address and trigger automatic alerts for any customers attempting to do so.

Another key component of our strategy to combat crime is our relationship with law enforcement. We have been committed since the beginning to building a collaborative partnership with law enforcement. In fact, my department, the Global Intelligence team, was created in 2016 to focus almost exclusively on law enforcement investigations and outreach efforts. Our mission in this respect is simple: Do everything we can, within the bounds of our strict privacy commitments to our customers, to help law enforcement pursue bad actors in the crypto space.

We do this in several ways. First, as I mentioned earlier, we have offered cryptocurrency investigations training, free of charge, to thousands of law enforcement officers around the world. These trainings range from short sessions on the basics of cryptocurrency to day-long intensive workshops. Our philosophy is that the better law enforcement understands cryptocurrency and the ways in which public blockchains can be analyzed to detect and investigate criminal activity, the more effectively they can safeguard our customers and the ecosystem as a whole.

Our investigators spend hours with law enforcement each week explaining how to interpret the blockchain information in our subpoena responses and directing officers to the tools and resources they need to pursue their investigations. If we see an opportunity to help a law enforcement officer who does not have access to blockchain analysis tools, perhaps by helping them trace ransomware payments or stolen funds, we do it without hesitation.

We have also had the honor of being invited to speak at numerous law enforcement conferences and we have frequently been asked to brief senior law enforcement officials on cryptocurrency trends. For example, we recently worked with the REACT Task Force, also know as the Regional Enforcement Allied Computer Team Task Force, in San Jose on a joint briefing for the Secretary of Homeland Security on the topic of crypto account takeovers and investment scams. We have also briefed senior leadership within the Secret Service, and we recently hosted a Secret Service agent for a 3-month secondment with my team.

The teaching and sharing go both ways. Some of the world's leading crypto investigations experts work for U.S. law enforcement agencies, and we are fortunate to be learning from them on a daily basis. We frequently participate in various public-private sector working groups and meet with law enforcement partners to learn about trends in crypto-related crime that may be affecting our customers. We, in turn, can use this information to enhance our compliance programs.

An example of this is the quarterly investigative "sprints" that my department organizes, each focused on a specific crime type, where we solicit large amounts of data and blockchain intelligence from law enforcement partners around the world and conduct in-depth investigations. Our two most recent sprints focused on Child Sexual Abuse Material ("CSAM") and ransomware, and both resulted in actionable intelligence to law enforcement. This would not be possible without the close relationships we have built with law enforcement.

While we are proud of our successes investigating criminal activity, there are several major challenges we face. A small group of non-compliant foreign cryptoexchanges are the venues used by criminal actors to cash out their illicit gains, and those foreign exchanges use jurisdictional arbitrage to avoid U.S. regulations. The industry as a whole is seeing crypto stolen through scams and thefts going to bad actors overseas, usually via unregulated exchanges. Criminal actors generally avoid exchanges, like Coinbase, that have AML/KYC programs because they would likely be identified by us, have their account frozen, or referred to law enforcement. As an example, research indicates that from 2017–2019, over 80 per-

cent of ransomware cash-out activity was handled by just four offshore entities.[2] Twenty-twenty-one data so far shows that ~64 percent of ransomware cash-outs occurred on just 3 foreign exchanges. Of the top 10 recipients of ransomware payments, 8 are offshore exchanges and 2 are mixing services.

Further, despite the incredible proliferation of crypto investigation expertise throughout law enforcement agencies over the last several years, we often run into situations where law enforcement—especially at the local level—lacks the tools and resources necessary to pursue crypto-related crime. This is especially true in large-scale cases where victims may be located across the country, or in cases where the criminals are based overseas.

The U.S. Government should develop tailored solutions in this space to effectively target illicit activity that uses crypto. We know that a vast amount of illicit activity is happening on a small set of non-compliant offshore exchanges and mixing services that enable criminal actors to monetize their activity. While the Department of Justice has authority to prosecute individuals and entities involved in facilitating illicit activity, even when that activity is located abroad, directing more of law enforcement's investigations and resources to pursue those bad actors could very effectively disrupt those actors' infrastructure in the near-term. Further, we would recommend that Congress ensures law enforcement is well-equipped to develop local-State-Federal task forces to share information and combat illegal activity, as well as fund international partnerships that will help combat efforts by unregulated international entities to move crypto in a manner that facilitates illegal activity.

In closing, thank you Chairwoman Slotkin, Ranking Member Pfluger, and Members of the subcommittee for holding this important hearing today. Coinbase is committed to working with Congress and law enforcement to combat illicit finance and terrorism, while also protecting the privacy and security of our customers. Combating illegal activity on our platform is core to our mission of enabling economic freedom in a trusted, secure, and compliant way. Thank you and I look forward to answering your questions.

Chairwoman SLOTKIN. Great. I thank all the witnesses for your testimony.

I will remind the subcommittee that we will each have 5 minutes to question the panel for our Members who come in and out.

I will now recognize myself for questions.

So I guess the question is, you know, can you help us understand—we talk about the transparency in blockchain technology, we talk about how in many ways it might be easier to trace for the organizations that are playing by the rules and doing things right, but I keep hearing—I mean I think the average person hears in the news particularly about criminals and ransomware attacks where criminals are asking the victims to pay in cryptocurrency. The most famous one and the one where we had a hearing up here in the Homeland Security Committee was the Colonial Pipeline attack where a ransomware attack by criminals led to the shutting down of that pipeline and resulted in, you know, gas lines in some places in the eastern United States. So it affected the average person pretty significantly.

Now, as I understand it, in that particular case—and frankly I think it is a rarity, but we—actually the FBI was able to get back some of the money that was ransomed. But it is more symbolic of what I think the public is hearing, which is that these ransomware attacks are being—people are being asked to pay in crypto.

I had recently had all of the superintendents from the K through 12 schools in my district in Washington and I said raise your hand if you have been the victim—someone has tried to attack you and ransom the data of your students. Every single superintendent raised their hand. So it is like it is mainstream.

[2] Chainalysis 2021 Crypto Crime Report (Jan. 19, 2021).

Why—with what you are telling us and the I guess increased transparency and traceability through blockchain technology, why would these bad actors be choosing cryptocurrencies as their demand of choice in all these attacks? Anyone—Mr. Levin, do you want to start and then we will go around the horn here?

Mr. LEVIN. Thanks, Chairwoman. It is a fantastic question.

The nature of cryptocurrency, and actually the nature of people who attack for financial motivation, is to maximize financial return when you are carrying out these types of cyber attacks. So, you know, if you think about the way in which a ransom, you know, affects these schools is that it is done to maximize the profit of the people carrying out the attack. Those people carrying out the attack are typically not in your district attacking their own schools. So the two features of cryptocurrency that are the most relevant in order to achieve proper maximization is that, you know, this is a payment system that is entirely global in nature and that money can be transferred instantaneously and completely globally.

You know, that feature is, you know, both a feature and, you know, in this instance, creating a vulnerability for us, but if you think about it, you know, the transparency that we have over being able to follow those payments and map out the full network that actually facilitates these ransomware like attacks is actually our opportunity.

So, you know, we at Chainalysis help in instances like the Colonial Pipeline, help the FBI and Government partners actually, you know, recover some of that money, but even more importantly, identify the full supply chain that actually leads up to these types of attacks. What is the cyber infrastructure that is being bought. That is where, you know, real disruption can occur.

Chairwoman SLOTKIN. Yes, I would just say that—before I maybe see if anyone else wants to offer—so while I see the opportunities, and clearly we capitalized on those opportunities in getting some money back from the Colonial Pipeline attack, so many bad actors are using this currency that there must be a lot of bad actors back in these home countries, wherever they are emanating from, who are willing to like pay out that, you know, crypto when it comes out of the system somewhere.

So I guess my question is, you know, like every industry, right, there are white hats and black hats, there are good guys and bad guys. Obviously you are here, so you are in the white hat category. But what is the problem and what should we be doing on the bad guys who are so clearly providing opportunities to these actors? I mean I don't think it is by accident that they are all using crypto as the way they want to be paid.

So, Ms. Smith, do you want to say something to that? Then, Mr. Kothanek, do you want to add?

Ms. SMITH. Certainly. I mean I would add that the solutions that both Mr. Levin and Mr. Kothanek highlighted in their testimony will help with this as well. It is more resources for law enforcement so that when these attacks happen and they are reported, that people are able to go and track down the source of this.

You know, the challenge I think with ransomware is it did exist 20 years before the creation of Bitcoin. It dates back to 1989. So it does exist. For the reasons that Mr. Levin described I do think

that it is currently a desirable form of payment. But as we see more and more stories of people tracking down the source of the ransomware, I think that we will see less of that happening.

I do think, however, we also have a cybersecurity problem. I mean in the most benign cases of ransomware are the ones that merely want money. There may be ransomware attacks in the future that go after our critical infrastructure that are looking to cripple our economy and cause harm to our people. So we want to make sure that our systems are strong and can prevent against these types of attacks happening to begin with. I think that would also go a long way toward stopping the problem.

Chairwoman SLOTKIN. Mr. Kothanek, do you want to add something before I turn to my Ranking Member here?

Mr. KOTHANEK. Yes, ma'am.

I think in the time remaining I would like to say that, you know, if you are a cyber criminal and you are using crypto, you are going to have a bad day. We are going to track you down and we are going to find your finance and we are going to hopefully help the Government seize that crypto. It is not a great way to facilitate crime.

As Jonathan was saying, the ability to track the crypto across blockchain is fairly substantial. If you are going to use a system like Coinbase to try to, you know, pull that money out, we are also going to find you and we are going to shut you down. We will have the information that we can provide to Federal law enforcement to help punish you.

Chairwoman SLOTKIN. Great. I will turn to Mr. Pfluger. Since it is just the two of us, we may ping pong back and forth for a bit here.

Mr. PFLUGER. Thank you, Madam Chair.

Excellent opening statements and it highlights the reason for this hearing and there are so many questions. So I will start, Mr. Levin, with you and just to ask you if you can elaborate on the—maybe some of the foreign adversary use of crypto to evade sanctions. Specifically what actions are you seeing taken by Iran to mine crypto and is there any Chinese or CCP investment in these operations?

Mr. LEVIN. Thank you—sorry—Congressman.

So the way that we see cryptocurrency being used by nation-state actors is that you have countries like North Korea that actually have cyber operations that have been targeting cryptocurrency exchanges and projects to steal cryptocurrency to raise funds for their operations. We have also seen not so much Iranian nation-state-level actors, but we have seen ransomware emanate from Iran as well that was actually taken down by OFAC sanctioning the main intermediaries that were the enablers of these types of campaigns. So, you know, when we see—you know, you mentioned mining activity in both Russia and Iran, mining is a global competition. What that means is is that, you know, the more actually that the United States can have clean and efficient mining operations in this country, it actually reduces the profitability of any of the operations of any of the miners that are operating outside of the United States.

So you are actually—you know, we have not seen a large amount of cryptocurrency mining being able to be done at a nation-state level due to the fact the private industry is actually large and these operations are fairly sophisticated to be able to be in that global operation.

So, you know, when we have seen cryptocurrency used in countries like the ones that we are concerned about, you know, often times these are, you know, smaller actors, there are, you know, organized crime groups that we are concerned about that we track very closely. But we don't see sort-of the systemic use of cryptocurrency by the nation-state level. You know, maybe with the exception of North Korea. The United States has also done a good job of actually being able to disrupt and seize some of that money that has been stolen by North Korea in the past.

Mr. PFLUGER. Thank you.

Mr. Kothanek, can you walk us through your KYC, Know Your Customer, and anti-money-laundering process that you use to verify users and ensure that they are not engaged in illicit activity and how you balance that with the privacy protections that are needed, especially here in the United States for Americans? Are you with us? Is——

Chairwoman SLOTKIN. I think you need to unmute, sir.

Mr. KOTHANEK. Very sorry about that.

Chairwoman SLOTKIN. There we go.

Mr. PFLUGER. No problem.

Mr. KOTHANEK. Thank you for your question, sir.

So Coinbase, as alluded to, has a very substantial AML and BSA program and KYC. So when a customer signs up for the account, we are going to take a risk-based decision on that account. We are going to grab their ID, we are going to have a copy of that, we are going to have their address, we are going to ask them questions, for example, like, how much money do you plan on moving through our system? We put that into our system and we are constantly updating our algorithms and our TMS system to be able bounce off against that information. If anything falls out of, you know, spec, so to speak, with that information, we will, you know, ask further questions.

As a regulated money transmitter and money service business, the United States will require to maintain a BSA and AML program just like any other financial institution that is out there. I think the importance of that is that along with the device ID, along with the IP addressing, along with the other information that we collect and the way we do social media checks, we provide something that if you are a bad actor, if you are breaking the law, we are going to be able to provide that information to law enforcement. It also helps us track and monitor transactions and be able to identify that on the blockchain. If there is a fraud attempt, for example, and other exchanges or law enforcement reaches out to us, we can quickly track down that crypto that enters our system and take corrective actions on that.

Mr. PFLUGER. Thank you so much.

Mr. KOTHANEK. Did that answer your question?

Mr. PFLUGER. Yes. I feel confident we will have another round, so I will yield back at this time.

Chairwoman SLOTKIN. Indeed.

The Chair recognizes Mr. LaTurner from Kansas.

Mr. LATURNER. Thank you, Madam Chairwoman.

My first question is for Mr. Levin.

Do some cryptocurrencies tend to be favored by nefarious actors over others? How about specific exchanges? Could you explain why? Are they more difficult to trace or more accessible to the user if you go cryptocurrency by cryptocurrency?

Mr. LEVIN. Thank you, Congressman.

The way in which we see the adoption specifically in relation to terrorist financing in cryptocurrencies is again a profit maximizing and global fundraising effort by terrorist organizations. For that, again, the global nature and the instant transfer of cryptocurrencies is largely done with the most liquid and accessible cryptocurrencies, which are the most possible, including Bitcoin.

You know, there are anonymizing technologies that are implemented in some cryptocurrencies and, you know, we do see some actors in minority moving to those. But, again, their usability is less than the most liquid and popular cryptocurrencies where there is better infrastructure. So, you know, for the most part we see, you know, the activity centered in the most liquid and popular cryptocurrencies, which allows us to have the techniques and transparency that allows us to go after that.

In terms of, you know, the different businesses—and you referred to the exchanges—I will echo the comments earlier, that there are, you know, several international jurisdictions where we need to actually help them build capacity to investigate and oversee the cryptocurrency markets in those countries to be better partners to the United States to weed out this activity. Actually I think that is something that, you know, this committee in concert with, you know, partners at the State Department can actually help, you know, move against those gaps in the system.

Mr. LATURNER. Thank you for that.

My next question is for Kristin Smith.

As you know well, cryptocurrency is being used more and more by people for legitimate reasons. While most crypto transactions are made for legal reasons, criminals and terrorists are still benefiting from the anonymity provided by cryptocurrencies. How can the Government reconcile policy that is beneficial to the expanding cryptocurrency platform while also responding to the bad actors who bend the digital asset to their will?

Ms. SMITH. Thank you for your question, Mr. LaTurner.

I think it is important to remember that there is regulation in this space. If you go back to 2013, the Financial Crimes Enforcement Network was one of the very first agencies of its kind globally, but the first Federal agency in the United States to put forth policies in this space. I think for those of us working and building in the crypto industry, we don't want illicit actors to be using these networks either. I think the goals there are mutual, that we want to find the policies in order to do that.

So I think we have made tremendous strides in putting the right regulatory framework in place and also building out the technologies available to help track bad actors on the internet. What we need to do is continue, like Mr. Levin was saying, to put re-

sources into these efforts, to do the training here in the United States of our Federal, State, and local law enforcement, but also helping our international counterparts make sure that they have the ability to do the same level of investigation and analysis we do here in the United States. So I think these are mutual goals.

I would note that—and Chairwoman Slotkin noted this in her testimony—if you look last year, the percentage of illicit finance by volume was up 79 percent, but if you look at the overall increase in transactions in this space, it is up 567 percent.

So the good news is as more and more people are using crypto networks and transacting using crypto networks, the percentage of illicit use is, you know, increasing at a far less pace. So I think that as more and more criminals realize that these networks are transparent, that there is a very good chance that they will be caught if they are conducting activity in this space. You know, we are going to to continue to see the divide where there is more legitimate uses and far fewer illicit financial uses.

Mr. LATURNER. Thank you very much, Ms. Smith.

Madam Chairwoman, I yield back.

Chairwoman SLOTKIN. Thank you.

The Chair recognizes for 5 minutes the gentleman from New Jersey, Mr. Gottheimer.

Mr. GOTTHEIMER. Thank you, Chairwoman Slotkin. I thank the witnesses for your perspective today on these critical tools.

I released a draft of the Stablecoin Innovation and Protection Act earlier this year that would establish definitions and requirements for bank and non-bank issuers of qualified stablecoins. Under the bill a qualified stablecoin would have to be backed 100 percent by cash or cash equivalents to be considered qualified. The bill would also ask the office of the comptroller of the currency and task them with establishing anti-money-laundering and Know Your Customer guardrails for qualified stablecoins.

Unlike some of my colleagues on this committee, I believe digital assets have the potential to revolutionize the way we do business around the globe and I believe the United States should be a global leader in developing systems to manage this emerging technology.

I guess if I can start with you, Ms. Smith.

If Congress looks at crypto legislation through a partisan lens and fails to enact meaningful reform soon, do you believe we will see further volatility like we saw a few weeks ago with TERA? Do you believe Congress failing to act on crypto legislation poses a threat to our National security?

Ms. SMITH. Thank you, Mr. Gottheimer. Thank you for your leadership in the crypto space. I think that your stablecoin legislation is by far the most comprehensive proposal we have seen over here in the House and appreciate your leadership in this space.

I do think there are some regulatory gaps. As I had mentioned before, there is a lot of regulation in this space and Federal agencies for the most part have done a very good job of interpreting the rules that they have today to apply to cryptocurrency. But this is a very different technology and there are some holes. I think there are two areas in particular that will go a long way toward protecting consumers better, but also maybe helping with some of the

events that we saw a couple of weeks ago where one cryptocurrency sort-of entirely collapsed.

One of them is to provide some guardrails around dollar-backed stablecoins. I think that is a very important topic. It is one that the President's working group has issued a report on. There have been several hearings in Congress.

The other area that I think would go a long way toward addressing that is coming up with an appropriate framework for spot exchange regulation. This is something that is very clearly not authorized to any Federal agency today and it is a space where Congress also should act. Your colleagues on the House Agriculture Committee have put forth legislation called the Digital Commodity Exchange Act, which is by no means perfect, but by far the most comprehensive effort we see. I think if there was a scenario where exchanges registered with the Commodity and Futures Trading Commission as a crypto exchange and there were disclosures that the exchanges provided to customers about what is backing the cryptocurrency, whether it be a stablecoin or other. I think that would go a long way toward preventing the problems that we saw a couple of weeks ago.

Mr. GOTTHEIMER. Thank you, Ms. Smith.

I share the concerns my colleagues have expressed by the use of cryptocurrencies by bad actors. Just last year I was shocked to see a report that Hamas and its affiliates received a flood of donations in Bitcoin after resuming their horrific attacks on Israel and the West Bank. My bill, the Hamas International Financing Prevention Act, would put sanctions on any foreign states that fund Hamas and punish those nations for supporting such violence.

I am concerned, however, that Hamas may operate in countries that lack the capacity or willingness to police illicit uses of digital currencies.

I guess I will turn to you, Mr. Levin.

As you know, the blockchain technology that supports digital assets often holds insights that help law enforcement and government track the flow of digital assets and can provide indications of specific actors that have held them. Even though, again, some of my colleagues don't understand the value of blockchain, what do you believe are the biggest obstacles preventing foreign governments and financial bodies from implementing AML, KYC guardrails that would prevent funds from reaching bad actors?

Mr. LEVIN. Thank you, Congressman.

I share the concern. The way that we think that many countries around the world need to be able to investigate this is through actually acquiring technology and adopting it. The innovation behind cryptocurrencies mean that these governments need to have dedicated people that actually understand cryptocurrencies and while they are bolstering their basic forms of AML oversight, you know, they need additional help and training from experts. We actually in this country have the ability to use the State Department and other resources at our disposal to add to their capacity, particularly in places where we feel like there are gaps in this capacity in those countries. But with that, there is no obstacle actually for them being able to weed out this activity and collaborate in the global effort against terror.

Mr. GOTTHEIMER. Thanks. May I continue?

Ms. Smith, can I follow up and ask—get your perspective on that same question, if you don't mind? Also if you can give me a sense of what areas of the world are you most concerned about as well.

Ms. SMITH. Yes, no, absolutely. I mean I echo everything Mr. Levin had said.

You know, the Financial Action Task Force, which is an interagency kind-of—or an international sort-of working group of regulators in this space, meets frequently to discuss these topics. Part of the process that they undertake are these mutual evaluations of different countries. There is a list that they publish every year, it is called "the grey list", that lists several companies that are really sort-of behind the level of standards that we see in other countries. So I will be happy to send that list to your staff. It is often countries that have less-developed economies, those that are in parts of the world that maybe have a little bit less rule of law. I think that if we can work to coordinate with them, that this will go a long way toward addressing those issues.

Mr. GOTTHEIMER. Thank you so much.

Can you just add a little bit more about any other obstacles you believe are preventing foreign governments and financial bodies from implementing some of these AML, KYC critical guardrails?

Ms. SMITH. Well, I think a lot of it is the standard issue, right. It is resources, it is training, it is lack of priority perhaps within parts of their government. I think that, you know, international pressure in this space is important. I think that legislation like yours is important. I think that, you know, we need to make sure that we continue to have a dialog that, you know, this—the nature, as Mr. Levin pointed out earlier, of these cryptocurrencies is that they are global. So we have to work globally in order to make sure that we have appropriate standards that are similar from jurisdiction to jurisdiction.

Mr. GOTTHEIMER. Thank you.

I yield back.

Chairwoman SLOTKIN. Thank you.

We will now go into a second round and I will recognize myself for 5 minutes and I will keep us to better time here.

Quick questions. Can you help me understand—you know, many folks have suggested that the war between Russia and Ukraine is sort-of the first moment where we are seeing the introduction of cryptocurrencies as an asset, frankly, I think to both sides. We certainly know that the Russians and the country of Russia are where many of these ransomware and criminal groups and sometimes, you know, bad actors representing the state are emanating from. But I also understand that in the early days of the war, President Zelinski was helping to fund his government by setting up around him his own cryptocurrency Dow.

So can someone speak to kind-of how the crypto is engaged in sort-of our most recent war?

Ms. Smith.

Ms. SMITH. Yes. No, thank you for the question, Chairwoman Slotkin.

It is very interesting. I think at the beginning of this there was a tremendous amount of concern that despite the sanctions effort

by the United States and other countries on Russia, that they would perhaps use cryptocurrencies as a way to skirt those sanctions. It is important to remember that sanctions apply to cryptocurrencies just as they apply to dollars or seashells or whatever form of currency might be transacting in. That any U.S. person anywhere in the globe has an obligation, whether as an individual or a company, to not transact with those on the sanctions list.

So that was certainly though a concern in the beginning that cryptocurrency might somehow be used.

The truth of the matter is it goes to—it is a liquidity issue, as Mr. Levin was talking about before. The trading pairs with Bitcoin, Ethereum, other popular cryptocurrencies, and Rubles, are not large enough to compete with the amount of money that Russia needs in order to take on this transaction. Folks like Coinbase, Chainalysis, law enforcement, are watching very closely to make sure that cryptocurrency isn't being used in this way.

I think where cryptocurrency is being used has been a really fascinating thing to observe. There have been two main developments. The first is that the last I checked somewhere over $150 million of donations have gone directly to the Ukrainian government and NGO's that are helping with the effort. That was global money that was collected instantaneously and quickly in a time of crisis, which I think has been really, really heartening to see.

We have also heard stories though—and I think this is incredibly important—that in times of crisis where people are forced to flee their homes because they are able to have self-custody and have assets in cryptocurrency, they can take them with them. They don't have to go to a bank that might not be open or might have run out of cash, they don't have to deal with the inflation that could be happening in their environment. So I think that we are seeing a lot of stories about individuals who have had to uproot their lives, but are still able to take their savings with them. So I think that has been an important story that has come out of this conflict as well.

Chairwoman SLOTKIN. Mr. Levin, do you want to add anything to—I just think it is a historic moment in the history of warfare; as someone who is from the CIA and the Pentagon, to see how cryptocurrency is playing a role on frankly potentially both sides.

So can you speak a little bit to that in the minute-and-a-half I have left?

Mr. LEVIN. Yes, Chairwoman. Thank you so much for this. I do agree that this is the first moment that we have really seen cryptocurrency enter a modern conflict.

The way that the donations have occurred actually are that it was faster to be able to get money into the Ukraine through the use of cryptocurrency than any other financial means necessary. Obviously the magnitude of assistance that has been, you know, dedicated by United States and allies, you know, actually is a lot larger than $150 million. That being said, you know, within minutes, you know, money was sent into the country that actually provided the ability for the Ukrainian government to buy bullet-proof vests, emergency meals when they needed it the most.

So I think that the global nature and the instantaneous nature of cryptocurrencies was a very important part of that being used in the conflict.

The other thing that I would note is that, you know, what we do observe in the cyber realm is, you know, increased attacks, increased threats on Ukrainian infrastructure. Some of that does relate to cryptocurrency where we are able to use the transparent nature to actually track Russian activity on these types of networks. That means that we can actually assess, you know, potentially predicated attacks on Ukrainian infrastructure and U.S. infrastructure through the use of tracking cryptocurrency purchases for infrastructure.

Chairwoman SLOTKIN. Well, I think it is a fascinating case study and I think it would be super interesting for someone to write a piece about, you know, the kind of captures, the lessons learned.

I recognize the Ranking Member, Mr. Pfluger, for 5 minutes.

Mr. PFLUGER. Thank you, Madam Chair.

Great discussion so far.

I would like to kind-of just take a step back a little bit.

Ms. Smith, you mentioned—you made a comment about critical infrastructure and if we back out a little bit—we have been focused on crypto and how it is being used potentially in the terror realm, but what kind of guardrails, policy guardrails or—you know, the nature of trade right now is just—it is so international and especially with the cyber domain. What are we looking at as gaps or vulnerabilities just in the cyber domain that we need to be taking a closer look at that then potentially open up the vulnerabilities that you mentioned when it comes to critical infrastructure and how crypto would interact with that.

Ms. SMITH. Yes, no, I think that figuring out how to boost the cyber defenses for our critical infrastructure providers is incredibly important. I mean I believe it was with the Colonial Pipeline hack where there wasn't even two-factor authentication or even a password in some cases, right. So a lot of times it is making sure that our small businesses or our businesses that aren't as technologically savvy, that they have the tools and the education and information that they need in order to protect their own infrastructure.

I would say, though, for the crypto industry, which is obviously much more technologically sophisticated, that they have very strong defenses in place. There have been situations, not so much in the United States, but overseas where there have been hacks or mistakes that have happened that have caused people to lose assets. But I think the thing that is important to remember when you are looking at blockchains is that blockchains are immutable and they can't be changed. They are incredibly strong and the networks that run these blockchains are also incredibly strong. I think that the strength of a crypto network is that it is decentralized. So unlike a comparable network that might be run by a single company, there is a lot of vulnerability there when you only have one actor. But when you have these decentralized where there are players and participants from all over the world that are helping with the operation of the network, they are incredibly strong and we have not seen situations in the—I don't know, where are we at, 13

years now with Bitcoin—we have never once seen any sort of hack within the Bitcoin blockchain itself. So it is an incredibly strong technology and one of the reasons why so many people are excited to be building on it.

Mr. PFLUGER. Thank you. I think it speaks to the public-private partnerships on the security side. I forget who mentioned about the mining operations that are happening here. Was that you, Ms. Smith? Or was it——

Mr. LEVIN. That was me, Ranking Member.

Mr. PFLUGER. Can you talk through—are you talking about the facilities being housed in the United States? I mean the actual—where the databases and the computers and all that? Is that what you are referring to?

Mr. LEVIN. Yes, Ranking Member. There are significant amounts of operations where you have data centers with mining equipment that are using, you know, renewable energy, for example, in this country or excess energy in certain cases to actually mine cryptocurrency. It is a vibrant industry with—you know, that—it is actually growing at an increasing pace actually.

Mr. PFLUGER. Let me just ask this specific question, because a lot of these are actually happening in my district. Is this something—and I would like maybe all of your input on this—is this something that we should be exploring, we should be encouraging per competition to compete with foreign actors?

Mr. LEVIN. Yes, Ranking Member. I think that, you know, for instance I imagine it is generating a lot of jobs, for example, in your district. Encouraging actually the development of, you know cryptocurrency security and the provision of these networks in this country is about us taking a lead position in the industry. It does make it, as I said, less profitable for adversaries. You know, the more efficient, the more developed that this industry gets in this country, it is a global competition by its very nature. So I do encourage us to look at how we can bolster the industry domestically.

Mr. PFLUGER. I see head nods from Ms. Smith.

Mr. Kothanek, your take on that?

Mr. KOTHANEK. Yes, sir.

I think this is a great issue and I believe our country should be the first in this kind of technology. We have brilliant talented folks across the United States that are able to kind-of come up with great solutions to very challenging problems. I feel United States is the place where we should be investing in this technology.

Mr. PFLUGER. Ms. Smith.

Chairwoman SLOTKIN. I am sorry. I am going to try to stick us to 5 minutes. I know we have got a couple of other Members who have joined us.

The Chair recognizes for 5 minutes the gentleman from Rhode Island, Mr. Langevin.

Mr. LANGEVIN. Thank you, Madam Chair. Can you hear me OK?

Chairwoman SLOTKIN. We can.

Mr. LANGEVIN. Great. All right. I wanted to thank our—Madam Chair, thank you for holding this hearing, and the Ranking Member, the witnesses for testimony today.

So I had a few questions. I wanted to start off though, unfortunately I was not able to join on the—to the Government website

as a participant, but I was listening to the entire hearing through the public channel, so I did hear the testimony. I wanted to start with going back to the Chairwoman's opening question, because I don't think it was quite fully answered, or at least I missed a step in there. So perhaps that's the issue.

But with respect to crypto and the transparency, and it is being used as kind-of the payment method of choice by these bad actors that are carrying out ransomware attacks, particularly in Colonial, you didn't quite—at least I didn't quite understand the reason why it is not more traceable if crypto payments are so transparent and you can see where it is going.

Now I chair the Cyber Subcommittee on the House Armed Services Committee. I have had General Nakasone, who as you know heads up NSA and U.S. Cyber Command, and we discussed this issue. I won't get into the Classified answers that he gave, but ostensibly getting some of the money back with that Colonial Pipeline attack was more of an anomaly that we were able to do that because we had certain information, which I won't get into. But why isn't it more traceable or not more actionable that we could get all of the money back, not just some of the money, which was happened in Colonial? Is it that they—I know that your answer you said that they can move it around quickly or instantaneously. It is that they take the money out and transfer it to something that is more traditional currency and that is why we can't get it back and just seize it all?

But if you could more fully answer the Chairwoman's question.

Mr. LEVIN. Thank you, Congressman. It is a good clarifying question and I am happy to sort-of distinguish the difference between traceability on the one hand and what I would call seizability on the other.

So if you have the blockchain, you have every single transaction that has ever happened. That is always going to be there and, you know, through the technology that we have at Chainalysis it is possible to trace that the end points where it does intersect with local currency. Yes, you know, in this instance, you know, traceability is always there. But in terms of the actions that can be taken and, you know, not going into the specifics on the Colonial Pipeline case, just being able to see the money does not mean that we can actually go and take the money from the person who is in control of that money.

So this is where, you know, we need to——

Mr. LANGEVIN. Why is that? Why is that?

Mr. LEVIN. So the way in which cryptocurrency works is that, you know, it is controlled by a private key, a secret that someone holds. If you do not gain access to that secret, you do not have permission on the cryptocurrency network to move the funds that are associated with that secret. So, you know, it is possible in this—in cryptocurrency to hold, you know, currency locally just to you your person, the same way that you can hold $100 bill inside your wallet.

So, you know, we would need to have physical access or, you know, cyber access to a private key in order to move those funds in this type of case.

Mr. LANGEVIN. OK. Thank you for clarifying.

So let me ask this other question before time runs out.

So do you see opportunities to improve law enforcement training and expertise on cryptocurrency and blockchain analysis in the context of domestic and foreign terrorism? If so, how can Congress support those efforts?

Mr. LEVIN. Thank you, Congressman.

The ability for the different agencies to actually have training programs, you know, is a resource—is largely a resource question.

Chairwoman SLOTKIN. Sorry. Mr. Kothanek, if you can just mute for just a second.

Thank you.

Mr. LEVIN. Thank you, Congressman.

It is largely a question of resources and the need for basic levels of training to be given to really all law enforcement components that deal with this. You know, it is a horizontal issue that crosses not just the cyber realm, but across these different agencies. I think it needs to be recognized as a basic capability that goes across, you know, the entire breadth of Government agencies. That is largely a resource and strategy question.

Chairwoman SLOTKIN. All right. We will have to leave it there.

The Chair recognizes for 5 minutes the gentleman from the great State of Michigan, Mr. Meijer.

Mr. MEIJER. Thank you, Madam Chair. Can you hear me?

Chairwoman SLOTKIN. Indeed.

Mr. MEIJER. Thank you. Thank you for holding this panel today and to our Ranking Member and to all of our witnesses.

Earlier this week I was in district talking with a constituent who has a business that focuses on both preventing but also the recovery of funds that were transferred illicitly through business email compromise. I think one of the big challenges that sector has, and we have seen just doubling of the amount of funds that have been gained through illicit wire fraud, you know, getting into a pattern of life analysis, being able to compromise someone's email and then sharing inaccurate wiring instructions, especially in one-off transactions. Now, their goal is to stop that illicit flow prior to it hitting a bank account work and then be converted into cryptocurrency and, as is often the case—and as Mr. Levin was describing—the challenge is then on the traceability side, which is they have seen those funds just go into, you know, one wallet and then, you know, you have many different wallets that are dovetailed.

You know, on that initial step of trying to prevent, you know, funds that have been illicitly gained or have been stolen from getting converted into cryptocurrency—because we have discussed some of those traceability problems, are there any steps—and maybe this is for both Mr. Levin and also Mr. Kothanek—any steps that could be taken so that once we get—and I think the numbers that we have, that $7.8 billion increase in trading volume for illicit addresses between, you know, 2020 and 2021, what can we do kind-of left of there, you know, recognizing those challenges once those transactions kind-of get within the cryptocurrency space?

Mr. LEVIN. Thank you Congressman. I will go first and I will pass it to my esteemed colleague who will be able to fill in the rest.

The ability for us to take down enabling infrastructure is really at the core of preventing further business email compromise. If you

saw yesterday the Department of Justice announced the take-down of a Social Security and fraud shop on-line that actually, you know, sold these types of credentials that actually lead to the types of social engineering attacks that cause business email compromise. If we can actually, you know, use cryptocurrency analysis to look at, you know, what is the proceeds being used for, what is the infrastructure being bought by the cyber actors that we are going after, we can cut off these attacks before the actually hit our businesses.

So, you know, I think that that is, you know, at the far left of what we want to be doing, is making sure that, you know, our Government agencies have the resources to be able to go after the enablers in this ecosystem that actually are the root cause of, you know, these problems.

You know, once it gets into cryptocurrency, you know, it is important that the Government actually shares information with the private sector. You know, it is important that OFAC designates addresses and associates that to threat actors so that the industry can act. You know, there needs to be much greater partnership between private and public sectors in order to be able to combat these threats in real time. That is also a kind-of global issue. You know, I recognize that FinCEN has done a lot of good work on business email compromise internationally to help with some of those funds being seized in a rapid response program. I think that that, you know, needs to be extended and used in the cryptocurrency context as well. But, you know, I will say that, you know, at Chainalysis we are able to identify, you know, these types of actors and label it in real-time systems that helps businesses, you know, actually act on this information. The traceability of it means that we can then map out the entire network that is involved in, you know, going after our businesses and creating the fraud.

Mr. KOTHANEK. Yes, sir. If I can add very quickly—and thank you for this question. This is right in the wheelhouse of my team and I think, very quickly, one of the things that we have been working on with our law enforcement partners and partners at financial institutions. The faster that we can find out about this type of issue or this business email compromise, the quicker the action that we can take on the account. So what we have, for example, is IC3 with the FBI will very quickly reach out to us they have been notified of a compromise. They contact us. My duty investigator goes into the account, takes a look at the account, is able to very often freeze funds, or we can track it very quickly to another exchange that we can cooperate with and law enforcement is able to pull back those funds, you know, through the seizure process and help recover those funds. I think the more practice we have at, so to speak, and the more that we are able to communicate with our partners in law enforcement and in the financial world that we will help them, the better off we are all going to be.

Mr. MEIJER. Thank you, Madam Chair.

I yield back.

Chairwoman SLOTKIN. Thank you.

We will go into a final round of questions. I apologize, the Ranking Member had to head to the floor.

I will recognize myself for 5 minutes and then I know at least Mr. Langevin and potentially Mr. Meijer wanted to do a second round.

So I guess the thing I will say to sort-of—in my concluding question is I—part of the reason we have this hearing was to try and set us off, the Congress and the cryptocurrency community, on a better foot than we now find ourselves with the big social media giants. I think the story line that at least carries the day up here is that the social media companies told us in the late 1990's and 2000's—I wasn't here—but the lore goes like don't touch us, don't touch us, don't touch us, please don't provide any regulation. You will kill entrepreneurialism and all this good spirit. Then kind-of things turned on them, particularly recently, and users were frustrated with the policies by these private companies. Suddenly Facebook is targeting, you know, my Facebook feed, saying, Congress, you are so lame, you haven't, you know, updated regulations since the 1990's. So it is I would say—a charitable view is that they played their relationship with the U.S. Congress wrong. We have all kinds of problems up here. I would never say we are in a good place on having agreement on how to think about dealing with the social media companies, but my plea is that we not go down the same road with the cryptocurrency community, that we instead work together and figure out how to put in the right left and right limits that gives the white hats, the good guys in the industry, the protections you need and the perception you need, which is that you root out bad guys, you don't allow criminals to use your networks, and then allows law enforcement to properly hyper-target the bad guys and go after the bad guys.

So in that spirit of open arms and wanting to do things differently and learn the lessons of a different new industry, could you all talk about—I know this is going to be difficult, but if you were in our shoes, what would you do to make sure that bad actors couldn't credibly use your platforms and other platforms? I know we have talked about money, but we can always talk about money for law enforcement, but what literal law would be advantageous to your community? Knowing that the answer of nothing please is not going to boomerang well on you all.

Ms. Smith.

Ms. SMITH. No, thank you. I think it is an important question.

I mean, listen, there is really good policy in place and FinCEN and OFAC have been doing a really good job. I do think thought that we need to watch very closely what is happening in the illicit finance space. If we see that there are changes in the types of tokens that are being used, we might need to look at enhanced Know Your Customer measures for certain tokens. I think that, you know, one exciting development going on in the industry right is the development of identity solutions that might require an update down the road. Because if you think of today, if you go to a bar, you show your ID with your name, your address, your height, your weight, you know, all of your personal information when all that bar needs to know is that you are over 21. They don't need to know anything more specific than that. There are really interesting things going on in the digital identity space today that will allow

for individual wallets to be able to carry information with them about the person without having to share the information.

So I think one of the most important things we can do is follow the development of that technology, because we might be able to change the structure of the regulations that we have in place today to be more effective as the technology evolves.

Chairwoman SLOTKIN. Thank you.

Mr. Levin.

Mr. LEVIN. Thank you, Chairwoman. It is the question.

The thing that we need to sort out first is the innovators in this country need to know exactly where they stand with regulators. Today there is a gray area and a lack of legal certainty if you are innovating in, you know, stablecoins for example, that, you know, even building sort-of projects like, you know, helium and infrastructure that can actually allow people to have, you know, physical networks that are joined by cryptocurrency that are, you know, the market innovation that we all want. So I think that that is really important.

I think from preventing illicit activity, and I will highlight two sort-of big ideas. One is on the information-sharing side. You know, it is important that Congress provides adequate legal frameworks and certainty to be able to share information across borders as well as domestically, you know, when it comes to sharing information with private industry on this.

Finally, I think it is important that actually we think about approaches where we have centers where public-sector agencies as well as private-sector agencies can jointly come together to actually fight in this and use the nature of the technology to detect and prevent illicit activity.

Chairwoman SLOTKIN. Thank you. Thank you for that.

The Chair recognizes for 5 minutes the gentleman from Michigan, Mr. Meijer.

Mr. MEIJER. Thank you, Madam Chair.

One question that I posed when we held a similar hearing with the Secret Service and DHS several months ago, and this may be an unfounded concern, but given how broad the ecosystem is of various digital are in cryptocurrencies, you know, and outside of the main, you know, large, better-established—and frankly, that we have certainly seen fluctuations in their value in the past couple of months—you know, harder to manipulate or harder to rapidly inflate the value of a Bitcoin versus, you know, some much smaller altcoin where instead—and this is my concern and I just want to pose it to our witnesses to see if it is well-founded or, frankly, not—that illicit actors may—and especially in the ransomware space—may request, you know, an investment in a very low-market cap, very poorly capitalized coin because that million-dollar transfer coming from a ransomware attack then being able to raise that overall value of that coin, you know, pump that up and then allow them on the flip side, whoever was owning, you know, that one cent coin that went to a dollar coin, be able to dump it on the other end in a way of evading, you know, some of the more well-established ways of tracing those flows. Is that a well-founded fear? Have we seen any evidence of that yet? You know, are there ways in which the large diversity of coins, those altcoins that could be,

you know, exposing us to risk that—you know, above and apart from just the general cryptocurrency space?

Just wanted to throw that out to the witnesses and, I don't know if you want to start, Mr. Levin? Then maybe Mr. Kothanek and Ms. Smith.

Mr. LEVIN. Thank you. Thank you, Congressman.

Definitely an interesting, you know, thought about how exactly, you know, criminals are moving money. I often say that, you know, the creativity of this is something that we have to keep on top of. There is always new innovation.

That being said, you know, when it comes to specifically ransomware, and even terrorist financing organizations that are raising capital, I go back to the idea of profit maximization, revenue maximization, which is about using the most liquid forms of cryptocurrency. So we don't see, you know, the use of this long tail of cryptocurrencies, of coins that no one has ever heard of actually being used as a payment instrument largely because, you know, the victim has never heard of it and maybe doesn't trust it as much and doesn't know, you know, what they may be getting themselves into.

So, you know, where we have seen the use of the long tail—you know, I would say it goes back to your concerns around market manipulation or actually in the laundering process of these coins. The good news is is that most of the long tail are just carbon copies or, you know, are as transparent as, you know, Bitcoin and Ethereum. So, you know, a large transaction in a low-volume, low-liquidity coin is very traceable when it comes to, you know, it being used in a laundering process. So oftentimes doesn't actually, you know, give the sort-of anonymity or obfuscation that the person is trying to occur.

I would say that, you know, when it comes to monitoring for market manipulation, you know, I think it is really important that we encourage the regulators that have jurisdiction over that to actually have the technology to monitor this proactively rather than reactively.

Mr. MEIJER. Thank you. Mr. Kothanek——

Mr. KOTHANEK. Yes, sir.

Mr. MEIJER [continuing]. Anything to add?

Mr. KOTHANEK. Yes, sir, absolutely. Thank you for the question.

So I think that, you know, one of the things that I appreciate about this topic is that, for example, when Coinbase lists a coin on our system, they go through a due diligence process. You know, we interact with these different altcoin operators and for the most part they are great people, they are good companies, they have solid backgrounds, they have solid foundations to their coin. What that means to me and what that says to me is they are somebody that we can reach out to and they are not going to get in bed, so to speak, with a ransomware provider or—you know, they are not going to purposely break the law in that way.

So I think your question is a good one, but it is a little bit—you know, it is not very realistic because I think the providers of these altcoins are just great companies that are going to do a good job, just like Coinbase does, just like the other exchanges out there

often do. Yes, I think that doesn't make it very easy for these companies to be taken advantage of.

Chairwoman SLOTKIN. We will have to leave it at that. Thank you.

The Chair recognizes for 5 minutes the gentleman from Rhode Island, Mr. Langevin.

Mr. LANGEVIN. Thank you, Madam Chair.

So did either Ms. Smith or Mr. Kothanek have anything to add on the first question in terms of traceability and, you know, to recover Bitcoin when we do know where it is or was the answer fully, you know, given? Is that fine? If not, I want to go to Mr. Kothanek about law enforcement training and see if he had anything to add there.

Mr. KOTHANEK. Yes, sir. Great question. Great question, sir. Thank you very much for that.

So I think regarding law enforcement training, if I can go back a little bit to when I was with Paypal and a lot of folks were—you know, in the law enforcement community were kind-of No. 2 pencil folks. They were struggling a little bit with the technology. Fast-forward now to when I joined Coinbase in 2014 and even now, I have been incredibly impressed with Federal law enforcement, State, and local, international law enforcement and their ability to kind-of keep up with this technology. Some of them are enthusiasts and they are very well-versed in not only computer technology, the internet, and cyber crime, but they understand crypto. Those that don't reach out to us and we often provide training. My staff loves to sit down with law enforcement, visit with them, and provide soup-to-nuts training. We will sit down with them and they will either start, you know, at a very basic level or we will go up to advanced, you know, blockchain tracking to help them out. Whatever they need. I think law enforcement knows that we are available. I know, you know, Chainalysis has some great training programs as well.

I think we are very well-covered with law enforcement. We just need to help get them some more resources so they can have the money to do that.

Thank you.

Mr. LANGEVIN. Thank you.

Ms. Smith, have anything to add?

Ms. SMITH. You know, the only thing I would add is that every conversation that I have with someone in law enforcement, particularly those who have been involved in these investigations, I ask would you rather be dealing with criminals that are holding a bag of cash or that have a wallet of Bitcoin, and they say wallet of Bitcoin every time because they are successful. I think the fact that we see so many headlines about different criminal activity involved in cryptocurrency is actually a feature not a bug, right. This means we are finding them. I think it is the stories that we don't see, where criminals are using cash, that we just don't—aren't able to trace and we don't have any headlines.

So I think the fact that we are able to trace these transactions and in many cases ultimately lead to arrests, is a positive thing and would encourage all the training we need to get law enforcement to be able to maximize the pursuit of the criminals.

Mr. LANGEVIN. Thank you.

Let me turn to Mr. Levin if I could. I know we touched on this subject a bit, may do a deeper dive on it. In your company's analysis, have you observed state-sponsored organizations engaging with terrorist groups in pursuit to log their cryptocurrency or otherwise engage in illicit activity on blockchain? Also in your company's analysis, do you observe different terrorist organizations adopting different tactics as they use cryptocurrency and cryptocurrency exchanges? If so, what factors do you think account for those variances?

Mr. LEVIN. Thank you, Congressman.

The way the different terrorist organizations use funds really divides into two types of usage. The first is, you know, global finance campaigns where groups are actually using cryptocurrency addresses that they publish on-line, that they solicit donations on to finance, you know, their operations. Then the second way that we see terrorist organizations use cryptocurrencies is actually in the purchase of cyber infrastructure or enabling infrastructure that helps them with, you know, recruitment or radicalization or cyber operations. So, you know, the levels of sophistication among these groups is really the main determinant of the different techniques and strategies that they employ.

In general, I would say that we see a much lower level of sophistication in terrorist organizations' use of cryptocurrency than we do in the nation-state actors or organized cyber crime groups. So, you know, we tend to see very low levels of sophistication, which has led to, you know, law enforcement being very successful in actually combatting especially the global financing campaigns that have been run by these terrorist organizations. Actually, you know, we are able to enumerate, you know, exactly how much money they have been raising—not a very a minuscule amount compared to their overall operating budgets.

Mr. LANGEVIN. Thank you.

My time has expired.

I yield back.

Chairwoman SLOTKIN. Thank you.

I would say, as we conclude here, for me some of the big takeaways and hopefully for you all—and thank you to Mr. Langevin for putting a fine point on it—the difference between traceability and retrievability, which I can imagine from my past life is going to be of a lot of interest to the National security world and making sure we understand how not just to see bad actors and see bad activity, but actually do something about it. But then also just I think hopefully you believe the bipartisan commitment to try and have a different story that we all follow in terms of the relationship between Congress and the crypto community. We don't want it to be the same way it has been around kind-of the big tech and social media. I hope you don't want that either. What I would encourage is that we will always be open to white papers or, you know, policy papers, ideas that you have because I think the worst-case scenario is you get a bunch of people up here who don't understand the technology, whose public is saying we don't know what this is, our kids are investing in, but we don't know if it is a scam, you know, people ransoming us. Basically policy based on fear and

reactionism. That is what we don't want. That would be bad for everybody.

So I encourage your energy around engaging with us early and often.

To that point, I was really heartened to see actually in the United Kingdom that the parliamentarians, the parliament there basically invited in the crypto community and they had a closed-door—I don't know if it was a meeting or a summit or a conversation. I would offer that might be a really useful thing to think about doing toward the end of this year, taken out of the election cycle, and have that conversation. Again, just education for those who aren't on the committee and to just keep the dialog open.

So with that, I want to thank our witnesses for your valuable testimony. Thank you for piping in and for the Members for their questions.

The Members of the subcommittee may have additional questions for the witnesses and we ask that you respond expeditiously in writing if possible to those questions.

The Chair reminds Members that the subcommittee record will be remaining open for 10 business days.

Without objection, the subcommittee stands adjourned.

[Whereupon, at 10:36 a.m., the subcommittee was adjourned.]