S. HRG. 117–677

UNDERSTANDING THE ROLE OF DIGITAL ASSETS IN ILLICIT FINANCE

HEARING

BEFORE THE

COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS UNITED STATES SENATE

ONE HUNDRED SEVENTEENTH CONGRESS

SECOND SESSION

ON

EXAMINING DIGITAL ASSETS TO LEARN HOW THEY WORK AND THE RISKS THEY CREATE FOR CONSUMERS AND THE FINANCIAL SYSTEM

MARCH 17, 2022

Printed for the use of the Committee on Banking, Housing, and Urban Affairs

Available at: https://www.govinfo.gov/

U.S. GOVERNMENT PUBLISHING OFFICE
52–387 PDF WASHINGTON : 2023

COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS

SHERROD BROWN, Ohio, *Chairman*

JACK REED, Rhode Island
ROBERT MENENDEZ, New Jersey
JON TESTER, Montana
MARK R. WARNER, Virginia
ELIZABETH WARREN, Massachusetts
CHRIS VAN HOLLEN, Maryland
CATHERINE CORTEZ MASTO, Nevada
TINA SMITH, Minnesota
KYRSTEN SINEMA, Arizona
JON OSSOFF, Georgia
RAPHAEL WARNOCK, Georgia

PATRICK J. TOOMEY, Pennsylvania
RICHARD C. SHELBY, Alabama
MIKE CRAPO, Idaho
TIM SCOTT, South Carolina
MIKE ROUNDS, South Dakota
THOM TILLIS, North Carolina
JOHN KENNEDY, Louisiana
BILL HAGERTY, Tennessee
CYNTHIA LUMMIS, Wyoming
JERRY MORAN, Kansas
KEVIN CRAMER, North Dakota
STEVE DAINES, Montana

LAURA SWANSON, *Staff Director*
BRAD GRANTZ, *Republican Staff Director*

ELISHA TUKU, *Chief Counsel*

DAN SULLIVAN, *Republican Chief Counsel*

CAMERON RICKER, *Chief Clerk*
SHELVIN SIMMONS, *IT Director*
PAT LALLY, *Hearing Clerk*

C O N T E N T S

THURSDAY, MARCH 17, 2022

WITNESSES

ADDITIONAL MATERIAL SUPPLIED FOR THE RECORD

UNDERSTANDING THE ROLE OF DIGITAL ASSETS IN ILLICIT FINANCE

THURSDAY, MARCH 17, 2022

U.S. SENATE,
COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS,
Washington, DC.

The Committee met at 10 a.m., via Webex and in room 538, Dirksen Senate Office Building, Hon. Sherrod Brown, Chairman of the Committee, presiding.

OPENING STATEMENT OF CHAIRMAN SHERROD BROWN

Chairman BROWN. The Senate Committee on Banking, Housing, and Urban Affairs will come to order. We have two witnesses in person, two remote. Thanks to all of you. This is in hybrid format, obviously.

In 2019, a doctor's office in the Mahoning Valley in Ohio, the Youngstown area, experienced a disturbing attack. Hackers locked the office computers, making them unusable. They even faxed over a ransom note, promising to unlock the computers if the practice turned over $75,000, in Bitcoin.

Not long ago, a Syrian group tied to al Qaeda put out a call for donations to help buy weapons. Their social media post said that supporters should "donate anonymously with cryptocurrency."

"Donate anonymously with cryptocurrency."

A week ago today, the Justice Department announced an indictment of two individuals who allegedly turned the profits of scams into cryptocurrency. Then they would send the crypto overseas, where it could be turned back into cash.

This Committee has been examining digital assets to learn how they work and the risks they create for consumers and the financial system. We have also considered how digital assets can put workers' hard-earned money at risk.

We are here today because crypto also can be used to make it easier to commit crimes, facilitating illicit finance, terrorism, and other forms of criminal activity, and threatening our national security. Bad actors around the world, from hackers, scammers, and drug traffickers to terrorist groups and pariah regimes, have sought digital assets to facilitate their crimes and intimidation.

In October 2020, under the last Administration, the Justice Department concluded, quote, "cryptocurrency technology plays a role in many of the most significant criminal and national security threats that the United States faces."

To be sure, criminals have tried to cover their tracks for years with sham accounting and banks that looked the other way. But

there is a simple reason that crypto appeals to crime rings and scam artists.

The dollar has safeguards to protect against crime and illicit activity. Companies that deal with real money are required to know their customers and report suspicious transactions. They need to keep records.

And even when crypto companies are covered by the law, too many do not play by the same rules, especially offshore crypto operators that are not subject to U.S. law. Shady crypto companies that fail to adequately monitor activity on their platforms essentially give criminals a green light.

Digital assets make it easier to move money under pseudonyms. They make it easier for money launderers to use webs of transactions across the globe to cover their tracks, and that makes it harder for law enforcement to trace illicit funds.

FinCEN, the Financial Crimes Enforcement Network, the Treasury bureau charged with safeguarding our financial system from abuse, warned last week that Russian actors could even use crypto to get around sanctions.

So sophisticated bad actors can use digital assets in ways that, if they were using dollars, would likely raise red flags and get them stopped in their tracks.

Last year, FinCEN fined a crypto exchange $100 million. For 6 years, the only identification the company bothered to get from customers was an email address. That no-questions-asked approach enabled more than $200 million in suspicious transactions.

But the problem is not only shoddy compliance. It is more fundamental. We hear all the time about how "innovative" cryptocurrency is. But criminals innovate, too. Crypto allows money launderers and terrorists to do things they never could have done with dollars. There is a whole new vocabulary to explain cryptocurrency illicit activity.

Take what is known as "chain hopping." That is when someone launders money by changing funds from one cryptocurrency ecosystem to another, to make it harder to track. Or look at so-called "rug pulls." That is when you set up a sham digital asset project online, raise as much money as you can, scamming investors all the while, and then run off with the cash.

Then there is Hydra, the world's largest "darknet." It is an online black market for drugs, for stolen credit card numbers, and for cyberattack services, all enabled by crypto. Our laws and law enforcement agencies need to keep pace with these bad actors that will exploit every opportunity and stay, as the old clich? says, one step ahead of the law. And so far, with lax rules and little oversight, we have given them plenty of those opportunities.

Crypto lets money launderers, hackers, and rogue regimes invent new ways to hide and move money in the dark. It lets hackers and scammers create new ways to steal or defraud. And if we allow them to get out ahead of us, our safety and security are at risk.

Law enforcement is doing what it can. They use techniques to stop cybercrime that did not exist three decades ago. Financial regulators leverage new data and resources to expose fraud and manipulation in our markets. Crypto technology also embeds information that allows law enforcement and national security officials to

track and trace where it has been, though not necessarily who owns it. That is where the tough new money laundering and beneficial ownership law that we all passed bipartisanly last year will help.

But as these problems continue to grow, we cannot sit on the sidelines. We need to take a clear-eyed look at how these assets can endanger consumers and our security.

Last month, the FBI announced the creation of a new unit dedicated to tracking down illicit crypto. The Justice Department is dedicating more resources and staff to cracking down on crime using digital assets.

We need to take a whole-of-Government approach to the problem if we are going to keep up with crypto in illicit finance.

President Biden understands that. His Executive order on crypto assets last week will drive progress on this issue. It was comprehensive. It was done right. It will jumpstart a coordinated strategy from law enforcement and regulators to fight bad actors who want to use crypto.

Ultimately, we just cannot sit back and watch cybercriminals, rogue regimes, terrorists, and others create a shadow financial system that works essentially only for them. The financial system should work for American families and small businesses. Everything we do on this Committee has that goal in mind. It means that we cannot let abuses of digital assets endanger our financial and our national security.

As crypto technology evolves, this Committee must continue to work together to craft a way forward on these issues. The stakes are high, and the American people are counting on us.

Ranking Member Toomey.

OPENING STATEMENT OF SENATOR PATRICK J. TOOMEY

Senator TOOMEY. Thank you, Mr. Chairman.

This hearing is about digital assets and illicit finance, and while this is an important topic and is appropriate to discuss and understand this topic, we also need to work to ensure regulatory clarity for digital assets.

Digital assets, including cryptocurrencies and their underlying distributed ledger technology, have enormous, tremendous potential benefits. Some are already being realized. As the White House itself recently stated, the U.S. must maintain its leadership in this space, which is why lawmakers and regulators should do nothing to harm America's longstanding tradition of fostering technological innovation.

Unfortunately, I am concerned that the current lack of regulatory clarity here at home is undermining that tradition and driving innovation abroad. We need Congress to work together to enact a regulatory framework specific to digital assets that provides this much-needed clarity.

While today's topic is illicit finance, I think an important backdrop for this hearing is Russia's invasion of Ukraine. By starting the largest land war in Europe since World War II, Russia has unleashed the greatest threat to global security in recent memory.

The sanctions imposed thus far by the Biden administration are harmful to the Russian economy, but not crippling. Sanctions have

purposefully allowed Russia to continue exporting oil and gas, funding Putin's war machine with what could be as much as $5 to $7 billion each week, coming from the West. Cutting off this revenue stream and getting more lethal aid to Ukraine are the two things we could do to maximize the chances that Ukraine wins this war, and Putin comes to understand this war was a calamitous mistake.

To cutoff Putin's oil and gas sales globally, the Administration and Congress should impose secondary sanctions on Russia's entire financial sector. This would force the world to choose between doing business with Russia or with the United States. I urge the Administration to impose these sanctions and give Ukraine a fighting chance to win this war.

I am concerned that part of today's hearing will be spent disparaging cryptocurrencies and trying to draw some connection between them and Russian sanctions evasion. There is no sanctions regime that is completely watertight, so it is quite possible that an oligarch somewhere that may be using a variety of tools, including crypto, to try to hide some assets.

But according to Administration officials across multiple agencies, there is simply no evidence of cryptocurrencies being used by Russia to evade sanctions in any significant way.

Just this month, FBI Director Christopher Wray told the Senate Intelligence Committee that, quote, "the Russians' ability to circumvent the sanctions with cryptocurrency is probably highly overestimated," end quote. Acting FinCEN Director Him Das said, and I quote, "we have not seen widespread evasion of our sanctions using methods such as cryptocurrency," end quote. And the director of cybersecurity for the National Security Council said, and I quote, "the scale that Russia would need to successfully circumvent all U.S. and partners' financial sanctions would almost certainly render cryptocurrency as an ineffective primary tool for the State," end quote.

The facts are clear and the Administration has discovered this. Russia cannot meaningfully use cryptocurrencies to evade current sanctions.

While there has been virtually no evidence of that evasion taking place, Ukraine has been actively using cryptocurrencies to do tremendous good. Cryptocurrency donations for Ukraine have reached approximately $100 million, which has helped Ukrainians defend their country against this terrible invasion. These funds have gone toward more than 5,500 bulletproof vests, they have bought 500 helmets, and over 410,000 meals, among other things. Ukraine's Deputy Minister of Digital Transformation has said that, and I quote, "each and every helmet and vest bought via crypto donations is currently saving Ukrainian soldiers' lives," end quote.

We are fortunate to have as a witness today someone deeply affected by the war in Ukraine and the use of cryptocurrency to help Ukraine and its citizens. Michael Chobanian is the Founder of KUNA Exchange, a local cryptocurrency exchange based in Ukraine. For the past several weeks, Mr. Chobanian has been instrumental in coordinating efforts so individuals all around the world can contribute cryptocurrencies in support of Ukraine's defense.

Crypto's remarkable nature is that anyone across the globe can contribute to this type of effort, almost instantaneously, at very low cost. It is in this context that we should examine cryptocurrencies and their relation to illicit finance.

Throughout history, criminals have always tried to utilize new technologies for nefarious gain. But that is not a reason to stifle new technological developments. Crypto can be used to empower individuals and promote personal autonomy, but it can also support the detection and prevention of illicit crime. According to Chainalysis, transactions involving illicit addresses account only for 0.15 percent. That is less than two-tenths-of-1-percent of cryptocurrency transaction volume last year.

And this should be no surprise. The traceable nature of most cryptocurrencies is a factor making them terribly risky to utilize for criminal purposes. Just look at the Colonial Pipeline hack, which was one of the most disruptive ransomware attacks on record. The Department of Justice recovered 85 percent of the Bitcoins that the pipeline paid in ransom, dealing a very significant blow to the hackers.

One of today's witnesses, Michael Mosier, can speak directly about the characteristics of cryptocurrencies that help detect criminal activity. Mr. Mosier is the former Acting Director for the Financial Crimes Enforcement Network, or FinCEN, at the U.S. Treasury Department. His Government experience makes him uniquely qualified to discuss the topics before us today.

Today I hope the Committee takes a thoughtful and reasonable approach to this topic, acknowledging both the risks that cryptocurrencies present, but also their incredible potential. I thank the witnesses for their testimony and participation today, and I look forward to the discussion.

Chairman BROWN. Thank you, Senator Toomey.

I will introduce the four witnesses. We will hear from Jonathan Levin, Cofounder and Chief Strategy Officer at Chainalysis, Inc; Michael Mosier, the General Counsel of Espresso Systems and Former Acting Director and Deputy Director and Digital Innovation Officer at FinCEN. They both are sitting at the table in front of us.

And appearing remotely, as Senator Toomey said, is Michael Chobanian, Founder of KUNA Exchange, President of Blockchain Association of Ukraine. Welcome. And Shane Stansbury, a Fellow at the Duke University School of Law, Former Assistant U.S. Attorney.

Mr. Levin, please proceed. Thank you.

STATEMENT OF JONATHAN LEVIN, COFOUNDER AND CHIEF STRATEGY OFFICER, CHAINALYSIS, INC.

Mr. LEVIN. Chairman Brown, Ranking Member Toomey, and distinguished Members of the Committee, thank you for having me here today to testify about this topic at an important time, as we have put significant sanctions on Russia to end the war in the Ukraine and we work together on a full Government digital asset policy, as according to President Biden's Executive order, put in place last week.

My name is Jonathan Levin, and I cofounded Chainalysis 8 years ago with Michael Gronager.

At the turn of the 20th century, my family fled the pogroms of Eastern Europe to look for a better life in the West. They left with nothing. People in the Ukraine today are fleeing their homes and crossing borders, leaving loved ones and possessions behind.

We, as a global community, have come together at an unprecedented pace to counter this movement. This has been due to the speed of information that is possible with the internet, and this ultimately has to be matched with the speed and inclusiveness of finance.

The transparency that the internet has created about these atrocities has not been matched by the transparency realized in financial services. Bitcoin and Ethereum are technologies that pose the greatest opportunity to increase the degree of transparency and financial services, included the excluded, and create new ways for commerce to happen.

Bitcoin has evolved over the last decade. It started off as just a promising technology, but today there is a community of more than 100 million people who depend on it. It has also spurred the creation of other digital communities. Commerce, such as music, art, and even electric vehicles depend on the underlying technology.

Chainalysis is the blockchain data platform. We provide data, products, services, and research to Government agencies, financial institutions, and the digital asset industry, more broadly. Through the use of our software, law enforcement has managed to take down the largest darknet markets, prevent the use of cryptocurrency for terrorist financing, and has prevented scams and investigated ransomware campaigns, as previously mentioned.

Tens of thousands of cases and investigations have taken place on our platform by both public sector and private sector in the fight to remove illicit activity from cryptocurrencies. Our compliance software enables AML compliance for the digital asset industry to ensure their compliance with obligations under the Bank Secrecy Act.

The blockchain's transparency and the permanence of the records that are contained within this allow us to root out this illicit activity. Law enforcement leverages the permanence of these records and its openness to take proactive steps in being able to investigate crimes without the need to serve subpoenas or have reporting requirements.

When it comes to the use of sanctions as a tool for national security, OFAC has used the fact that there is compliance among the exchange to foster a degree of sanctions across the Russian ecosystem. In September 2021, OFAC sanctioned SUEX and Chatex, effectively removing these enablers as exchanges from the digital asset ecosystem.

We at Chainalysis have also, last week, released a free and open sanctions screening tool for everyone in the industry to be able to screen against addresses that are listed on the OFAC SDN list.

Just with any new technology, criminals have found innovative ways to exploit digital assets. As mentioned previously, illicit transactions only represent 0.15 percent of total transaction volume, as outlined in the Chainalysis Crypto Crime Report. I have included

a much deeper analysis in my testimony, and I am happy to answer questions on it.

The sanctions imposed on Russia demonstrate the power of investing in financial technology and the dominance of the dollar that we managed to achieve over the course of the 20th century. We need to make sure that we continue to invest in financial technology and build the financial rails that will be used by the global in the 21st century. Embracing digital assets will help the U.S. build this future. These new rails can be built in a way that encourages transparency and that not only protects our national security and public safety but actually enhances it.

At the end of my testimony I have written some recommendations about how regulators and Congress can act to reduce illicit activity in digital asset markets, and I am very happy to answer questions.

Chairman BROWN. Thank you, Mr. Levin.

Mr. Mosier, please proceed. Welcome again to the Committee.

STATEMENT OF MICHAEL MOSIER, FORMER ACTING DIRECTOR, DEPUTY DIRECTOR/DIGITAL INNOVATION OFFICER, FINANCIAL CRIMES ENFORCEMENT NETWORK (FINCEN)

Mr. MOSIER. Thank you, Chairman Brown, Ranking Member Toomey, Members of the Committee.

My grandfather was a justice of the peace in a small mining and steel town in Western Pennsylvania. Sadly, he died long before I was born. But I treasure one of his 1953 election campaign cards. It says, "Endorsed by labor and avowed enemy of Communism". Those statements represent a sense of collective empowerment as well as vigilance that power can be oppressive.

The desire to protect personal sovereignty led me to public service. After pro bono cases to help victims of domestic violence I became a prosecutor at the Manhattan District Attorney and eventually Deputy Chief in the Department of Justice, investigating kleptocracy and the financing of human trafficking.

Protecting self-determination, as enshrined in the Constitution, is a critical part of public service. To that, when we speak of illicit finance we must also not forget the defenders of democracy whose financing may be considered "illicit" to autocrats and invading armies. The same cryptographic capabilities discussed here today enabled secure, auditable, humanitarian aid to 60,000 health care workers in Venezuela, under a repressive regime. No doubt the regime there considered it subversive "illicit" finance, but to the White House and Treasury who approved it, it was cryptographically secure humanitarian aid.

As we debate risks of technology based on cryptography it is critical to remember that encryption has protected and reflected our democratic values for years. Likewise, in the past few weeks, tens of millions of dollars' worth of cryptocurrency were donated to Ukraine, faster and more aid than the U.N. provided. With the transparency of Government-identified wallets on a public ledger, far more accountability than the U.N.'s Oil-for-Food scandal.

A few observations about ransomware in particular. Ransomware dates back to 1989, two decades before the emergence of Bitcoin. Yes, Bitcoin has become a preferred payment method because of

speed and perceived anonymity. However, public ledgers offer law enforcement significant visibility and investigative benefits over opaque international banking. We saw this with the recovery of $2.3 million from the Colonial Pipeline attackers.

The increase in ransomware has more to do with other developments. First, the advent of ransomware-as-a-service, making kits widely available, regardless of coding skills, and drastically reducing barriers to entry. And the use of double extortion, greatly increasing payouts by also threatening to expose stolen data, not just lock the computer.

We also know from SolarWinds that there are plenty of malign actors driven by nonfinancial incentives. Over-attributing cybercrime to cryptocurrency misses critical causes and preventive measures that could be taken.

Certainly there is work to be done yet for Web3 to be safely accessible, but the early internet had a lot of fraud and exploits as well. Instead of shutting down the internet, we worked persistently to find the balance while prioritizing risks and pathways to consensus and clarity.

If you want to tangibly impact illicit finance here are three concrete actions you can take.

First, pass the budget that was due last October. Fifteen months after landmark AML modernization legislation, FinCEN and OFAC are without the roughly $74 million increase in personnel and technology, while more and more are demanded of them. Resource them for their current job before burdening them—and industry—with more unfunded mandates.

Second, resource and expansively clarify the AML whistleblower program to empower crowdsourced leads related to corruption and abuse. Explicitly include any violation of money laundering, not just the BSA.

Last, press FATF representatives to focus on regulatory arbitrage through baseline consistency across jurisdictions before adventuring into new rules. We know that the gaps are concentrated at a small group of foreign centralized exchanges. Help diligent U.S. exchanges by leveling the playing field before expanding the rules to mere developers, in conflict with our Constitution.

I will close at that. Constitutional principles set the foundation for our country and our standing in the world. As we see in unified solidarity with Ukraine, principles are a key rallying point in the global battlefield of ideals. Thank you for this opportunity to advance our ideals today.

Chairman BROWN. Thank you, Mr. Mosier.

Mr. Chobanian is joining us remote. Mr. Chobanian, welcome.

STATEMENT OF MICHAEL CHOBANIAN, FOUNDER OF KUNA EXCHANGE, PRESIDENT OF BLOCKCHAIN ASSOCIATION OF UKRAINE

Mr. CHOBANIAN. Good day. Can you hear me? I guess so. Good day.

So my name is Michael Chobanian. I am the founder of KUNA Exchange, and I am also the President of Blockchain Association of Ukraine. Currently we serve more than 450,000 users.

I would like to tell my story. You have my statement to read, but I would like to do a bit of storytelling. So on 24th of February, I woke up at 5 a.m. because I heard really loud noises, and my windows were shaking, my house was shaking, and I immediately understood that the war had started. So I woke up, I went up on the internet, I googled, I saw that the formal proof that the war has started. My kid woke up, my wife woke up, and they asked me what was happening, and I said, "Russia has started war on us." And my kid asked, "How?" because we have so many friends in Russia. How could this happen? And I could not give her an answer.

So a few hours later we had to leave my home. This is pretty much all I have left—a few sweaters, sneakers, and jeans—and the same with the other probably three million people, we had to flee toward Western Ukraine.

So a couple of hours later, when we got to Western Ukraine, I decided that we have to set up a fund in order to help my people, my army. I knew that the army was in terrible conditions in terms of supplies, considering that we were fighting the probably second-largest army in the world.

So we set up a fund, and a few hours later I was approached by the Minister of Digital Transformation and we discussed that instead of setting up a few smaller funds it is better to set up one big Government fund in order to, first of all, give transparency, in order to speed up the process of buying all the vital goods for my people, for my army. And basically we set up a fund, and now it is being run by both Ministry of Digital Transformation and by the Ministry of Defense.

Right now we already collected more than $50 million in equivalent. We are reaching for about $100 million. Mr. Chairman stated what exactly we bought with it. This is just a tiny fraction of what we bought. We also had opportunity to supply finance to the cities like Mariupol, to Kharkiv, which are now enclosed and captured by Russians. The internet still works there so we can supply crypto there, and, with this crypto, people can buy food and whatever is required there.

Our fund, well, because it is run on my exchange, it is fully compliant with the current laws and regulations in Ukraine. That is why we are working with the Government. Yesterday the President has signed the bill and now crypto is fully legal in Ukraine.

In terms of sanctions, because, Mr. Chairman and Vice Chairman, you also said about the sanctions, so the first thing that we did as a crypto community in Ukraine, we shut down all the robo-operations, because that was a big hole in the sanctions list. And sanctions really help because that is how we would fight with economic means.

Unfortunately, not all crypto companies followed our lead. Namely, Binance still works with the ruble, and it is a big hole in the sanctions so we are likely to investigate more on this.

Also there was the note, Mr. Chairman, that Russians could use crypto to avoid sanctions. This is not exactly true. I am the person who is behind all the numbers. I know how it happens. So it is impossible, physically impossible to transfer large amounts of money from fiat into crypto. And again, even if they do, which is impos-

sible, as I said, there is nothing they can do with it. Their yachts are being arrested. Their house is being arrested. They cannot travel to the civilized world. So for them it just done numbers, which are pretty useless.

But I have to stress this out, and I have to stress this out very clearly, that there are a lot of Russians in Russia and outside of Russia who rely on crypto. These people are basically the opposition to the Putin regime, and we have to make sure that when you draft the laws that we do not actually kill this opposition within Russia that could actually help us bring down the regime.

And the final I would like to read from much of my statement. By concluding, I would like to thank the U.S. Senate and U.S. people for the opportunity to stand here and speak on these vital issues. Our Nation is eternally grateful for all the help given by our international friends. Namely, yesterday we received the news that a lot of weapons will be given by U.S. country and by the U.K. and other European partners. I truly believe that the unprecedented global unity and support for Ukraine during this unmerited, unwanted, and unnecessary bloodshed can put an end to Putin's reign of terror and lead us to an even brighter future.

Thank you, and Slava Ukraine.

Chairman BROWN. Thank you, Mr. Chobanian, and best wishes to you and your family. Mr. Stansbury, remote, I believe, from North Carolina.

STATEMENT OF SHANE STANSBURY, ROBINSON EVERETT DISTINGUISHED FELLOW IN THE CENTER FOR LAW, ETHICS, AND NATIONAL SECURITY, AND SENIOR LECTURING FELLOW, DUKE UNIVERSITY SCHOOL OF LAW

Mr. STANSBURY. Chairman Brown, Ranking Member Toomey, distinguished Members of the Committee, thank you for the opportunity to testify today.

I am a Senior Fellow in the Center on Law, Ethics, and National Security at Duke Law School, where I teach primarily in the areas of cybercrime and national security. I spent more than 8 years as a Federal prosecutor in the United States Attorney's Office for the Southern District of New York.

Today I have been asked to talk about the role of cryptocurrencies in illicit activity and also the challenges facing law enforcement, so I will begin with some context.

Criminals have always sought to take advantage of new forms of technology to facilitate illegal activity. Over the last two decades, the pace at which they have done has increased dramatically as the internet, social media, smartphones, and other innovations have changed the way we communicate.

As a prosecutor, I saw digital communication like social media and encrypted messaging apps revolutionize the way that terrorist organizations recruit members and carry out operations. And, of course, drug traffickers and criminals of all types also adopted these technologies to further their criminal conduct.

So in similar ways, cryptocurrency is changing the way that criminal finance illegal activities. In some ways we have been here before, but in other ways cryptocurrencies present new and distinct challenges. Because they are decentralized, easy to use, and hold

the promise of at least some level of anonymity, cryptocurrencies can act as magnets for illicit activity.

Cryptocurrency is now a multibillion-dollar business for criminals. It is used in connection with virtually every type of crime—child exploitation, human trafficking, extortion, fraud, you name it.

Perhaps nowhere is cryptocurrency's role more vivid than in ransomware attacks. As many Americans know all too well, ransomware is no longer just a problem for U.S. businesses. It is a serious threat to our public safety and our national security. Look no further than the Colonial Pipeline attack last year, which caused fuel shortages throughout the Southeast United States. But that was only one incident among many. Hospitals, school districts, city governments, all of them are being victimized by this modern-day hostage scheme.

Cryptocurrency is the defining feature of modern ransomware, and the attraction for ransomware criminals is the same for other criminals—obscurity. Cryptocurrency ransom payments can often pass through multiple layers involving different entities, including entities outside regulated markets. Criminals employ a variety of methods along the way to hide their tracks, and I explain some of those methods in my written testimony.

Some of these same methods can be used by criminals who use cryptocurrency to launder proceeds or hide illicit assets without traditional intermediaries. Even the cryptocurrency market itself is providing new opportunities for crime. Wallets and exchanges have become targets for theft and fraud. Criminals both steal money directly and also engage in scams to defraud innocent investors in cryptocurrency.

In short, cryptocurrency-related crime is here and it is growing, and we should be clear that the threat is not just from ordinary criminals. Rogue Nation States like North Korea have increasingly turned to cryptocurrency theft and other crimes to help finance their regimes.

I would now like to just say a few words about the challenges for prosecutors and law enforcement. Law enforcement is getting much better at tracing digital assets used to commit and cover up criminal activity. With the help of forensic analysis and know-your-customer information from regulated entities, law enforcement can sometimes shine a light on an otherwise opaque world.

Last year, DOJ recovered a substantial portion of the $4.4 million in ransomware payments made in connection with the Colonial Pipeline attack, and just last month DOJ recovered a record $3.6 billion in cryptocurrency allegedly related to a 2016 hack. These are promising and welcome developments.

We should not be too quick to conclude that tracking down the criminals using cryptocurrency is always easy or even always possible. Even with the latest analytics, a single investigation can be resource intensive and take years. The hardest part of a cyber-related prosecution can often be demonstrating what investigators sometimes refer to as "hands on the keyboard." Prosecutors have to demonstrate, beyond a reasonable doubt, that an identifiable person was behind a particular act. Digital clues from cryptocurrency transfers can be invaluable, but they do not provide all the answers about who is behind the criminal activity.

When my colleagues and I investigated international money laundering cases we often connected dots because of information made available by institutions that followed their compliance obligations. That kind of information is sometimes available in today's cryptocurrency market but too often it is not. Not all platforms comply with existing regulations, and many operate in jurisdictions beyond the reach of the United States law enforcement agents.

At the end of the day, an investigation is only as successful as the information and resources available. Blockchain technology does offer fascinating possibilities, and I look forward to seeing how it develops, but we should also recognize the role that cryptocurrency is playing in criminal activity. Only then can we take steps necessary to protect our health, our safety, and our national security. Thank you.

Chairman BROWN. Thank you, Mr. Stansbury.

I will begin the questions with Mr. Levin, but first, Mr. Mosier, you mentioned the request for the dollars. The President signed the bill a couple of days ago with $50 million, a significant number obviously, to combat money laundering. So your request was granted.

Mr. MOSIER. Thank you. I will not take credit for that.

Chairman BROWN. Oh, go ahead.

Mr. Levin, you noted that in 2021 the volume of illicit crypto transactions grew something like, at least $14 billion, a pretty big number. You explained the methods criminals use to conceal their transactions, new tactics like chain-hopping or mixers to obscure the trail of funds.

These are the strategies they are using right now. Tell us, if you would, what are the emerging ways that illicit actors are exploiting digital assets to avoid detection and obscure their identities? What are their next moves that you expect?

Mr. LEVIN. Thank you, Chairman. So when it comes to these types of obfuscation techniques or any sort of anonymizing techniques that the criminals pursue this is a very cat-and-mouse type situation where Chainalysis, the business, we research these techniques and stay, oftentimes, one step ahead of these criminal actors.

And so you mentioned chain-hopping and mixing. I think the largest gap is truly on the offshore exchanges that you also mentioned, in being able to cash out these types of transactions. You will note in the Crypto Crime Report that we put forward there is a concentration of cashouts by ransomware actors at only a few destinations. And so if law enforcement could focus in on those we could get ahead of some of the illicit flows that you are concerned about.

Chairman BROWN. Thank you. Mr. Stansbury, it seems digital assets have enabled and emboldened whole new types of criminal activity. Look at ransomware, that you discussed. There are now criminal groups that license out ransomware software to other hackers, or take dark web markets, where people can buy and sell drugs and stolen credit card numbers using crypto.

Mr. Stansbury, how have criminals used features of digital assets to invent new kinds of crime, and as you answer that, what kinds of criminal conduct are built around these cryptocurrencies?

Mr. STANSBURY. Thank you, Senator. Yeah, I think I would divide it into a couple of different categories. As you mentioned, cryptocurrency has made some crimes, some existing crimes, easier and has changed the nature of some crimes, like extortion. Ransomware has been around for a while, but cryptocurrency has changed the way extortion looks, and ransomware is a perfect example of that. Cryptocurrency is now the currency for ransomware. A senior director in the FBI mentioned, just this year, that cryptocurrency is the exclusive medium for exchanges for ransomware. So in some ways it has made things easier for existing crimes and changed the nature of those crimes.

In other ways it has provided new opportunities for new crimes. The DOJ Cryptocurrency Enforcement Framework from a couple of years ago I think does a nice job of outlining that and framing it. But I would say that any time you build a new financial ecosystem it presents new opportunities for criminals, obviously. And so that means that exchanges can be hacked by North Korea. It means that wallets can be hacked. It means that there are new scam opportunities, and we have seen a variety of those scams increase in frequency over the last year. In fact, Chainalysis does a nice job of describing some of those techniques.

So it both can contribute to existing crime and also create new opportunities.

Chairman BROWN. Thank you. Mr. Chobanian, the 2022 Crypto Crime Report from Chainalysis pinpoints Russia as a leader in illicit criminal activity using digital currency. Many ransomware groups, like Evil Corp—that is actually what they call themselves—are based there. Moscow is a hub, as you know, for crypto money laundering.

Why is it important that we crack down on Russia's cybercrime that uses digital assets?

Mr. CHOBANIAN. Very good question. Well, obviously, cybercrime is not good but I will have to stress out one thing. Think of crypto as energy, for example, nuclear energy. You can use nuclear for good, to create cheap energy, or you can create bombs with nuclear energy. So the same with crypto. You can use it for good or you can use it for bad. It depends on who uses it and how he uses it.

So in terms of hackers, and especially Russian hackers, I think that pretty much they are stuck in Russia right now and there is nothing that they can do with this crypto, as I said before. I mean, they are sitting in a city where you cannot even go to McDonald's. You cannot buy any of the Western world goods and services. So the only thing they can do is just look at the numbers. So right now I do not see that there is a big problem, but it potentially could be a big problem if something happens to Russia, not the way that we plan in Ukraine.

Chairman BROWN. Thank you. Senator Toomey.

Senator TOOMEY. Thank you, Mr. Chairman. Mr. Chobanian, first let just say our heart breaks for you and your family like it does for the several million Ukrainians that have been forced from their homes by this outrageous and completely unjustified brutal attack by Russia. And we are particularly grateful that you have taken the time to join us, despite the experience you are going through.

I wonder if you could just tell us, in a simple way, for a layman to understand, you mentioned that you are on track, you are hopefully going to raise $100 million from donations from people all around the world who want to help Ukraine. Why is this being done through crypto? Why are not people just sending dollars and yen and euro and other currencies?

Mr. CHOBANIAN. Very good question. Thank you. The banking system I your country is totally different to my country. So for you it is easy just to press two numbers and you can send any amount to other participants that you want. With crypto in Ukraine it is slightly different. The first problem that we are solving is urgency. So in order for U.S. dollars to actually land in Ukrainian bank accounts it takes at least 1 day, if we are lucky, but usually it takes 2 days. If it is a Friday afternoon you have to wait until Monday.

For my country, which is fighting right now with bare hands, time is the vital thing. So for the crypto, which works 24/7, we receive money instantly and we can spend money instantly, and by "money" I am speaking in the broader terms.

So yeah, that is the key thing. And the other thing is that with crypto we can attract donations from pretty much anyplace in the world, even countries which do not have access to banking but they have crypto, like in Africa or in Asia.

Speed, urgency, and ease of use.

Senator TOOMEY. And it is inexpensive, is it not?

Mr. CHOBANIAN. It depends. Here it depends which currency you are sending us. So Bitcoin and Ether is slightly expensive, but again, it is like $10, $20, maximum $50. But at this point it does not really matter. Here what we are fighting for is speed. The faster we buy the helmets, the faster we buy the bulletproof vests, the faster we buy the first aid kits, the more people I can save in my country. So here I am praying just for crypto because it is so fast.

Senator TOOMEY. And given the disruptions to daily life in Ukraine, has there been an increase in the use of crypto as a medium of exchange? Are ordinary people using crypto to buy ordinary things, in some cases, because, of course, that is not common in the United States.

Mr. CHOBANIAN. Well, even before the war Ukraine was the number one country per capita in terms of crypto wallets and crypto usage. Now it is probably double that. The reason for that is you cannot buy U.S. dollars on the bank accounts right now because national bank closed that option on the day of the war.

So if you want to buy something abroad, the only option that you have—and if you have like local currency, hryvnia, on the bank account or you have cash in U.S. dollars in Ukraine, yeah, that is it, the two options. So the only option to actually buy something abroad, you need U.S. dollars, and you cannot buy them. With the crypto you can actually buy USDT, which is a token, which is backed one-to-one to U.S. dollar. You can buy that with local currency. You can use that to pay for the helmets in Europe or in U.S. The transaction takes about 10 minutes, and that is it. And that is the only option for these small and medium businesses and for regular people like me.

Senator TOOMEY. Thank you very much. This question is for both Mr. Mosier and Mr. Levin. So we all want to make sure we have

got the tools to find the bad guys, and there are bad guys out there. For a very long time we have had reporting requirements for financial institutions that serve as this massive dragnet, like require banks to report every single transaction over $10,000.

Now we know, we have long known, that the vast, overwhelming majority of those transactions are perfectly legitimate, but we did not have a way of sort the good from the bad so we report them all, and we have this expensive, inefficient mechanism for this over-reporting in the hopes that, well, at least we will sweep up the bad guys too.

With crypto we have a whole new kind of technology, it seems to me, and I guess what I would like you to comment on is rather than apply the old, outdated, like literally 50-year-old technology to crypto, should we be thinking about using the tools that crypto avails us to zero in on the likely problematic transactions rather than having this universal reporting requirement that sweeps in preferably legitimate transactions? If you could both comment on that, I would appreciate it.

Mr. MOSIER. I will start. Thank you. Thank you, Senator Toomey. No, I think it raises a really important question and something that we struggled with at FinCEN, both from a resource and a technology perspective and also with protecting personal data. And I think there is another piece of that, which is when we collect data we are regularly asked, I think legitimately, by the public and by Congress, "OK, what have you done with that, that it was worth the burden?" And, in fact, every rulemaking requires a burden assessment on industry for that.

And I think what we struggled with was getting the tools and the technology to be able to sort through the data that we had—indeed, they still continue to do that—and we are always conscientious that if we are creating new reporting requirements, will we be able to use it, and will we be able to use it fast enough?

So I think given, what Mr. Levin will surely talk to you about, the capabilities and what we, I think, have all discussed in terms of the public transparency, the critical piece right now is it is on a public ledger. We do not really need you to send stuff in. What we need are the tools to sort through that efficiently and connect it across data. It is already actually exceptionally clean data because it is structured data. It is numbers. It is alphanumerics. It is not the old days of fax machine and people writing it into the wrong format and we cannot sort it. So it is actually quite good data. It is just the ability to use it.

Mr. LEVIN. Thank you, Senator Toomey, and I agree sort of with the premise of the question. The problem with a reporting requirement with a fixed number means that that becomes a difficult thing to change over time and creates sort of a deluge of information around something that seems fairly arbitrary in nature.

When it comes to the blockchain, there is a complete set of records out there for everyone to look at, that actually also updates in real time, so there is no waiting for reporting to happen. And so not only are you able to access it, you are able to access it faster than you would otherwise be able to in a reporting sense, and then actually being able to sift through what is illicit activity from what is regular commerce is much easier in a cryptocurrency context

than in traditional finance, where you are looking for behavioral patterns.

So I think when it comes to thinking about regulating the digital asset economy we have to take into account those unique attributes of the technology and think about sort of as my esteemed colleague here said, the scarce resources that there are in Government agencies to actually look at this and invest in the technology to be able to have that real-time oversight of the sector.

Senator TOOMEY. Thank you, Mr. Chairman.

Chairman BROWN. Senator Menendez, from New Jersey, is recognized.

Senator MENENDEZ. Thank you, Mr. Chairman.

I have raised concerns in the past with Iran's practice of mining cryptocurrency in order to launder its sanctioned oil and natural gas reserves into cash. Because the main cost associated with mining cryptocurrency is energy, I worry that the Russian Government will also look to mining as a way to evade sanctions.

According to the Cambridge Bitcoin Electricity Consumption Index, Russia accounts for 13.6 percent of all Bitcoin mining, as measured by energy consumption, so they certainly have the infrastructure for such activities.

So, Mr. Stansbury, are there tools that would allow financial institutions and regulators to prevent use of mining to avoid sanctions?

Mr. STANSBURY. There are tools available to regulators, but I think largely it is all on the enforcement front. You are right that Iran has successfully mined cryptocurrency to its advantage. There is also a lot of reporting about North Korea that has turned to cryptocurrency to fund its regime. So it is a huge problem.

But I think that mostly we need to look, on the enforcement front, how are these Nation States able to bypass sanctions? How are they able to convert the cryptocurrency that they are mining because they are moving it across borders and somehow converting it to a medium that they can use. So that, I think, is where most of the problem lies.

Senator MENENDEZ. Mm-hmm. And Mr. Levin and Mr. Chobanian, what is your understanding of the links between Russian miners and the Russian Government?

Mr. LEVIN. Michael, you can go first.

Mr. CHOBANIAN. Thank you. So I can say that probably there is none because Russian miners are just regular people, the businessmen who are doing it for principles of crypto, because they believe in this technology or especially if they want to earn money, that is what they do. But again, when you talk about sanctions on a Government level, what kind of sums are we talking about? If we are talking about billions then I can answer you right now—it is impossible to substitute Bitcoin or any other cryptocurrency for U.S. dollars on the Government level.

You cannot transfer that easily a couple of billions of dollars without anyone noticing on the physical level, so I would like to stress this point. It is not an issue of the big numbers, and smaller numbers, you know, it is not about buying oil or buying weapons, or buying anything else with these small numbers in U.S. dollars. Thank you.

Senator MENENDEZ. Interesting.

Mr. LEVIN. Yes, and I would agree with what Mr. Chobanian said. I think the only other thing to raise is that it has been possible for U.S. law enforcement and the intelligence community to actually identify and attribute Russian Government activity inside the crime cases when it comes to the issues of ransomware, hacking, or other forms of financial crime. And so it is the case that we need to further the capabilities of those agencies to get close to the operatives and the operations of Russia in this domain to continue to understand the evolving picture.

Senator MENENDEZ. Mm-hmm. Now there is a difference between the Russian Government and Russian oligarchs. The Government's relationship with exchanges, both foreign and domestic, is going to be an increasingly key element in enforcing sanctions going forward. We are seeing, with the current crisis in Ukraine, that law enforcement is reliant on exchanges themselves to screen users and block sanction targets.

Mr. Stansbury, what are the risks to U.S. persons and institutions that are trading with exchanges in Russia and other jurisdictions with poor monitoring and know-your-customer rules?

Mr. STANSBURY. One of the risks is scam, fraud, and theft. So, you know, there is a degree of risk that any consumer is taking when they place their investment money into the cryptocurrency ecosystem, and in a high-risk environment like that I think that is one of the chief concerns, particularly as cryptocurrency grows in popularity and less-sophisticated investors get into the market.

Senator MENENDEZ. And finally, Mr. Levin, your firm estimates that of all the ransomware payments made in 2020, 15 percent of them carried a risk of sanctions violations. So essentially victims of ransomware attacks are increasingly finding themselves targeted by sanctions entities and therefore victims that make ransom payments in cryptocurrency may themselves be committing sanctions violations. How should we, in Congress, think about addressing this problem without undermining the efficiency of our sanctions tools?

Mr. LEVIN. Thank you, Senator. It is a delicate balance between the issue of sanctioning and disrupting the cybercrime activity and raising the deterrence against such attacks. And so I think the effective sanctions against entities like Evil Corp that have been sort of behind these types of attacks has meant that there are fewer firms that are willing to actually pay those ransoms, which does actually reduce the incentive by which they have to attack our population.

And so I think it is another example of how effective sanctions can be when it comes to disrupting activity that we are worried about for our public safety.

Senator MENENDEZ. Thank you, Mr. Chairman.

Chairman BROWN. Thank you, Senator Menendez.

Senator Hagerty, for Tennessee, is recognized.

Senator HAGERTY. Thank you, Mr. Chairman, and Happy St. Patrick's Day to everybody today.

Over the past year, law enforcement has recovered billions in stolen crypto. All of this has been done in an ecosystem that has been often described as anonymous, illicit, the Wild West, in fact, of il-

licit finance. But in my view it is inconsistent with the architecture of blockchain technology because most cryptocurrencies are built on a public ledger, that makes the chain of ownership visible, and by extension, it makes it traceable to any token's existence at any point.

Mr. Levin, I will start with you. Cryptocurrencies are pseudo-anonymous, right? The wallets addresses themselves do not identify the owners. But with the proper tools and proper legal authority what capabilities exist to actually track and identify illicit actors in cryptocurrencies such as Bitcoin?

Mr. LEVIN. Thank you, Senator, and it is an important point to make because it is often conceived that cryptocurrency is not as transparent as it actually is. So when it comes to having the necessary tools in place, Chainalysis, what we do is we map all the transactions that occur in cryptocurrencies to the entities and services that people are using to conduct that activity. And so the fact that all of the industry and all of law enforcement and the regulatory authorities can all have access to that same information about what services and what entities are behind these transactions, you know, that allows us to take unprecedented steps in being able to collaborate on weeding out illicit activity.

You point out that the Government has also managed to seize record sums of money from these cases in a world in which people thought that it was anonymous and that it was unable to be seized. So law enforcement can have these types of successes in this environment.

Senator HAGERTY. I think it is interesting, when you compare cryptocurrency to cash, on the other hand, and if you think about cash, cash is fully anonymous. It is untraceable. There is no underlying record of the chain of ownership with cash, and no one knows where a particular $100 bill may have been, whose hands it may have passed through, or how many hands it may have passed through.

So it seems to me that an individual that wants to break the law without being traced would probably find cash a more attractive alternative than cryptocurrency. Do you agree that cash is less traceable than cryptocurrency?

Mr. LEVIN. Indeed, Senator, cash is far less traceable than cryptocurrency for the point that you point out. The other thing about this is that it is the case that law enforcement also has the permanence of the record when it comes to cryptocurrency. The cases far back in the past can be solved based on information that is collected in the future.

The problem with a cash transaction is that when I hand you a $10 bill that is a completely ephemeral event, and that is never captured forever. And so your prosecutors are able to actually leverage the permanence of the blockchain to have conclusive evidence of the type of illicit activity that we are worried about, which is another deterrent against criminals using it.

Senator HAGERTY. Yeah, I completely agree. Yet when you go back to thinking about cash, I do not hear anybody saying that we ought to outlaw the use of cash. Do you hear that? I do not think so.

In reality, the mischaracterization that crypto is the Wild West of illicit finance, you know, I would hate to see that be used in a way to open the door to drop a morass of regulation on an industry that poses so much potential for America and for our competitive advantage.

Mr. Levin, I would like to continue to follow up there. There is a lot of discussion here on Capitol Hill that Congress needs to craft legislation to make it harder to use cryptocurrency to evade sanctions. One of your firm's specialties is tracking cryptocurrency transactions and monitoring potentially illicit activity. So hypothetically, how would someone trying to evade sanctions convert their cryptocurrency holdings into fiat without interfacing with the banking system?

Mr. LEVIN. So, Senator, the question about how to move from cryptocurrency into traditional finance requires a traditional financial institution, and there are these interfaces that have been, you know, the subject of anti-money laundering legislation globally. And so I think, to your question, you cannot move from cryptocurrency into traditional finance without interfacing with one of those institutions that has the regulatory obligations that protect us against its abuse.

Senator HAGERTY. The sanctionable regulatory obligations, just to be clear.

Mr. LEVIN. Yes.

Senator HAGERTY. Mr. Mosier, just very quickly, I think that there has been a lot of attention paid to the possibility that digital assets are undermining America's sanctions regime, and I would like to get your perspective on what Congress can or should do to help authorities and firms in the crypto space more effectively fight illicit finance.

Mr. MOSIER. Thank you, Senator Hagerty. Yes, I think the most important thing that Congress can do is help provide clarity. There are a lot of crypto firms out there that would like to be certain in that they are complying with the law, and I think there is a lot of debate, particularly across the SEC and the CFTC, about what exactly is needed to be in compliance.

Senator HAGERTY. And who is in charge of compliance?

Mr. MOSIER. And who is in charge of compliance. And I think there are a lot of people that really want to have a business model that is successful for everybody, and, by the way, that means a safe financial system that people feel comfortable putting their money into, and they are just looking to know "what exactly should I do, what is the standard and what should I meet?"

Senator HAGERTY. I appreciate your point on certainty and clarity. Thank you, Mr. Chairman.

Chairman BROWN. Thank you, Senator Hagerty.

Senator Tester, from Montana, is recognized.

Senator TESTER. Thank you, Mr. Chairman. I want to thank you all for being here, both virtually and in person. I am going to start out with a question that has already been probably answered but I just want to hear it from your lips to my ears. And that is, do you think Putin and the oligarchs are using cryptocurrency to get around sanctions? Yes or no.

Mr. LEVIN. Sorry. Is that a question for me, Senator?

Senator TESTER. It is for you first, Mr. Levin. I am going to go down the list, but very quickly.

Mr. LEVIN. Thank you, Senator. So we have not seen evidence of Russia or Putin systematically using cryptocurrencies to evade sanctions at this moment in time.

Senator TESTER. OK. Mr. Mosier, would you like to respond to that?

Mr. MOSIER. Thank you, Senator Tester. No, in fact, I will quote my successor, as counselor to the Deputy Secretary of the Treasury, who recently said, "You cannot flip a switch overnight and run a G20 economy on cryptocurrency. There just isn't the liquidity."

Senator TESTER. OK. And Mr. Chobanian?

Mr. CHOBANIAN. I would say no, and the reason for that is they tried to ban crypto for a long, long time, and the only time when they said that probably they should reconsider their decision is after the war. So I would say most definitely no.

Senator TESTER. Thank you. And Mr. Stansbury, do you have an opinion on that?

Mr. STANSBURY. I would just add that I think there might be a difference between individuals engaging in that activity and whether it is occurring at scale. I think the possibility is certainly there, which is why DOJ has recently set up a task force to address just that issue.

Senator TESTER. OK. And so, Mr. Levin, I think that you pointed out that the reason why crypto is safe is because it is totally trackable. Correct?

Mr. LEVIN. The inherent transparency does provide advantages, yes.

Senator TESTER. So we had folks that came after the Colonial Pipeline with ransomware, and we got 85 percent of the money back. Why did we not get 100 percent, if it is totally trackable?

Mr. LEVIN. That is a great question. I think when it comes to the ability to see the money versus seize the money, it is a distinction which is not always the case. There was a 100 percent degree of transparency about where the money was actually going, but in terms of actually the operation to be able to recover the funds, you know, that is not always 100 percent possible.

Senator TESTER. Mr. Stansbury, the question for you is in your statement you had talked about the fact that is very difficult to connect people with the payments when it comes to illegal activity. Is that pretty much what you said? I was just curious.

Mr. STANSBURY. Yes, Senator, thank you. I was making the point that it can sometimes be difficult to connect the last two dots in terms of linking cryptocurrency payments to specific individuals. Firms like Chainalysis can do a fantastic job of looking at patterns and giving law enforcement a lot of tools to follow financial transactions on the blockchain, but ultimately you have to connect those things to real people, and that is not always available just through analytics.

Senator TESTER. All right. And so if you cannot connect people with payments, how can you hold people accountable for illegal activity?

Mr. STANSBURY. There are a lot of tools at law enforcement's disposal, but, you know, things have to go right. I think a good exam-

ple is the recent seizure announced by DOJ last month, the record seizure of cryptocurrency payments. Now those are allegations so I want to be careful and say that.

But they worked for 5 or 6 years to connect the dots, and even though they were able to identify certain payment patterns by those individuals who were in possession of Bitcoin that came from the hack of an exchange back in 2016, it really took sort of traditional law enforcement tools like search warrants, and it also depended on the fact that, for example, the defendants were living in plain view in New York City, and they were using cloud storage accounts that were within the reach of U.S. law enforcement so they could serve search warrants on those accounts.

So it is really fact dependent, Senator, on whether law enforcement is going to be able to sort of get that last piece of the puzzle.

Senator TESTER. Well I certainly appreciate all your perspectives, and I can tell you that the reason, at least from my perspective, why cash is a whole lot different than cryptocurrency is it takes a lot of suitcases to transfer the kind of cash that you are talking about, what I believe is a simple press of a button in crypto.

I think this is a great hearing. I think that there is far more information to be fleshed out there, and I want to thank the Chairman for holding it.

Chairman BROWN. Thank you, Senator Tester.

Senator Smith, from Minnesota, is recognized.

Senator SMITH. Thank you very much, and I agree, Senator Tester, this is a very interesting hearing and I am grateful for our panelists for being here today.

So as we focus on controlling the illicit use of crypto there is this discussion about how we should regulate it, and how we should regulate digital assets in order to control the bad guys. And so to a certain extent it seems like what we are trying to do is to fit this new technology into existing regulatory frameworks. So, for example, should we think of digital assets as commodities in the jurisdiction of the CFTC, or should we think about it as security in the jurisdiction of the SEC, and maybe neither of those frameworks are the right way of thinking about it.

But it seems to me that without some regulatory framework, without a cop on the beat, so to speak, we are at a great disadvantage in terms of cracking down on illicit use. So I am not advocating for one framework versus the other, but I am wondering—Mr. Levin, I am going to ask you this—I guess the first question is what impact is there when, with a lack of a clear regulator or regulatory framework, what impact does that have? Let me ask you that first.

Mr. LEVIN. Thanks, Senator, and I share the concern that you have when it comes to the clarity point. And the impact of that on really the U.S. and the industry in general is that there is less funding available, there are fewer innovators actually going to work on this type of technology inside this jurisdiction, which gives rise to the possibility that the financial rails that are going to govern the 21st century are going to be built outside of this country and beyond our ability to have real insight, and the records of what is actually happening in these types of new payment systems.

So I think the twofold is that we are going to lose out on a very large economic promise, which is that this is an economic industry that will create dynamism in this economy, but second, we may lose out on the national security risk, that we lose some visibility into what could be conducted on these rails if they are built outside of this country.

Senator SMITH. So if we are building a regulatory framework that becomes a standard, then we have, by definition, more national security benefit because we understand what those standards are and we have more control.

Mr. LEVIN. Yeah, that would be correct, Senator.

Senator SMITH. And it is sort of a truism of business, in general, broadly speaking, when they think about regulation that they will say, "I just want to know what the rules are so that I can follow them, and I want an even playing field," the good businesses, the businesses that are operating above board. It seems like that would be pretty much the same view if you look at digital assets and crypto.

Mr. LEVIN. Yes, Senator, indeed. So the industry in this country has done a lot of work on collaborating with regulators on the different proposals that are being put in place. They participate extensively in public consultation on this type of regulation, and there have been a lot of efforts on educating regulators, policymakers on really the unique attributes of cryptocurrencies and what potential it has for really novel types of oversight.

And I think one of the points here is that the transparency of cryptocurrencies and the availability of the data means that there can be greater oversight for these financial regulators in novel ways that actually this Committee has been very focused on achieving in broader financial services and actually setting up a regulatory architecture that can endure over time but costs less for business and is more effective.

Senator SMITH. And Mr. Stansbury, to the same extent that having an understandable regulatory framework can create a fair and even playing field for good actors, how do you respond to this if you are trying to figure out how to crack down on the bad actors? What impact does the lack of a clear regulator or a clear regulatory framework have if you are trying to take advantage of the system, like we know some are?

Mr. STANSBURY. Thank you, Senator. Yeah, I think the lack of clarification lends itself, obviously, to the sort of murky situation that we have now where we clearly have a group of exchanges working in the cryptocurrency world that are trustworthy, doing the right things, and that are providing the kind of know-your-customer information and things that are helpful to prosecutors and investigators. But the lack of clarity also contributes, I think, to a very large ecosystem of institutions that are working outside that.

And so I think the clarity would help, but also I think enforcing the Bank Secrecy Act more aggresively could help, and drafting maybe tighter rules on money transmitters like cryptocurrency exchanges and payment providers. There has been some movement like that, but those things help on the enforcement front because it helps push people toward the legitimate exchanges, I think.

Senator SMITH. Thank you very much. Thank you, Mr. Chairman.

Chairman BROWN. Thank you, Senator Smith.

Senator Warren, from Massachusetts, is recognized.

Senator WARREN. Thank you, Mr. Chairman.

The cryptocurrency market has exploded over the past few years, with the volume of crypto transactions reaching nearly $16 trillion last year. That is up about 600 percent just from 2020.

Now most of that growth has been driven by speculation and gambling, but we also know that crypto provides a new payment option for criminals and cheats, and it is how those who attack our systems with ransomware collect their money, with the least risk that they will be caught. In fact, according to one of our witnesses who is here with us today, about three-quarters of the money collected in ransomware attacks last year went to Russia-linked actors. So Russians certainly know how to run illegal scams through crypto. And we know that other countries have used crypto to evade sanctions.

Mr. Levin, your company tracks illicit finance in crypto. Do you know which countries have already used crypto to evade sanctions?

Mr. LEVIN. Thank you, Senator, for the question. It is an incredibly important issue and something that we spend a lot of time researching and detecting, actually.

So when it comes to sanctions evasion the transparency of the blockchain actually does——

Senator WARREN. Excuse me. My question was do you know the three countries that have already used crypto in order to evade financial sanctions?

Mr. LEVIN. We have detected the use of cryptocurrency in Venezuela, Iran, and North Korea.

Senator WARREN. OK. And just last week, FinCEN, the Federal agency responsible for identifying financial crimes, issued a warning that in light of the sanctions against Russia, quote, "sanctioned persons, illicit actors, and their related networks or facilitators may attempt to use crypto and anonymizing tools to evade U.S. sanctions and protect their assets around the globe," end quote.

Even so, the crypto industry claims that Russians cannot use crypto to hide their wealth because the $3 trillion crypto market is too small and too transparent for that to work.

So let us test that out just a little bit. Mr. Levin, let us consider one of Putin's cronies, who already has a billion or so in crypto, that he wants to hide from the Governments that are enforcing sanctions on oligarchs. Now, can this oligarch make it harder to trace his money if he hops from one blockchain to another, if he deposits those tokens into a couple of wallets that do not require him to provide identifying information, and if uses a mixing service that launders his money with other people's money?

Mr. LEVIN. Thank you, Senator. So the scenario that you describe where an oligarch has $1 billion to be able to launder requires significant amounts of liquidity to be able to obfuscate that amount of money through the use of cryptocurrency. In fact, many times we have been able to identify——

Senator WARREN. I am sorry. Let me just remind you of what my question was again. What I am asking is about the tools that are

available. Now he may have to break it up into multiple pieces of who knows, $100 million at a crack. But the question I am asking is does hopping from one blockchain to another, does depositing tokens in a couple of wallets that do not require him to provide identifying information, and does using a mixing service all make it easier for him to hide his money?

Mr. LEVIN. So, Senator, the answer to that question is no, because the chain-hopping that occurs, you need to actually provide the tokens, which in a transparent way allows you to move across blockchains. We have actually got software that allows——

Senator WARREN. So you do not think chain-hopping makes it any easier to hide your money? How about depositing tokens in wallets that do not require identifying information?

Mr. LEVIN. You can always split the money up into wallets that do not require——

Senator WARREN. And that would help hide the money?

Mr. LEVIN. But that does not remove the record of where the money actually sits——

Senator WARREN. The question I am asking is does it make it harder to track the money?

Mr. LEVIN. No. So it does not make it harder to track the money because there is——

Senator WARREN. And using a mixing service, you are telling me, does not make it harder to launder money?

Mr. LEVIN. The daily liquidity value of mixing services globally is about $30 million. And so, therefore, it would——

Senator WARREN. So he might have to do this day by day?

Mr. LEVIN. And we have done extensive work in tracking large sums of money through mixers that have led to the arrests of people and the disruption of their activities.

Senator WARREN. You know, I am actually a little surprised by your answer, since you charge a lot of money to untangle and track assets through the system, and the system keeps developing more ways to obscure that money, and that is part of what you advertise.

But I want to get on to a question with Mr. Stansbury. You are a former Assistant U.S. Attorney who has led major cybercrime and money laundering investigations. So let me ask you, is it possible that the oligarch, my hypothetical oligarch, could now buy and sell some of the things that he wants—diamonds, art, maybe even real estate—without ever needing to put his money into the formal banking system, which also would make it harder for law enforcement to catch him?

Mr. STANSBURY. Thank you, Senator. Yes, it is theoretically possible in today's market. Obviously, it is hard, but at least if he is able to go to a friendly jurisdiction and use cryptocurrency exchanges or some other platform that is not in compliance with internationally recognized anti-money laundering standards, as you have suggested, that is possible. There is also some reporting recently of jurisdictions being friendly for some purchases of real estate and other items through cryptocurrency.

Senator WARREN. So no one can argue that Russia can evade all sanctions by moving all its assets into crypto, but for Putin's oligarchs who are trying to hide, well, a billion or two, a few hundred million, crypto looks like a pretty good option.

And that is why I am introducing today my Digital Asset Sanctions Compliance Enhancement Act, along with nine members of the Banking Committee, including the Chairman of the Senate Armed Services Committee, the Chairman of the Senate Intelligence Committee, and the Chairman of the Defense Appropriations Subcommittee, and several other Senators. This is a bill that would authorize the President to sanction foreign crypto firms that are doing business with sanctioned Russian entities, and authorize the Secretary of the Treasury to act.

Thank you for being indulgent, for letting me run over on time. I appreciate it.

Senator TOOMEY [presiding]. Senator Lummis.

Senator LUMMIS. Thank you, Mr. Chairman. I appreciate your appearing here today. Thank you for joining us.

Mr. Mosier, I want to ask you a straightforward question, based on your law enforcement experience at the Treasury Department. If an investigator was forced to choose between investigating an illicit finance case involving cash or digital assets, which do you believe most would choose, and why?

Mr. MOSIER. Thank you for the question, Senator Lummis. I think there is no question—and this comes from time at the Department of Justice and also being the head of enforcement at OFAC—it is far, far faster to get to the critical point that you need to dig deeper with cryptocurrency, given the nature of the public ledger. This is for several reasons. One, you have a public, immutable ledger.

So if you take the example of when OFAC designates an address, within hours mathematical heuristics from Chainalysis, TRM, Elliptic, all these tools out there, are quickly building out all the public ledger networks that are associated with that address through cospending and other relatively mathematically certain ways of at least knowing what the association is. In the fiat world, you seen an address and for the next 3 years you do Mutual Legal Assistance Treaty requests and hope that you get something back. You guess what regional banks might be involved, based on the customers you think it is going to be, and send subpoenas, and hope that they come back. And then you manually try to associate addresses with entities. It is just exponentially faster.

Senator LUMMIS. Thank you. Mr.—is it Le-VIN or LEV-in?

Mr. LEVIN. Senator, I respond to either, but it is Levin.

Senator LUMMIS. Levin. OK. Thank you. Chainalysis found that approximately 0.15 percent of all digital asset transactions were related to illicit finance in 2021. Is that correct?

Mr. LEVIN. Yes, 0.15 percent. Yes.

Senator LUMMIS. The United Nations recently estimated that money laundered in the traditional financial system is between $800 billion and $2 trillion in U.S. dollars a year. So how does that compare with digital assets?

Mr. LEVIN. Thanks, Senator. So just to put the like-for-like comparison, it is important to look at the percentages as estimates. And so in the traditional financial sector, the OCED and IMF and others, estimates somewhere between 2 to 5 percent of world financial flows are related to money laundering and illicit flows, comparing that to the 0.15 percent when it comes to cryptocurrencies.

Senator LUMMIS. So clearly cryptocurrencies have a smaller illicit use than fiat currencies.

Mr. LEVIN. Yes, Senator, that is correct.

Senator LUMMIS. OK. Is Mr. Chobanian online?

Mr. CHOBANIAN. Yes, I am.

Senator LUMMIS. Oh, excellent. I have a question. Hi, Mr. Chobanian. I so appreciate your being here. I want to ask you about the record sums of money that the people of the world have donated to Ukraine using digital assets over the last few weeks. How long did it take for you to set up the infrastructure to begin accepting donations, and how long does it take for the Ukrainian Government to begin to use those donations?

Mr. CHOBANIAN. Thank you. So the setup was about 10 minutes. The hardest part was to actually put the addresses on Twitter because we had to go through the bureaucracy of who is in charge of a Twitter account of Ukraine. And in terms of usage, the minute the crypto landed on these addresses, the Government could use them, so immediately. No bureaucracy here.

Senator LUMMIS. So how long and how burdensome would it have been for you to accept donations using traditional forms of payment from other countries, including wire transfers?

Mr. CHOBANIAN. If I can remember and recall correctly, I think it took National Bank about 10 days to post the IBAN and the rest of the correspondent addresses needed to wire the money to Ukraine.

Senator LUMMIS. So digital assets have made an important difference to the defense of Ukraine. Is that true?

Mr. CHOBANIAN. I am sorry, differently. We actually received the first humanitarian aid on the second day after we received the first crypto, so we spent it immediately, and the next day the goods were in Ukraine, less than 24 hours. Is that the answer?

Senator LUMMIS. That is the answer, and I am so pleased you were willing to take the time to be with us today, because while a lot of attention has been paid here in Congress to whether the Russians could use digital assets to evade sanctions, there has been very little attention paid to how much the existence of digital assets have benefited the Ukrainians in being able to get badly needed supplies.

So I am deeply grateful to all of our witnesses today. Thank you very much, Mr. Chairman. I yield back.

Senator TOOMEY. Is Senator Warner with us remotely?

Senator WARNER. I am, Senator Toomey. I am here.

Senator TOOMEY. Senator Warner is recognized.

Senator WARNER. Thank you, and I do appreciate you and the Chairman holding this hearing, and I think there is a little bit of a conundrum here, as somebody who has been looking at this issue for some time, as Chair of the Intelligence Committee. I am not sure the kind of positing of this is an either/or circumstance is the correct posit. I believe there is some value in digital assets. I think we need to continue to explore it.

And, you know, candidly, I want to acknowledge Senator Lummis' last point with our witness from Ukraine. This has been a way to move assets to the Ukrainian people in a relatively fast way, and I want to commend that.

But I also want to start—and I am actually proud to be one of the sponsors, along with Senator Warren, because I am hugely concerned that because of some of this ease of transferring of assets that has helped the Ukrainian people, as we have seen from some of the press reports and we litigate the Reuters article, that that same ease and, frankly, lack of transparency has allowed, and will allow Russian oligarchs—and I hope we can move further and not just sanction the top oligarchs but we ought to sanction the whole Russian Duma for being complicit with Putin's illegal invasion of Ukraine. But that same ease is allowing conversion of fiat currency to crypto, to then potentially buying properties in Nations around the world that have accepted this.

But I want to start with Mr. Stansbury, because on the whole question of ransomware, I respectfully disagree very strongly with Mr. Levin's analysis of 0.15 in terms of illicit payments, and again, one of the reasons why we passed—and I appreciate everybody's support on this—a mandatory cyber reporting bill. We only had about a third of the cyber incidents being reported to the Government that need to be reported, so can share, frankly, with our private sector partners. But I can assure you, and we saw this with the Colonial Pipeline incident, that I believe the volume of ransomware that is paid in crypto assets, Bitcoin, et cetera, is exponentially higher.

Mr. Stansbury, the continued growth and profitability of ransomware, do you see that connection to the ability and the liquidity brought about by cryptocurrencies, and that interaction? I think it is, again, much higher than what the other witness testified to.

Mr. STANSBURY. Thank you, Senator Warner. I would agree, and, in fact, the FBI and other agencies have indicated that ransomware incidents are much, much higher than all of those that we hear about and know about, obviously, because not all of them are reported, and I think we have a lot of unknowns.

And in terms of where the trends are going, I think that probably tells you a lot of what you need to know. Last year, in October, in a FinCEN report, it was revealed that SARs filed, in I think 2021, were projected—in the first half of 2021—were projected to have a higher ransomware-related transaction value than SARs filed in the previous 10 years combined.

So I think the trend tells us that cryptocurrency works. The fact that it is the exclusive tool for ransomware actors I think tells us a lot. So I would look at that evidence as much as anything else.

Senator WARNER. And I completely agree with that, and again, I think one of the things that this new law will have is cyberincident reporting but also there will be some ransomware reporting, so we will have, candidly, better data.

And the notion, frankly, that the Russian Government, in one effort, did help us potentially identify some of the Colonial Pipeline ransomware criminals, using crypto as their payment methodology sure as heck means the Russian Government knows how to use this currency, knows how to use this payment method. And I think we need to make sure there is not the leakage of these sanctions.

We all want to sanction the bad guys in Russia. I think we ought to broaden those sanctions, and I think the legislation—and I hope

we will be able to work through this and gain broader-based support, that Senator Warren and a group of us, eight of us, nine of us, have put together, will ratchet off that ability to evade those critically important sanctions.

I know I have gone over time, but I hope we can come back, Mr. Chairman, and revisit this issue in a broader way. Thank you.

Chairman BROWN [presiding]. Thank you, Senator Warner.

Senator Cortez Masto is recognized, from Nevada.

Senator CORTEZ MASTO. Thank you, Mr. Chairman, and thank you to the panelists.

Let me associate myself with some of the comments by Senator Warner, and let me start with this to the panelists.

Mr. Levin, let me start with you. What are the illicit finance risks of digital assets? We are hearing from law enforcement agencies that there are still concerns around the use of cryptocurrency, that it is still an attractive vehicle for illicit financial activity. What do we need to be aware of?

Mr. LEVIN. Thank you, Senator. The law enforcement agencies that are responsible for investigating these illicit flows need more resources to be able to get their arms around this new technology. They have to adapt a whole new way of policing, and they need new techniques and methods to be able to get after these types of crimes. Particularly in the realm of cybercrime and cyber-enabled crime, cryptocurrencies have been used to effect by those actors. But with the appropriate tooling we have seen successes when it comes to everything from the types of money laundering infrastructure that helps facilitate these types of crimes.

Alexander Vinnik is sitting in jail in France, having started BTC-e, which was one of the major sorts of Russian money laundering operations, in a historical sense. And so, you know, cryptocurrencies with the appropriate techniques from law enforcement agencies can actually combat these types of illicit flows.

Senator CORTEZ MASTO. And Mr. Mosier, do you feel the same way?

Mr. MOSIER. I do, Senator Cortez Masto. Thank you for asking. And actually I just want to underscore one part of what Mr. Levin said. As the Acting Director of FinCEN and Deputy Director, I pushed and pushed and had the same argument with the Office of Management and Budget and the White House repeatedly saying there is an enormous amount of data here and transparency. We need the tools to be able to do it.

What I got were questions of, "Why do you need more than one?" or "Why do you need more than one license?" "Can't you just call somebody else who has one and ask them to look it up?" And I had to explain to them, as the former in-house counsel at Chainalysis, I am certain that is a violation of license terms to simply not buy a license and have someone else look it up for you.

And actually, part of the benefit of having a public ledger and the ability to monitor in real time to go after the people that are doing these things is that you need the tools to do it in real time to benefit from this. We do not have to wait 3 years for a Mutual Legal Assistance Treaty, but we do need the resources to do it.

Senator CORTEZ MASTO. Right.

Mr. MOSIER. Thank you.

Senator CORTEZ MASTO. No, I appreciate that, because I also know that the concern—I have worked in law enforcement for a number of years addressing money laundering issues, right. The drug cartels in Mexico, they are always trying to figure out how they can move cash, whether it is actually a briefcase full of case, then to debit cards, to some other form or system. And we are always trying to follow the money, as you said, and track it as quickly as possible to lead us to that criminal activity or terrorist activity, whatever it is.

Do either of you think that digital currency or cryptocurrency is going away?

Mr. LEVIN. Senator, I do not think cryptocurrency is going away. In fact, I think that it will continue to become a more important financial rail for commerce more broadly. And I think what you are seeing is that at the beginning of cryptocurrencies we had cryptocurrencies that represented themselves in these communities that use them.

But increasingly you see it intersecting with a broad range of industries. And so if you look at the art market today or you look at the music industry, or even how people manage their data for their electric vehicles, there are ways in which these types of value are being represented on these cryptographically secure ledgers to introduce brand new ways of conducting markets. So I do not believe it is going away.

Senator CORTEZ MASTO. Thank you. And Mr. Stansbury, any comment to add to the questions that I have just asked?

Mr. STANSBURY. No, Senator.

Senator CORTEZ MASTO. Thank you. And let me also say this to Mr. Chobanian. First of all, let me just say our thoughts are with you and your family and all Ukrainian citizens right now as they fight the cruel and deadly invasion ordered by Putin. And thank you for your comments around the benefits that you are seeing right now with respect to the cryptocurrency and the support for Ukraine. But is there concern that you have about how the people in Russia are opposing Putin's murderous regime by the use of cryptocurrency?

Mr. CHOBANIAN. That is correct. They are running away from ruble, and most of them are running away physically from Russia. And the only way for them to exist outside of Russia right now is actually cryptocurrency. You are not being able to buy a house or a car but at least you can survive.

Senator CORTEZ MASTO. Thank you. I know my time is up. I am going to submit some of my questions for the record, the remaining of them. But this is such an important panel. Thank you all for being here.

Chairman BROWN. Thank you, Senator Cortez Masto.

Senator Reed, from Rhode Island, is recognized.

Senator REED. Thank you very much, Mr. Chairman, and thank you, gentlemen, for your testimony.

I think one of the premises we are beginning is that you can divide the world into good actors and bad actors, and the bad actors can use cryptocurrency with great efficiency and great effect. The good actors, they are good people, but we are focused on the bad

actors. And I think in Chainalysis you basically identify wallets that are connected to a bad actor. How do you do that, Mr. Levin?

Mr. LEVIN. Thank you, Senator. So we track all cryptocurrency transactions, so not just the good actors and not just the bad actors. We track the entire ecosystem to be able to map really which services are present, putting those transactions into these ledgers and facilitating the movement of currency.

And so when it comes to illicit activity we track ransomware actors and all of their enablers by actually gathering intelligence about those ransomware campaigns. We can actually also make transactions with these types of actors. We have a team of about 50 people that are specialist researchers that conduct collection on these types of illicit activities and specialize in specific types of crime, to be able to label that in our system so that not only can law enforcement partners investigate those types of crimes but our private sector customers can screen for that type of risk in these transactions, and prevent it, and report them as suspicious activity reports to FinCEN.

Senator REED. So effectively you are employing human intelligence to analyze the activity that is going on, and then you are identifying the bad actors and communicating that to your clients and others. But how effective are you in identifying the bad actors since there is so much anonymity in the system?

Mr. LEVIN. Thank you, Senator. Yes, so the way in which this works is that not only do we have the ability to collect human intelligence on this activity but actually because of the transparency we actually can further the identification of the activity beyond the individual incident that we have detected.

And so maybe just to go back to the question about ransomware reporting from Senator Warner is that actually we tend to have higher estimates of the amount of ransomware revenue being generated, because we can take a solo incident of ransomware reporting and broaden that out to be able to identify all of the activity that that campaign has been running.

So I think it is important to see that we only need to see them once, and we can then unravel the financial network, due to the completeness of it and the transparency.

Senator REED. Just a final quick question. Can you reach down to identify real individuals?

Mr. LEVIN. So, Senator, we do not collect information about individual people. That is collected by the regulated financial institutions that have to have their KYC processes, and then law enforcement typically uses their legal authorities to go and further their investigation and collect that piece of information.

But the interesting thing is that the investigation can progress a lot faster and you can complete the picture of the entire financial network when it comes to cryptocurrencies without actually get down into the individual identity.

Senator REED. Just another quick question. Our assumption, I think, is that the oligarchs and the bad actors of the world deliberately have put in their portfolios cryptocurrency. That is an avenue they want to exploit. Is that your sense too?

Mr. LEVIN. Senator, I think that assumption, you know, may be something that we can easily have a hypothetical scenario in which

that is the case. I think when you look at the actual data about the amount of wallets that are present, and you look at the concentration of cryptocurrency and its use, I think the most sophisticated actors in Russia when it comes to cryptocurrency have been largely around sort of large cybercrime rings and not sort of large sums of money with Russian oligarchs.

Senator REED. Thank you. Just a final question, and I do not expect an answer. But to what extent do we have to worry about cryptocurrency displacing fiat currency so that there is really no way for the Federal Reserve, for example, to control or attempt to control the economy?

Mr. LEVIN. Yeah, Senator, it is obviously a question that requires deep inspection. But the quick answer is that cryptocurrencies represent global communities and new ways of commerce, and I think it is more beneficial to view cryptocurrencies as truly a technology that enables a lot more industries and a lot more business models that can change the way—you know, away from, say, rent-seeking organizations to a much more distributed economy. And so I think that would complement, actually, the issuance of the dollar.

Senator REED. Thank you very much. Thank you, Mr. Chairman.

Chairman BROWN. Thank you, Senator Reed.

Senator Van Hollen, of Maryland, is recognized.

Senator VAN HOLLEN. Thank you, Mr. Chairman. I thank all of you for your testimony, and I want to thank the Chairman and Ranking Member for holding this series of hearings of cryptocurrency, because I think everybody is working to get up to speed on the public policy challenges. And clearly there are benefits, as has been described in this hearing, and there are also risks.

And I think it is fair to say, and I have been trying to follow the testimony from my office, is that for people who engage in ransomware, I mean, cryptocurrency is the preferred method of payment today. That happened in Baltimore City. Baltimore City was the victim of a ransomware attack. They insisted on payment in Bitcoin. That was the case in the Colonial Pipeline. I mean, we recovered some of it, a lot of it. But is that not a fact, that right now at least the people perpetrating these crimes perceive this method of payment to be the best in terms of hiding their identity? Mr. Levin.

Mr. LEVIN. Thank you, Senator, and yes, I was very intimately familiar with the Baltimore case, where ransomware has affected people's lives.

So when it comes to being able to detect this, and the reason why criminals actually use it, is they are economic actors and so they are looking for methods that maximize profitability first, not necessarily their anonymity. And so cryptocurrency has been used in ransomware cases because it is easy to acquire Bitcoin, it is easy to send that Bitcoin anywhere in the world, and that is why it has risen to prominence inside ransomware.

But those actors typically feel like they are beyond the reach of the law, and that has systematically become not the case as we have become a lot better at detecting the entire financial network that actually enables ransomware.

And so if you look at the NetWalker case, where an affiliate of a ransomware campaign was arrested up in Canada, that was

made possible because we can see the entire business model of these ransomware campaigns on the blockchain, and so we can identify those enablers and shut them off, which would start to disrupt the amount of ransomware that affects this country.

Senator VAN HOLLEN. Right, and a lot of the testimony here has been that because of the blockchain technology we are better able to at least track the identity of a digital wallet. Then there is always the challenge of figuring out who is behind the digital wallet.

But in the Colonial Pipeline case, as I understand it, the FBI was able to get the key to the digital wallet. Is that your understanding?

Mr. LEVIN. Senator, yes, that is my understanding too.

Senator VAN HOLLEN. Which is a different method of recovering the payment than hacking into the system, or does that amount to the same thing?

Mr. LEVIN. So, Senator, the details of all of the way in which the FBI managed to retrieve those funds are not necessarily in the public domain, but the way in which this occurs is access to the key itself rather than hacking into the entire system. The Bitcoin system is secure. Someone's ability to hold those keys can be a vulnerability that could be exploited in those types of cases.

Senator VAN HOLLEN. So I want to press this point a little bit because it is getting to the other side of the equation, which is on the one hand people say, well, cryptocurrencies are a secure way for someone, a criminal, to hide their assets, but we also have cases like the Colonial Pipeline but also cases where crypto exchanges have been hacked, right? I mean, there are numerous examples of crypto exchanges being hacked. Is that not the case?

Mr. LEVIN. Yes, that is the case, Senator.

Senator VAN HOLLEN. And, you know, this Committee has had a conversation about if you are an investor in a cryptocurrency what is your recourse if a cryptocurrency exchange that you have invested in gets hacked. Are you able to recover your assets? And right now there is no protection.

Can you just speak, though, to the question of vulnerability and hacking of the crypto systems, because that seems to be another area where, on the one hand we say they are very difficult to penetrate, but increasingly this seems more like the arms race, right, where people just try to leap ahead of the technology. What is the vulnerability in terms of hacking?

Mr. LEVIN. Thanks, Senator, and it is an incredibly important issue, particularly for consumers. So when it comes to the ability to hack into exchanges, these are financial intermediaries, where someone is holding funds on behalf of someone else. And in those instances, that is where regulation can come in and be very helpful in establishing sort of best practices and standards by which those exchanges and financial intermediaries should hold funds the same way that other financial institutions do.

And increasingly what you see is, you actually see the largest custodians in the world—you know, the Bank of New York, Mellon—actually come into crypto custody to be able to offer really robust custody solutions, the same way that we have for traditional securities and other financial instruments.

And so I think what we will see is that there is an increase in the maturity of the types of actors actually entering this market, where those types of vulnerabilities, at least on the exchange level, will start to be closed. We do see vulnerabilities starting to emerge in other parts of the ecosystem that do also need some more attention, but this is something that matures over time with the technology and also with the actors that get involved in the industry.

And so I think you are seeing a very positive direction with that, with the types of actors that are now stepping into the space.

Senator VAN HOLLEN. Thank you. No, I agree with the Ranking Member's observation that this is an area that is here to stay and does require regulation, and we need to be very sort of up to speed on how we go about doing that. But this is one of the areas, it seems to me, where consumers beware and where regulation could be important.

Thank you, Mr. Chairman.

Chairman BROWN. Thank you, Senator Van Hollen.

Senator Sinema is recognized from her office, from Arizona, from her office.

Senator SINEMA. Thank you, Mr. Chairman, and thank you to the witnesses for being here today.

Arizonans and Americans stand with the people of Ukraine in opposition to Russia's illegal war. Just yesterday we heard from President Zelenskyy in a joint address to Congress about the tools Ukrainians need to defend themselves. I am committed to working with my Senate colleagues to deliver more military equipment and humanitarian support to Ukrainians.

Our efforts to crack down on illicit financing are an integral part of this strategy, as we work to break the supply chains and the financing of Putin's war machine and to bring this needless violence to an end.

Mr. Levin, thank you for being here today. Your company, Chainalysis, has helped law enforcement and our sanctions professionals track down illicit activity on the blockchain. I appreciate your team's willingness to proactively brief my staff last year on your company's work. For many, the idea that your company could help connect illicit activity on a supposedly anonymous platform to real people is surprising. Your testimony spoke to this, but briefly, how does your company manage to catch illicit activity in cryptocurrency without attempting to break the blockchain or undermine the integrity of the distributed ledger?

Mr. LEVIN. Thank you, Senator, for the question. The ability for us to actually detect illicit activity on the blockchain depends on our ability to actually see the transactions. And so the public nature of the blockchain means that our team can look at every single transaction that has ever happened in the majority of cryptocurrencies. And we use a combination of human intelligence, where we are actually able to collect information and transact on these networks, with our machine learning algorithms that allow us to tie different transactions together to form a full picture of the way the services are being used by people to use cryptocurrency technology both for good and for bad.

And so, you know, what it takes is a team of specialists and a lot of dedication over the last 8 years to build an expertise in how

cryptocurrencies can be abused, and we are able to map out the full wallet infrastructure that these illicit actors are using and provide that in our tools, both to our private sector customers and the public sector.

Senator SINEMA. Thank you. Some more sophisticated criminals will use tactics like chain-hopping or make use of mixer or tumbler services, where they will repeatedly move transactions between and within cryptocurrencies to make it harder to track funds. Do your company services offer an effective response to these evasion tactics, and what is the biggest limiting factor in the services that your company can provide?

Mr. LEVIN. Thank you, Senator. So yeah, when it comes to the issues of chain-hopping and mixing I will take them separately.

So the ability to chain-hop often requires transactions where you lock up a cryptocurrency asset on one chain to unlock a rapt version on another chain, which is commonly referred to as chain-hopping. That activity can be seen on the blockchain, and we have released the ability to actually do cross-chain investigations on our investigation platform. So that type of activity actually does not provide the level of anonymity that it may seem in the name of it.

When it comes to mixing services, we have, and not necessarily completely publicly been seen to actually have techniques that have the ability to de-mix certain transactions. And so our research and development efforts consistently keep with the way that people try and obscure themselves in financial transactions, and we have actually seen successes operationally, and we would be happy to follow up with a separate briefing on that, to actually find ways to de-mix transactions and find the individuals responsible at the end of it.

So that is where we invest R&D efforts in continuing to keep up and actually stay ahead, mostly, of the way in which criminals use or abuse cryptocurrencies.

Senator SINEMA. Thank you. Mr. Chobanian, thank you so much for being here with us today, and I want to express my continued solidarity with the people of Ukraine.

Yesterday, President Zelenskyy signed a law legalizing cryptocurrency in Ukraine. Can you share a bit about why this was important and how Web3 technologies are providing new tools to help the people of Ukraine weather this illegal war and unprecedented humanitarian crisis?

Mr. CHOBANIAN. Hello. Thank you. So yeah, we have an official law now. The next step would be to make changes to the tax laws, and after that the law will be in place.

So basically what it does, it provides rules of the game for the business in crypto on how we can operate, whether we can open a bank account—obviously, we will be—what are the rules for AML/KYC in regard to crypto, who is in charge, whether us or in the banks, and so on and so on. So basically within the year after we finish the war we are going to have the full market. And I see that you are still discussing whether to ban or allow crypto in U.S. I invite all U.S. companies to come to Ukraine and open up there. You can use Ukraine as a sandbox for U.S. I do not see a problem here.

Web3, it is basically going to change the world. It will be the technology that we are going to use to rebuild my country, namely

the blockchain, because it shows the transparency of everything, and that is the main topic that we have been discussing for the past hour. Thank you.

Chairman BROWN. Thank you, Senator Sinema.

Senator Daines is recognized, from Montana.

Senator DAINES. Chairman Brown, thank you. I think this topic is really important for us to be discussing, given the war in Ukraine and recent comments. I strongly believe that President Biden should never have given a green light on Putin's Nord Stream 2 pipeline in the first place. In fact, I had Ukrainian leaders in my office September 30th—I went back and grabbed the memo—leaders from Odessa, Deputy Mayor, former member of Parliament, current member of Parliament. They were in my office pleading with us to stop the Nord Stream 2 pipeline. That was September 30th.

And while I am disappointed in my colleagues across the aisle—and by the way, if you want to see what is going on in Odessa just look at the latest press reports. They are gearing up right now. They think that is going to be the next battle city. They call it the Southern Capital of Ukraine, beautiful port city, the Black Sea, and the Russians look like they are headed there next, and they are hoping to save this beautiful opera house, other great community there in Odessa. But it is what it is at the moment.

I am disappointed that my colleagues across the aisle voted against reimposing sanctions on the Russian pipeline earlier on, despite the pleas from the Ukrainians. I believe we can all agree that the sanctions that have been imposed thus far have had a significant impact on the Russian economy, and that is probably to say the least.

And while it is possible, it is unclear to me that digital assets are being used by Russia to evade the sanctions in any meaningful way. In fact, Treasury officials, including the Financial Crimes Enforcement Network, have stated this to be the case.

Legitimate crypto intermediaries, such as CoinBase, Gemini, others abide by KYC and AML standards, are interactively updating their standards to comply with the sanctions. Even actors utilizing so-called dark web typically need to involve a financial institution obligated to AML and sanctions requirements to convert crypto assets into fiat currency.

At the same time, we have seen the Ukrainian Government explicitly solicit crypto donations. On Monday, the Ukrainian Government launched a crypto donation website, partnering with FTX, Everstake, and the KUNA Exchange, based in Ukraine, which will route donated crypto to the National Bank of Ukraine. According to the Ukrainian Government, over $100 million in crypto donations have poured into the website and other smaller funds. This demonstrates, I believe, how powerful crypto and other digital assets can be as a tool to revolutionize finance in the speed at which donations can flow around the world.

Now turning to my questions. Mr. Mosier, can you describe the process of converting digital assets into fiat, and related to that, would someone trying to evade sanctions be able to do this?

Mr. MOSIER. Thank you for the question, Senator Daines. So actually it is a complicated process because you have got to get li-

quidity on the other side to begin with. Someone has to want your rubles, and there are not a lot of people in the world right now that want rubles. So first you have the market problem.

Second, you have to find somebody that is willing to make that trade that also feels comfortable that they are not violating any sort of global laws that they are going to be come after with, whether it is sanctions or domestic currency controls. But most likely it is not going to be anyone outside of Russia, that is for sure, because, first of all, no one wants the ruble, and second, they have their own jurisdictions enforcement to look at, and they have global sanctions in probably the most united front that we have seen, certainly in the Western Bloc.

Senator DAINES. So drawing from your past experience at the Office of Foreign Assets Control and FinCEN, do you think blockchain technology provides certain benefits with regard to the ease of detecting illicit financial flows?

Mr. MOSIER. Absolutely, I do, Senator. And I think it is an important question because there are two benefits to blockchain technology that are important to think of from an American perspective. One is the ability to much faster home in on what is the bad actor that we need to worry about, because you can follow the transactions almost indefinitely, and it is an immutable public ledger, which means you can share that information with partners around the world. But I think there is another important piece here. We are sometimes talking about privacy like it is an obstacle, but privacy is part of the Constitution, as a matter of security and personal sovereignty. That is not just something to slow down investigations. It is something that we also want to protect vulnerable people. That is why we have subpoenas. That is why there is court process about this. And so what this does is instead of the dragnets, that Senator Toomey had mentioned before, is you focus on what we have already identified through activity——

Senator DAINES. I would think the Ukrainians at the moment would be very sensitive to the issue of privacy.

Mr. MOSIER. Exactly. Absolutely, sir.

Senator DAINES. In my remaining time I want to ask a question to Mr. Chobanian. Mr. Chobanian, can you describe how the Ukrainian Government has utilized the crypto donations that have been received to date?

Mr. CHOBANIAN. Sure. It is public information. We bought helmets, bulletproof vests. We bought the first aid kids, blood-stopping wound, something—I do not know what is the real name of it—the scopes, and then we bought a lot of rations for the soldiers, close to 500,000. We delivered money to, for example, people in Mariupol, to people in Kharkiv, to people in Sumy. So we actually sent money in crypto to those cities and they managed to buy, well, first of all, changed it to local currency or directly using crypto, to buy food and distribute it among the citizens of those cities. So these are the examples of how we are using money. Everything is transparent, so it is fantastic. I would say it is a lifesaving thing. It is impossible to do with a regular banking system.

Senator DAINES. I am out of time, Mr. Chairman. Thank you.

Chairman BROWN. Thanks, Senator Daines.

In the interest of time—Senator Toomey has one short question—I will provide a question in writing to Mr. Stansbury and then we will wrap.

Senator TOOMEY. Thank you very much, Mr. Chairman, for that indulgence. The question is for Mr. Chobanian. Reading a section of the legislation that Senator Warren referred to, one of the things I am concerned about is it would impose the equivalent of really secondary sanctions on anyone doing crypto business with anyone from Russia. I know the intent is to go after oligarchs, but it looks to me like it would have a hugely negative impact on anybody in Russia engaged in any kind of crypto transactions.

And so my question, Mr. Chobanian, is, could you just talk to us a little bit about the overlap or the correlation between those Russian people who use crypto and those who are opposed to what Putin is doing, those who are maybe hostile to his regime?

Mr. CHOBANIAN. There is a very good correlation here. Well, first of all, the people who are using crypto in Russia are at least intelligent, they have money, and they understand technology. So these are clever people, obviously. And they do not watch TV, so they are not zombies of the regime, so they understand what is happening around the world. They travel the world. They see the Western world. They see how it is different to the regime in Russia.

So these people are actually our closest friends, because they oppose Putin just as much as we do. Unfortunately, they cannot really do much because they do not have any insurance to fight the regime, at least from their point of view.

So for us, yeah, it is very important—and I want to stress this out again, that it is very important that we do not block the regular people in Russia who are actually opposition within Russia. We only have to go after the sanctioned list and sanctioned people, and these people actually have much, much more wealth accumulated. So for them it is probably the average, you know, amount that they want to hide is in hundreds of millions. For the regular Russians it is probably $1,000 or $10,000, in equivalence.

So we have to make sure that we do not block these people and we still allow for the opposition to survive, both within Russia and outside. Because as you know, they cannot use Visa or MasterCard outside of Russia right now, so the only means of payments they have is cash or crypto. That is it. And considering that all of the anarchy we see imposed in the world right now, you can only exchange crypto to like, I think it is $1,000 in most of the jurisdictions. So we have to make sure that we do not, you know, cutoff these people from actually surviving.

Senator TOOMEY. Thank you, Mr. Chairman.

Chairman BROWN. Thank you, Senator Toomey. For Senators who wish to submit questions for the record those questions are due 1 week from today, Thursday, March 24th. Witnesses, please, if you can, you will have 45 days to respond to any questions.

Thank you again for the testimony from the four of you. Thank you. And Mr. Chobanian especially, good luck to you.

This Committee is adjourned. Thanks.

[Whereupon, at 12:12 p.m., the hearing was adjourned.]

[Prepared statements, responses to written questions, and additional material supplied for the record follow:]

PREPARED STATEMENT OF CHAIRMAN SHERROD BROWN

In 2019, a doctor's office in the Mahoning Valley in Ohio experienced a disturbing attack: hackers locked the office computers, making them unusable. They even faxed over a ransom note, promising to unlock the computers if the practice turned over $75,000—in Bitcoin.

Not long ago, a Syrian group tied to al Qaeda put out a call for donations to help buy weapons. Their social media post said that supporters should "donate anonymously with cryptocurrency."

"Donate anonymously."

A week ago today, the Justice Department announced an indictment of two individuals who allegedly turned the profits of scams into cryptocurrency. Then they'd send the crypto overseas, where it could be turned back into cash.

This Committee has been examining digital assets to learn how they work and the risks they create for consumers and the financial system. We've also considered how digital assets can put workers' hard-earned money at risk.

We're here today because crypto also can be used to make it easier to commit crimes—facilitating illicit finance, terrorism, and other forms of criminal activity, and threatening our national security. Bad actors around the world—from hackers, scammers, and drug traffickers, to terrorist groups and pariah regimes—have sought digital assets to facilitate their crimes and intimidation.

In October 2020, under the last Administration, the Justice Department concluded that, "cryptocurrency technology plays a role in many of the most significant criminal and national security threats that the United States faces."

To be sure, criminals have tried to cover their tracks for years with sham accounting and banks that looked the other way. But there's a simple reason that crypto appeals to crime rings and scam artists.

The dollar has safeguards to protect against crime and illicit activity. Companies that deal with real money are required to know their customers, and report suspicious transactions. They need to keep records.

And even when crypto companies are covered by the law, too many don't play by the same rules—especially offshore crypto operators that aren't subject to U.S. law.

Shady crypto companies that fail to adequately monitor activity on their platforms all but give criminals a green light.

Digital assets make it easier to move money under pseudonyms. They make it easier for money launderers to use webs of transactions across the globe to cover their tracks. And that makes it harder for law enforcement to trace illicit funds.

And, the Financial Crimes Enforcement Network—FinCEN, the Treasury bureau charged with safeguarding our financial system from abuse—warned last week that Russian actors could even use crypto to get around sanctions.

So sophisticated bad actors can use digital assets in ways that, if they were using dollars, would likely raise red flags and get them stopped in their tracks.

Last year, FinCEN fined a crypto exchange $100 million. For 6 years, the only identification the company bothered to get from customers was an email address. That no-questions-asked approach enabled more than $200 million in suspicious transactions.

But the problem isn't only shoddy compliance. It's more fundamental.

We hear all the time about how "innovative" cryptocurrency is. But criminals innovate, too. Crypto allows money launderers and terrorists to do things they never could have done with dollars. There's a whole new vocabulary to explain cryptocurrency illicit activity.

Take what's known as "chain hopping." That's when someone launders money by changing funds from one cryptocurrency ecosystem to another, to make it harder to track.

Or look at so-called "rug pulls." That's when you set up a sham digital asset project online, raise as much money as you can, scamming investors, and then run off with all the cash.

Then there's Hydra, the world's largest "darknet." It's an online black market for drugs, stolen credit card numbers, and cyberattack services, all enabled by crypto.

Our laws and law enforcement agencies need to keep pace with bad actors that will exploit every opportunity.

And so far, with lax rules and little oversight, we've given them plenty of those opportunities.

Crypto lets money launderers, hackers, and rogue regimes invent new ways to hide and move money in the dark. It lets hackers and scammers create new ways to steal or defraud. And if we allow them get out ahead of us, our safety and security will be at risk.

Law enforcement is doing what it can. They use techniques to stop cybercrime that didn't exist 30 years ago. Financial regulators leverage new data and resources to expose fraud and manipulation in our markets.

Crypto technology also embeds information that allows law enforcement and national security officials to track and trace where it's been—though not necessarily who owns it. That's where the tough new money laundering and beneficial ownership law we enacted last year will help.

But as these problems continue to grow, we can't sit on the sidelines. We need to take a clear-eyed look at how these assets can endanger consumers and our security.

Last month the FBI announced the creation of a new unit dedicated to tracking down illicit crypto. The Justice Department is dedicating more resources and staff to cracking down on crime using digital assets.

We need to take a whole-of-Government approach to the problem, if we're going to keep up with crypto in illicit finance.

President Biden understands that. His Executive order on crypto assets last week will drive progress on this issue. It will jumpstart a coordinated strategy from law enforcement and regulators to fight bad actors who want to use crypto.

Ultimately, we can't just sit back and watch cybercriminals, rogue regimes, terrorists, and others create a shadow financial system that works for them.

The financial system should work for American families and small businesses. Everything we do on this Committee has that goal in mind. That means that we cannot let abuses of digital assets endanger our financial and national security.

As crypto technology evolves, this Committee must continue to work together to craft a way forward on these crypto policy issues. The stakes are high, and the American people are counting on us.

PREPARED STATEMENT OF SENATOR PATRICK J. TOOMEY

Thank you, Mr. Chairman.

This hearing is about digital assets and illicit finance. While it is appropriate to discuss and understand this topic, we also need to work to ensure regulatory clarity for digital assets.

Digital assets, including cryptocurrencies and their underlying distributed ledger technology, have tremendous potential benefits. As the White House itself recently stated, the U.S. must maintain its leadership in this space, which is why lawmakers and regulators should do nothing to harm America's longstanding tradition of fostering technological innovation.

Unfortunately, I am concerned that the lack of regulatory clarity here at home is undermining that tradition and driving innovation abroad. We need Congress to work together to enact a regulatory framework specific to digital assets that provides this much-needed clarity.

While today's topic is illicit finance, the real backdrop for this hearing is Russia's invasion of Ukraine. By starting the largest land war in Europe since World War II, Russia has unleashed the greatest threat to global security in recent memory.

The sanctions imposed thus far by the Biden administration are harmful to the Russian economy, but not crippling. The President has said "all options are on the table" in terms of sanctions. So what are we waiting for?

Sanctions have purposefully allowed Russia to continue exporting oil and gas, funding Putin's war machine with what could be as much as $5 to $7 billion each week. Cutting off this revenue stream and getting more lethal aid to Ukraine are the two things we could do to maximize the chances that Ukraine wins this war, and Putin comes to understand this war was a calamitous blunder.

To cut off Putin's oil and gas sales globally, the Administration and Congress should impose secondary sanctions on Russia's entire financial sector. This would force the world to choose between doing business with Russia or the United States. I urge the Administration to impose these sanctions and give Ukraine a fighting chance to win this war.

I am concerned that part of today's hearing will be spent disparaging cryptocurrencies, trying to draw some connection between them and Russian sanctions evasion.

There is no sanctions regime that is completely water tight. So it's quite possible that an oligarch somewhere may be using a variety of tools, including crypto, to try to hide some assets.

But according to Administration officials across multiple agencies, there is simply no evidence of cryptocurrencies being used by Russia to evade sanctions in any significant way.

Just this month, FBI Director Christopher Wray told the Senate Intelligence Committee that "the Russians' ability to circumvent the sanctions with cryptocurrency is probably highly overestimated." Acting FinCEN Director Him Das said that "we have not seen widespread evasion of our sanctions using methods such as cryptocurrency." And the director of cybersecurity for the National Security Council said that "the scale that Russia would need to successfully circumvent all U.S. and partners' financial sanctions would almost certainly render cryptocurrency as an ineffective primary tool for the State."

The facts are clear and as the Administration has found: Russia cannot meaningfully use cryptocurrencies to evade sanctions.

While there has been virtually no evidence of Russia meaningfully using cryptocurrencies to evade sanctions, Ukraine has been actively utilizing cryptocurrencies to do tremendous good. Cryptocurrency donations for Ukraine have reached approximately $100 million, which has helped Ukrainians defend their country against Russia's invasion.

These funds have gone towards more than 5,500 bulletproof vests, 500 helmets, and 410,000 meals, among other things. Ukraine's Deputy Minister of Digital Transformation has said that "each and every helmet and vest bought via crypto donations is currently saving Ukrainian soldiers' lives."

We're fortunate to have as a witness today someone deeply affected by the war in Ukraine, and the use of cryptocurrency to help Ukraine and its citizens. Michael Chobanian is the Founder of KUNA Exchange, a local cryptocurrency exchange based in Ukraine. For the past several weeks, Mr. Chobanian has been instrumental in coordinating effforts so individuals all over the world can contribute cryptocurrencies in support of Ukraine's defense.

Crypto's remarkable nature is that anyone across the globe can contribute to this type of effort, almost instantaneously, at very low cost. It is in this context that we should examine cryptocurrencies and their relation to illicit finance.

Throughout history, criminals have always tried to utilize new technologies for nefarious gain. But that is not a reason to stifle new technological developments.

Crypto can be used to empower individuals and promote personal autonomy, but it can also support the detection and prevention of illicit crime. According to Chainalysis, transactions involving illicit addresses account only for 0.15 percent of cryptocurrency transaction volume last year.

This should be no surprise: the traceable nature of many cryptocurrencies is a factor making them terribly risky to utilize for criminal purposes. Just look at the Colonial Pipeline hack, which was one of the most disruptive ransomware attacks on record. The Department of Justice recovered 85 percent of the bitcoins that the pipeline paid in ransom, dealing a significant blow to the hackers.

One of today's witnesses, Michael Mosier, can speak directly about the characteristics of cryptocurrencies that help detect criminal activity. Mr. Mosier is the Former Acting Director for the Financial Crimes Enforcement Network, or FinCEN, at the U.S. Treasury Department. His Government experience makes him uniquely qualified to discuss the topics before us today.

Today I hope the Committee takes a thoughtful and reasonable approach to this topic, acknowledging both the risks cryptocurrencies present, but also their incredible potential. I thank the witnesses for their testimony and participation today, and look forward to the discussion.

PREPARED STATEMENT OF JONATHAN LEVIN

COFOUNDER AND CHIEF STRATEGY OFFICER, CHAINALYSIS, INC.

MARCH 17, 2022

Chainalysis

Written Testimony of Jonathan Levin
Co-Founder and Chief Strategy Officer
Chainalysis Inc.

Before the
Senate Banking Committee

Hearing on
Understanding the Role of Digital Assets in Illicit Finance

Thursday, March 17, 2022

Chairman Brown, Ranking Member Toomey, and distinguished members of the Committee. Thank you for inviting me to testify before you today on this very important topic.

My name is Jonathan Levin and I co-founded Chainalysis Inc. in 2014 with Michael Gronager, CEO of Chainalysis. I currently serve as Chief Strategy Officer.

My family fled the pogroms of Eastern Europe and Lithuania to look for a better life in the West. They took nothing with them. We have a similar situation at present today in Ukraine where many people are crossing borders having left loved ones and possessions behind. We are connected to them through our commitment to humanity and democracy. This global community, organized on the internet, to provide support, humanitarian aid and assistance requires new ways to represent, store and transfer value. The pace of finance will always lag but ultimately catches up with the pace of information.

It is this ability for global communities to come together in this way that sparked my interest in digital assets 10 years ago. Bitcoin for me asked the best questions about the potential for global communities to coalesce around new systems of value and complement our existing financial infrastructure. It was clear that the existing financial infrastructure would not cover all of the ways that our children would want to organize, having grown up on the internet. Bitcoin is an example of a community that has evolved from no people knowing or caring about it 10 years ago to a more than 100 million strong community in its own right–and one that has spurred the innovation of many more digital asset communities around music, art, decentralized finance and even electric vehicles. These communities have now turned into economies that will continue to proliferate and impact many parts of the globe and the economy.

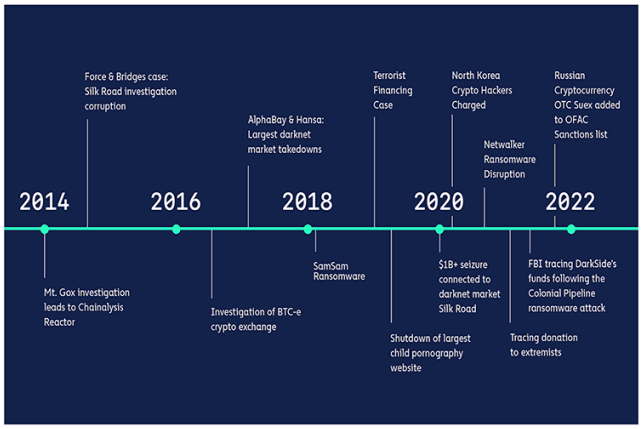
The Committee has selected excellent time to hold this hearing : a week after President Biden's Executive Order launched a whole-of-government approach to digital asset policy and just under a month after Russian troops invaded Ukraine triggering broad sanctions by the US and its allies that includes digital assets, provide the immediate context for today's important discussion. We applaud the members of the Banking Committee to taking a constructive approach to engaging with this technology. Digital asset markets now have a market capitalization of just under $2 trillion. Moreover, according to a recent Harris poll an estimated 28% of Americans trade digital assets, in addition to 12% who have traded them in the past.

Chainalysis is the blockchain data platform. We provide data, software, services, and research to government agencies, exchanges, financial institutions, and insurance and

Chainalysis

cybersecurity companies. Chainalysis currently has over 660 customers in 65 countries. We currently have over 600 employees globally, 361 of whom are in the United States, across 27 states and the District of Columbia. Like many other digital asset-sector companies, we are growing rapidly and expect to hire over 300 additional employees in the US over the next year.

Our data platform powers investigation, 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 digital assets safely. We have worked closely with law enforcement and regulators as they have worked to disrupt and deter illicit uses of digital assets. Below is a list of cases where we are able to publicly disclose our involvement:



Chainalysis' 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 digital asset ecosystem, enabling the realization of the technology's potential.

In my testimony and its appendices, I outline the many ways that digital assets can be exploited by illicit actors. Just as with any new technology, criminals have found ways to exploit digital assets. I want to be clear, though – and Chainalysis does a great deal of research on this front – that these transactions are the exception to the rule. Our 2022 Crypto Crime Report was released last month and it shows that transactions involving illicit addresses represented just 0.15% ($14 billion) of digital assets transaction volume in 2021 (not including centralized exchange volumes). This is because digital asset usage is growing faster than ever before and the legitimate use of digital assets is vastly outpacing the growth in their criminal use. This figure may rise slightly as we identify more addresses associated with illicit activity and incorporate their transaction activity

into our historical volumes, and it also only reflects on-chain activity. This means, for example, that illicit activity happening within exchanges is not captured, as we do not have the internal order book data of exchanges. Those caveats aside, I do think it is important to note that illicit activities using digital assets is reflective of significantly less than 1% of transaction volumes, and this is thanks in part to the types of tools we provide to digital asset companies to support their AML/CFT compliance and the excellent work of law enforcement and regulators.

If there is one point we want to make to the Members of the Banking Committee, it is that the transparency of blockchains enhances the ability of policymakers and law enforcement to detect, disrupt and, ultimately, deter illicit activity. When it comes to detecting and disrupting illicit activity, by mapping a single illicit actor to a wallet address, e.g., a ransomware attacker or sanctions evader, 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, expensive 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.

It is through this transparency that law enforcement, leveraging Chainalysis tools, was able to trace the Colonial Pipeline ransomware attackers (see case study below) and ultimately recover many of the funds sent to the attackers. It is also through this transparency that Chainalysis is able to produce a comprehensive global survey of illicit activity involving digital assets through our annual Crypto Crime Report ("Crime Report"). Key findings from the 2022 Crime Report published last month are highlighted below.

Moreover, a financial system built on blockchain rails can enhance the effectiveness of financial regulation more broadly. Policymakers should consider not just integrating digital assets into existing regulatory structures but leveraging their capabilities to improve oversight to reduce systemic risk and to protect consumers, among other traditional financial regulatory goals. With a blockchain-based financial system, regulators could have a real-time view into financial flows, risk exposures, and interconnectedness across all asset classes. Advanced risk analytics could provide regulators the ability to easily independently stress test the entire portfolio of a financial institution, as well as an entire financial system using current or historic portfolio data. Enhanced transparency afforded by blockchain technology could also facilitate and improve the efficacy of regulator and independent examinations, including as they relate to disclosure and reporting.

My testimony today will cover these topics:

- How blockchain data and analysis benefits investigations into illicit activity involving digital assets
- An overview of illicit activity involving digital assets from our Crime Report
- The risk of the use of digital assets by Russian specially designated nationals and blocked persons ("SDNs") to evade US sanctions
- Chainalysis' recommendations for how Congress and regulators can act to better detect, disrupt, and deter illicit uses of digital assets, including sanctions evasion

In **Appendix A,** we provide a summary of the 2022 Crime Report and in **Appendix B,** analysis relating to self-custodied "unhosted" wallets, putting their potential use by illicit actors in appropriate context. In **Appendix C,** we included a glossary of digital asset service types, including legal entities like retail exchanges or illicit activities like darknet markets, ransomware, or scamming.

Before I launch into these topics, I want to highlight Chainalysis' announcement last week of free tools for digital asset businesses, including decentralized web3 organizations like decentralized exchanges ("DEXes"), decentralized finance ("DeFi") platforms, distributed autonomous organizations ("DAOs") to help them comply with sanctions requirements. These tools – an API and an on-chain oracle – will provide any digital asset business, protocol, organization, or developer a programmatic way to quickly check whether or not an address is on the sanctions list before allowing it to connect with their service.

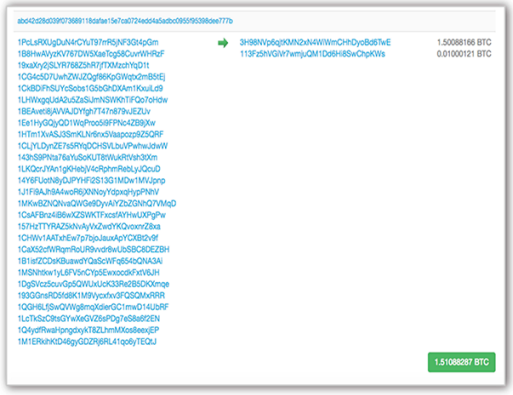
We are excited about the potential of DeFi to democratize finance by putting asset owners of any size on equal footing with traditional market makers to earn returns based on contributing liquidity. Our tools help DeFi users remain compliant with sanctions requirements and therefore help unlock the potential of DeFi.

How blockchain data and analysis benefits investigations into illicit activity involving digital assets

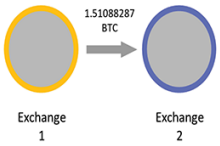
It is a common misconception that digital assets are completely anonymous and untraceable. In fact, the transparency provided by many digital assets' public ledgers is much greater than other traditional forms of value transfer. Digital assets are assets that are issued and transferred using distributed ledger or blockchain technology, including, but not limited to, cryptocommodities, cryptocurrencies, non-fungible tokens ("NFTs"), securities tokens, stablecoins, etc. To understand the role of illicit activity in the digital markets, we need to set the stage by highlighting a foundational feature of blockchains: their transparency.

Each transaction on the blockchain is transparent and recorded in real-time on an immutable transaction ledger. Holdings of digital assets are visible as wallet balances which are also transparent and recorded on an immutable ledger. While the blockchain ledger publicly shows a string of random numbers and letters that transact with another string of random numbers and letters, the use of tools like Chainalysis enables these records to be transformed into an audit trail for monitoring current activity as well as historic activity by tying wallet addresses to real-world identities. Below shows what

you might directly observe on a blockchain:



Chainalysis can translate the digital asset wallet addresses into real identities, i.e. a 1.51088287 transfer of Bitcoin from Exchange 1 to Exchange 2:



Chainalysis' core database maps these random characters on a blockchain – digital asset addresses– to real-world services and activities. This is how the blockchain can be used as an audit trail for monitoring current activity as well as historic activity. It should be noted that the extent of this audit trail is limited to identified wallets and digital assets held by custodians on behalf of their beneficial owners, which, most importantly includes digital asset exchanges and increasingly, banks and other fiduciaries. Because the blockchain is permanent and immutable, investigators or consumers are able to see transactions in real-time or access them years later with confidence the records have not been altered. The same is not always the case with traditional fiat investigations and other asset types.

In part due to the ability to leverage the transparency of digital assets and blockchain analytics, law enforcement has been able to disrupt terrorist financing campaigns, dismantle child sexual abuse material websites, and seize the ill-gotten proceeds of darknet marketplace administrators and the Colonial Pipeline ransomware attackers.

Blockchain analysis tools like ours are also used by financial institutions and digital asset exchanges to ensure they are meeting their anti-money laundering requirements. These tools can detect and alert users to patterns of potential high-risk activity among their customers. Using these tools, businesses can identify whether their customers are

attempting to transact with US Treasury Office of Foreign Assets Control ("OFAC") sanctioned individuals, entities, or jurisdictions, or cashing out funds generated from darknet markets, scams, fraud, and other forms of illicit activity.

Blockchain and investigative analyses can be used to determine ownership or control of additional addresses associated with sanctioned individuals or entities based on information OFAC has provided publicly. For example, if OFAC lists a digital asset address as an identifier associated with a particular individual, using blockchain analytics, we can identify other wallet addresses likely controlled by the same individual and label them so that our customers also identify them as belonging to the sanctioned individual. Likewise, additional assets such as tokens or forks of blockchains, associated with the addresses and entities identified by OFAC can be determined through blockchain analytics.

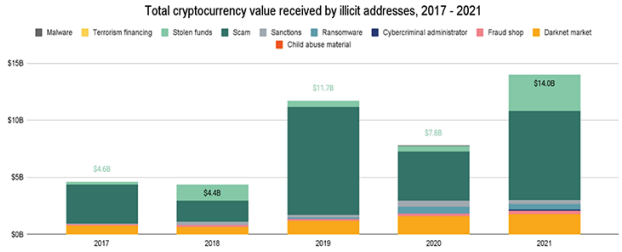
When OFAC lists digital asset addresses as identifiers associated with sanctioned entities, they are quickly labeled in our tools as sanctions-related and our customers receive alerts on historical or future exposure to these addresses. This means our technology enables digital asset exchanges and financial institutions to ensure that their customers are not interacting with addresses associated with sanctioned persons and identify and freeze any accounts that attempt to do so.

Blockchain analytics can also be used to identify trends and develop intelligence about who may be facilitating the evasion of sanctions or money laundering or other illicit activity. Using tools like the ones that Chainalysis develops, it's possible to map out illicit activity networks and patterns, something that would not be easily paralleled in traditional finance investigations. For example, by tracking their payments, our customers can identify virtual private network ("VPN") services, bulletproof web hosting services, and other providers sanctioned or malicious actors are using. All of this information is valuable intelligence that can allow investigators to determine new trends and patterns in sanctions evasion [and illicit finance] so that they can combat them.

Because of their inherent transparency and traceability, there are many advantages to digital assets when it comes to investigating sanctions evasion and illicit activity. Traditionally, bad actors have attempted to use misspellings, code words, and other techniques to evade sophisticated sanctions screening and anti-money laundering countermeasures. But with digital assets, the unforgeable addresses represent unavoidable, definitive evidence on a transparent record. Additionally, unlike some forensic evidence that degrades over time, blockchain evidence is permanent and immutable. What's more, our ability to analyze this evidence is only getting more sophisticated. Criminals who thought they evaded detection in months and years past often find they've left a permanent audit trail for law enforcement to follow.

An overview of illicit activity involving digital assets from our Crime Report

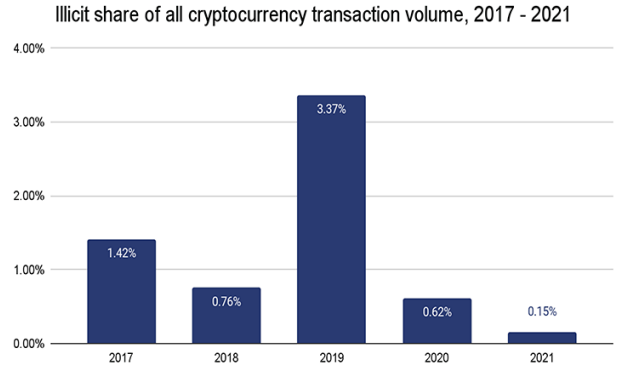
Digital asset-based crime hit a new all-time high in 2021, with illicit addresses receiving $14 billion over the course of the year, up from $7.8 billion in 2020. It is very important to note that these and below estimates of illicit activity are likely to rise as Chainalysis identifies more addresses associated with illicit activity and incorporates their transaction activity into our historical volumes. For instance, we found in our last Crypto Crime Report that 0.34% of 2020's digital asset transaction volume was associated with illicit activity — we can now revise that figure to 0.62%.



Note: "Cybercriminal administrator" refers to addresses that have been attributed to individuals connected to a cybercriminal organization, such as a Darknet market.

But those numbers don't tell the full story. Digital asset usage is growing faster than ever before. Across all digital assets tracked by Chainalysis, total transaction volume grew to $15.8 trillion in 2021, up 567% from 2020's totals. Given that roaring adoption, it's no surprise that more cybercriminals are using digital assets. But the fact that the increase was just 79% — nearly an order of magnitude lower than overall adoption — might be the biggest surprise of all.

In fact, with the growth of legitimate digital asset usage far outpacing the growth of criminal usage, illicit activity's share of digital asset transaction volume has never been lower.



Transactions involving illicit addresses represented just 0.15% of digital asset transaction volume in 2021 despite the raw value of illicit transaction volume reaching its highest level ever. The yearly trends suggest that with the exception of 2019 — an extreme

outlier year for digital asset-based crime largely due to the PlusToken Ponzi scheme — crime is becoming a smaller and smaller part of the digital asset ecosystem.

The 0.15% of illicit transaction volume should be considered alongside illicit actors' digital asset holdings. It is impossible to know for sure, but we can estimate total illicit actor holdings based on the current holdings of addresses Chainalysis has identified as associated with illicit activity. As of early 2022, addresses believed to be associated with illicit actors held at least $10 billion worth of digital assets, with the vast majority of this held by wallets associated with digital asset theft. $10 billion is approximately 0.55% of the total digital asset market capitalization, which as of March 10, 2022, stood at $1.8 trillion.

We also need to note that these numbers only account for funds derived from "digital asset-native" crime, meaning cybercriminal activity such as darknet market sales or ransomware attacks in which profits are virtually always derived in digital assets rather than fiat currency. It's more difficult to measure how much fiat currency derived from offline crime — traditional drug trafficking, for example — is converted into digital assets to be laundered.

To put the 0.15% illicit activity volume number or 0.55% illicit actor digital asset holdings of total digital asset market capitalization in context, we note that the United Nations in 2020 estimated that money laundering activity accounted for $1.6 trillion per year or 2.7% of global GDP. According to one study, overall criminal activity imposes costs of about 3% of US GDP on the economy while another study published by an economist at the U.S. Bureau of Economic Analysis found that in 2017 crime in the US accounted for about 1.12% of US GDP.

Law enforcement investment in detection and disruption in the digital assets markets are, in my opinion, more likely to yield relatively better results per dollar invested than similar interventions in the broader economy. Compared to the non-digital asset economy, meaning anti-money laundering countermeasures (including ex ante measures like transaction monitoring controls or ex post measures like enforcement action and asset seizure) are generally more effective because a few key successes by law enforcement can disrupt a sizeable proportion of digital asset-related illicit activity, whereas an equivalent intervention in the non-digital asset economy is likely to yield less in terms of relative impact on reducing crime.

One promising development in the fight against digital asset-related crime is the growing ability of law enforcement to seize illicitly obtained digital assets. In November 2021, for instance, IRS Criminal Investigation announced that it had seized over $3.5 billion worth of digital assets in 2021 — all from non-tax investigations — representing 93% of all funds seized by the division during that time period or about 25% of illicit activity Chainalysis has identified to-date for 2021 (although the illicit activity underlying these seizures didn't necessarily occur in 2021). We've also seen several examples of successful seizures by other agencies, including $56 million seized by the Department of Justice in a digital asset scam investigation, $2.3 million seized from the ransomware group behind the Colonial Pipeline attack, and an undisclosed amount seized by Israel's National Bureau for Counter Terror Financing in a case related to terrorism financing.

For additional details of the different types of crimes that we see exploit the use of digital assets, please see the Appendix, where I outline the trends we see related to scamming,

theft, malware, ransomware, terrorist financing, illicit activity with suspected links to North Korea, and illicit activity with suspected links to Iran, as well as present a case study of the Colonial Pipeline case.

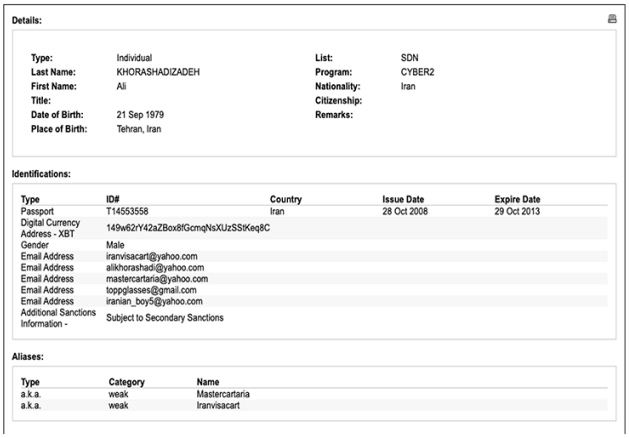
The risk of the use of digital assets by specially designated nationals and SDNs to evade US sanctions

Background regarding digital assets and sanctions

Since November 2018, OFAC has included 180 digital currency addresses in eight different designations. This has included designations against Chinese nationals for narcotics trafficking and money laundering, associates of the Democratic People's Republic of Korea ("DPRK") Lazarus Group, Russian nationals for their involvement in disinformation campaigns, and Russian cyber actors involved in digital asset exchange hacks. In April 2021, the Biden Administration announced several new sanctions against Russian intelligence service disinformation outlets and designated a Pakistani organization that provided cyber actors, including Russian disinformation actors, fraudulent identity documents used in the digital onboarding process at financial institutions.

On the SDN List, OFAC lists "Digital Currency Address" under sanctioned entities or individuals as identifiers as shown in the example below.

Example of OFAC "Digital Currency Address" Listing



Details:

Type:	Individual	**List:**	SDN
Last Name:	KHORASHADIZADEH	**Program:**	CYBER2
First Name:	Ali	**Nationality:**	Iran
Title:		**Citizenship:**	
Date of Birth:	21 Sep 1979	**Remarks:**	
Place of Birth:	Tehran, Iran		

Identifications:

Type	ID#	Country	Issue Date	Expire Date
Passport	T14553558	Iran	28 Oct 2008	29 Oct 2013
Digital Currency Address - XBT	149w62rY42aZBox8fGcmqNsXUzSSfKeq8C			
Gender	Male			
Email Address	iranvisacart@yahoo.com			
Email Address	alikhorashadi@yahoo.com			
Email Address	mastercartaria@yahoo.com			
Email Address	topgglasses@gmail.com			
Email Address	iranian_boy5@yahoo.com			
Additional Sanctions Information -	Subject to Secondary Sanctions			

Aliases:

Type	Category	Name
a.k.a.	weak	Mastercartaria
a.k.a.	weak	Iranvisacart

OFAC has issued an "Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments" (in October 2020), as well as a brochure on Sanctions Compliance Guidance for the Virtual Currency Industry" (in October 2021). OFAC's advisory bolstered previous government guidance not to pay ransomware attackers, who typically demand ransom be paid in digital assets, as this incentivizes future attacks, and goes a step further in warning that ransomware victims and intermediaries and consultants who facilitate

such payments could face heavy penalties associated with sanctions violations. It also noted that license applications made to OFAC that involve ransomware payments would be presumptively denied. The brochure outlined sanctions-related compliance requirements for digital asset businesses, consequences for non-compliance and examples of how timely reporting can mitigate those consequences, and best practices for building a risk-based compliance program.

On March 11, 2022 the White House announced that through new guidance, the Department of Treasury will continue to make clear that Treasury's expansive actions against Russia require all U.S. persons to comply with sanctions regulations regardless of whether a transaction is denominated in traditional fiat currency or virtual currency.

Under 2013 guidance from FinCEN, digital asset exchanges must register as money services businesses ("MSBs"). They therefore must meet certain anti-money laundering/countering the financing of terrorism (AML/CFT) requirements under the Bank Secrecy Act, including (i) establishing AML programs, (ii) adhering to certain regulatory reporting requirements, and (iii) maintaining certain books and records. This includes complying with sanctions regulations. This has led US-based digital asset exchanges to establish KYC programs to verify the identity of their customers and use transaction monitoring solutions to detect suspicious activity, making it more difficult for illicit actors or those trying to evade sanctions to cash out their ill-gotten digital assets for fiat currency.

Current Chainalysis assessment of Russian sanctions evasion risk using digital assets

Our current assessment is that Russian SDNs are more likely to channel a greater portion of funds through traditional money laundering means, e.g., the "Russian laundromat" scheme, or through the use of alternative currencies and payment networks than through digital assets. Digital asset markets are a less useful tool for the sanctions evader relative to traditional financial systems for the following reasons:

- **High likelihood of detection:** Illicit activity, including sanctions evasion, is relatively easy to detect and monitor because of the immutable and transparent nature of blockchains. The ability to detect illicit activity is enhanced further through the use of blockchain analysis tools like those Chainalysis develops. In contrast, traditional financial networks require reconciliation, often conducted manually, of different ledgers of record across different institutions in different jurisdictions with different regulators, e.g., bank account or transfer records, customs records, etc. Moreover, investigation of financial activity through bank or payment records is generally historical while investigation of blockchain activity can be conducted in real-time.

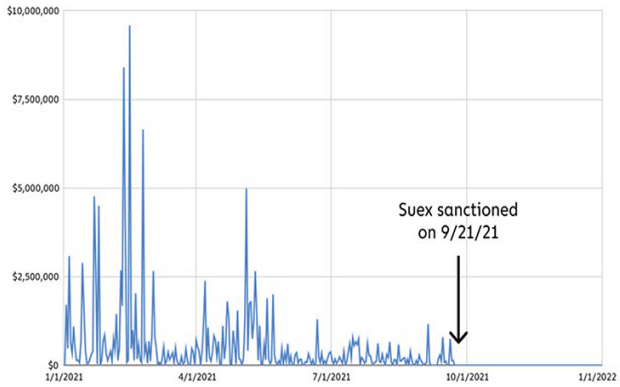
- **High likelihood of seizure:** Because digital asset payment flows are easier to trace with limited reliance on process to obtain records, e.g., subpoenas, and can be monitored in real-time, this makes them more likely to be seized before illicit actors can move them off of a blockchain. See discussion above regarding the Colonial Pipeline ransomware fund seizure or the seizure of funds with connections to the Silk Road darknet market.

- **Countermeasures are particularly effective:** On September 21, 2021, OFAC announced sanctions against SUEX, a digital asset exchange that facilitated

transactions involving illicit proceeds from at least eight ransomware variants. According to OFAC, over 40% of SUEX's known transaction history was associated with illicit actors.

After SUEX's designation, inbound transfers of digital assets into SUEX dropped to effectively zero.

Suex daily cryptocurrency value received, 2021



Compliant digital asset market participants have proven effective at stopping the flow of funds to SDNs with digital asset wallet addresses. Sanctions are particularly effective in disrupting financial intermediaries in a digital asset network because once such an intermediary is designated, funds associated with it can be broadly flagged to compliant participants in the network as very high risk not just to immediate counterparties, but counterparties downstream. For example, if SUEX transfers funds to Wallet A and Wallet A transfers to Wallet B and Wallet B to Exchange X in order for Wallet B to cash-out, using a tool like Chainalysis, Exchange X will be able to trace the source of funds to SUEX, an SDN, and therefore block the transfer. Sanctions are therefore very effective at disrupting liquidity flowing through digital asset SDN intermediaries.

In contrast, source of funds would be more easily obscured in the traditional financial system. For example, if a bank intermediary is sanctioned (Bank A) and it transfers funds to Company B (which could be a shell company) who transfers to Company C who then transfers to Bank X, Bank X is less likely to trace source of funds through to Bank A and therefore facilitate Bank A's sanctions evasion, reducing the efficacy of sanctions as a foreign policy tool. At minimum, it would be slower and more costly for Bank X to determine source of funds for Company C in a traditional financial system relative to an equivalent financial intermediary in a blockchain system.

While the disruption of funds to wallet addresses included on sanctions lists is effective at disruption reception and transmission of funds for SDN digital asset intermediaries, traditional bank SDNs generally continue receiving and transmitting funds. One can

therefore imagine that in a blockchain-based financial system, sanctions could be a more effective, less leaky, foreign policy tool for protecting US national security versus the current system.

Chainalysis' recommendations for how Congress and regulators can act to better detect, disrupt, and deter illicit uses of digital assets, including sanctions evasion

Below we provide some short-term recommendations aimed specifically at reducing the risk of sanctions evasion via digital assets and longer-term recommendations aimed at improving detection, disruption and deterrence of broader illicit uses of digital assets.

Short-term recommendations

- **Include digital asset wallets in designations when available.** Sanctions authorities should continue to work together and in cooperation with regulated institutions, as well as blockchain intelligence companies like Chainalysis, to identify links between SDNs and digital asset wallet addresses. As described above, the inclusion of wallet addresses as identifiers has been very effective at shutting off flows related to those wallets because compliance teams are readily able to screen for these addresses and freeze funds.

- **Consider designating specific services that facilitate sanctions evasion.** In the event that digital asset services such as exchanges and mixers are facilitating an unacceptable amount of sanctions evasion (something that could be transparently and quickly determined using blockchain intelligence as described above), OFAC may consider sanctioning the entities that facilitate sanctions evasion, just as they did with the designations of SUEX and Chatex.

- **Expand information sharing.** Information sharing is fundamental to the US government's ability to respond to the risks of illicit cyber activity to operate with better awareness of the threat landscape and should be expanded wherever possible.

Long-term recommendations

- **Congressional appropriations that fund blockchain intelligence capabilities.** We commend the Consolidated Appropriations Act for FY 2022 for increasing funding for FinCEN and the Office of Terrorism and Financial Intelligence ("TFI") in the Department of Treasury. We recommend that FinCEN and TFI, along with law enforcement, market regulators, and national security agency stakeholders, invest in blockchain intelligence and analytics capabilities, both headcount and tools/services, that will enhance their ability to detect, disrupt, and deter illicit uses of digital assets.

- **In addition to blockchain intelligence technology, Congress should ensure adequate funding, resources, and training for government agencies charged with investigating the illicit use of digital assets, including sanctions evasion**. Many government agencies have limited or inconsistent personnel dedicated to investigating the illicit use of digital assets because of a lack of training resources and a lack of funding for new personnel, tools, and training. Ensuring that these efforts are well-funded would ensure that when digital assets are exploited by

criminals, investigators can trace these illicit transactions, seize funds, and bring criminals to justice.

- **Improve and promote interagency coordination through the creation of a Virtual Asset Coordination Center.** A coordination center would allow USG agencies to leverage existing capabilities across agencies, reduce duplication of efforts, and ensure that agencies are learning from each other, engaging in best practices, and sharing information through a shared real-time view on the illicit use of digital assets.

- **Provide market regulators with clear oversight authority over financial digital assets.** We recommend that jurisdictional authorities over financial (e.g., commodities and securities) digital assets be clearly allocated among the current leading market regulators, i.e. the Commodity Futures Trading Commission ("CFTC") and Securities and Exchange Commission ("SEC"), to provide the digital asset industry with legal clarity and statutory directives that provide these agencies with guidance and powers to police financial digital assets markets in a manner that reflects the unique risks and opportunities of the technology, e.g., as it relates to promoting investor protection, cybersecurity, market surveillance, and conflicts of interest, among other things. National security will be furthered by empowering the front-line market regulators to have a clear regulatory perimeter, reinforcing the capabilities of the broader government, including law enforcement.

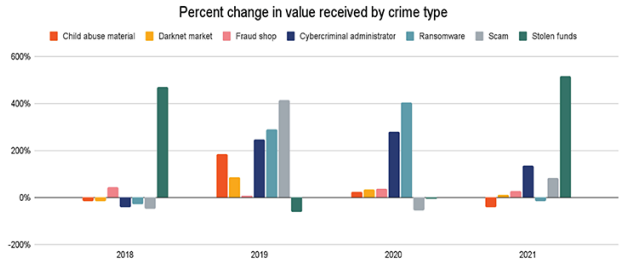
The opportunity for policymakers, including this Committee, is to ensure that they understand and are balancing the benefits of this technology with the commitment to public and investor protection, as well as our need to retain the United States' dominance when it comes to providing the financial rails that everyone transacts with in a manner that not only protects our national security but enhances it. I look forward to working with you all in the future as you consider policies and legislation in this space.

Chainalysis

APPENDIX A
Overview of 2022 Crime Report

In this Appendix, we will look at different categories of crime that exploit digital assets. More specifically, below we describe data relating to the extent of (1) scamming, (2) theft, (3) ransomware, (4) a case study of the Colonial Pipeline ransomware case, illicit activity with suspected links to (5) North Korea, (6) Iran, and (7) Russia, (8) terrorist financing, and (9) malware.

Based on our data, we can break down types of digital asset-based crime by transaction volume and analyze trends over time. Two categories stand out for their growth: stolen funds and, to a lesser degree, scams. DeFi is a big part of the story for both.



1. Scamming

Scamming revenue rose 82% in 2021 to $7.8 billion worth of digital assets stolen from victims. Over $2.8 billion of this total — which is nearly equal to the increase over 2020's total — came from rug pulls, a relatively new scam type in which developers build what appear to be legitimate digital asset projects before taking investors' money and disappearing. Please keep in mind as well that these figures for rug pull losses represent only the value of investors' funds that were stolen, and not losses from the DeFi tokens' subsequent loss of value following a rugpull.

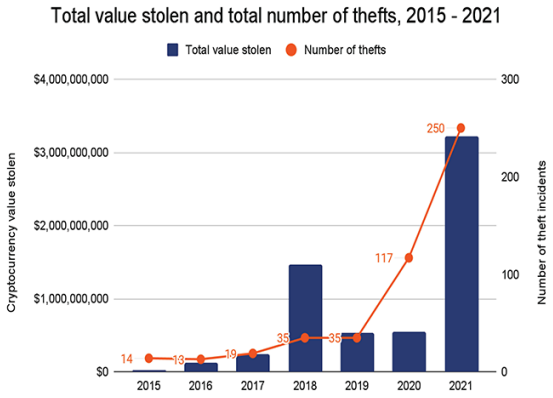
We should note that roughly 90% of the total value lost to rug pulls in 2021 can be attributed to one fraudulent centralized exchange, Thodex, whose CEO disappeared soon after the exchange halted users' ability to withdraw funds. However, every other rug pull tracked by Chainalysis in 2021 involved DeFi projects. In nearly all of these cases, developers have tricked investors into purchasing tokens associated with a DeFi project before draining the funds provided by those investors, sending the token's value to zero in the process.

We believe rug pulls are common in DeFi for two related reasons. One is the excitement around DeFi. DeFi transaction volume has grown 912% in 2021, and the incredible returns on decentralized tokens like Shiba Inu have many excited to speculate on DeFi tokens. At the same time, it's very easy for those with the right technical skills to create new DeFi tokens and get them listed on exchanges, even without a code audit. A code

audit is a process by which a third-party firm or listing exchange analyzes the code of the smart contract behind a new token or other DeFi project, and publicly confirms that the contract's governance rules are ironclad and contain no mechanisms that would allow for the developers to make off with investors' funds. Many investors could likely have avoided losing funds to rug pulls if they'd stuck to DeFi projects that have undergone a code audit – or if DEXes required code audits before listing tokens.

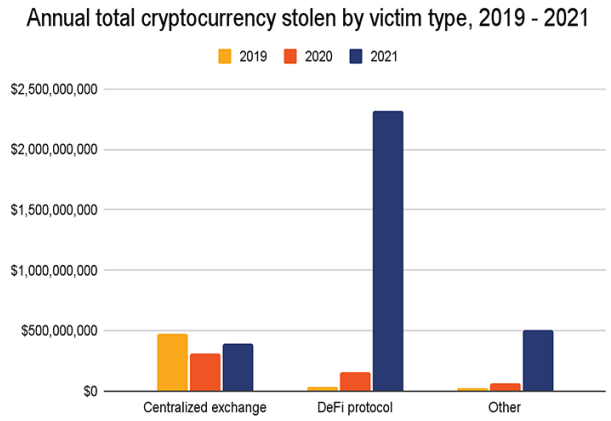
2. **Theft**

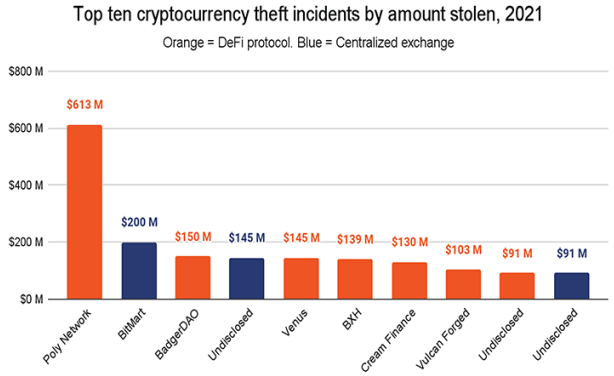
2021 was a big year for digital thieves. Throughout the year, $3.2 billion in digital assets were stolen from individuals and services — almost 6x the amount stolen in 2020.



Digital asset theft grew disproportionately in 2021, with roughly $3.2 billion worth of digital assets stolen in 2021 — a 516% increase compared to 2020. Roughly $2.2 billion of those funds — 72% of the 2021 total — were stolen from DeFi protocols. The increase in DeFi-related thefts represents the acceleration of a trend we identified in last year's Crime Report.

Chainalysis



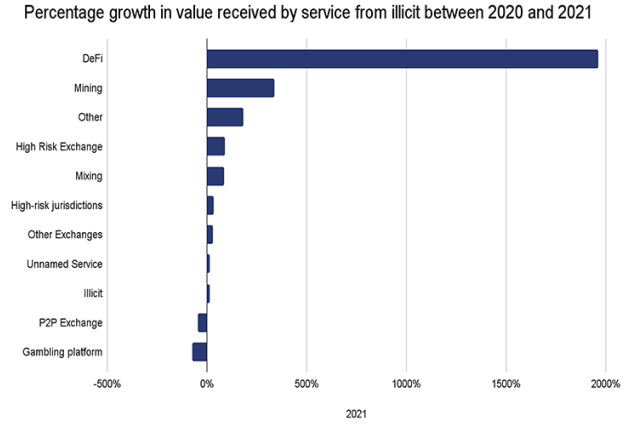


As is the case most years, the ten largest hacks of 2021 accounted for a majority of the funds stolen at $1.81 billion. Seven of these ten attacks targeted DeFi platforms in particular.

In 2020, just under $162 million worth of digital assets was stolen from DeFi platforms, which was 31% of the year's total amount stolen. That alone represented a 335% increase over the total stolen from DeFi platforms in 2019. In 2021, that figure rose

another 1,330%. In other words, as DeFi has continued to grow, so too has its issue with stolen funds. Most instances of theft from DeFi protocols can be traced back to errors in the smart contract code governing those protocols, which hackers exploit to steal funds, similar to the errors that allow rug pulls to occur.

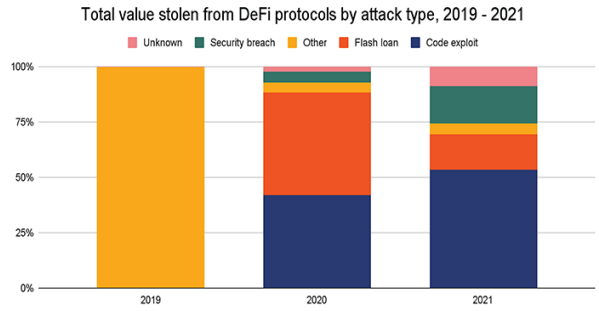
We've also seen significant growth in the usage of DeFi protocols for laundering illicit funds, a practice we saw scattered examples of in 2020 and that became more prevalent in 2021. The graph below looks at the growth in illicit funds received by different types of services in 2021 compared to 2020.



DeFi protocols saw the most growth by far in usage for money laundering at 1,964%.

With the increased prominence of smart contract capabilities that power DeFi platforms, deeper vulnerabilities have begun to emerge around the software underpinning these services. In 2021, code exploits and flash loan attacks—a type of exploit involving price manipulation—accounted for a near-majority of total value stolen across all services at 49.8%. And when examining only hacks on DeFi platforms, that figure increases to 69.3%.

Chainalysis



These exploits occur for a variety of reasons. For one, in keeping with DeFi's faith in decentralization and transparency, open-source development is a staple of DeFi applications. This is an important and broadly positive trend: since DeFi protocols move funds without human intervention, users need to be able to audit the underlying code in order to trust the platform. But this also stands to benefit cybercriminals, who can analyze the scripts for vulnerabilities and plan exploits in advance.

Another potential point of failure is DeFi platforms' reliance on price oracles. Price oracles are tasked with maintaining accurate asset pricing data for all digital assets on a platform, and the job isn't easy. Secure but slow oracles are vulnerable to arbitrage; fast but insecure oracles are vulnerable to price manipulation. The latter type often leads to flash loan attacks, which extracted a massive $364 million from DeFi platforms in 2021. In the hack of Cream Finance, for example, a series of flash loans exploiting a vulnerability in the way Cream calculated yUSD's "pricePerShare" variable enabled attackers to inflate yUSD price to double its true value, sell their shares, and make off with $130 million in just one night.

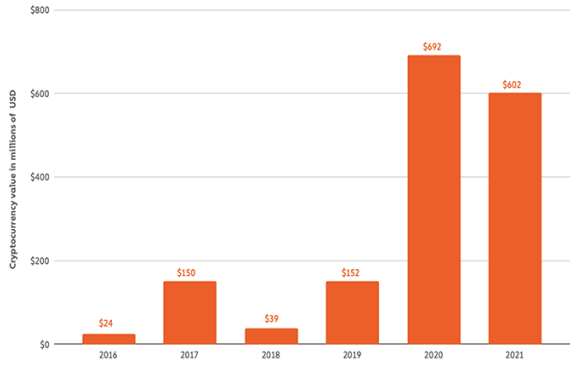
3. Ransomware

Ransomware is a type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files. Usually ransomware attackers gain access to victims' systems through some form of fraud, phishing for passwords in particular, or when a victim unknowingly visits an infected website that then results in malware being downloaded and installed without the user's knowledge.

Ransomware attackers often extort digital assets from their victims in return for access to their systems. These demands for digital assets include the ransomware attacker's wallet address that Chainalysis is then able to track.

Chainalysis

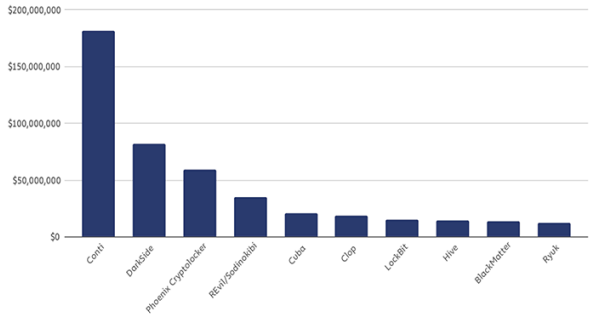
Total cryptocurrency value received by ransomware addresses | 2016–2021



As of March 14, 2022, we've identified just over $699 million worth of ransomware payments in 2021. However, just like last year, we know that this figure will likely increase as we record new ransomware recipient wallet addresses. The data we published in the 2022 Crime Report on February 16 had $602 million in 2021 ransomware payments.

Conti was the biggest ransomware strain by revenue in 2021, extorting at least $200 million from victims.

Top 10 ransomware strains by revenue | 2021

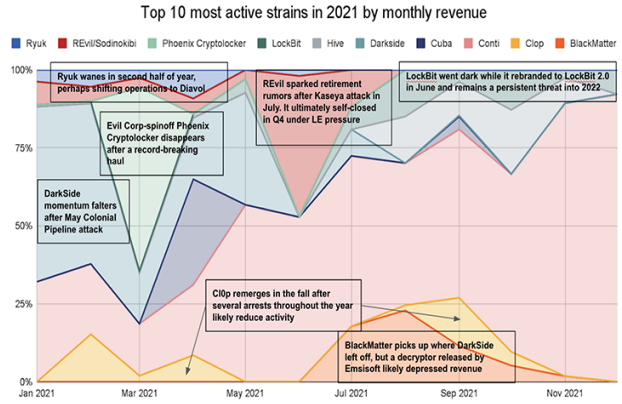


Believed to be based in Russia, Conti operates using the ransomware-as-a-service (RaaS) model, meaning Conti's operators allow affiliates to launch attacks using its ransomware program in exchange for a fee.

DarkSide is also notable, both for ranking second in 2021 in funds extorted from victims that we've been able to identify, and also for its role in the attack on oil pipeline Colonial Pipeline, one of the year's most notable ransomware attacks. The attack caused fuel shortages in some areas, which were exacerbated by subsequent panic buying as word of the attack's impact spread. The Colonial story serves as an important reminder of one reason ransomware attacks are so dangerous: They frequently target critical infrastructure we need to keep the country running — not just energy providers, but food providers, schools, hospitals and financial services companies as well.

However, as I discussed earlier in my testimony, the Colonial Pipeline attack also turned into a success story, as the U.S. Department of Justice was able to track and seize $2.3 million of the ransom that Colonial paid to DarkSide. Law enforcement's growing ability to seize payments after they're made represents a huge step forward in the fight against ransomware. It also serves as one more reason why more victims should report attacks — even if you pay, law enforcement may be able to help you get those funds back.

Overall, 2021 also saw more active individual ransomware strains than any other year.At least 140 ransomware strains received payments from victims at any point in 2021, compared to 119 in 2020, and 79 in 2019. Those numbers are emblematic of the intense growth of ransomware we've seen over the last two years. Most ransomware strains come and go in waves, staying active for a short amount of time before becoming dormant. We show this on the graph below, which shows how the top ten ransomware strains ebbed and flowed in activity throughout the year.

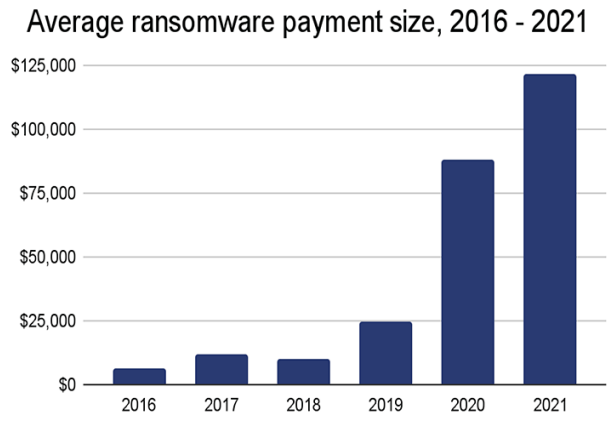


Conti was the one strain that remained consistently active for all of 2021, and in fact saw its share of all ransomware revenue grow throughout the year. Overall though, Conti's staying power is increasingly outside the norm.

The growing number of active strains and generally short lifespan of most strains is also a result of rebranding efforts. More and more in 2021, we saw the operators of strains publicly "shut down" before re-launching under a new name, presenting themselves as a separate cybercriminal group. Often, the rebranded strain's financial footprint on the

blockchain aligns with that of the original, which can tip investigators off as to who's really behind the new strain.

Ransomware payment sizes also continued to grow in 2021, a trend we've observed every year since 2018.



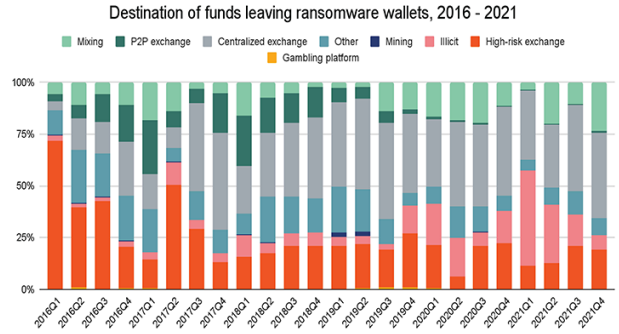
The average ransomware payment size was over $118,000 in 2021, up from $88,000 in 2020 and $25,000 in 2019. Large payments such as the record $40 million received by Phoenix Cryptolocker spurred this all-time high in average payment size. One reason for the increase in ransom sizes is ransomware attackers' focus on carrying out highly-targeted attacks against large organizations. This "big game hunting" strategy is enabled in part by ransomware attackers' usage of tools provided by third-party providers to make their attacks more effective. These tools range from illicit hacking aids to legitimate products, and include:

- Rented infrastructure such as bulletproof web hosting, domain registration services, botnets, proxy services, and email services to carry out attacks.
- Hacking tools like network access to already-infiltrated networks, exploit kits that scan victims' networks for vulnerabilities, and malware programs that help attackers distribute ransomware more effectively.
- Stolen data such as passwords, individuals' personally identifiable information, and compromised remote desktop protocol (RDP) credentials, which help attackers break into victims' computer networks.

Usage of these services by ransomware operators spiked to its highest ever levels in 2021.

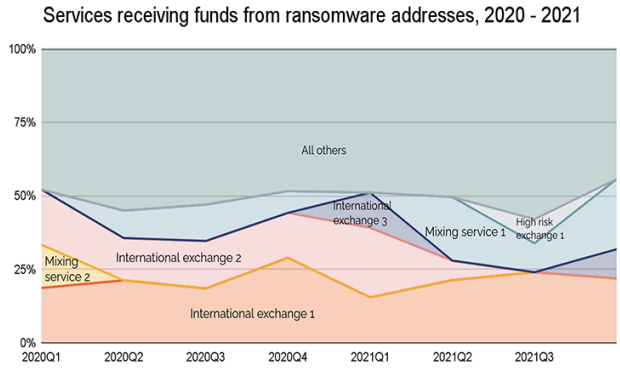
Another important trend to monitor in ransomware is money laundering. The graph below shows where attackers move the digital asset they extort from victims.

Chainalysis



Over the last few years, most ransomware strains have laundered their stolen funds by sending them to centralized exchanges. We also see substantial funds sent to both mixers and addresses associated with other forms of illicit activity.

The money laundering trends get even more interesting if we drill down to the individual services receiving funds from ransomware.



Amazingly, 56% of funds sent from ransomware addresses since 2020 have wound up at one of six digital asset businesses:

- Three large, international exchanges
- One high-risk exchange based in Russia
- Two mixing services

Chainalysis

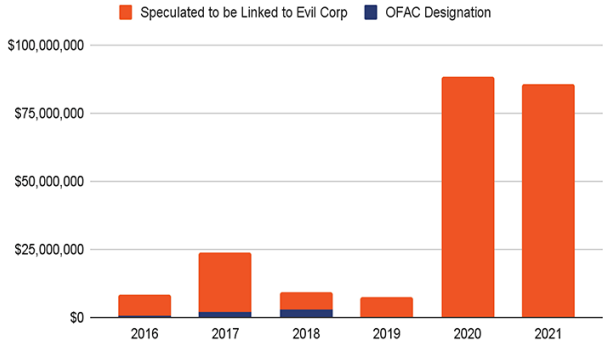
Similar to the rebranding activity we described above, these money laundering trends show how small the ransomware ecosystem really is. That's good news, as it means the strategy for fighting ransomware is likely simpler than it appears at first glance. By cracking down on the small number of services that facilitate this money laundering activity, law enforcement can significantly reduce attackers' options for cashing out, reducing the financial incentive to carry out ransomware attacks and hampering ransomware organizations' ability to operate.

Most ransomware attacks appear to be financially motivated. However, others appear to be motivated by geopolitical goals, and seem more geared toward deception, espionage, reputational damage and disruption of the enemy government's operations.

In cases where a ransomware strain contains no mechanism to collect payment or allow victims to recover their files, we can be more certain that money isn't the attackers' primary motivation. And that's exactly what we saw in a recent ransomware attack on Ukrainian government agencies by hackers believed to be associated with the Russian government.

Some ransomware payments carry with them sanctions risk for the victim. Virtually all ransomware payments with sanctions risk was due to payments to ransomware strains thought to be associated with Evil Corp, a cybercriminal organization whose leadership reportedly has ties to the Russian government.

Ransomware payment value with sanctions risk by risk type, 2016 - 2021



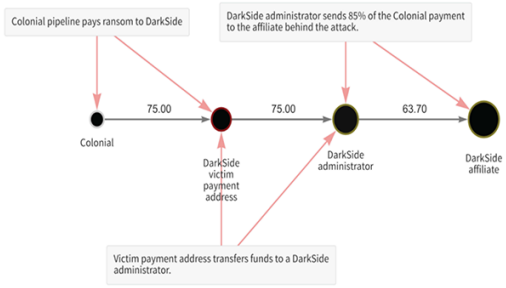
4. Colonial Pipeline case study

On May 7, 2021, Colonial Pipeline, an oil pipeline company that supplies energy to the southeastern United States, fell victim to a ransomware attack, forcing it to temporarily cease operations. Within hours of the attack, Colonial paid a ransom of 75 Bitcoin — worth roughly $4.4 million at the time — to DarkSide, the Russia-based cybercriminal

group responsible for the attack. Six days later, Colonial was able to resume operations, but during that time, the shutdown combined with panic buying as the news spread resulted in fuel shortages in several areas.

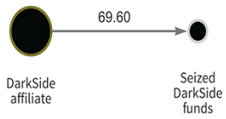
One month later, the Department of Justice announced that it had managed to seize $2.3 million worth of Bitcoin from Colonial's ransom payment following an FBI investigation. Chainalysis' tools aided the FBI.

Below is a chart describing the ransom payment itself and the initial movement of funds using Chainalysis Reactor, our blockchain forensics product.



First, on the left, we see the initial payment of 75 Bitcoin from Colonial to the address provided by the attackers. Soon after, that address transferred the funds to an address controlled by DarkSide's administrators, who then sent 63.7 Bitcoin — 85% of Colonial's payment — to the affiliate who controlled the attack. That point is key — DarkSide operates on the Ransomware as a Service ("RaaS") model, meaning the affiliates who carry out the attack effectively "rent" usage of DarkSide's technology from the core group of administrators who created and manage the ransomware strain itself. Administrators take a small cut of the payment from each successful attack in return, as we see above.

After tracking the funds to the affiliate's address, FBI investigators were able to seize the funds on May 28, 2021.



The Colonial Pipeline seizure represents a huge step forward in the fight against ransomware, and especially ransomware strains that attack our critical infrastructure. We continue to monitor the movement of funds using our tools so that we can provide helpful insight to authorities as they investigate further and, hopefully, seize the remainder of the funds.

5. Illicit activity with suspected links to North Korea

North Korean cybercriminals launched at least seven attacks on digital asset platforms that extracted nearly $400 million worth of digital assets last year. These attacks targeted primarily investment firms and centralized exchanges, and made use of phishing lures, code exploits, malware, and advanced social engineering to siphon funds out of these organizations' internet-connected "hot" wallets into DPRK-controlled addresses. Once North Korea gained custody of the funds, they began a careful laundering process to cover up and cash out.

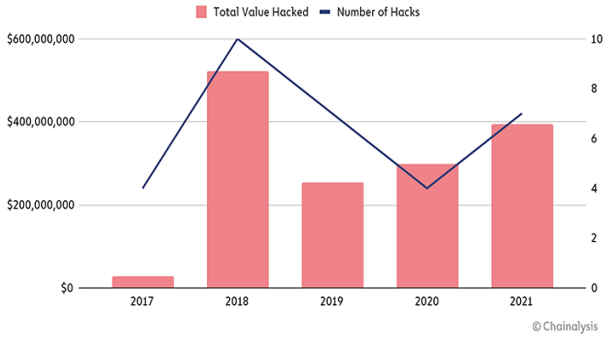
These complex tactics and techniques have led many security researchers to characterize cyber actors for the DPRK is especially true for APT 38, also known as "Lazarus Group," which is led by DPRK's primary intelligence agency, the US- and UN-sanctioned Reconnaissance General Bureau. While we will refer to the attackers as North Korean-linked hackers more generally, many of these attacks were carried out by the Lazarus Group in particular.

Lazarus Group first gained notoriety from its Sony Pictures and WannaCry cyberattacks, but it has since concentrated its efforts on digital asset crime—a strategy that has proven immensely profitable. From 2018 on, the group has stolen and laundered massive sums of virtual currencies every year, typically in excess of $200 million. The most successful individual hacks, one on KuCoin and another on an unnamed digital asset exchange, each netted more than $250 million alone. And according to the UN security council, the revenue generated from these hacks goes to support North Korea's WMD and ballistic missile programs.

In 2021, North Korean hacking activity was on the rise once again. From 2020 to 2021, the number of North Korean-linked hacks jumped from four to seven, and the value extracted from these hacks grew by 40%.

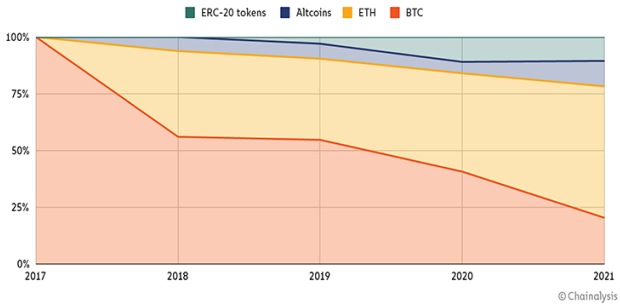
Chainalysis

North Korean-linked hacks by total value hacked and total number of hacks



Interestingly, in terms of dollar value, Bitcoin now accounts for less than one fourth of the digital assets stolen by DPRK. In 2021, only 20% of the stolen funds were Bitcoin, whereas 22% were either ERC-20 tokens or altcoins. And for the first time ever, Ether accounted for a majority of the funds stolen at 58%.

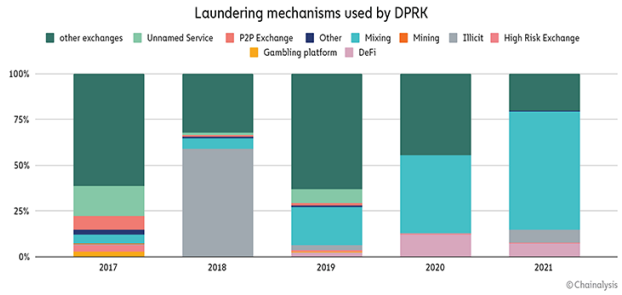
Share of funds stolen by DPRK by coin type



The growing variety of digital assets stolen has necessarily increased the complexity of DPRK's digital asset laundering operation. Today, DPRK's typical laundering process is as follows:

6. ERC-20 tokens and altcoins are swapped for Ether via decentralized exchange (DEX)
7. Ether is mixed
8. Mixed Ether is swapped for Bitcoin via DEX
9. Bitcoin is mixed
10. Mixed Bitcoin is consolidated into new wallets
11. Bitcoin is sent to deposit addresses at crypto-to-fiat exchanges based in Asia —potential cash-out points

In fact, we observed a massive increase in the use of mixers among DPRK-linked actors in 2021.

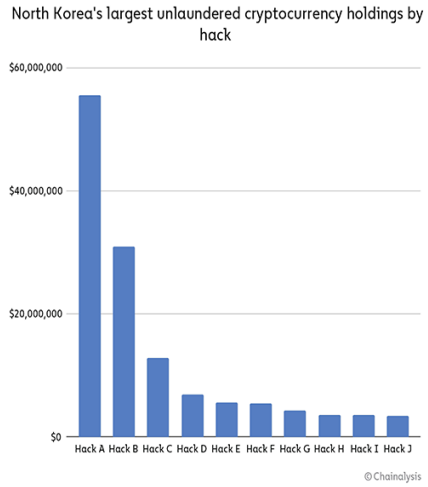


More than 65% of DPRK's stolen funds were laundered through mixers this year, up from 42% in 2020 and 21% in 2019, suggesting that these threat actors have taken a more cautious approach with each passing year.

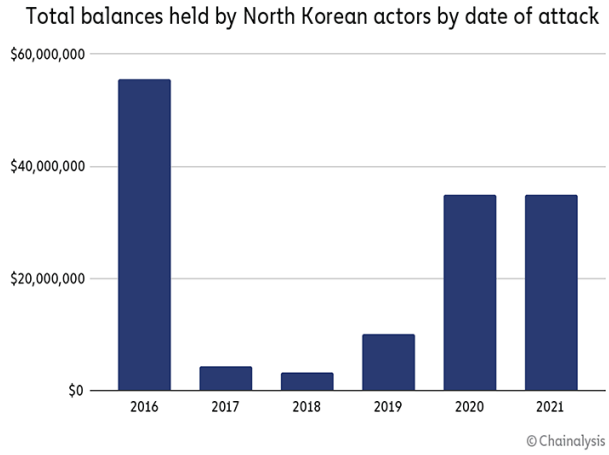
Why mixers? DPRK is a systematic money launderer, and their use of multiple mixers —software tools that pool and scramble digital assets from thousands of addresses—is a calculated attempt to obscure the origins of their ill-gotten digital assets while offramping into fiat.

Why DeFi? DeFi platforms like DEXs provide liquidity for a wide range of ERC-20 tokens and altcoins that may not otherwise be convertible into cash. When DPRK swaps these coins for ETH or BTC they become much more liquid, and a larger variety of mixers and exchanges become usable. What's more, DeFi platforms don't take custody of user funds and many do not collect know-your-customer ("KYC")) information, meaning that cybercriminals can use these platforms without having their assets frozen or their identities exposed.

Chainalysis has identified $170 million in current balances—representing the stolen funds of 49 separate hacks spanning from 2017 to 2021—that are controlled by North Korea but have yet to be laundered through services. The ten largest balances by dollar value are listed below.



Of DPRK's total holdings, roughly $35 million came from attacks in 2020 and 2021. By contrast, more than $55 million came from attacks carried out in 2016—meaning that DPRK has massive unlaundered balances as much as six years old.



This suggests that DPRK-linked hackers aren't always quick to move stolen digital assets through the laundering process. It's unclear why the hackers would still be sitting on

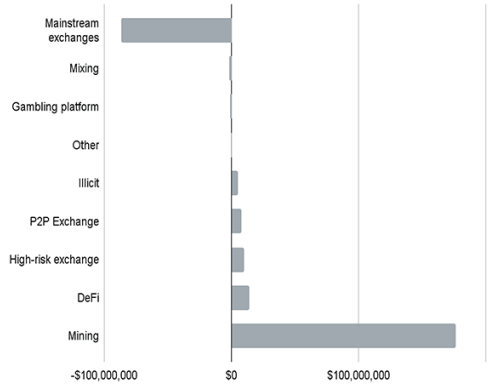
these funds, but it could be that they are hoping law enforcement interest in the cases will die down, so they can cash out without being watched.

6. Illicit activity with suspected links to Iran

Iran faces some of the most extensive U.S. sanctions of any country. Per the United States Treasury's Office of Foreign Assets Control (OFAC), U.S. businesses and individuals are effectively banned from transacting with Iranian businesses, including its biggest financial institutions and central bank. Some in the Iranian government have called for the country to use digital assets to circumvent these sanctions, and Bitcoin mining may provide the perfect opportunity to do so. As one of the world's largest energy producers, Iran has the low-cost electricity needed to mine digital assets like Bitcoin cheaply, providing an injection of monetary value that sanctions can't stop.

Our research indicates Iranian Bitcoin mining is well underway at a surprisingly large scale. From 2015 to 2021, we found that Bitcoin mining funneled more than $186 million into Iranian services, most of it within the past year.

Net flows to and from Iranian services, 2015 - 2021



Iranian state actors are well aware of the opportunity. In 2019, the Iranian government created a licensing regime for digital asset mining. And in March of this year, a think tank tied to the President's office released a report stressing its benefits.

But the costs have extended beyond just electricity. The Iranian government has had to ban Bitcoin mining twice this year due to frequent blackouts, many of which Iran's state power agency has blamed on unlicensed Bitcoin mining. And unlicensed Bitcoin miners, for their part, allegedly account for "some 85%" of all activity in the country, per the Iranian president.

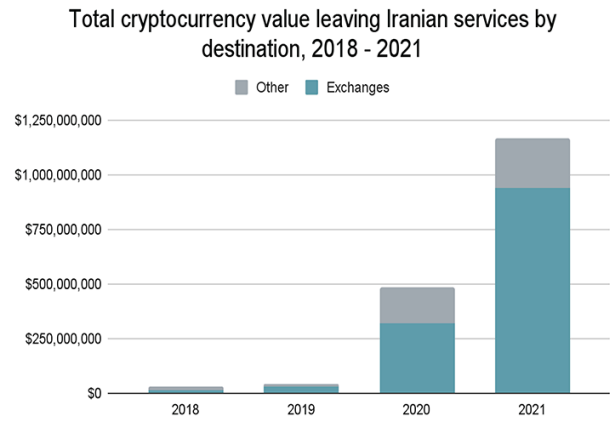
It has also opened up a new avenue of risk for digital asset businesses. U.S. businesses could face penalties or even criminal prosecution if found in violation of OFAC sanctions, which prohibit U.S. persons or companies from servicing financial accounts belonging to

Chainalysis

Iranian persons or companies. That being said, businesses can monitor for exposure to Iranian miners to reduce this risk considerably.

It's also important to note that a nexus to sanctions is more attenuated at the transaction/mining fee level. If a U.S. business were to engage in a transaction and the fees paid from said transaction were received by an Iranian miner, the payer and payee would have had no say in who could receive these fees—the receiver of which is determined automatically by Bitcoin's proof-of-work protocol. To date, sanctions risk appears most prominent when a U.S. business transacts directly with the miner themselves.

Many exchanges operating in jurisdictions without active sanctions, however, continue to provide financial services to Iranian businesses. In fact, in 2021, services outside of Iran received $1.16 billion from Iranian services—more than double the value received last year.

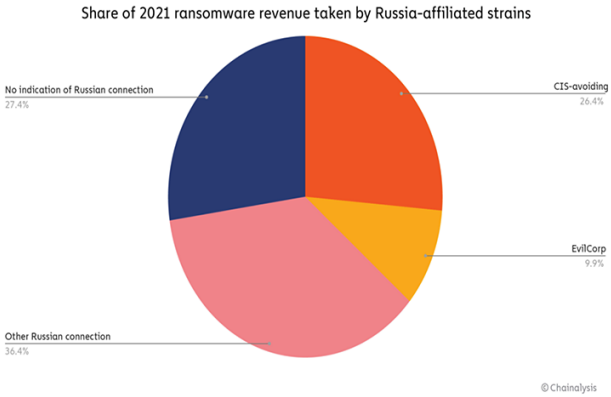


This transfer of funds from mining pools to Iranian services to services in the wider digital asset ecosystem is a corridor through which Iran evades sanctions.

7. Illicit activity with suspected links to Russia

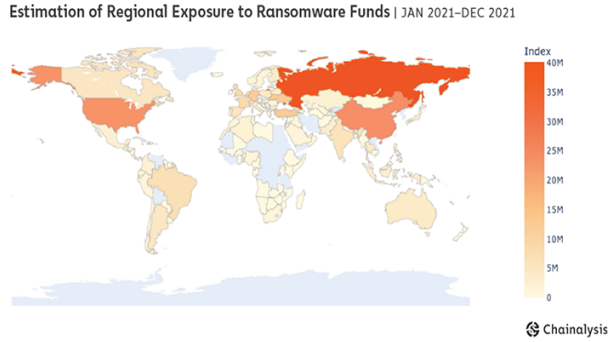
I show on the pie chart below the share of total ransomware revenue that went to strains affiliated with Russian organizations in 2021.

Chainalysis



Overall, roughly 74% of ransomware revenue in 2021 — over $400 million worth of digital assets — went to strains we can say are highly likely to be affiliated with Russia in some way.

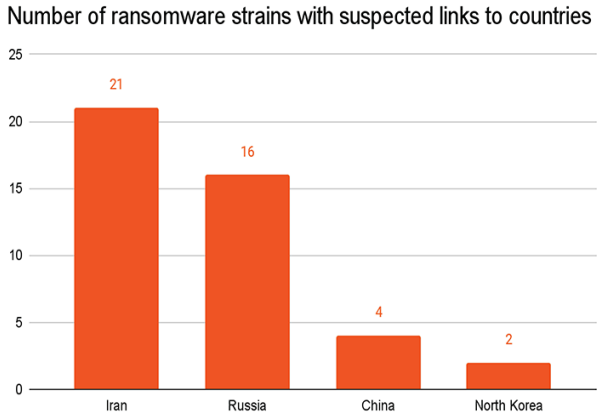
Blockchain analysis combined with web traffic data also tells us that after ransomware attacks take place, most of the extorted funds are laundered through services primarily catering to Russian users.



An estimated 13% of funds sent from ransomware addresses to services went to users estimated to be in Russia, more than any other region. A huge amount of digital asset-based money laundering, not just of ransomware funds but of funds associated with other forms of cybercrime as well, goes through services with substantial operations in Russia.

Russia-affiliated attackers aren't the only ones using ransomware for geopolitical ends. Cybersecurity analysts at Crowdstrike and Microsoft have concluded that many attacks

by ransomware strains affiliated with Iran, mostly targeting organizations in the U.S., the E.U., and Israel, are geared more toward causing disruption or serving as a ruse to conceal espionage activity. Generally speaking, Chainalysis has seen significant growth in the number of ransomware strains attributed to Iranian cybercriminals in the past year — in fact, Iran accounts for more individual identified strains than any other country.

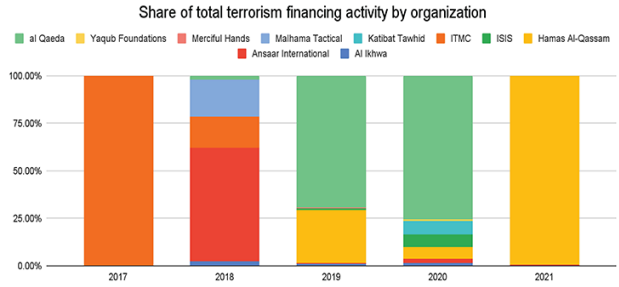


8. Terrorist financing

By the end of 2021, we've identified a number of terrorist organizations that have attempted to finance their operations with digital assets. What's harder to find, however, is a group that has gotten away with it.

- In 2019 and 2020, al-Qaeda raised digital assets through Telegram channels and Facebook groups. Thanks to the FBI, HSI, and IRS-CI, more than $1 million was seized from a money service business ("MSB") operator who facilitated some of these transactions.
- In early Spring of 2021, al-Qassam Brigades, Hamas' military wing, collected more than $100,000 in donations. In July, the Israeli government seized much of it from associated MSBs.

Chainalysis



9. Malware

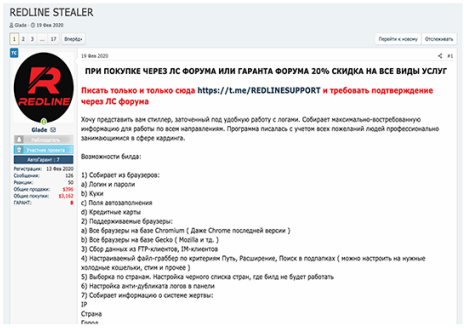
Malware refers to malicious software that carries out harmful activity on a victim's device, usually without their knowledge. Malware-powered crime can be as simple as stealing information or money from victims, but can also be much more complex and grand in scale. For instance, malware operators who have infected enough devices can use those devices as a botnet, having them work in concert to carry out distributed denial-of-service ("DDoS") attacks, commit ad fraud, or send spam emails to spread the malware further.

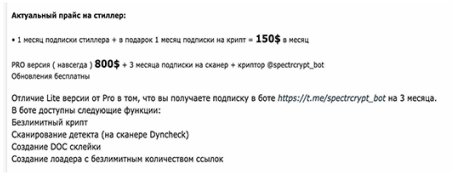
The malware families we discuss here are all used to steal digital assets from victims, though some of them are used for other activities as well. The grid below breaks down the most common types of digital asset-focused malware families.

Type	Description	Example
Info stealers	Collect saved credentials, files, autocomplete history, and digital asset wallets from compromised computers.	Redline
Clippers	Can insert new text into the victim's clipboard, replacing text the user has copied. Hackers can use clippers to replace digital asset addresses copied into the clipboard with their own, allowing them to reroute planned transactions to their own wallets.	HackBoss
Cryptojackers	Makes unauthorized use of victim device's computing power to mine digital asset.	Glupteba
Trojans	Virus that looks like a legitimate program but infiltrates victim's computer to disrupt operations, steal, or cause other types of harm.	Mekotio banking trojan

Chainalysis

Many of the malware families described above are available to purchase for relatively little money on cybercriminal forums. For instance, the screenshots below show an advertisement for Redline, an info stealer malware, posted on a Russian cybercrime forum.

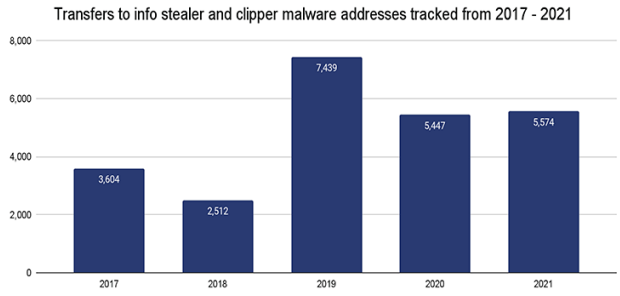




The seller offers cybercriminals one month of Redline access for $150 and lifetime access for $800. Buyers also get access to Spectrum Crypt Service, a Telegram-based tool that allows cybercriminals to encrypt Redline so that it's more difficult for victims' antivirus software to detect it once it's been downloaded. The proliferation of cheap access to malware families like Redline means that even relatively low-skilled cybercriminals can use them to steal digital assets. Law enforcement and compliance teams must keep this in mind, and understand that the malware attacks they investigate aren't necessarily carried out by the administrators of the malware family itself, but instead are often carried out by smaller groups renting access to the malware family, similar to ransomware affiliates.

The graph below shows the number of victim transfers to digital asset addresses associated with a sample of malware families in the info stealer and clipper categories investigated by Chainalysis.

Chainalysis



Note: This graph does not reflect activity by cryptojackers or ransomware.

Overall, the malware families in this sample have received 5,974 transfers from victims in 2021, up from 5,449 in 2020.

Chainalysis

APPENDIX B

Self-custody or "unhosted" wallets

Below we provide analysis relating to self-custodied "unhosted" wallets, putting their potential use by illicit actors in appropriate context.

In December 2020, when Treasury published a notice of proposed rulemaking for transactions with unhosted wallets and certain foreign jurisdictions, Chainalysis reviewed the data on cryptocurrency transactions involving unhosted wallets.

The data showed that the majority of the funds held in unhosted wallets often come from virtual asset service providers ("VASPs") and are related to investing purposes or are the vehicle for individuals or organizations to move funds between regulated exchanges.

It is important to mention that 2021 data didn't vary significantly in comparison to the 2020 analysis. There are still three trends related to the usage of unhosted wallets.

The vast majority of the bitcoin funds transferred to unhosted wallets came from VASPs

During Q3 of 2021, almost 83% of the bitcoin sent from an unhosted wallet to another unhosted wallet originated from cryptocurrency exchanges, and only 2% came from illicit services. This means that in the vast majority of cases law enforcement can investigate illicit activity related to unhosted wallets by working with cryptocurrency exchanges, which are obligated entities, and obtain KYC information from them through legal process.

The majority of bitcoin sent to non-VASPs are eventually sent to a VASP

A high number of the transfers sent and received by unhosted wallets have VASPs on the other side of the transaction. If cryptocurrency is being used for illicit purposes, eventually criminals will need to cash their illicit proceeds out. This means going through a cryptocurrency exchange (we can see this behavior reflected in our data). As long as they are in a country that regulates cryptocurrency exchanges – and this list is growing – exchanges will collect KYC information. Access to this information is vital to financial crime investigations.

During Q3 2021, the percentage of funds that were not sent to an exchange service decreased from 29% to 18% in comparison with Q2 2020. While the percentage of funds sent to exchanges increased from 62% to 71%. This means that crypto holders moved the funds they were holding inside unhosted wallets to an exchange, maybe to take out some profits due to the crypto bull market we experienced this year.

The transaction activity levels among unhosted wallets highly suggests that their primary use is for investment

Chainalysis

After funds are deposited to an unhosted wallet from an exchange, the percentage of bitcoin moved to another unhosted wallet in a given month is significantly low. The majority of the bitcoin stays in the original wallet for a long period of time. On average, the funds originated from a VASP to unhosted wallets move only once a month, which likely indicates that the primary use case is investment.

Chainalysis' robust blockchain dataset provides key insights into the role of unhosted wallets in the cryptocurrency ecosystem. If the main purpose of these regulatory requirements is to decrease illicit transactions and avoid money laundering, targeting unhosted wallets may not accomplish the intended objective.

What our blockchain analysis data makes clear is that unhosted wallets are not inherently risky and unhosted wallets do not inhibit law enforcement's ability to investigate the illicit use of cryptocurrency. Blockchain analytics can inform risk analysis and compliance programs so that risks can be mitigated responsibly and effectively by compliance teams.

Chainalysis

APPENDIX C

Glossary
Chainalysis Service Category Definitions

Most cryptocurrency volume travels through services, including legal entities like retail exchanges or illicit entities like darknet markets. To identify and assess the risk of a service, Chainalysis groups the wallet addresses into clusters. Then we attribute the clusters to specific entities and organizations (e.g., a particular exchange, mixing service, or darknet market, etc.). After attributing the clusters to a specific entity, we then categorize them according to the type of real-world service that they belong to. Chainalysis refers to these categories as Service Categories.

Child abuse material site
Child abuse material includes forums and sites operating on the dark web which facilitate the buying, selling, and the spread of child sexual abuse material. These sites are often coded and difficult to access.

Darknet markets
Darknet markets are commercial websites that operate on the dark web, which can be accessed via anonymizing browsers or software such as Tor or I2P. These sites function as black markets by selling or advertising illicit goods and services such as drugs, fraud materials, and weapons, among others. Darknet markets use cryptocurrency payment systems, often with escrow services and feedback systems to help develop trust between the vendor and customer. Darknet markets have become more security conscious over the past few years due to multiple law enforcement shutdowns.

Decentralized exchange contract
Decentralized exchanges are services which facilitate cryptocurrency and token trades by using automated smart contracts. Trades on a decentralized platform are peer-to-peer and have no third party or central authority other than the smart contract which executes the trades.

ERC-20 token

ERC-20 tokens are a blockchain-based asset that can be sent and received using an Ethereum wallet. It is the technical standard for most smart contracts on Ethereum blockchain, enabling token issuance for ICOs (a crowdfunding mechanism).

Ethereum contract

Ethereum is a blockchain with its own cryptocurrency and a built-in functionality for smart contracts. Smart contracts can store information related to a deal and automatically self-execute when the terms of the contract are fulfilled. Smart contracts can be agreed upon and enforced between two parties without the need for a third, since they don't actually execute until each side has fulfilled their obligations.

Exchanges
Exchanges allow users to buy, sell, and trade cryptocurrency. They represent the most important and widely-used service category in the cryptocurrency industry, accounting for 90% of all funds sent by services.

Fraud shop

Chainalysis

Financially motivated shops selling different types of data including, PII (Personally Identifiable Information), credit card data, stolen accounts, and more. Unlike Darknet Markets, Fraud Shops are normally operated by a single actor/team and are the sole merchant within the service. Fraud shops also tend to have behavioral differences from darknet markets such as top-up depositing of funds (incremental increases to the total amount), as well as no customer withdrawals. Therefore, most outgoing transactions can be linked to the operators of the Fraud Shop.

Gambling
Online gambling can take many forms from resembling a typical casino where you can play card games like blackjack and poker, slot games and the like, to sites for wagering bets on sports or eSports outcomes.

The industry has been an early adopter of cryptocurrency. Users will send cryptocurrency as a convenient alternative to fiat, and get started betting. Gambling is treated differently depending on the jurisdiction, and many sites have lax KYC requirements. Because of this, there's potential for these sites to be used for laundering money. Many of these companies are located in/operating out of island nation-states (such as Curaçao, Cyprus, or Malta).

High risk exchange
Chainalysis' designates an exchange as high risk according to the following criteria:

- **No KYC**: The exchange requires no customer information before allowing any level of deposit or withdrawal. This is also applicable if they require name, phone number, or email address but do not attempt to verify that this information actually belongs to the customer.
- **Criminal ties**: The exchange has publicly documented ties to criminal activity.
- **High risky exposure**: The exchange has high amounts of exposure to risky services such as darknet markets, other high risk exchanges, or mixing. Chainalysis examines if the exchange's exposure to illicit activity is an outlier compared to other exchanges. A service with direct high risk exposure one standard deviation away from the average across all exchanges identified by Chainalysis over a 12 month period is considered a high risk exchange.

High risk jurisdiction
The high risk jurisdiction category comprises cryptocurrency services that are based in specific jurisdictions, including Iran and Venezuela. Chainalysis considers both cryptocurrency activity as well as the global regulatory landscape when deciding which jurisdictions to include in this category. Given stringent guidelines for the financial system's interactions with Iran and Venezuela, Chainalysis has opted to more prominently surface services operating in these areas. Chainalysis will continue to add services to this category over time.

Hosted wallets

Hosted wallets are an alternative to core wallets (full node wallets). Wallet software allows users to store their public and private keys, and connects to blockchain nodes to transfer funds and check balances. Wallets that control the user's private keys are considered custodial, or hosted, while software that allows users to retain full control of private keys is considered non-custodial.

Hosted wallets can be risky because the user doesn't actually hold their funds, thus opening the possibility of being scammed. It's also possible the service does not implement sufficient security measures, and is vulnerable to attack. However, a reputable hosted wallet service that takes advanced security measures is likely more reliable and convenient than a non-technical or careless individual.

ICO

An ICO (Initial Coin Offering) is a means of crowdfunding for new cryptocurrency or related projects, similar to an IPO in the traditional market. The entity behind the new cryptocurrency makes their pitch and sells units of the token to investors in exchange for fiat currency or more mainstream cryptocurrencies like Bitcoin or Ether.

Many ICOs have proven to be scams. There are countless examples of bad actors who build a flashy site promoting an ambitious project, raise funds through an ICO, then pocket the money and walk away.

Illicit actor organization

Individuals and/or organizations that operate directly or indirectly in various forms of illicit activities. These entities are directly or indirectly involved with risky entities such as darknet markets, fraud shops, extremist financing, hacking, etc.

Lending contract

Lending is one of the biggest uses for smart contracts and DeFi currently. Holders of assets can lend them to others and earn interest on the loan. Borrowers have to put up collateral above the value of the loan to protect against price fluctuations.

Merchant services

Merchant services are authorized financial services that enable businesses to accept payments on their customer's behalf. They are also known as payment gateways or payment processors. These services allow merchants to accept cryptocurrency for invoicing and online or in-person payments. This often includes conversion to local fiat currency and settling funds to the merchant's bank account.

Merchant services is generally a low-risk category. Users mostly comprise mainstream, traditional businesses on one end and their customers on another. However, it's worth noting that scammers sometimes integrate merchant services with a malicious website to accept cryptocurrency payments from their victims.

Mining and Mining pools

Mining is the process by which cryptocurrency is generated. Mining pools are special services where miners can pool their resources - typically GPU or specialized ASIC mining hardware - together towards mining cryptocurrency. By pooling mining resources the pool has a bigger chance of mining a block and the returns are divided among all the miners according to how much mining power each contributed.

Mining pools typically only receive funds from direct mining activity, and as such are typically low risk. However, a pool that accepts deposits from sources other than mining can be exploited for money laundering.

Mining is used for coin generation, when new coins are minted from the mining process.

Chainalysis

Mixing services
Mixers are websites or software used to create a disconnection between a user's deposit and withdrawal. Mixing is done either as a general privacy measure or for covering up the movement of funds obtained from theft, darknet markets, or other illicit sources.

Mixers typically pool incoming funds from many users and re-distribute those funds with no direct connection back to the original source.

Other
This category is used when the entity does not represent a widely popular field of operation or is a particular type of operation or entity such as donation addresses, social network bots, seized funds, among others. This category does not have any inherent risk but may contain risky entities.

Peer to peer (P2P) exchange

P2P exchanges are online sites that facilitate the buying, selling, and trading of cryptocurrency between two individuals while, usually, not being directly in possession of the funds. Some P2P exchanges will not require any KYC, making them attractive for money laundering activities.

Protocol privacy

Protocol privacy applies to the two shielded pools built into the Zcash blockchain.

Zcash offers users the possibility to encrypt blockchain activity; this is known as shielding. Zcash provides this capability through shielded pools - a collection of encrypted addresses where the balances and transactions within the pool are always encrypted. Transactions into, out of, and between the pools are transparent but the counterparty addresses within the pool remain encrypted. The pools appear in Reactor as named entities and single address clusters, which are categorized as Protocol privacy. While we can't show activity or addresses within the pool, we display activity into and out of the pool.

Mined ZEC cannot be sent straight to transparent addresses but must first go to one of the shielded pools. Hence receiving exposure from a shielded pool doesn't necessarily mean that the funds were mixed or deliberately obfuscated. Other users must opt in to take advantage of Zcash's privacy features. Roughly 14% of Zcash transactions involve one of Zcash's two shielded pools.

Ransomware
Ransomware is special malware designed to encrypt a victim's computer data and automatically request a ransom to be paid in order to decrypt the data. Attackers employ social engineering and phishing schemes that trick people and organizations into downloading the malicious software.

Sanctions
Sanctions refer to entities listed on economic/trade embargo lists, such as by the US, EU, or UN, with which anyone subject to those jurisdictions is prohibited from dealing. Currently this includes the SDN list of the US Department of the Treasury's Office of Foreign Assets Control. The prohibition on dealing includes any instrumentalities of the sanctioned entities, including operating companies, bank accounts, and cryptocurrency addresses used by the sanctioned entities. In some instances, persons subject to those

jurisdictions are also required to block/freeze assets belonging to the sanctioned entities to prevent further benefit or movement.

Scam
Scams can impersonate a variety of services, including exchanges, mixers, ICOs, and gambling sites. This category also encompasses scam emails, extortion emails, and fake investment services. They usually offer unrealistic returns on investment, many times trying to mask a pyramid scheme, or pretend to have incriminating personal data on the victim and ask for money in order to not disclose it.

Smart contract

Some blockchains have a built-in functionality for smart contracts. Smart contracts can store information related to a deal and automatically self-execute when the terms of the contract are fulfilled. Smart contracts can be agreed upon and enforced between two parties without the need for a third, since they don't actually execute until each side has fulfilled their obligations.

Stolen funds
Stolen funds comprise instances of hacked exchanges and services. Attackers engage in sophisticated and persistent social engineering, and exploit pre-existing vulnerabilities to transfer funds from exchange hot wallets to their control. The payoff for actors can be enormous with single incidents often resulting in tens of millions of dollars in losses.

Terrorist financing
Terrorist financing pertains to the funding of designated terrorist groups and affiliates of terrorist groups, entities, and individuals. Financing is fundamental for the survival and operation of terrorist groups and is used to support a multitude of their activities, including recruitment, propaganda, day-to-day activities, and military operations. Terrorist groups secure the flow of funds in a variety of ways, including through the use of cryptocurrencies.

Token smart contract

Tokens are a blockchain-based asset that can be sent and received using a wallet. There are different technical standards for the different types of smart contracts on various blockchain, enabling token issuance for ICOs (a crowdfunding mechanism).

Unnamed Service

Clusters we identify as behaving as services fall into this category. These are services that have not yet been identified but show the behavior expected of a service. There isn't a standard risk for this category, but once any entity in this category is identified, it is labeled and moved to an appropriate category.

PREPARED STATEMENT OF MICHAEL MOSIER

FORMER ACTING DIRECTOR, DEPUTY DIRECTOR/DIGITAL INNOVATION OFFICER,
FINANCIAL CRIMES ENFORCEMENT NETWORK (FINCEN)

MARCH 17, 2022

Thank you Chairman Brown, Ranking Member Toomey, and Members of the Committee for holding this hearing and inviting me to participate. It's an honor to be here. Congress represents the breadth of viewpoints across our society and has a critical role in reflecting and protecting the democratic foundation and personal sovereignty of the people.

My grandfather was a justice of the peace in a small mining and steel town in Western Pennsylvania. Sadly, he died long before I was born. But I treasure one of his campaign cards from a 1953 election that announces: "Endorsed by Labor. An avowed enemy of communism". Those juxtaposed statements encapsulate a sense of collective empowerment of the time, but also a resolute vigilance against totalitarian collectivism. They underscore the importance of maintaining a balance. Of sufficiently empowering people, organizations, and Governments to prevent abuse, while ensuring checks on that power, so that it is not itself used to abuse.

A desire to protect personal sovereignty in the face of abuse led me to public service. As a new lawyer at a firm, I took on pro bono cases to help victims of domestic violence obtain protective orders, then wanted to do more. I became a State prosecutor at the Manhattan District Attorney and eventually a Federal prosecutor at the Department of Justice (DOJ), investigating kleptocracy as well as the financing of human trafficking. Preservation of self-determination has guided me through roles as Deputy Chief in DOJ's Money Laundering Section, Director at the White House National Security Council, OFAC Associate Director, Counselor to the current Treasury Deputy Secretary, and, most recently, Acting Director of FinCEN.

From my experiences,[1] I have seen firsthand that, yes, investigative ability is critical, including as a deterrent; but we must not confuse tools with the mission, which is to preserve the self-determination upon which our country was founded, and to empower people to be able to thrive and protect themselves. Preserving this balance requires a thoughtful approach to new technologies. If every new technology is viewed with suspicion, we risk harming the citizens we've sworn to protect. At FinCEN, we constantly invited the public for conversations, from cryptography professors, to civil society explaining how vulnerabilities are turned against people under authoritarian rule, constitutional privacy and speech experts, child exploitation and anticorruption groups, and core developers of privacy technology. This education was nearly weekly—an obligation as public servants to ensure we reflected all the perspectives of the people we serve.

The Anti-Money Laundering Act (AML Act)[2] passed last year modernizes 2 our approach to financial integrity, including the need to prioritize some risks over others, and to strike a balance that guarantees opportunity. That balance is also reflected in our separation of powers and our Constitution. Because no matter the best intentions, people are fallible. In thinking about self-determination, when we speak of "illicit finance," we must not forget defenders of democracy whose financing might be considered "illicit" to the autocrats and invading armies they resist. As we painfully see around the world right now, it is fundamental to democracy that people have the opportunity to protect themselves in the face of fallibility and brutality.

The same cryptographic capabilities discussed here today enabled secure, auditable humanitarian aid to 60,000 health care workers in Venezuela under a repressive regime, accomplishing a major foreign aid objective tied to a White House national security emergency.[3] The best way to send Office of Foreign Assets Control (OFAC)-authorized aid that would not be intercepted by the Venezuelan regime was to do it outside of their domestic banking system, through USDC cryptocurrency, and using Virtual Private Networks (VPNs).[4] No doubt the Venezuelan regime con-

---

[1] General Counsel, Espresso Systems. Previously: Acting Director, Dep.Dir./Digital Innovation Officer, FinCEN; Counselor (cybersecurity and emergent technology) to the Deputy Secretary of the Treasury; in-house counsel, Chainalysis; Director (transnational organized crime), White House National Security Council; Associate Director, OFAC; Deputy Chief, Money Laundering Section, USDOJ; adjunct professor, Georgetown University Law Center.

[2] *https://www.fincen.gov/anti-money-laundering-act-2020*

[3] *https://www.circle.com/blog/circle-partners-with-bolivarian-republic-of-venezuela-and-airtm-to-deliver-aid-to-venezuelans-using-usdc*

[4] *https://www.ft.com/content/2a271032-35b4-4969-a4bf-488d4e9e3d18*

sidered the use of those previously frozen assets "illicit finance," but to us they were cryptographically secure humanitarian aid.[5]

Likewise, in the past few weeks, tens of millions of dollars worth of cryptocurrency were donated by the public to Ukraine—faster and more aid than the U.N. provided. Further, the transparency of Government-identified wallets on a public ledger is a substantial improvement in accountability from U.N. aid through traditional banking, like the U.N. Oil-for-Food scandal.[6] Streaming in 24/7, with no limited banking hours; with fewer intermediaries to be disrupted or take fees off the top; and available with a mere phone app. No doubt, the Russian Government considers that money "illicit" and would stop it if they could. Resilient money is part of a duality of sovereignty that, like most things, can be considered good and bad.

For policymakers, the key is to find a balance that doesn't merely chase bad actors but also prevents exploitation of the vulnerable from the start. Having spent decades with victims of crime, I can say: you will never make them whole. Even if you get some of the money back—and rarely will you get it all back—you will never undo the trauma of being violated, exploited, and having your vulnerability exposed so concretely. We must empower people to protect themselves from exploitation, not just avenge the victims. Cryptocurrencies, like the cryptography with which they are built, can be used in crime, but we'd be naive to think they are not also powerful tools to empower and protect the innocent.

Related to democracy and threat prevention, while briefly serving as Counselor to the current Treasury Deputy Secretary, my portfolio was cybersecurity and emergent technology in the wake of the SolarWinds cyberattack. The Russian Foreign Intelligence Service spent months inside computers across the private sector and Government agencies. It confirmed[7] what we had been saying for years: that cybercrime is not just about the money. Over-attributing cybercrime to cryptocurrency misses significant operating models and preventive measures that can be taken.

Having worked on cybercrime for years, including at FinCEN and the National Security Council, here are a few *observations about ransomware* in particular:

1. Ransomware dates back to 1989, two decades prior to the emergence of Bitcoin in 2009. Payments have come in a variety of fiat "digital" methods such as online payment processors, credit cards, and other traditional money transmission services for decades.
2. Yes, cryptocurrency has become the recent payment of choice because of the speed and its perceived anonymity. However, payments made in cryptocurrency offer Law Enforcement significant visibility and investigative benefits over opaque banking, as we saw with the recovery of $2.3 million in cryptocurrency from the Colonial Pipeline attackers. There are many other examples of cases being solved much faster because cryptocurrency was involved, cases where we could immediately identify on a public ledger which Virtual Asset Service Provider (VASP) to subpoena using immutable public evidence rather than years of Mutual Legal Assistance Treaty (MLAT) process and guesswork about which bank might be involved due to opaque wire transfers and shell companies.
3. The increase in ransomware payments has less to do with criminals reflecting current financial trends, and more to do with three practical emergences:
   a. First, the advent of *Ransomware-as-a-Service*, making kits widely available, regardless of coding skills, drastically reducing barriers to entry;
   b. Second, the use of *double extortion*, greatly increasing payouts by also threatening to expose stolen data, not just lock the computer; and
   c. Third, wide adoption of *cyber insurance*, which, while good in itself, also means ransomware actors know victims have ability to pay, driving up demands and payouts.

In light of these three substantial factors, it greatly oversimplifies the issue to blame "cryptocurrency" for payments increasing. Ignoring the variety of factors at play, this claim fails to recognize that part of the solution is having cyber insurance policies require that the policyholder develop and maintain meaningful cybersecurity practices as one of the best ways to help reduce payments—and, importantly, reduce victims from the beginning. A ransomware attack avoided is a bigger victory

---

[5] *https://www.ft.com/content/2a271032-35b4-4969-a4bf-488d4e9e3d18*
[6] *https://www.law.nyu.edu/news/IILJ-IRAQ-OILFOOD*
[7] *https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic*

than a perpetrator apprehended. We make decisions everyday about balancing risk and opportunity to thrive. The best defense against cybercrime is disconnecting computers. But we have decided that it's better to manage risk rather than stop communicating, creating, and transacting across the world seamlessly. Likewise, we decided as a Nation that although encryption itself makes it more difficult for the Government in some instances to monitor activity, that security also protects people from hackers and protects human rights actors from autocrats so they can promote democratic discourse. As Sen. Wyden has said, "Secure, encrypted communications give people the power to organize and access information that authoritarian regimes don't want seen. End-to-end encryption is life or death for people living in authoritarian countries like Russia, China, or Saudi Arabia."[8] The democratic resilience of cryptography doesn't stop with mere messages.

If we chronically underestimate what cryptocurrencies can do for democracy, we also grossly overestimate its use in crime. For perspective, "Chainalysis's 2022 Crypto Crime Report" estimated crypto-illicit finance at $14 billion, about 0.15 percent of all transaction volume in 2021.[9] The UNODC estimates fiat illicit finance between $800 billion—$2 trillion, or 2–5 percent of global GDP—that fiat illicit percentage is up to 33 times higher than crypto's percentage.[10] For scale, crypto's 2021 illicit finance number of $14 billion is comparable to the $12.4 billion lost by bank customers through overdraft fees alone in 2020.[11] Apples to oranges perhaps, but meaningful context in terms of scale of impact on consumers. Note, it is impossible to have an overdraft with crypto, because there is no double-spending. That alone is $12.4 billion back to some of the most economically vulnerable people. Not to mention mandatory account minimums that have kept roughly 3.5 million U.S. households unbanked, which crypto does not have.[12]

There is work to be done yet for cryptocurrency. There are too many exploits, rugpulls and scams. The early internet had a lot of fraud and exploits as well. You'd order something online and have no idea whether you'd actually get it. It took years to work out consumer protections, and certainly data privacy and protection remains elusive to this day. But we haven't decided to shut down the internet. We work persistently to find the balance and prioritize risks. As an example of the wisdom in fully exploring positive uses for edge technology before preemptively overreacting, the U.K. previously talked of banning The Onion Router, or Tor, browser, which was originally designed by the U.S. Naval Research Laboratory and provides multilevel encrypted access to the internet.[13] Now the BBC is broadcasting via Tor in Russian and Ukrainian to bring the free flow of information to where BBC signals have been blocked.[14]

And how should we prioritize risks in the context of the Russian invasion? A senior Administration official said on background call to the Digital Assets Executive order: "I will say, on Russia, in particular, the use of cryptocurrency we do not think is a viable workaround to the set of financial sanctions we've imposed across the entire Russian economy and, in particular, to its central bank." Similarly, my successor as Counselor to the Deputy Secretary[15] recently said, "You can't flip a switch overnight and run a G20 economy on cryptocurrency. It's an access problem, it's a rails problem, and it's just a basic liquidity problem. Certainly there's going to be an element [of crypto] that's part of their playbook, but it frankly isn't at the top of the list."[16]

Three Recommendations

If you want to tangibly impact illicit finance, here are three concrete actions you can take now:

1. First, pass the budget that was due last October. Fifteen months after the passage of landmark AML modernization legislation, none of the tens of millions of dollars needed to implement it has been appropriated. Under a Continuing Resolution, FinCEN and OFAC are without the roughly $74 million increase

---

[8] *https://twitter.com/RonWyden/status/1499384550165725190?s=20&t=1UzXFuPoX4czlgMBVYSg*
[9] *https://blog.chainalysis.com/reports/2022-crypto-crime-report-introduction/*
[10] *https://www.unodc.org/unodc/en/money-laundering/overview.html*
[11] *https://www.forbes.com/advisor/personal-finance/how-to-prevent-overdraft-fees/*
[12] *https://twitter.com/-amanda-fab/status/1479629264194572291?s=21*
[13] *https://www.bbc.com/news/technology-50150981*
[14] *https://www.bbc.com/news/technology-50150981*
[15] *https://www.whitehouse.gov/briefing-room/press-briefings/2022/03/09/background-press-call-by-senior-administration-officials-on-the-presidents-new-digital-assets-executive-order/*
[16] *https://twitter.com/aredbord/status/1500116597607915527?s=21*

for personnel and technology, while more and more are demanded of them.[17] Empower FinCEN to use the data already coming to them before burdening them—and industry—with additional data collection for which they will be asked what good use they made of it. They are being set up for failure by unfunded mandates.

2. Second, resource and expansively clarify the AML and Kleptocracy whistleblower programs. The AML Whistleblower Program should explicitly include sanctions evasion and any violation of money laundering laws in 18 U.S.C. §1956, not just BSA violations, so that everyone is clear to crowd-source leads related to corruption and abuse, and that it is "administrative" forfeiture amounts that are excluded from awards. Also, provide the separate Kleptocracy Whistleblower Program with dedicated funds and much higher caps, for the people risking their lives under autocratic regimes. Not resourcing whistleblower programs is doubly bad because it sets them up for failure, which undermines the whole system of people who want to help—from whistleblowers to overburdened public servants.
3. Third, reduce global regulatory arbitrage. According to Chainalysis, crypto–money-laundering activity is "heavily concentrated . . . at a surprisingly small group of services," which we know to be foreign, high-risk, centralized exchanges.[18] With limited resources, we must prioritize. Help the diligent U.S. exchanges working hard to do things right. Further, until there are global registration standards to identify trusted exchanges to send personal information, industry cannot implement the Travel Rule. Congress should press U.S. FATF representatives to focus on standardized licensing across jurisdictions, instead of FATF developing new, expansive definitions of "Virtual Asset Service Provider" that include software developers in a way that FinCEN cannot implement under our Constitution.

In closing, thank you again for this opportunity. Conversation is the fastest and most democratic way to ensure we are not underestimating or overestimating nuanced risks and opportunities. That is also the value of robust Notice and Comment periods for rulemakings, for which I argued strenuously with Secretary Mnuchin around the rushed wallets rulemaking that I opposed. We cannot claim to know more than all of the public. That is not how we best protect and empower. Your invitation shows dedication to discourse, and I am so grateful.

Our President issued an Executive order last week that lays out an ambitious and thoughtful approach to empowering innovation to increase the innovative resilience and economic strength of our country—clear national security goals. All I ask is that you give our Nation and President that chance to complete the studies so that we are clear on opportunities and real risks before rushing ahead of the smart and dedicated public servants working hard for years to protect and empower our country's and the world's democratic values. We compete with China and Russia through the power of ideals and democratic freedom that show the world what is possible such that they want to join us. Democratic discourse and personal sovereignty are foundational to our country. And, as we see in the unified solidarity with Ukraine, principles are a key national security defense in the global battlefield of ideas and ideals.

I will end with a quote engraved at the National Memorial for Peace and Justice, informally known as the National Lynching Memorial, to remind us that personal sovereignty requires vigilance, and that we always need a dynamic tension of personal empowerment in relation to the potential for politically sanctioned injustice, which is hardly far in our rearview mirror. Thinking also, in his own personal, local way, of my grandfather, who as justice of the peace got up everyday knowing that justice is a constant struggle for many. And of course thinking of so many people around the world living this right now, and our obligation to do better:

For the hanged and beaten.
For the shot, drowned, and burned.
For the tortured, tormented, and terrorized.
For those abandoned by the rule of law.
We will remember.
With hope because hopelessness is the enemy of justice.
With courage because peace requires bravery.
With persistence because justice is a constant struggle.
With faith because we shall overcome.[19]

Thank you.

---

[17] *https://financialservices.house.gov/news/documentsingle.aspx?DocumentID=407592*
[18] "2020 Chainalysis Crypto Crime Report", p.10.
[19] *https://ideas.ted.com/this-is-sacred-ground-a-visit-to-the-lynching-memorial-in-alabama/*

PREPARED STATEMENT OF MICHAEL CHOBANIAN

FOUNDER OF KUNA EXCHANGE, PRESIDENT OF BLOCKCHAIN ASSOCIATION OF UKRAINE

MARCH 17, 2022

My name is Michael Chobanian, and I am a Ukrainian fintech entrepreneur and crypto enthusiast. In 2014, I founded KUNA—Eastern Europe's first Bitcoin agency which has since transformed into a full-fledged cryptocurrency exchange with more than 450,000 users worldwide.

On February 24th, the Russian Federation attacked my homeland with a full-scale war. Thousands of civilians have been killed and hundreds of homes have been destroyed. By the Ministry of Finance's accounts, the damage from the Russian invasion has already amounted to $500 billion dollars—and the number rises daily.

From the invasion's first moment, we at KUNA decided to act swiftly to help our army and the people who suffered most due to these horrific events. In collaboration with the Ministry of Digital Transformation and the Ministry of Defense, our team launched the official Crypto Fund of Ukraine to solicit cryptocurrency donations. The majority of funding comes through crypto assets such as Bitcoin and Ethereum, where AML technologies (e.g., Chainalysis, Crystal Blockchain) have been successfully implemented. All crypto that we received and converted was analyzed for illegal activity. These solicited funds are used to purchase much needed medical supplies, military equipment, and humanitarian aid here in Ukraine.

As of today, the Fund has collected more than $50 million dollars in donations, while shooting for a $100 million dollar goal.

One of our top priorities throughout this fundraise was to ensure the transparency of the donation process. While KUNA is providing the technological platform for crypto donations, the Ukrainian Government—specifically, the Ministries of Digital Transformation and Defense have ultimate control of the funds and it is they who are responsible for the fund's distribution. KUNA is serving a strictly technical and organizational role in the fundraising process and coin management—crypto banking.

I would also like to address the sanctions many crypto platforms are currently imposing on Russia-based crypto accounts. Being the founder of a crypto exchange and a Ukrainian patriot, I have decided to cease all support for the Russian ruble on KUNA. Although it wasn't an easy decision, I believe it was the right one. We can't support Russia while Ukrainian people are being killed and cities are being bombed and attacked by ballistic missiles. Many crypto platforms adopted similar initiatives such as blocking the accounts of sanctioned Russian officials and businessmen who support Putin's regime.

I am sure that you will do everything possible to protect Ukraine, Europe, and the entire democratic world from bloody authoritarian Russian aggression. To stop Russia in its tracks, and to bring about a more democratic world with personal freedom through cryptocurrency, we appeal to crypto exchanges worldwide, including Binance, to block any interaction with sanctioned individuals until the fall of Putin's regime and end of aggression against Ukraine.

Nevertheless, crypto remains a viable option for Russians who oppose the war and wish to stand up against Putin's regime. The ruble has already reached historical lows and keeps falling, while Russia's GDP has lost $30 billion, or 9 percent, in 2022. Many civilians justifiably fear the seizure of retail deposits and want to protect their capital. Purchasing digital assets is an effective means by which ordinary Russian citizens can demonstrate their opposition to Putin's regime by moving their savings out of the financial system of the Russian ruble.

By concluding, I would like to thank the U.S. Senate for the opportunity to stand here and speak on these vital issues. Our Nation is eternally grateful for all the help given by our international friends and partners. I truly believe that the unprecedented global unity and support for Ukraine during this unmerited, unwanted, and unnecessary bloodshed can put and end to Putin's reign of terror and lead to an even brighter future for tomorrow.

Slava Ukraine!

PREPARED STATEMENT OF SHANE STANSBURY

ROBINSON EVERETT DISTINGUISHED FELLOW IN THE CENTER FOR LAW, ETHICS, AND NATIONAL SECURITY, AND SENIOR LECTURING FELLOW, DUKE UNIVERSITY SCHOOL OF LAW

MARCH 17, 2022

Chairman Brown, Ranking Member Toomey, and distinguished Members of the Committee, thank you for the opportunity to testify today.

I am a Senior Lecturing Fellow in Law and the Robinson Everett Distinguished Fellow in the Center on Law, Ethics, and National Security at Duke University School of Law. At Duke, I teach primarily in the areas of cybercrime and national security law.

I previously spent more than 8 years as a Federal prosecutor in the U.S. Attorney's Office for the Southern District of New York (SDNY). At SDNY, I spent much of my time investigating and prosecuting transnational crimes, including terrorism, cybercrime, international narcotics trafficking, money laundering, international public corruption, and global weapons trafficking. I also served as a representative in the Department of Justice's (DOJ) National Security Cyber Specialists Network.

Although my testimony is based on my experience as a prosecutor and my current academic work, I am testifying today on my own behalf. No organization has paid for or approved this testimony.

Introduction

Criminals have always sought to take advantage of new forms of technology to facilitate their illegal activity. Over the last two decades, the pace at which they have done so has increased dramatically as the internet, social media, smartphones, and other innovations have changed the way we communicate and do business. I witnessed these rapid changes firsthand as a Federal prosecutor focused on terrorism, international narcotics trafficking, and other transnational crimes.

For example, my colleagues and I saw new digital communication methods revolutionize the way terrorist organizations recruit members, spread propaganda, and carry out operations. An early example was the launching in 2010 by al Qaeda in the Arabian Peninsula (AQAP) of a digital English-language magazine that could be easily distributed around the world through social media channels. Not long after that, we saw the Islamic State of Iraq and al Sham (ISIS) take that strategy to another level. The group expanded its reach by exploiting a variety of platforms, including social media networks such as Twitter and Facebook and encrypted messaging apps like Telegram. These technologies allowed the group to reach individuals around the world at a speed and scale previously unthinkable—sometimes to devastating effect. Of course, these new technologies did not just benefit terrorists. Drug traffickers and criminals of all types were quick to adopt social media, encrypted messaging apps, and other tools to better communicate with one another and carry out their illicit operations.

In the same way these technologies revolutionized the way terrorists and criminals communicate, cryptocurrency has provided new avenues for how they finance illegal activities. I will describe some of those avenues in a moment. But it is worth noting at the outset that in its current form cryptocurrency presents challenges that are in some ways distinct from technologies previously adopted by bad actors. Because of their principal features, cryptocurrencies can often act as magnets for criminal activity. They are decentralized, borderless, and most provide a high degree of anonymity. Add to these features other advantages—such as convenient access, storage, and transfer—and it is not hard to see why many criminals are attracted to cryptocurrency.

How Criminals Use Cryptocurrency To Facilitate Criminal Activity

As DOJ has explained, criminals can exploit cryptocurrency in several different ways, including (1) using cryptocurrency to facilitate the commission of crimes, or to support terrorist activity; (2) using cryptocurrency to illegally hide financial activity, such as through money laundering or sanctions evasion; and (3) committing crimes within the cryptocurrency market itself. [1] I will highlight a few examples of each of these types of activities.

The most obvious way cryptocurrency has changed the criminal landscape is simply by making some crimes easier to commit and harder to detect. By avoiding or

[1] U.S. Dep't of Justice, "Report of the Attorney General's Cyber Digital Task Force: Cryptocurrency Enforcement Framework" (Oct. 2020), at 5–6, available at: *https://www.justice.gov/archives/ag/page/file/1326061/download*.

minimizing cash transactions or bank transfers, criminals can seek to accomplish more easily one of their chief objectives—not getting caught.

My colleagues at SDNY saw this phenomenon firsthand in the early days of Bitcoin's adoption, when they were investigating the now infamous Silk Road website, which allowed users to buy and sell illegal drugs and other unlawful goods and services anonymously and beyond the reach of law enforcement. Bitcoin was the established currency on Silk Road, and it served as the perfect vehicle for anonymous, illegal transfers. With criminals free to buy, sell, and trade without ever having to exchange cash or deposit money in a mainstream account, the website flourished. At the time of its seizure in 2013, Silk Road was considered the most sophisticated criminal marketplace on the internet, having been used by several thousand drug dealers to distribute hundreds of kilograms of illegal drugs. [2]

Since that time, cryptocurrency has grown even more popular—and unfortunately so has its use in criminal conduct. Cryptocurrency is now used in connection with a broad array of illicit activity, ranging from child exploitation and human trafficking to extortion and fraud. [3] According to one estimate, illegal cryptocurrency transactions reached a record total of more than $14 billion in 2021. [4] There are also signs that terrorists may be turning to cryptocurrency to finance their operations. In August 2020, DOJ seized millions of dollars as part of a wide-scale seizure of cryptocurrency tied to the al Qassam Brigades (Hamas's military wing), al Qaeda, and ISIS. [5]

Perhaps nowhere is cryptocurrency's role in criminal activity more vivid than in ransomware attacks. [6] As many are aware, ransomware is not just a growing problem for U.S. businesses, [7] but also a serious threat to public safety and national security. The hack of Colonial Pipeline in 2021 was perhaps the most visible reminder of this fact, but it did not stand alone. In 2021, U.S. agencies observed incidents involving ransomware against 14 of the 16 U.S. critical infrastructure sectors. [8] Thousands of hospitals, school districts, city governments, and other institutions in the U.S. have been impacted in recent years by this modern-day hostage scheme.

Cryptocurrency's primary appeal for ransomware criminals is the same as for other cybercriminals: obscurity. Indeed, cryptocurrency's central features make it particularly well-suited to the model of ransomware that has emerged in recent years. Under the so-called "Ransomware-as-a-Service" (RaaS) model, a developer typically licenses ransomware tools to affiliates, sometimes in exchange for a share of ransomware payments. [9] As is the case with other types of illicit monetary transfers, payments in ransomware attacks often do not travel directly from the victim to the perpetrators, but rather through multiple layers involving different entities, each of which may or may not be part of a regulated financial market.

The cryptocurrency market offers multiple opportunities for obfuscation along the path from payor to payee. One well-known technique is the use of "mixing" or "tumbling" services, which allow for the commingling of legitimate cryptocurrency trans-

---

[2] "Manhattan U.S. Attorney Announces the Indictment of Ross Ulbricht, the Creator and Owner of the 'Silk Road' Website", U.S. Dep't of Justice (Feb. 4, 2014), available at: *https://www.justice.gov/usao-sdny/pr/manhattan-usattorney-announces-indictment-ross-ulbricht-creator-and-owner-silk-road*.

[3] DOJ Cryptocurrency Enforcement Framework, supra n. 1, at 6–7. See also U.S. Gov't Accountability Off., GAO-22-105462, "Virtual Currencies: Additional Information Could Improve Federal Agency Efforts To Counter Human and Drug Trafficking", (Dec. 2021), available at: *https://www.gao.gov/assets/gao-22-105462.pdf*.

[4] Chainalysis, "The 2022 Crypto Crime Report" (Feb. 2022), at 3, available for download at: *https://go.chainalysis.com/2022-Crypto-Crime-Report.html*.

[5] "Global Disruption of Three Terror Finance Cyber-Enabled Campaigns", U.S. Dept. of Justice (Aug. 13, 2020), available at: *https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns*.

[6] See, e.g., Erik Schatzker, "FBI Calls Crypto 'Only Game in Town' as Ransomware Flourishes", Bloomberg.com (Feb. 16, 2022), available at: *https://www.bloomberg.com/news/articles/2022-02-16/fbi-calls-crypto-only-game-intown-as-ramsonware-flourishes*.

[7] U.S. Dep't of the Treasury, Fin. Crimes Enf't Network, Financial Trend Analysis: "Ransomware Trends in Bank Secrecy Act Data Between January 2021–June 2021" (Oct. 15, 2021), at 1 (describing ransomware as "an increasing threat to the U.S. financial sector, businesses, and the public"), available at: *https://www.fincen.gov/sites/default/files/2021-10/Financial%20Trend%20Analysis-Ransomware%20508%20FINAL.pdf*.

[8] Cybersecurity & Infrastructure Security Agency, Alert (AA22-040A): "2021 Trends Show Increased Globalized Threat of Ransomware", (Feb. 9, 2022), available at: *https://www.cisa.gov/uscert/ncas/alerts/aa22-040a*.

[9] Institute for Security and Technology, Combatting Ransomware (Apr. 2021), at 16–17, available at: *https://securityandtechnology.org/wp-content/uploads/2021/09/IST-Ransomware-Task-Force-Report.pdf*.

missions with those involving illicit payments, thereby making the criminal activity harder to trace. [10]

Another established method is "chain hopping," whereby criminals move illicit transmissions from one cryptocurrency to another using some form of cryptocurrency exchange. By using this method, criminals shift their digital trail from one cryptocurrency's blockchain to another cryptocurrency's blockchain, again making the illicit assets much harder to trace. [11]

A final example is the use of a so-called "privacy coin," such as Monero, to obfuscate illicit transactions. Unlike a cryptocurrency like Bitcoin, which relies on a public blockchain and reveals some information about the transaction itself (albeit not specific identifying information about the participants), a privacy coin generally adds another layer of anonymity by obscuring virtually all details of the transaction. [12]

These and other obfuscation methods make cryptocurrency attractive not only for the actual execution of crimes like ransomware, but also for money laundering and other efforts to conceal and promote criminal conduct. That criminals would adopt this new tool is not surprising. As a prosecutor, I regularly witnessed drug traffickers and corrupt officials look for innovative methods to avoid the scrutiny of U.S. financial authorities, particularly when they were trying to move money across borders.

But some of cryptocurrency's features—such as decentralized operation and control, and opportunities for anonymity—make it particularly enticing as a money laundering instrument. Criminals seeking to move illicit funds across borders can avoid risky intermediaries; they may have a network of options available at the click of a button. Their work is made easier by actors who expressly build technologies to reduce or avoid regulatory compliance. Indeed, as cryptocurrencies become more common and accepted, criminals could choose to keep their profits in cryptocurrency for use in other illicit activities.

Finally, cryptocurrency itself can create entirely new avenues for criminal activity. As DOJ has noted, because of cryptocurrency's features and the fact that much of its market is characterized by opaqueness, wallets and exchanges can become attractive targets for theft and fraud. [13] By one estimate, last year criminals stole approximately $3.2 billion worth of cryptocurrency and earned more than $7.8 billion from cryptocurrency-related scams. [14] As cryptocurrency grows in popularity, these crimes could increasingly harm the general public and less sophisticated investors. And the threat is not just from ordinary criminals. Rogue Nation States have turned to cryptocurrency theft and other crimes to finance their regimes, as witnessed by North Korea's reported theft of hundreds of millions of dollars in cryptocurrency. [15]

The Challenges Cryptocurrency Presents for Law Enforcement

The same factors that make cryptocurrency attractive to criminals can present challenges for prosecutors and law enforcement agents seeking to stop illicit activity.

As I mentioned previously, criminal actors are always looking for new ways to commit crimes or hide their illicit proceeds. Some find particularly clever methods for covering their tracks, and it is the job of investigators and prosecutors to use the tools at their disposal to find and assemble the pieces of the evidentiary puzzle.

When my colleagues and I investigated international money laundering cases, dedicated investigators spent countless hours analyzing records requested from financial entities to establish the use of shell companies, phony accounts, and other means to conceal the transfer and ownership of illicit funds. We were often successful because of the cooperation of international partners and because of the financial information made available by regulated institutions that followed their compliance and disclosure obligations. But much of the cryptocurrency ecosystem operates outside of the universe of resources that prosecutors and investigators routinely rely upon to gather the information they need to establish criminal malfeasance.

To be sure, law enforcement is getting much better at tracing digital assets used to commit and cover up criminal activity. With forensic blockchain analysis and access to other helpful information, like know-your-customer (KYC) information pro-

---

[10] See, e.g., "DOJ Cryptocurrency Enforcement Framework", supra n. 1, at 41–44.
[11] See, e.g., id.
[12] See, e.g., id. at 4, 41.
[13] See, id. at 15–16.
[14] "Chainalysis 2022 Crypto Crime Report", supra n. 4, at 5–6.
[15] Kevin Collier, "North Korea Stole a Record $400 Million in Cryptocurrency Last Year, Researchers Say", NBC News (Jan. 13, 2022), available at: *https://www.nbcnews.com/tech/security/north-korea-stole-record-400-million-cryptocurrency-last-year-research-rcna12080*. See also DOJ Cryptocurrency Enforcement Framework, supra n. 1, at 1, 16 (describing the threats posed by North Korea, including through illicit mining of cryptocurrency).

vided by regulated entities, law enforcement can penetrate the otherwise opaque world of illicit cryptocurrency transfers. Last year, we witnessed DOJ recover a substantial portion of the $4.4 million in ransomware payments made in connection with the Colonial Pipeline attack discussed previously.[16] And just last month, DOJ recorded its largest financial seizure ever when it recovered $3.6 billion in cryptocurrency allegedly related to the 2016 hack of the virtual currency exchange Bitfinex.[17] These are indeed promising and welcome developments.

It would be somewhat naive, however, to conclude from these developments that tracing and recovering cryptocurrency assets is always easy—or even always possible. Even with the latest blockchain analytics, investigations can take years to complete. Frequently, the hardest part of a cyber-related prosecution is demonstrating what investigators sometimes refer to as "hands on the keyboard." Digital breadcrumbs left by criminals can prove invaluable to investigators. But ultimately prosecutors must demonstrate that an identifiable person is behind the criminal activity. And in a criminal case, that identity must be established beyond a reasonable doubt. That is, of course, as it should be, but in cryptocurrency-related cases prosecutors will often have the distinctive challenge of relying on a very complex series of digital patterns and transactions to meet their burden.

That crucial connection of a criminal's identity to their criminal conduct is one of the main challenges posed by cryptocurrency. A public blockchain can be helpful, but often it can get one only so far. Prosecutors can spend years trying to penetrate the layers of obfuscation by savvy criminals. Even if they succeed, they may still face obstacles due to the current state of the cryptocurrency market.

Criminal investigations are only as successful as the information available. Sometimes prosecutors and investigators will get the information they need. For example, if a cryptocurrency exchange used by a criminal is complying with KYC and other regulatory requirements, that may provide the information needed for learning the criminal's identity or developing other leads. But too often this is not the case. Not all cryptocurrency platforms comply with existing regulations, and many operate in jurisdictions with less stringent requirements or beyond the reach of relevant treaties.

This information gap could grow wider if more cryptocurrency platforms move to a decentralized model or if more anonymous instruments such as privacy coins gain wider adoption. This is a remarkable period for technological innovation. Blockchain technology offers fascinating possibilities for the future, and I look forward to seeing how it might be applied to enrich our society. But we should also recognize the serious role that cryptocurrency is playing in criminal activity. Only then can we take the steps necessary to protect our health, our safety, and our national security.

---

[16] "Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside", U.S. Dep't of Justice (Jun. 7, 2021), available at: *https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside*.

[17] "Two Arrested for Alleged Conspiracy To Launder $4.5 Billion in Stolen Cryptocurrency", U.S. Dep't of Justice (Feb. 8, 2022), available at: *https://www.justice.gov/opa/pr/two-arrested-alleged-conspiracy-launder-45-billion-stolen-cryptocurrency*. It should be noted that this case is pending and the criminal charges remain allegations.

RESPONSES TO WRITTEN QUESTIONS OF CHAIRMAN BROWN FROM JONATHAN LEVIN

Q.1. In your oral testimony, you noted that, with respect to the use of digital assets in illicit finance, there is a distinction between "the ability to see the money versus seize the money." You also noted that even when there is "100 percent degree of transparency about where the money was actually going," the "operation . . . to recover the funds . . . is not always 100 percent possible."

Please discuss the challenges involved in seizing or recovering digital assets that are identified as illicit.

A.1. With traditional finance, if you find the funds, they are either in tangible cash/assets you can seize or are held by a centralized third-party financial institution who in many cases you can require to hand over control of the assets through appropriate legal process. This is not always the case in the decentralized world of digital assets.

Law enforcement seizures of digital assets are generally the result of three possible scenarios. The first involves quality investigative work that leads law enforcement to finding the information they need—such as a criminal's private keys or recovery seeds—to seize their ill-gotten gains from their private wallet. The second involves serving legal process, such as a seizure warrant, on a service or financial institution where the funds may be located—like a digital asset exchange—that has custody of a criminal's illicit funds. And the third involves the criminal, coconspirators, or accomplices agreeing to turn over the funds, usually as a form of cooperation.

Save for these scenarios, it can be quite difficult to seize and recover funds. This means if you track the funds and they are in a private wallet, exercising control over those funds to recover them requires you to obtain the access credentials for the private wallet yourself.

In spite of these challenges, we have seen law enforcement demonstrate success in this regard, leading to significant asset seizures, such as the recent DOJ seizure of $3.6 billion in stolen digital assets directly linked to the 2016 hack of Bitfinex, a digital asset exchange. There will be some cases in which illicit wallets may have been identified, but do not produce immediately actionable results.

There are two scenarios we outline below: challenges in seizing funds held in private, or noncustodial wallets, and challenges in seizing funds held by digital asset exchanges.

Seizing Funds Held in Private Wallets

If digital assets are held in a private wallet controlled by private keys known only by the owner of that wallet, there is generally no third party (such as a bank or financial institution like in traditional finance) that you can require to provide control of those funds/assets to you. This is true even if you know where the funds are located (e.g., digital asset wallet address). That said, if law enforcement obtains the private keys or recovery seeds for a criminal's personal wallet, or if they are able to obtain cooperation from them or their collaborators, they may be able to seize the funds.

There are potential exceptions. For example, Tether has some centralized aspects to it. The Tether white paper suggests they can

freeze and even burn Tether stored on an address and reissue equivalent value tokens to, say, the victim of stolen funds or seizing Government agency.

If you can't access the private wallet to move the funds, regardless of being able to see them or knowing where those funds are stored (in which addresses) you have no way to exert control over them to seize them. It is, however, possible to "watch" these wallets using blockchain analysis tools to see if they move in the future. Eventually criminals will want access to their funds and will need to move them to an off ramp, such as a digital asset exchange. The November 2020 seizure of $1 billion of bitcoin seized in relation to the Silk Road case is a great example of law enforcement being able to watch and seize funds years later.

Seizing Funds Held by Digital Asset Exchanges

In addition, it will not always be possible to seize funds which have been tracked to a custodial wallet. Legal challenges may frustrate seizure orders from one jurisdiction from being exercised or executed in another jurisdiction. Some jurisdictions or exchange services are cooperative, and others are not, either because they are not yet regulated, or because they are noncompliant. Some digital asset exchanges have detailed contact information and instructions for serving legal process and others have limited contact information, are nonresponsive, or may be engaged or controlled by an illicit service. These enforcement issues are not unique to digital assets as similar challenges exist with traditional finance. However, they can be amplified given the decentralized and cross-border nature of some of these services which may or may not be registered in the jurisdictions in which they operate.

Q.2. Approximately how frequently is law enforcement able to convert the identifications of illicit wallets into successful investigations? In other words, please discuss your understanding of the proportion of known illicit wallet addresses that are ultimately implicated in indictments or illicit asset seizures.

A.2. There have been a number of seizures that have been publicized recently, including in the Silk Road, Colonial Pipeline, and Bitfinex cases. While we work with a number of Government agencies, including law enforcement agencies, we do not have statistics on the number of cases involving digital assets they are working or what percentage of wallet addresses Chainalysis has identified as associated with illicit activity are being actively investigated, leading to indictments or seizures. We would defer to the Department of Justice, the Department of Homeland Security, the Department of Treasury, the U.S. Postal Inspection Service, and the many State and local law enforcement agencies who conduct investigations into the illicit use of digital assets.

It may also be of interest that we are able to account for both the sum amount of cryptocurrency holdings that can be traced back to illicit sources, as well as the total balances of criminal whales, meaning criminals holding $1 million or more in cryptocurrency. We outline this in this blog post: "Criminal Whales Hold over $25 Billion in Cryptocurrency From Multitude of Illicit Sources" from

February 2022: *https://blog.chainalysis.com/reports/2022-crypto-crime-report-preview-criminal-balances-criminal-whales/*.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR REED FROM JONATHAN LEVIN

Q.1. The Chainalysis 2022 "Crypto Crime Report" finds that "[t]ransactions involving illicit addresses represented just 0.15 percent of cryptocurrency transaction volume in 2021 despite the raw value of illicit transaction volume reaching its highest level ever."

Please describe the caveats and qualifications with relying on this statistic as an indicator of illicit finance activity conducted using cryptocurrency.

A.1. In our research for the "Crypto Crime Report", and for our research more broadly, we only count criminal wallets that we have attribution on. This means that we are missing wallets we don't know to be related to crime. Considering we are always learning about new wallets and clustering new services, our data improves with time. For example, at the time of writing last year's Crypto Crime Report, we reported 2020's illicit share of cryptocurrency activity to be 0.34 percent. But a year later, when we recalculated that metric based on additional intelligence, that number rose to 0.62 percent. The reason for the change is the identification of more addresses associated with illicit activity that were active in 2020.

In addition, we don't include in our high-level estimates crime that is conducted off-chain, or not "cryptocurrency native". When we refer to something as "cryptocurrency native", we mean that the crime is practically dependent on cryptocurrency, or inherently intertwined with it. For example, darknet markets run entirely using cryptocurrency. It is easy to identify their customers and vendors by examining the flow of funds going into and out of those wallets. However, investigators sometimes encounter criminals engaged in traditional, non-cryptocurrency native crimes, such as traditional drug trafficking that occurs on the streets but uses cryptocurrency to pay distributors or launder illicit proceeds. In these cases, the funds on-ramp (likely through a VASP) from fiat, rather than moving from an identified illicit service, so it may be more difficult to determine that the funds are illicit proceeds. However, once investigators determine that someone they are investigating is using cryptocurrency to launder their illicit proceeds—perhaps via bank records they have obtained via legal process showing fund transfers to cryptocurrency exchanges—they can serve legal process to any VASPs shown on the bank records, obtain associated cryptocurrency addresses, and conduct blockchain analysis to determine how the cryptocurrency is being used.

Q.2. Please provide Chainalysis' most recent available figure regarding cryptocurrency transaction volume involving illicit addresses.

A.2. According to a calculation done on April 14, 2022, total illicit transaction volume for 2022 YTD is $8.69B, compared to $2.5T in total economic activity. This means that the illicit share is 0.35 percent of all transaction volume in 2022 YTD. This figure includes

the seized funds associated with the Bitfinex hack, which totaled $3.65 billion. The percentage of all transaction volume associated with illicit wallets is approximately 0.2 percent without the funds associated with that one incident.

RESPONSES TO WRITTEN QUESTIONS OF CHAIRMAN BROWN FROM MICHAEL MOSIER

Q.1. At the hearing, you discussed how a public blockchain ledger provides certain advantages for law enforcement with respect to tracing illicit transactions, as compared to cash.

Do digital assets also provide illicit actors advantages as compared to cash, specifically in illicit actors' ability to quickly make large, cross-border transactions? What are they, if so?

A.1. In thinking about the advantages of digital assets over cash—whether for illicit or licit actors—it is helpful first to recognize that we have had digital versions of cash for many years, in the form of wire transfers, ACH, and digital payments through banks and money services businesses (MoneyGram, Western Union, Venmo, Zelle). For clarity in my response, I will refer to "cryptocurrency," to distinguish from long-existing "digital payments," since the cryptographic security that allows for a public ledger is a distinguishing feature. In the same way that digital payments over the last several decades provide speed and volume advantages to carrying physical cash, so do recent evolutions in cryptocurrency that are based on a cryptographically secure, public digital ledger. Like wire transfers, each cryptocurrency transaction is pseudonymous, with cryptographically determined alphanumeric identifiers. In contrast to prior/existing digital payments, cryptocurrency transactions are on a public ledger, so can be traced nearly indefinitely forward and backward, whereas a traditional financial institution can only see a transaction as far as the next recipient financial institution—or less, in the instance of cash.

In traditional finance and prior digital payments, pseudonymous wire transfer identifiers are connected to "identities" that are spoofed, bought, created out of shell companies, or hidden behind several layers. Likewise, there are challenges in the cryptocurrency space with concretely connecting the alphanumeric identifiers of an address. However, it is important to note that, in contrast to the opacity of wire transfers that use pseudonymous identifiers within an interbank messaging system that is not publicly visible—and certainly not visible beyond the next recipient—cryptocurrency on the public ledger can be viewed for many, many transactions forward and backward. Therefore, cryptocurrency's theoretical benefits to illicit actors in terms of speed and volume are also undercut by the public visibility through blockchain analytics and even saavy public watchers of block explorers to identify activity that indicates suspicious transactions. That makes it very difficult to move substantial sums through cryptocurrency without being detected as major money movements. Indeed, there are multiple "whale watchers" in the public who call out significant cryptocurrency movements for public notice of either potential market-impacting transactions or suspicious activity, such as positioning for an exploit or trying to cash out hack proceeds at an exchange.

The cash-out point highlights that the ability to buy real world goods and services with cryptocurrency remains quite limited. It would be difficult to pay your mortgage, tuition, car payments, fuel, groceries, utilities, etc., using cryptocurrency. Therefore, users generally need to exchange their cryptocurrency for fiat currency through a registered virtual asset service provider (VASP), which, at least in the United States, requires Know Your Customer (KYC) practices, like traditional money services businesses. Therefore, the identity risk level in cryptocurrency is not greater than fiat digital payments money services businesses transactions. In fact, there is much greater public transparency in cryptocurrency, including for VASPs to monitor transaction activity far beyond the next hop, compared to the opacity of fiat digital payments and limited visibility to one "hop," therefore lending greater ability to assess direct and indirect risk in cryptocurrency.

In addition, distinct from the opacity of fiat digital payments, in virtual assets, the entire public sees transfers on the blockchain. We have seen repeatedly that the broader public collectively detects suspicious activity even before the more limited law enforcement resources and calls out the activity publicly. Indeed, in multiple instances the public exposure and collective action has led attackers to return the money. That collective vigilance is not possible with opaque fiat digital transfers. Further, the immutable, publicly visible ledger for cryptocurrency provides a long term, reliable record that cannot be unilaterally changed. Therefore, for law enforcement purposes, evidence is effectively preserved, while investigations can continue. That provides more time for law enforcement to investigate before trails run cold. For example, in February 2022, the Department of Justice solved a prior cyber hacking case where approximately $4.5 billion (in today's value) was stolen from a hacked exchange that occurred in 2016.[1] The persistant visibility of the hacked funds on a public ledger enabled something that would be almost unheard of in fiat currency to solve so many years later with so much of it still in place, rather than largely spent, due to the need to off-ramp cryptocurrency but difficulty of doing so, when the public funds have been determined to be tainted. Indeed, the couple was arresting while still trying to cash out to fiat, 6 years later.

Therefore, while there are speed advantages to cryptocurrency over cash—just like there have long been speed advantages to fiat digital payments for many years—cryptocurrency has far more traceability, with a permanent trail and public visibility. In light of that, an illicit actor choosing pragmatically is more likely to prefer the limited visibility of fiat digital payments over cryptocurrency, or stick with the true anonymity of cash, precious metals, or other trade-based laundering like oil or coal. Indeed, the lack of transactional privacy from every public eye has been a limitation on the use of cryptocurrency in the business payments space.

Q.2. On cross-border activity, do you think a new cross-border rule from FinCEN would help law enforcement by providing them with more information to address those problems? Please explain.

---

[1] *https://guardian.ng/news/american-couple-arrested-for-planing-to-launder-4-5-billion-stolen-bitcoin/*

A.2. I encourage you to contact FinCEN for the latest assessment of law enforcement's needs and whether reporting of cross-border electronic funds transfer information would be helpful to their efforts. Such a rule would need to be carefully considered, and balance the benefits to law enforcement with the substantial costs it would likely impose on both the public and on FinCEN. As you know, FinCEN is currently developing the beneficial ownership database required by the Corporate Transparency Act despite not receiving the promised funding from Congress, as noted in my written testimony, so I am hesitant to add unfunded mandates without their buy-in.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR REED FROM MICHAEL CHOBANIAN

Q.1. During an interview on March 19 with CoinDesk TV, you stated that "[t]he problem with Binance is not just that they still continue working on both sides, it's that they showed cooperation with the Russian Government before the war, and as far as I know, they still continue cooperating with the Russian Government." Please describe your understanding of how Binance, one of the largest cryptocurrency exchange in the world, is "cooperating with the Russian Government."

A.1. At the time of the publication on Coindesk, my statement was based on the information that I received from the "market". Now we have a research by Reuters that sheds light on the operations of Binance in Russia. *https://www.reuters.com/technology/how-crypto-giant-binance-built-ties-russian-fsb-linked-agency-2022-04-22/*

RESPONSES TO WRITTEN QUESTIONS OF CHAIRMAN BROWN FROM SHANE STANSBURY

Q.1. As discussed at the hearing, blockchain technology can enable the tracing of illicit transactions to specific wallets. What challenges does law enforcement face in using tracing data to seize illicit assets or arrest illicit actors?

A.1. Even when investigators are equipped with blockchain tracing information, they face the challenge of linking illicit transactions to specific individuals or entities. That challenge is made more difficult in today's regulatory environment because part of the cryptocurrency market remains opaque. If a bad actor uses a cryptocurrency platform that is complying with know-your-customer (KYC) and other regulatory requirements, the information gained can help bridge the gap between illegal activity and a person's identity. Too often, however, bad actors are able to use services that do not comply with—or are not subject to—existing regulations and/or operate in jurisdictions with less stringent requirements. [1] As a result, criminal conduct can go undetected by law en-

[1] See, e.g., Financial Action Task Force (FATF), "Second 12-Month Review of Revised FATF Standards—Virtual Assets and VASPs" (July 5, 2021), at 2 (finding that 70 of 128 reporting jurisdictions had not yet implemented FATF's revised standards for virtual assets, and that the "lack of regulation or the lack of enforcement of regulation in jurisdictions is allowing for juris-

Continued

forcement, and even illicit transactions identified through blockchain analysis can remain unattributed. Law enforcement may face even greater information gaps in the future if, for example, more cryptocurrency services move toward a decentralized model not run by a single entity or if anonymity-enhancing instruments such as so-called "privacy coins" gain wider adoption.

Jurisdictional issues also can pose challenges for law enforcement. Cryptocurrency moves quickly and easily across borders, without the need for centralized intermediaries, and illicit assets may be hosted in wallets or accounts that are beyond the reach of U.S. authorities or their international partners. For example, illicit assets located in an "unhosted" wallet (i.e., a digital wallet not hosted by a third-party institution, and which the user independently controls) that is stored locally in an uncooperative jurisdiction may be difficult to seize even with the assistance of tracing data. Likewise, a criminal defendant may reside in a jurisdiction where extradition or removal is unlikely, making arrest and prosecution more challenging.

Law enforcement authorities can face a variety of other hurdles, particularly given the range of increasingly sophisticated obfuscation methods available to criminals. However, one of the main challenges they face is one of resources. Cryptocurrency-related crime continues to rise, with growing implications for everyday Americans, and bad actors continue to find new, complex ways to obscure their illegal activity. Although private-sector firms can provide needed assistance to investigators in tracing illicit activity, that assistance is insufficient. More agents and prosecutors with relevant expertise and training are required, and they need to be equipped with the tools and support needed to develop evidence for successful prosecutions. The Department of Justice (DOJ) and investigating agencies have made important strides recently in prioritizing cryptocurrency-related crime, but Congress should ensure that they are given the funding and resources needed to keep pace with the scale and severity of the threat.

Q.2. After a wallet involved in an illicit transaction is identified, based on your experiences or observations, how long have investigations into illicit financial activity typically taken to conclude? How much time does law enforcement usually require to seize illicit assets held at a wallet known to be illicit? What are the impediments to seizing illicit assets from known wallets?

A.2. Investigations into illicit financial activity can vary in length depending on a range of factors such as the complexity and sophistication of the criminal activity, the geographic scope of the conduct, and the resources available to law enforcement. Criminal investigations also are sometimes accelerated based on law enforcement priorities, a defendant's decision to travel, or other considerations.

---

dictional arbitrage and the raising of [money laundering and terrorist financing] risks"), available for download at: *https://www.fatf-gafi.org/publications/fatfrecommendations/documents/second-12-month-review-virtual-assets-vasps.html*. See also U.S. Dep't of the Treasury, "National Money Laundering Assessment" (Feb. 2022), at 41 (observing that a "large number" of virtual asset service providers operating abroad, including those interfacing with the U.S. financial system, have "substantially deficient" anti-money laundering programs), available at: *https://home.treasury.gov/system/files/136/2022-National-Money-Laundering-Risk-Assessment.pdf*.

In some cases, investigations can move rapidly. For example, in March 2022, the U.S. Attorney's Office for the Southern District of New York charged two individuals in connection with a so-called "rug pull" involving nonfungible tokens (NFTs). According to the Government's allegations, the investigation began in January 2022, when law enforcement received reports from investors in the scam, and the defendants were arrested approximately 2 months later. [2]

Other investigations progress more slowly. For example, in 2016, U.S. law enforcement began investigating the hack of Bitfinex, a virtual currency exchange. In February 2022, almost 6 years later, law enforcement recovered some of the stolen funds and arrested two individuals accused of laundering cryptocurrency stolen in the hack. [3]

Whether and how quickly law enforcement can seize cryptocurrency from accounts known to contain illicit proceeds is fact dependent. In the Bitfinex case, for example, investigators seized a large portion of the stolen cryptocurrency shortly after gaining access to one of the relevant wallets. However, the case was exceedingly complex and took years to reach that stage. Investigators also were aided by favorable facts that helped them access the wallet and allegedly link it to the defendants. The defendants, for example, resided in New York and allegedly used email and cloud storage accounts that could be reached through U.S. process. In 2021, agents were able to obtain a search warrant for one of the cloud storage accounts, which contained a file listing 2,000 virtual currency addresses—almost all of which were linked to the 2016 hack—along with corresponding private keys. According to investigators, that information allowed them ultimately to seize, via a court order, the remaining illicit assets from the digital wallet that contained the addresses. [4]

Seizures in other circumstances can be even more challenging. Even if investigators can link a particular digital wallet to criminal conduct by a specific person or entity—which can be a difficult task in itself, given the types of obfuscation often employed—they may ultimately face jurisdictional or technical obstacles. For example, as described previously in response to Question 1, an unhosted wallet could be stored locally (and potentially offline) in a foreign jurisdiction. [5] A seizure in such circumstances could prove difficult, particularly if the relevant jurisdiction does not have a cooperative relationship with U.S. law enforcement.

---

[2] "Two Defendants Charged In Non-Fungible Token (NFT) Fraud And Money Laundering Scheme", U.S. Dept. of Justice (Mar. 24, 2022), available at: *https://www.justice.gov/usao-sdny/pr/two-defendants-charged-non-fungible-token-nft-fraud-and-money-laundering-scheme-0*. In considering the length of any investigation, it is worth noting that many criminal investigations continue after an individual defendant is arrested or assets are seized.

[3] See Complaint (Statement of Facts), United States v. Lichtenstein, No. 22-mj-00022-RMM (Feb. 7, 2022), available at: *https://www.justice.gov/opa/press-release/file/1470211/download*; "Two Arrested for Alleged Conspiracy To Launder $4.5 Billion in Stolen Cryptocurrency", U.S. Dep't of Justice (Feb. 8, 2022), available at: *https://www.justice.gov/opa/pr/two-arrested-alleged-conspiracy-launder-45-billion-stolen-cryptocurrency*. The two defendants are not charged in connection with the Bitfinex hack itself. It should also be emphasized that both cases described here remain pending, and the facts discussed remain allegations.

[4] See Complaint (Statement of Facts), United States v. Lichtenstein, supra n. 3.

[5] In the example given above from the Bitfinex case, the wallet described was unhosted, but it was within the reach of U.S. law enforcement authorities, and investigators allegedly were able to link it to identifiable U.S.-based individuals.

Q.3. Based on your observation, approximately how frequently is law enforcement able to convert identifications of illicit wallets into successful investigations? Relatedly, do you know of any law enforcement agency, or market research organization, that has identified or estimated the proportion of known illicit wallet addresses that are ultimately implicated in indictments or illicit asset seizures?

A.3. In part because of the confidential nature of law enforcement investigations, I do not know what proportion of the digital wallets that have been linked to illicit activity have been implicated in investigations or prosecutions at the federal or other levels. Nor am I currently aware of publicly available reports detailing such information, although some blockchain analytics firms publish their own estimates of various statistics relating to cryptocurrency-related crime, and other parties have begun to track cryptocurrency-related enforcement actions.[6] It should be noted that the amount of illegal conduct is likely higher than industry-reported estimates for a given year. Blockchain analytics firms routinely revise upward their own estimates of illicit transaction volume as more addresses linked to criminal activity are found.[7]

Q.4. Illicit finance investigations are complex, and often involve an array of law enforcement entities and officials. Please describe the agencies and actors typically involved in an illicit finance investigation involving digital assets. For example, the recent recovery of $4.5 billion in cryptocurrency involved several federal agencies and multiple U.S. Attorney offices.

A.4. At the Federal level, a criminal investigation of illicit activity involving cryptocurrency can include, among others:

- Prosecutors from one or more U.S. Attorneys' Offices and, depending on the nature of the case, potentially other components of DOJ (e.g., the Money Laundering and Asset Recovery Section (MLARS); the Computer Crime and Intellectual Property Section (CCIPS); the National Security Division (NSD));
- Agents from various investigative agencies, including, but not limited to, the Federal Bureau of Investigations (FBI), the Internal Revenue Service—Criminal Investigations (IRS–CI), and/or Homeland Security Investigations (HSI);
- State and local law enforcement agencies; and
- International law enforcement agencies and other partners.

In addition, in Federal criminal investigations, it is common for prosecutors and agents to coordinate with regulatory bodies such as the Securities and Exchange Commission (SEC) and the Commodity Futures Trading Commission (CFTC), as well as components of the U.S. Department of the Treasury (including, for example, the Financial Crimes Enforcement Network (FinCEN), the Office of Foreign Assets Control (OFAC), and the IRS).

---

[6] See, e.g., Chainalysis, "The 2022 Crypto Crime Report" (Feb. 2022), available for download at: *https://go.chainalysis.com/2022-Crypto-Crime-Report*; Morrison Cohen LLP, "The Morrison Cohen Cryptocurrency Litigation Tracker" (May 3, 2022), available for download at: *https://www.morrisoncohen.com/news-page?itemid=471*.

[7] See, e.g., "Chainalysis 2022 Crypto Crime Report", supra n. 6, at 4.

Q.5. The Justice Department's recent enforcement report on crypto crimes notes that the illicit use of cryptocurrency falls into three broad categories. Bad actors may exploit crypto to: (1) engage in financial transactions associated with crimes, such as buying and selling drugs or weapons on the dark web, leasing servers to commit cybercrimes, or soliciting funds to support terrorist activity; (2) engage in money laundering or shield otherwise legitimate activity from tax, reporting, or other legal requirements; or (3) commit crimes directly implicating the cryptocurrency marketplace itself, like stealing cryptocurrency from exchanges through hacking or using the promise of cryptocurrency to defraud unwitting investors. From your experience as a prosecutor and your general knowledge of the industry, which of these three categories do you think Congress should be most concerned about, and what other categories of illicit activity involving crypto should Treasury and the Justice Department prioritize in their enforcement efforts?

A.5. The Justice Department's report provides a useful framework for understanding the variety of ways cryptocurrency can be used by bad actors. However, I am not in a position to prioritize one category of cryptocurrency-related crime over others. Each type of crime can pose threats to U.S. citizens in different and important ways, and in fact the categories frequently overlap and reinforce one another. For example, criminals engaged in ransomware attacks or the defrauding of unwitting investors regularly rely on money laundering to further their illicit activities. Moreover, a range of dangerous threat actors—rogue Nation States, terrorists, and criminal networks—have proven that they will engage in harmful conduct that spans multiple categories.

Some threats, of course, do affect a broader set of victims or interests. For example, ransomware attacks, which rely almost exclusively on cryptocurrency as a means of payment, pose a serious and ongoing threat not only to U.S. businesses, but also to our national security. I trust my former colleagues at DOJ and their regulatory counterparts to identify the most serious threats based on the latest intelligence, and to set enforcement priorities accordingly. Congress should provide law enforcement and regulators with the resources necessary to act on those priorities.

ADDITIONAL MATERIAL SUPPLIED FOR THE RECORD

LETTER SUBMITTED BY NAFCU

NAFCU
3138 10th Street North
Arlington, VA 22201-2149
703.522.4770 | 800.336.4644
f: 703.524.1082
nafcu@nafcu.org | nafcu.org
National Association of Federally-Insured Credit Unions

March 23, 2022

The Honorable Sherrod Brown
Chairman
Committee on Banking, Housing, and Urban Affairs
United States Senate
Washington, DC 20510

The Honorable Pat Toomey
Ranking Member
Committee on Banking, Housing, and Urban Affairs
United States Senate
Washington, DC 20510

Re: Tomorrow's Hearing on "Strengthening Oversight and Equity in the Appraisal Process"

Dear Chairman Brown and Ranking Member Toomey:

I write to you today on behalf of the National Association of Federally-Insured Credit Unions (NAFCU) to share our thoughts on issues of importance to credit unions ahead of tomorrow's hearing entitled "Strengthening Oversight and Equity in the Appraisal Process." NAFCU advocates for all federally-insured not-for-profit credit unions that, in turn, serve over 127 million consumers with personal and small business financial service products. We would like to thank you for holding this important hearing and the opportunity to provide input on the appraisal process.

NAFCU appreciates the work of the Administration and Congress on this important issue. NAFCU has discussed the issues of appraisal modernization and appraisal bias with the U.S. Department of Housing and Urban Development (HUD) as it embarked upon its Interagency Task Force on Property Appraisal and Valuation Equity (PAVE). NAFCU has also been engaged with the Federal Housing Finance Agency (FHFA) on appraisal-related policies, practices, and processes.

Multiple studies have shown that biases in appraisals exist across the board. Freddie Mac[1] and Fannie Mae[2], the government-sponsored enterprises (GSEs), have found that appraisal disparities exist for communities and borrowers of color. The Consumer Financial Protection Bureau and other federal regulators, including the FHFA, have also acknowledged that appraisal discrimination plagues the mortgage market.[3] Appraisal reform is essential in order to address this widely recognized issue. The use of technology is a start to addressing appraisal biases. NAFCU has recommended that the FHFA work with the GSEs, other federal regulators, and The Appraisal Foundation to diversify the appraisal industry by expanding participation of people of color in the appraisal industry, updating standards to root out bias more clearly, and providing training for appraisers to understand and identify implicit bias.

[1] *Racial and Ethnic Valuation Gaps in Home Purchase Appraisals* (September 2021). https://www.freddiemac.com/research/insight/20210920-home-appraisals.
[2] *Appraising the Appraisal* (February 2022). https://www.fanniemae.com/media/42541/display.
[3] *Federal Interagency Comment Letter on Appraisal Discrimination*. (February 4, 2022). https://files.consumerfinance.gov/f/documents/cfpb_appraisal-discrimination_federal-interagency_comment_letter_2022-02.pdf.

Property value is a key determinant of borrower credit risk and an important aspect of the mortgage process. An appraisal should be an objective way to assess a home's market value. Appraisals are important to protect all parties involved in the homebuying process, including the lender, borrower, and seller, and appraisers should be objectively assessing a home's market value to ensure that the amount of money requested by the borrower is appropriate. Credit unions routinely confirm the consistency, fairness, and accuracy of appraisals they receive, and NAFCU sees the modernization of the appraisal process as a logical step to support continued innovation of the housing finance system and a way to help mitigate the risk of human error or bias.

There is a need for consistent, reliable technology to simplify the appraisal process, make it more efficient, and reduce bias and discrimination. At the same time, regulatory agencies charged with ensuring the integrity of algorithmic valuation models should take care not to develop rules that will chill innovation or prevent smaller community financial institutions from embracing new technology due to compliance costs. In other contexts, such as lending, artificial intelligence and machine learning models have demonstrated that automated processes can expand access to credit while ensuring compliance with fair lending laws.[4] The same forward thinking should be applied to appraisals.

NAFCU members also report that there is a lack of standardization between appraisers and throughout the appraisal process, the effects of which are carried over to the borrower in terms of overall costs. NAFCU supports alternative appraisal processes such as appraisal bifurcation, desktop appraisals, and exterior only appraisals, which can help with flexibility. When alternative processes, aside from traditional appraisals, can be employed, we believe lenders should be allowed the flexibility to use them at their discretion to find the best way to meet the needs of their members. During the pandemic, the Federal Housing Administration (FHA) and the Department of Veterans Affairs (VA) permitted desktop and exterior only appraisals, but the FHA has since discontinued the flexibility for desktop only appraisals and the VA has discontinued the use of both desktop and exterior only appraisals. NAFCU urges Congress to investigate this decision and require HUD to permanently permit the FHA and VA to accept desktop and exterior only appraisals for all approved mortgages. Likewise, the GSEs should continue to permit desktop only and exterior only appraisals for all mortgages they purchase from lenders.

Credit unions also continue to see significant appraisal challenges in servicing rural areas. NAFCU's member credit unions would like to provide all their products and services, including mortgage loans, to their members in the rural communities they serve. Often, credit unions are the only financial institutions in a rural community, increasing the need for a more streamlined appraisal process so that these communities have easy access to safe, affordable mortgage credit. In rural communities, the appraisal process is less efficient than anywhere else. Moreover, credit unions have been faced with severe difficulties in securing an appraiser to complete traditional appraisals in these rural areas and sometimes even in urban areas. The ability to use desktop appraisals or other alternatives as well as automated valuation models and appraisal waivers in rural areas will decrease the strain placed on NAFCU's member credit unions and their member-borrowers when it comes to financing the purchase of a home through the mortgage loan process.

---

[4] CFPB, "An update on credit access and the Bureau's first No-Action Letter," (August 6, 2019), available at https://www.consumerfinance.gov/about-us/blog/update-credit-access-and-no-action-letter/.

NAFCU believes it is important to remove bias in the appraisal process and to strive for enhanced standards and consistency for appraisers. We strongly support efforts to expand the diversity of the appraiser workforce as well, as this can help significantly to reduce bias and discrimination. The use of new technologies, including artificial intelligence and machine learning, can also pave the way for a more fair and transparent appraisal process. Although algorithmic determinations of value may present different challenges, incorporating technologies to assist in the valuation process and serve as a check on the accuracy and consistency of appraisals would likely reduce bias and discrimination.

We thank you for the opportunity to share our thoughts and recommendations and look forward to continuing to work with you on improving the appraisal process. Should you have any questions or require any additional information, please contact me or Jake Plevelich, NAFCU's Associate Director of Legislative Affairs, at jplevelich@nafcu.org.

Sincerely,

Brad Thaler

Brad Thaler
Vice President of Legislative Affairs

cc: Members of the U.S. Senate Committee on Banking, Housing and Urban Affairs

STATEMENT SUBMITTED BY AEI HOUSING CENTER

AEI Housing Center

Comments on PAVE's "Action Plan to Advance Property Appraisal and Valuation Equity: Closing the Racial Wealth Gap by Addressing Mis-valuations for Families and Communities of Color"

Edward Pinto - Director, AEI Housing Center (PintoEdward1@gmail.com)
Tobias Peter – Assistant Director, AEI Housing Center (Tobias.Peter@AEI.org)
March 2022

On March 23rd, the Interagency Task Force on Property Appraisal and Valuation Equity (PAVE), composed of thirteen federal agencies and offices, released its report entitled "Action Plan to Advance Property Appraisal and Valuation Equity: Closing the Racial Wealth Gap by Addressing Mis-valuations for Families and Communities of Color."

Commentary on PAVE's conclusion:

PAVE concluded that "Homeownership is often hindered by inequities within current home lending and appraisal processes, which research shows disproportionately impact people in communities of color."

As noted in the Executive Summary, the report largely rests on three studies for its conclusion: (i) a report by the Brookings Institution, (ii) a note by Freddie Mac, and (iii) a blog post by FHFA.[1] In our work, we have issued lengthy critiques that discredit the first two studies (see our rebuttal to Brookings and to Freddie Mac) and now take the opportunity to respond to the FHFA study.[2] Here is a summary of our findings:

The Brookings and Freddie Mac studies are not based on rigorous data analysis. Most importantly, they conflate race with socio-economic status (SES), i.e. income, buying power, marriage rates, credit scores, etc. **Race-based gaps found in the Brookings and Freddie Mac studies either entirely or substantially disappear when adjusting for differences in SES.** Furthermore, our analyses show that similar gaps are present in majority White or White-only tracts across different SES levels, raising serious questions regarding a race-based explanation.[3] We also addressed a rebuttal from the Brookings authors to our critique. We found that Perry and Rothwell's (2021) rebuttal to our critique supported our claim of omitted variable bias, failed to rebuke our methodology, and never addressed our case studies. We also presented solutions based on our findings. The Freddie Mac study took pains to state that its research was both "exploratory" and "preliminary". Yet PAVE accepted Freddie Mac's findings at face-value, even

[1] Interagency Task Force on Property Appraisal and Valuation Equity (PAVE), *Action Plan to Advance Property Appraisal and Valuation Equity: Closing the Racial Wealth Gap by Addressing Mis-valuations for Families and Communities of Color*, March 24, 2022, pp. 2-3.
[2] Despite the AEI Housing Center having undertaken a significant body of research on the topic of racial bias in housing finance over a course of years and notwithstanding efforts to engage with PAVE and some of its members, we were unable to engage with PAVE and our work was not mentioned in the report. Yet, PAVE stated that "Over the past 180 days, the Task Force has undertaken a collaborative and comprehensive approach toward identifying actions to address appraisal bias. This approach involved extensive consultation with subject matter experts and leaders across industry, academia, trade and civil rights groups, and government."
[3] The same critique to the Brookings paper also applies to research by Howell and Korver-Glenn (2021) and a recent Redfin post on the same topic.

though research by Fannie Mae provides a likely, non-race based explanation for the valuation discrepancy found by Freddie Mac. It is worth noting that Fannie Mae's explanation castes a favorable light on the appraisal industry.

This conflation by both Brookings and Freddie Mac is of critical importance. While there is agreement regarding the symptoms observed by PAVE--racial and ethnic differences in homeownership rates, financial returns of owning a home, and median wealth--ascertaining the causes and workable solutions requires a competition of ideas.[4] PAVE excluded research that was inconvenient or inconsistent with the desired narrative and conclusion.[5]

The FHFA blog post, which we have not addressed until now, stated that in their "review of appraisals, we have observed references to race and ethnicity in the 'Neighborhood Description' and other free-form text fields in the appraisal form." FHFA concluded that the use of such references is evidence of bias as the "racial and ethnic composition of the neighborhood should never be a factor that influences the value of a family's home" and released 16 specific examples.

While we all can agree with FHFA's statement that "racial and ethnic composition of the neighborhood should never be a factor that influences the value of a family's home", the blog post failed to provide any specifics as to the frequency of such occurrences. It only stated:

> From millions of appraisals submitted annually, a keyword search resulted in thousands of potential race-related flags. Individual review finds many instances of keywords to be false positives, but the following are [16] examples of references when the appraiser has clearly included race or other protected class references in the appraisal.

Without more information, one is unable to discern whether this is evidence of a few bad apples or systemic behavior. This is made all the more problematic given that there is other evidence showing no systemic appraisal bias. Unfortunately, PAVE ignored that body of research, to wit:

- AEI Housing Center (2021) found that racial bias by appraisers on refinance loans is uncommon and not systemic. To evaluate the existence of bias, the AEI Housing Center assembled a unique dataset with over 240,000 loans for which we knew the race of the borrowers.
- Ambrose et al. (2021) concluded that "contrary to media allegations, our statistical analysis found that racial bias by appraisers on refinance loans is uncommon and not systemic."[6]
- Fannie Mae (2022) concluded that for refinance applications "Black borrowers refinancing their home on average received a slightly lower appraisal value relative to automated valuation

[4] The University of Wisconsin Board of Regents stated this concept best over 125 years ago: *"Whatever may be the limitations which trammel inquiry elsewhere, we believe that the great state University of Wisconsin should ever encourage that continual and fearless sifting and winnowing by which alone the truth can be found."* https://news.wisc.edu/sifting-and-winnowing-turns-125/

[5] This goes back to when President Biden in his January 26, 2021 "Memorandum on Redressing Our Nation's and the Federal Government's History of Discriminatory Housing Practices and Policies" for the Secretary of HUD cited as fact "a persistent undervaluation of properties owned by families of color." Thus, PAVE would need to conform to the President's stated narrative, notwithstanding strong evidence to the contrary. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/01/26/memorandum-on-redressing-our-nations-and-the-federal-governments-history-of-discriminatory-housing-practices-and-policies/

[6] Ambrose, Brent W., James Conklin, N. Edward Coulson, Moussa Diop, and Luis A. Lopez. "Does Appraiser and Borrower Race Affect Valuation?" Available at SSRN 3951587 (2021).

models" and that "the frequency of 'undervaluation' did not have a notable racial pattern."[7]Interestingly, Fannie Mae (2022) also rebuked the methodological approach in Freddie Mac's research note that was cited by PAVE as one of the three main studies.[8]

Our conclusion is that PAVE has misdiagnosed the problem.[9] PAVE proposed 21 agency actions. It is highly questionable that these will address racial and ethnic differences in homeownership rate, financial returns of owning a home, or median wealth. In some cases, they may make these differences worse or take the pressure off in finding effective solutions. It also must be noted that HUD, and its predecessors have played a major role in perpetuating segregation and racial wealth disparities.[10] This alone should give pause to any objective reader of the PAVE report.

Rather than PAVE's finding of "inequities within current home lending and appraisal processes, which research shows disproportionately impact people in communities of color" the real culprit are inequities in SES, which PAVE acknowledges when it states that "[m]uch of the gap in rates of homeownership can be traced to socio-economic factors that differ on average between Black and white homeowners." While lower SES certainly reflects a legacy of past racism and lingering racial bias, which leaves Blacks at a large income and wealth disadvantage relative to most Whites, PAVE should have addressed this in its

[7] Williamson, Jake and Mark Palim. "Appraising the Appraisal: A closer look at divergent appraisal values for Black and white borrowers refinancing their home." (2022).

[8] In particular, Fannie Mae wrote that "We chose to study refinance applications, as opposed to home purchase applications, because the appraiser in a refinance transaction typically interacts directly with the homeowner (i.e., the borrower), establishing a pathway for potential bias to influence the appraisal results. The race or ethnicity of the borrower is often disclosed in the loan data, making it possible to directly observe any correlation with value. On the other hand, in a purchase transaction, the appraiser typically does not interact with the buyer (i.e., the borrower) of the property but rather with the seller or the seller's agent. The availability of racial or ethnic data of sellers and real estate agents is limited, thereby making an analysis of valuation differences by different demographics for purchase transactions limited or incomplete relative to the analysis detailed below using refinance transactions." (p.3)

[9] At times, PAVE tried to have it both ways. On the topic of undervaluation, which is the main focus in the Freddie Mac analysis because of the negative impact on minority home buyers, the PAVE report stated that a lower appraisal can be beneficial to the buyer but hurtful to the seller as "it limits the seller's realized home equity gains and therefore impacts the seller's wealth." (p.15)

[10] As noted by PAVE throughout the 20th century, the "federal...government systematically implemented discriminatory policies that led to housing segregation." Not mentioned by PAVE was the U.S. Commerce Department's role in implementing a zoning regime designed to keep Black and ethnic-minorities out of single-family detached neighborhoods (see Chapter 1, AEI Light Touch Density E-Book), the 1949 Housing Act which resulted in the high-rise public housing and urban renewal programs, both of which worked to the great detriment of Black households and neighborhoods, the 1967 Presidential Task Force on Housing and Urban Development (headed by HUD Secretary Weaver), which proposed a 10-year housing program to eliminate all substandard housing in the U.S. (source: Lyndon Johnson Library), that was enacted in the 1968 Housing and Urban Development Act, the consequences of which led to HUD and FHA destroying many American cities, especially Black neighborhoods (Cities Destroyed Cash: The FHA Scandal at HUD), the Tax Reform Act of 1986, which created the Low Income Housing Tax Credit, which has perpetuated racial segregation (Chicago tax credit program mostly produces affordable housing in poor black areas, March 15, 2021), the Federal Housing Enterprises Financial Safety and Soundness Act of 1992, which granted HUD the authority to set affordable housing mandates for Fannie Mae and Freddie Mac, and HUD's 1995 National Homeownership Strategy: Partners in the American Dream, which led to over 10 million foreclosures and did much to create the wealth disparities Blacks now face. All of these failures may be traced to HUD, or its predecessor agencies responsible for federal housing policy.

policy recommendations. Thus, the PAVE Action Plan, by misdiagnosing the causes of the racial gap, will likely lead to unintended consequences as the Action Plan does not address the root problem.

We agree with PAVE that we ought to support opportunities for income and wealth growth among lower-income households. However, we should address the root cause for lower SES, and not unsubstantiated claims of systemic bias and racism in the housing finance sector.

Based on an objective diagnosis of symptoms and causes using rigorous data analysis, we propose the following solutions:

The housing policy solutions are:

- Building generational wealth through sustainable homeownership for low SES households by reducing leverage for aspiring low-income home buyers.
- Increasing supply and reducing income stratification through Light Touch Density.
- Promoting Walkable Oriented Development in existing neighborhoods with a mix of residential and commercial properties.

Other policy solutions, which might be explored, are:[11]

- Encouraging two parents in households with children (single-parent households have been found to be a significant SES factor by a wide ranch of academic researchers).
- Enacting occupational licensing reforms and allowing small businesses to be run out of one's home (this has been found to be a significant barrier to low SES households).
- More economical childcare by rolling back burdensome government regulations (childcare costs are a significant barrier to gainful employment by low SES households).
- Real school choice for access to quality elementary and secondary education (racial and ethnic minorities would benefit greatly from real school choice).
- Improving access to technical and apprenticeship training (this would open up access by low SES households to these well-paying jobs).
- Encouraging state and local governments to address public investment disparities relating to minority and lower income neighborhoods.

Recognizing the importance of SES factors is key to fashioning appropriate public and private responses. A misdiagnosis that focuses on other factors will not address the root problem and could potentially lead to unintended consequences. We must be mindful that many public policies aimed at addressing racial discrimination have had unintended consequences that have done substantial harm to low-income households generally, and minority households in particular.

[11] Many thanks to our AEI colleagues Naomi Schaefer Riley and Angela Rachidi for many of these ideas. Please see their thoughtful analysis: https://reason.com/2021/02/24/fix-family-poverty-with-free-markets-for-once/