VIRTUAL CURRENCY: FINANCIAL INNOVATION AND NATIONAL SECURITY IMPLICATIONS

HEARING

BEFORE THE

SUBCOMMITTEE ON TERRORISM AND ILLICIT FINANCE

OF THE

COMMITTEE ON FINANCIAL SERVICES

U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED FIFTEENTH CONGRESS

FIRST SESSION

JUNE 8, 2017

Printed for the use of the Committee on Financial Services

Serial No. 115–22

U.S. GOVERNMENT PUBLISHING OFFICE

28–177 PDF WASHINGTON : 2018

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

HOUSE COMMITTEE ON FINANCIAL SERVICES

JEB HENSARLING, Texas, *Chairman*

PATRICK T. McHENRY, North Carolina, *Vice Chairman*
PETER T. KING, New York
EDWARD R. ROYCE, California
FRANK D. LUCAS, Oklahoma
STEVAN PEARCE, New Mexico
BILL POSEY, Florida
BLAINE LUETKEMEYER, Missouri
BILL HUIZENGA, Michigan
SEAN P. DUFFY, Wisconsin
STEVE STIVERS, Ohio
RANDY HULTGREN, Illinois
DENNIS A. ROSS, Florida
ROBERT PITTENGER, North Carolina
ANN WAGNER, Missouri
ANDY BARR, Kentucky
KEITH J. ROTHFUS, Pennsylvania
LUKE MESSER, Indiana
SCOTT TIPTON, Colorado
ROGER WILLIAMS, Texas
BRUCE POLIQUIN, Maine
MIA LOVE, Utah
FRENCH HILL, Arkansas
TOM EMMER, Minnesota
LEE M. ZELDIN, New York
DAVID A. TROTT, Michigan
BARRY LOUDERMILK, Georgia
ALEXANDER X. MOONEY, West Virginia
THOMAS MacARTHUR, New Jersey
WARREN DAVIDSON, Ohio
TED BUDD, North Carolina
DAVID KUSTOFF, Tennessee
CLAUDIA TENNEY, New York
TREY HOLLINGSWORTH, Indiana

MAXINE WATERS, California, *Ranking Member*
CAROLYN B. MALONEY, New York
NYDIA M. VELÁZQUEZ, New York
BRAD SHERMAN, California
GREGORY W. MEEKS, New York
MICHAEL E. CAPUANO, Massachusetts
WM. LACY CLAY, Missouri
STEPHEN F. LYNCH, Massachusetts
DAVID SCOTT, Georgia
AL GREEN, Texas
EMANUEL CLEAVER, Missouri
GWEN MOORE, Wisconsin
KEITH ELLISON, Minnesota
ED PERLMUTTER, Colorado
JAMES A. HIMES, Connecticut
BILL FOSTER, Illinois
DANIEL T. KILDEE, Michigan
JOHN K. DELANEY, Maryland
KYRSTEN SINEMA, Arizona
JOYCE BEATTY, Ohio
DENNY HECK, Washington
JUAN VARGAS, California
JOSH GOTTHEIMER, New Jersey
VICENTE GONZALEZ, Texas
CHARLIE CRIST, Florida
RUBEN KIHUEN, Nevada

KIRSTEN SUTTON MORK, *Staff Director*

SUBCOMMITTEE ON TERRORISM AND ILLICIT FINANCE

STEVAN PEARCE, New Mexico *Chairman*

ROBERT PITTENGER, North Carolina, *Vice Chairman*
KEITH J. ROTHFUS, Pennsylvania
LUKE MESSER, Indiana
SCOTT TIPTON, Colorado
ROGER WILLIAMS, Texas
BRUCE POLIQUIN, Maine
MIA LOVE, Utah
FRENCH HILL, Arkansas
TOM EMMER, Minnesota
LEE M. ZELDIN, New York
WARREN DAVIDSON, Ohio
TED BUDD, North Carolina
DAVID KUSTOFF, Tennessee

ED PERLMUTTER, Colorado, *Ranking Member*
CAROLYN B. MALONEY, New York
JAMES A. HIMES, Connecticut
BILL FOSTER, Illinois
DANIEL T. KILDEE, Michigan
JOHN K. DELANEY, Maryland
KYRSTEN SINEMA, Arizona
JUAN VARGAS, California
JOSH GOTTHEIMER, New Jersey
RUBEN KIHUEN, Nevada
STEPHEN F. LYNCH, Massachusetts

CONTENTS

Page

Hearing held on:
June 8, 2017 1
Appendix:
June 8, 2017 37

WITNESSES

THURSDAY, JUNE 8, 2017

Brito, Jerry, Executive Director, Coin Center 5
Dueweke, Scott, President, the Identity and Payments Association 7
Haun, Kathryn, Lecturer, Stanford Law School, and former Assistant U.S. Attorney, U.S. Department of Justice 8
Levin, Jonathan, Co-Founder, Chainalysis 11
Wilson, Luke, Vice President, Business Development-Investigations, Elliptic .. 13

APPENDIX

Prepared statements:
Brito, Jerry 38
Dueweke, Scott 42
Haun, Kathryn 50
Levin, Jonathan 63
Wilson, Luke 70

ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

Lynch, Hon. Stephen:
CNAS report entitled, "Terrorist Use of Virtual Currencies," dated May 2017 71

VIRTUAL CURRENCY: FINANCIAL INNOVATION AND NATIONAL SECURITY IMPLICATIONS

Thursday, June 8, 2017

U.S. HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON TERRORISM
AND ILLICIT FINANCE,
COMMITTEE ON FINANCIAL SERVICES,
Washington, D.C.

The subcommittee met, pursuant to notice, at 10:03 a.m., in room 2128, Rayburn House Office Building, Hon. Stevan Pearce [chairman of the subcommittee] presiding.

Members present: Representatives Pearce, Pittenger, Rothfus, Messer, Tipton, Williams, Poliquin, Hill, Zeldin, Davidson, Budd, Kustoff; Perlmutter, Himes, Foster, Kildee, Sinema, Vargas, Gottheimer, Kihuen, and Lynch.

Ex officio present: Representative Hensarling.

Chairman PEARCE. The Subcommittee on Terrorism and Illicit Finance will come to order.

Without objection, the Chair is authorized to declare a recess of the subcommittee at any time.

Also, without objection, members of the full Financial Services Committee who are not members of the Subcommittee on Terrorism and Illicit Finance may participate in today's hearing.

Today's hearing is entitled, "Virtual Currency: Financial Innovation and National Security Implications."

I now recognize myself for 2 minutes to give an opening statement.

Innovation revolutionizes and simplifies our lives on a daily basis. In the past 30 years alone we have seen the emergence of the Internet as an open-source accessible information tool, the popularization of cell phones, the development and wide use of smartphones, faster and faster Internet and wireless access, and the list goes on and on.

For many of us in this room, the millennials excluded—and, frankly, based on the number of them in the lines at the Apple Store, I think they are even surprised at the existence and the evolution of this thing which never would have seemed possible in our wildest dreams.

The implications, of course, of this greater development and exploration into the digital age is the inability of government and regulatory bodies to keep up with the pace of development. Tech-

nology in the financial space is no exception, and that is what brings us here today.

From small business lending to virtual wallets, the creation of virtual currencies, the fintech space, as it is known, is rapidly evolving.

The benefits are clear. Families in underserved areas are finding more choice and options than ever before. People can pay for the goods in the store without the need for cards or cash. The possibilities of benefits are truly endless.

The subcommittee kicked off the work in this space last week with a briefing on blockchain, one of the major innovations driving this development. Today we will continue the conversation by examining how virtual currencies specifically pose a risk to our national security.

This will include questions such as: Does the creation of a currency that is completely decentralized from a governmental structure, administered through the use of peer-to-peer sharing, present a new threat to the safety and soundness of our banks and to our national security? What, if any, regulatory structure exists around these emergency forms of currency and technology? Does the notion of online peer-to-peer sharing provide an increased veil of secrecy that could be exploited by terrorists and illicit actors?

I thank our witnesses for being here today and I look forward to the conversation to come.

The Chair now recognizes the ranking member of the subcommittee, the gentleman from Colorado, Mr. Perlmutter, for 2 minutes for an opening statement.

Mr. PERLMUTTER. Thanks, Mr. Chairman.

And thanks, to our witnesses, for being here today.

Obviously, there is considerable interest in virtual currencies and cryptotechnologies, not only among speculators and traders but because of the promising benefits the underlying blockchain ledger technology has to offer. However, our subcommittee should remain focused on the national security implications, especially since cyber criminals and nation states are exploiting cryptocurrencies for illicit purposes.

Mr. Dueweke notes in his testimony: "Cyber criminals in Eastern Europe, North Korea, China, and Russia certainly are taking advantage of evolving technologies to underwrite terrorism and exchange ill-gotten gains. In fact, Russia has created its own cryptocurrency to support its hackers program so that they can cause mayhem around the globe."

The reality is criminals today use cash, money service businesses, and other means for illicit purposes, but we provided law enforcement the regulatory tools to catch the bad guys. The question is, does law enforcement have the tools to catch the criminals using these new technologies and currencies?

If the United States is to succeed in staying one step ahead of the bad guys then we must work with our national partners and international partners to adopt global methodologies and systems to ensure these new innovations are being used for legitimate purposes. The United States and Europe remain and maintain a fairly sophisticated Bank Secrecy Act and the money-laundering regu-

latory regime, but the question is, will China and Russia follow our lead?

The rise of new cryptocurrencies threatens to disrupt the way banking is philosophically conducted, potentially undermining the United States' dominance over money flows.

With that, I thank you, Mr. Chairman, and I yield back.

Chairman PEARCE. The gentleman yields back.

The Chair now recognizes Mr. Pittenger for 1 minute.

Mr. PITTENGER. Thank you, Mr. Chairman, and Ranking Member Perlmutter, for hosting us today for this cybersecurity hearing.

Cybersecurity is an important and evolving method of finance, and it is imperative that this committee fully understand how criminal and terrorist networks may use blockchain applications to fund illicit behavior. The United States must lead by example, with our regulatory and investigative structure, to ensure that terrorists cannot use cybercurrencies to fund their violent and malicious behavior.

Far too often, foreign governments have enough trouble enacting and enforcing their own CTF-AML laws related to traditional financial institutions, so we cannot assume that these same governments will have adequate capabilities to track and intercept financial anomalies located within blockchain applications. This committee must know what it takes, regarding both resources and legal authorities, for the U.S. Government to confidently enforce our terror financial and money-laundering laws with cybersecurity applications.

Thank you again, Mr. Chairman, and Mr. Ranking Member.

I yield back.

Chairman PEARCE. The gentleman's time has expired.

The Chair now recognizes the gentlelady from Arizona, Ms. Sinema.

Ms. SINEMA. Thank you, Chairman Pearce, and Ranking Member Perlmutter.

I appreciate the witnesses' testimonies and agree that we need a government-wide approach to evaluate and address the illegitimate uses and potential risks of virtual currency. I support a unified national strategy to combat terrorist and other illicit finance, and this strategy should include a comprehensive discussion of virtual currencies.

I look forward to hearing how we can most effectively use risk-based approaches to identify and mitigate the exploitation of virtual currencies by terrorists and criminals while allowing for innovation and growth in the fintech sector. In fact, how can we best use the innovation and growth within fintech to counter terrorist and other illicit finance?

Thank you again, Chairman Pearce and Ranking Member Perlmutter, for your leadership on this issue, and I continue to look forward to working with my colleagues on both sides of the aisle to keep all types of money out of terrorist hands and build on our progress to strengthen America's security.

Thank you, Mr. Chairman. I yield back.

Chairman PEARCE. The gentlelady's time has expired.

We now turn to the testimony of our witnesses.

Mr. Jerry Brito is the executive director of Coin Center, a nonprofit research and advocacy center founded in the public policy issues facing cryptocurrency technologies such as bitcoin. Previously, Mr. Brito directed the Technology Policy Program at the Mercatus Center of George Mason University, and he serves as an adjunct professor of law at George Mason University. Mr. Brito earned his J.D. from George Mason University School of Law, and his B.A. from Florida International University.

Mr. Scott Dueweke is the president of the Identity and Payments Association. He is also the president of Zebryx Consulting, providing public and private sector clients an understanding of the risks and rewards of identities and alternative payment systems.

Mr. Dueweke is an expert on identity, the blockchain, and alternative payment systems. He has advised financial institutions, the U.S. Government, and international law enforcement agencies on these matters.

Mr. Dueweke's experience in the blockchain and its underlying technology of public key infrastructure, or PKI, began in 1996 with his role as the global marketing manager for IBM's PKI group. Mr. Dueweke is a frequent speaker on identity, alternative payments, and the dark web at conferences worldwide and has been interviewed and quoted by media, including The Wall Street Journal, Fox News, Time, and Forbes.

Ms. Kathryn Haun served as a Federal prosecutor with the Department of Justice from 2006 until recently, and was DOJ's first ever coordinator for emerging financial technologies. Ms. Haun has investigated and prosecuted hundreds of violations of Federal criminal law in the United States with a focus on transnational and organized crime syndicates, cybercrime, the deep web, and digital currency, including a case against the former Federal agents investigating the illicit Silk Road marketplace.

Ms. Haun previously worked on national security issues and held senior positions at DOJ. Prior to that, she was in a private practice in D.C. Ms. Haun has clerked for U.S. Supreme Court Justice Anthony Kennedy as an honors graduate of Stanford Law School, where she has also taught a class on cybercrime and digital currency.

Mr. Jonathan Levin is co-founder of Chainalysis, which is the leading provider of anti-money-laundering software for bitcoin. Through formal partnerships with Europol and other international law enforcement, Chainalysis' investigative tools have been used globally to track, apprehend, and convict money launderers and cybercriminals.

Mr. Levin was previously CEO at Coinometrics, where he led a team of data scientists to measure the activity and the health of the bitcoin network. Mr. Levin was a postgraduate economist at the University of Oxford, where his research focused on virtual currencies, creating one of the first statistical models of bitcoin transaction fees.

Mr. Luke Wilson is the vice president of business development investigations with Elliptic, where he is primarily responsible for law enforcement engagement and investigations. Mr. Wilson has a unique skill set and a deep understanding of bitcoin and blockchain

owing to his 7 years of employment with the Cyber and Counterterrorism Division of the Federal Bureau of Investigations.

While at the FBI, Mr. Wilson constructed the first interagency task force for investigating illicit uses of bitcoin. As a subject matter expert, Mr. Wilson has advised the U.S. Government and regulators on digital currencies.

With his previous employment with the Department of Defense, and the Intelligence Committee, I think Mr. Wilson has over 17 years of law enforcement and intelligence experience, and we appreciate his participation in the hearing today.

Each of you will now be recognized for 5 minutes to give an oral presentation of your testimony. And without objection, each of your written statements will be made a part of the record.

Mr. Brito, you are now recognized for 5 minutes.

STATEMENT OF JERRY BRITO, EXECUTIVE DIRECTOR, COIN CENTER

Mr. BRITO. Mr. Chairman and members of the subcommittee, I would like to thank you for the opportunity to speak to you today.

What I would like to do is explain what bitcoin is, and why it is a groundbreaking innovation—perhaps as important as the Web; and why, like the Web, illicit actors are attracted to it. I will then briefly offer some thoughts on what can be done to prevent that.

Before the invention of bitcoin, for two parties to transact online always required a third-party intermediary—someone like PayPal or a bank. Unlike cash in the real world, which I can hand to you in person without anyone else between us, electronic payments required a third party, trusted by each of us, to verify and guarantee the transfer.

Introduced in 2008, bitcoin overcame a longstanding computer science problem and for the first time allowed the secure and verifiable transfer of digital assets between individuals without the need for third-party intermediaries—just like cash in the physical world.

The innovation of peer-to-peer transfers has unlocked an incredible array of socially beneficial and economically important uses. Not only are fast and inexpensive global money transfers and payments now possible, this technology is also being used to make possible micro-transactions, copyright registries and global rights management system, faster and more efficient trade settlements, more secure land title and property record systems, Internet of things networks, self-sovereign identity, and much, much more.

What gives this technology its innovative potential is that, because there are no third-party gatekeepers from which to seek access, it is an open and permissionless network—just like the Internet.

When Mark Zuckerberg decided to launch Facebook in his dorm room at Harvard he didn't have to first clear it with the management of Internet, Inc. He simply wrote the Facebook application and launched it on the Web. Like the Internet, it is the permissionless, open nature of bitcoin that will foster innovation.

Unfortunately, this also means that like the Internet, it is open to bad actors who take advantage of it. Criminals certainly use it

today, and we have begun to see some nascent interest from terrorist groups.

However, according to a recent report on the potential of terrorist use of digital currencies by the Center for a New American Security (CNAS), "Currently there is no more than anecdotal evidence that terrorist groups have used virtual currencies to support themselves."

While the potential is very serious, this, however, means that there is time to develop an appropriate response—a reasoned response that targets the threat while preserving the freedom to innovate.

The blockchain and digital currency community has been working for some time now to face this threat. Almost 2 years ago, the Coin Center helped co-found the Blockchain Alliance, a public-private forum that serves as an information-sharing conduit between law enforcement and industry.

Today the alliance is composed of 35 industry members, including the largest exchanges and digital wallet companies, and 36 members from the government, including DOJ, FBI, DHS, IRS, Secret Service, Interpol, Europol, and many others. Thanks to the cooperative work of the Blockchain Alliance, law enforcement today is better equipped than ever to take on this emerging threat.

However, the CNAS report I mentioned earlier found that our current regulatory framework impedes law enforcement in the private sector from collaborating more nimbly to weed out illicit actors. They found, "One particular challenge in this area is the requirement for a virtual currency firm to obtain licenses in all states in which it operates and maintain compliance consistent with both Federal and applicable state standards where they are licensed to operate. With only a single Federal registration for virtual currency firms, compliance costs would be more manageable for smaller firms and regulators would be better able to oversee firms."

The Coin Center could not agree more, and to promote a more uniform approach Congress should consider the Office of the Comptroller of the Currency—encourage him to offer Federal fintech charters to custodial digital currency firms. And Congress should also consider the creation of a new Federal money transmission license to take the place of State-by-State licensing.

As we discuss these questions today, I hope you will keep a few things in mind.

First, this is a technology that, like the Internet—or, indeed, like fire—can be used for good or for bad. Its inherent nature is neutral.

Second, this technology can't be put back in the bottle. Encouraging its legitimate use gives us more and better visibility into the network, while discouraging its use only cedes the network to bad actors.

And finally, while there is substantial criminal use, terrorist use, while obviously important to focus on, is still nascent and experimental, so there is time to develop a considered response.

Thank you.

[The prepared statement of Mr. Brito can be found on page 38 of the appendix.]

Chairman PEARCE. Mr. Dueweke, you are recognized for 5 minutes.

STATEMENT OF SCOTT DUEWEKE, PRESIDENT, THE IDENTITY AND PAYMENTS ASSOCIATION

Mr. DUEWEKE. Thank you.

Esteemed members of the subcommittee, I am honored to be testifying before you today on the important topic of virtual currencies and their role in enabling terrorism and illicit financial transactions. There are four major points I would like to make.

The first: Understanding the promise and peril of virtual currencies requires looking well beyond the bright, shiny bitcoin. Virtual currencies beyond bitcoin and other alternative payment systems create an expansive shadow network.

China and Russia are beginning to dominate a new global digital financial system of which we are not necessarily fully members of or aware of. And these new payment systems are helping to connect billions of unbanked and underbanked around the world, and we should always keep that in mind.

These billions of people who are using virtual currencies and other alternative payment and remittance systems for legitimate purposes are transforming economies through their use, especially in Asia and Africa. These systems now represent a major force for the financial inclusion of the more than 3 billion unbanked and underbanked around the world. That is an important point I hope you will remember as you examine the negative uses of these systems. There is a lot of positive going on.

How do we balance the profound benefits of these new fintech opportunities against the criminal use of these systems? It is critical that the entire scope of this ecosystem first be considered—its impact, its uses, its structure—before making judgments or creating laws and regulations that might have broad unintended consequences.

This ecosystem extends far beyond bitcoin and other cryptocurrencies and its roughly $100 billion market value of bitcoin today. Other virtual currencies, like the centralized Russian and Chinese virtual currencies, far exceed bitcoin, and their combined value with remittance systems and mobile payment systems exceeds $2 trillion.

A network of thousands of virtual currency exchangers connect these systems into one ecosystem, which should not be considered separately, but instead as an ecosystem together with the other parts of it.

Even bitcoin's impact extends far beyond its use as a cryptocurrency. For example, as Jerry mentioned, the blockchain can be used for many other purposes.

I am currently working with Saint Luke's University Healthcare Network to implement the blockchain to enhance the patient experience and to make it more secure and convenient. The blockchain is being implemented in financial institutions to transfer funds, at the New York Stock Exchange to modernize the trading of stocks, and in many other applications. It can also be applied to reduce fraud and graft in foreign aid programs while increasing its reach and impact while allowing full transparency and reduction in the approximately 30 percent of foreign aid that is lost to graft and corruption.

Not all blockchains are created equal, and new, more anonymous cryptocurrencies, such as Monero, Dash, and Zcash, are beginning to gain market share. These systems now account for about 1 percent of all cryptocurrency usage on the dark web and are increasing in popularity rapidly.

As these systems increase in usage, existing blockchain analysis tools will be challenged to remain relevant as these dark cryptocurrencies are designed to avoid the tracking of transactions, whereas bitcoin was designed to be transparent.

A new consideration of the use of cryptocurrencies by nation states includes the Russian Central Bank's announcement on June 3rd that they will be creating a national cryptocurrency. Considering that a large percentage of global criminal hackers are Russian language-speakers and our current stress with Russia and the United States and Europe, this development should be closely monitored.

How this cryptocurrency is set up will be telling. Will it have a publicly available and verifiable blockchain like bitcoin, or will it be a private or permissioned blockchain and be opaque to Western observers and regulators?

If private, it could be used to circumvent KYC and AML and be used to support proxy "patriotic hackers," as Vladimir Putin referred to them last week. This possibility already exists with Russian language centralized systems—especially WebMoney.

Hypothetically, what could these virtual currency systems be used for? I am especially referring to these centralized systems, not bitcoin as much.

First, balance of payment transfers between criminal organizations such as organized crime and drug cartels; second, fund transfers with pariah states; third, transfers with terrorists; fourth, enabling kleptocrats to move money from their country's coffers offshore—as I have said in the press, the next Panama Papers scandal could well be focused on these systems instead of traditional banking; and the funding of a virtual army of proxy hackers to do their patriotic duty.

So how do we cope with these daunting challenges on managing and balancing these? At the Identity and Payments Association we have launched a global nonprofit to create a public-private partnership to do precisely that.

In summation there is a shadow financial system that is thriving outside of our control. We need to take strong steps to understand, control, and counter it while encouraging the growth of these new alternative payment and virtual currency systems that are governed by the rule of law.

Thank you.

[The prepared statement of Mr. Dueweke can be found on page 42 of the appendix.]

Chairman PEARCE. Ms. Haun, you are recognized for 5 minutes.

STATEMENT OF KATHRYN HAUN, LECTURER, STANFORD LAW SCHOOL, AND FORMER ASSISTANT U.S. ATTORNEY, U.S. DEPARTMENT OF JUSTICE

Ms. HAUN. Thank you.

Mr. Chairman, Ranking Member Perlmutter, and members of the subcommittee, thank you for inviting me to testify on the role that financial innovation can play in facilitating but also in curtailing illicit finance.

In a year the market capitalization of bitcoin has gone from $6 billion to $40 billion, and the combined market cap of all cryptocurrencies now exceeds $90 billion. This number is rising every day.

More people are buying, selling, trading, and transacting in these currencies for plenty of legitimate uses. In fact, I know small business owners, academics, investors, and even government employees who use cryptocurrency, and these aren't people engaged in illicit acts. They are looking for ease of payments, fewer middlemen, lower fees, and greater privacy.

But early misuse is a fact of life with emerging technologies, and cryptocurrency is no exception. Although we now all use the Internet every day, in the beginning it was disproportionately used by child pornographers and online fraudsters, and it is still today used for good and bad, including by terrorists.

Now, the potential for terrorist use of cryptocurrencies exists, as it exists for cash or any other type of asset. To date, we have seen only limited instances of terrorists using cryptocurrency, but these instances are becoming more frequent.

It appears that terrorists are not using the registered exchanges in the United States but are using the unregistered overseas ones that don't allow for U.S. anti-money-laundering, or AML, requirements. They are also using anonymous peer-to-peer exchanges, like LocalBitcoins.com, which operates as a sort of Craigslist.

Now, none of the recent and horrific terrorist attacks have relied on cryptocurrencies for the simple reason that these attacks are, by and large, low-tech and inexpensive. Automatic weapons, trucks, suicide bombs, and plane tickets don't require large sums of money.

With the small amounts necessary to inflict massive harm, terrorists overwhelmingly use less traceable means, like cash and prepaid cards. We see more use of cryptocurrency in the areas of cybercrime, drug trafficking, money laundering, and financial fraud. These activities have major national security implications, of course. Ransomware is a compelling example because it can cripple critical infrastructure—hospitals, first responders, public transit systems.

Last month's WannaCry attack affected over 10,000 businesses, hospitals, and public agencies in over 153 countries, and that WannaCry attack wasn't even a very sophisticated attack. It is getting far worse, and ransomware's preferred currency is bitcoin.

However, while some features of cryptocurrencies may facilitate crimes, other features may thwart them.

One of the beneficial features of bitcoin is the decentralized nature of the blockchain, the technology underpinning it. The blockchain is decentralized over millions of computers so it is very difficult to hack.

For a nation state wanting to inflict harm, a cyberattack using malware against a major financial institution is a centralized target. But if our financial infrastructure ran instead on these decentralized systems, millions of computers across the world would

have to be hacked and they would have to be hacked simultaneously.

And cryptocurrency also helps us solve bad acts. In one case I brought as a prosecutor, we used blockchain patterns to identify rogue Federal agents on the Silk Road Task Force. In another case we solved major hacking and ransomware schemes by looking at the movement of bitcoin. Some cases aren't yet public, but we would not have solved them had these criminals not been using cryptocurrencies because investigators like digital footprints, and that is exactly what digital currencies provide.

Of course, we can only follow the money to an individual if they used an entity that follows AML laws—money laundering laws—since only then can we, as law enforcement, tie it to an entity or an actual identity. But many overseas exchanges do not require names, let alone identification, to open accounts, and this leads to creation of anonymous accounts. Nearly 100 percent of ransomware campaigns and hacking rings use these overseas unregistered exchanges.

We have gone after some of the exchanges in the United States like this with success, but the majority of noncompliant exchanges are overseas and this poses formidable legal challenges, jurisdictional challenges. Our antiquated Mutual Legal Assistance Treaty process, or the MLAT process, takes months of bureaucratic maneuvering, and that is in the best-case scenario when we have cooperative partners on other sides. And when we are dealing with an uncooperative country, we might not get any evidence at all.

We need more resources to quickly get at electronic evidence overseas, funding more attache positions and better systems for processing these MLATs, which are absolutely critical to us getting overseas electronic evidence.

For those entities in uncooperative countries we need more statutory authority to go after their business segments that rely upon U.S. companies for support: servers; communications; software; and banks. Now, there are numerous entities in the space with robust AML and compliance programs, and these platforms are some of our best partners.

In fact, the head of an agency in Treasury told me that the suspicious activity reports (SARs) that they are seeing out of digital currency companies are superior to those from large financial institutions despite fewer compliance resources. And in over a decade that I spent as a Federal prosecutor, the fastest turnaround I ever got on a subpoena was from a digital currency company.

But with broader adoption these companies' compliance resources are being stretched. We want them to be spending those resources on keeping bad actors off their platforms and developing tools to spot fraudulent activity, not addressing the vagaries of 50 different State regulatory regimes. The idea of a Federal solution to harmonize State laws is an area where Congress could help.

And also an area where Congress could help is we have an urgent need for resources to be devoted to this space immediately and across- the-board at all agencies. It is simply not sufficient to have only a handful of people at each Federal agency focused on cryptocurrency when it is affecting so many areas that touch upon our national security.

Thank you very much for inviting me to share my thoughts on this topic.

[The prepared statement of Ms. Haun can be found on page 50 of the appendix.]

Chairman PEARCE. Thank you.

Mr. Levin, before you are recognized, I realize now I was giving you an extra syllable in the name as I was pronouncing it during the introduction, so you can just put it on your asset sheet that you are worth more now here.

I now recognize you for 5 minutes.

STATEMENT OF JONATHAN LEVIN, CO-FOUNDER, CHAINALYSIS

Mr. LEVIN. Thank you, Mr. Chairman, Ranking Member Perlmutter, and members of the subcommittee.

My name is Jonathan Levin and I am one of the co-founders of Chainalysis. Chainalysis is the leading provider of investigation software and risk management solutions for virtual currencies. In this field, we identify illicit use of virtual currencies, including terrorist financing. We provide tools to private industry and law enforcement to mitigate these risks and the activity that poses a risk to our society.

I wish to divide my briefing into three significant sections that I believe are worth considering when looking at the risk of virtual currencies: first, the potential for virtual currencies; second, the nature of this technology; and finally, the current use of virtual currencies.

The Internet started in the early 1960s but did not enter the mainstream until the creation of an easy-to-use consumer layer and developer tools that happened in the mid-1990s. Today we almost all use the Internet every day prior to entering this room and even afterwards.

The U.S. Government played an instrumental role in providing essential layers for private industry to develop business models and products for us as consumers to use. However, there was no payments layer baked into the Internet.

This is where the motivation behind bitcoin came in.

Efforts to curb the demand for this new payment infrastructure have not led to success. In February 2017 the People's Bank of China put pressure on virtual currency exchanges to stop trading. This led to an uptick in peer-to-peer bitcoin transactions that are out of the purview of the state. The transaction volume went from 2.5 million RMB to over 100 million RMB on these exchanges, and these cannot be regulated and it diminishes the oversight of the state.

Bitcoin and other virtual currencies are decentralized, as we have heard, and as such they are censorship-resistant. Receiving bitcoin can be done by anyone with basic access to computing anywhere in the world.

There is no need to register or supply anyone with identifying information in order to receive bitcoin. There is no ability to freeze assets or seize someone's virtual currencies without obtaining access to their computer. Virtual currencies, in this way, are ulti-

mately bearer instruments, and the person in control of a private key is the ultimate owner of virtual currency.

In order to facilitate this system, however, bitcoin makes every transaction public. These transactions are recorded in a single transaction ledger, the blockchain. However, these entries are pseudonymous and do not relate to real-world entities.

Chainalysis analyzes this blockchain to identify which transactions have been performed by the same entity and links these entities to real-world services such as exchangers, merchant processors, and underground marketplaces. This blockchain analysis can identify the underlying activity behind virtual currency transactions and the on-ramps and off-ramps and the connections to the existing financial system.

Terrorist organizations are not in the business of speculating on the price of virtual currencies, but rather, they may be interested in using virtual currencies for the following use cases: using virtual currencies in cybercriminal activities to fund operations; crowdfunding operations from sympathizers around the world; and paying for everyday items and Internet infrastructure.

Cybercriminals so far have mainly used bitcoin to buy and sell capabilities to launch cyberattacks and extort their victims when they do. Their use of bitcoin cannot be attributed to anonymity but rather convenience and its ability to move and transcend borders.

There has not been any evidence yet of terrorist organizations running any of these criminal enterprises. We have heard of the recent ransomware campaign known as "WannaCry," and that was leveraged by cybercriminals rather than terrorist organizations. However, despite ransomware's ineffective campaign, some of these criminal enterprises are making substantial sums of money, as I allude to in my written testimony.

In July 2016 there was the only verifiable public case of crowdfunding known by a terrorist organization. The campaign was launched over Twitter and was not very successful and raised a total sum of $1,000.

The nature of virtual currencies meant that Chainalysis was able to size the potential threat and also identify the ultimate source and destination and connection to the existing financial system.

Terrorists, like any other person, may use bitcoin to pay for Internet infrastructure and everyday goods and services. There are merchants around the world that accept virtual currency, including blue chip companies. Using tools like ours at Chainalysis, these purchases can lead to useful leads in investigations and uncover the goods and services purchased as well as attribute the identity of the individuals.

The potential for virtual currencies to bring radical new business models to the Internet and ways of organizing social and economic relations remains large. The pace of change in this domain is rapid and the eventual outcomes unpredictable.

The current use of virtual currencies is mainly financial speculation on their eventual impact on the world. The use of virtual currencies by terrorist organizations is very limited due to lack of awareness and trust placed in virtual currencies.

There is a growing awareness among companies and government agencies about the potential threats and their topologies. Virtual

currencies continue, however, to evolve rapidly. Private businesses like ours and the public sector should endeavor to mitigate these threats but be cognizant of the future potential for this technology.

Thank you.

[The prepared statement of Mr. Levin can be found on page 63 of the appendix.]

Chairman PEARCE. Mr. Wilson, you are now recognized for 5 minutes.

STATEMENT OF LUKE WILSON, VICE PRESIDENT, BUSINESS DEVELOPMENT-INVESTIGATIONS, ELLIPTIC

Mr. WILSON. Thank you, Mr. Chairman.

And thank you, subcommittee members.

My name is Luke Wilson. I am the vice president of business development and investigations for Elliptic.

Elliptic software is used to identify illicit activity on the bitcoin blockchain and we provide our services to the leading bitcoin companies and law enforcement agencies globally. We are located in London and Arlington, Virginia.

Today's hearing on, "Virtual Currency: Financial Innovation and National Security Implications" is a very good first step toward understanding this quickly evolving technology. My previous employment with the FBI allowed me to investigate several crimes that involved bitcoins. My experience is that bitcoin is not or should not be alarming to investigators or private companies.

Bitcoin is thought to be anonymous by some criminals. In reality, it is far from anonymous, and companies like Elliptic have assisted law enforcement and private industries to identify who is behind the illicit bitcoin transactions.

Elliptic's software and expertise has assisted in terrorism, ransomware, cyber extortion cases, and illegal arms trafficking cases, to name a few. In all of these cases we have provided intelligence and leads that help investigators to trace bitcoin transactions and identify who is transacting.

This is all made possible by the record of transactions kept on the blockchain. All bitcoin transactions are stored on the blockchain, including those performed by criminals. The importance of this blockchain record cannot and should not be undervalued, as it provides a public and permanent and incorruptible record of transactions, the likes of which is not available with any other payment method.

I would really like to go through a couple of cases that I helped with when I was in the Bureau.

As I talk about the firearms case, this was a case that I helped with, actually, while at Elliptic. There was a law enforcement agency that was looking at an illegal arms trafficker. If the illegal arms trafficker did not purchase the illegal arms off of a dark market site using bitcoins, this individual would never have been placed in handcuffs and put in jail. It is because of the bitcoin blockchain that they were able to come to Elliptic and we were able to trace those transactions and find out where the individual was purchasing the firearms, and then now we could tie that back to that individual.

So when I say that we have a way to trace this, this is what law enforcement and private industry does. They come and talk to a company like Elliptic or Chainalysis.

My experience in counterterrorism and virtual currencies make me well-placed to evaluate the risk by the potential terrorist use of bitcoin. My experience is that there have been very few verified terrorism cases in which bitcoin was used, and that in all of these cases law enforcement was able to trace the flows of bitcoin to subjects and possible coconspirators.

While I cannot say what the future holds for terrorist use of bitcoin/virtual currencies, I can say that it is very small to date and that we have been successful in assisting law enforcement and private industries to combat that threat.

Thank you for your time.

[The prepared statement of Mr. Wilson can be found on page 70 of the appendix.]

Chairman PEARCE. I thank each one of you for testifying.

The Chair now yields himself 5 minutes for questions.

So, Ms. Haun, I was fascinated by Mr. Levin's comments in both his written testimony and his statement that most of the protocols and infrastructure are decades old, pioneered by academia and the government. And as you talked about the additional resources, is it even possible for someone in a bureau, someone in an agency to keep up with the fast pace of development? So address that if you can.

Ms. HAUN. Sure. Well, I think it is two-fold.

First it is personnel who require training and being brought up-to-speed on these technologies. But second, it is the systems, and I think the systems are very important because oftentimes we will be getting from these companies that are providing us metadata in response, for example, to a search warrant or a subpoena, and we on our old systems can't even access them. They won't even run that data, and that is a real problem.

I think yes, it is possible, but you have to look at the resource question from both personnel and systems resources. And I mentioned the same thing with respect to speeding up the processing of MLATs: it is not just personnel, it is also just the systems themselves.

Chairman PEARCE. Okay. So you bring in personnel today and you give them a really deep education and a year from now they have been covered up with investigations and keeping up.

Mr. Levin, are those personnel we bring on today going to be able to keep up?

Mr. LEVIN. I think that as we look forward to see what innovations happen, the incentive needs to be placed on the private sector to be able to provide tools and keep up with the innovation that happens. And I think that it is our duty to provide training and education as part of offering software and tools, and that is something that we are actively doing. It needs to be regular and it needs to be more frequent than it currently is.

Chairman PEARCE. That is kind of my impression, just sitting up here being pretty unfamiliar with any technology.

So do you envision, Mr. Levin, an ability to set up the protocol that will give the protections and yet allow access by law enforce-

ment to where we don't have to have the resources? Because, just as a policymaker I will tell you, I see an unending need to hire more personnel, and the personnel we hired last year are not going to be very good by next year, and the year after completely not up-to-date. And so we just keep building that bureaucracy.

Somewhere we need to get the mobileness to tap into the private sector's knowledge, and therefore we leave the law enforcement to the law enforcement people, not keeping up with technology.

So if either one of you—Mr. Luke, if you want to jump in here on this, too, I really would like a discussion kind of on that, and fairly short, I have 2 minutes here.

Lead off, Mr. Levin, if you would, and then I'll go to Ms. Haun and Mr. Wilson. I would really like your input.

Mr. LEVIN. I think that one thing that I have seen personally in law enforcement is actually the need to not hire new people every year and that people need to become subject domain experts in order to be able to counter the threats that we have, that someone coming in new would need to learn about the innovation of this technology and its history and its evolution rather than just the latest and greatest new bit of technology.

I think also I have seen several efforts by regulatory agencies and oversight agencies to automate processes to actually take away personnel from copying down notes off printed-out sheets and submit things programmatically that would definitely assist in making sure that the government's resources are best used.

Chairman PEARCE. Ms. Haun?

Ms. HAUN. Yes. I think it is also a question of shifting resources because I was brought into the department as a gang and murder prosecutor, and then I switched. So it is not that I became useless; I think you have personnel who are capable of adapting to new areas.

I think one of the problems is that the government and a lot of the agencies are very siloed. So, for example, we have a cyber unit, and only the cyber unit is maybe getting trained on these cryptocurrencies or the dark net; but the fact is it affects the narcotics unit, it affects the national security unit, it affects the white collar unit, the financial fraud unit, the public corruption unit.

So I think you can shift those resources, but it needs to be across-the-board.

At the same time, I do think resources are necessary for training not only in government but in the public-private partnerships. The Blockchain Alliance goes a long way. They have webinars that people can watch. So these are actually free resources.

Chairman PEARCE. Okay.

Mr. Wilson, and pretty briefly, I am out of time here.

Mr. WILSON. Yes, sir. I agree with Ms. Haun. It is overall training. Anything that you can do with regular cash you can do with bitcoin or virtual currencies, so there needs to be a centralized training.

And you have a huge—what is a technological gap, as well. Some law enforcement agencies and private industry are just now figuring out that you can trace these transactions.

I think those are two big areas.

I was a counterterrorism agent before I went to the Cyber Task Force. I took it upon myself to learn these things and put the task force together. So those are just some of the huge hurdles that they are facing out there.

Chairman PEARCE. Thank you.

Thanks to each of you.

My time has expired, and I recognize Mr. Lynch for 5 minutes.

Mr. LYNCH. Thank you very much, Mr. Chairman.

I just want to take a minute to say thank you to you, Chairman Pearce, and also Ranking Member Perlmutter, for your really forward-leaning approach on this issue.

And I also want to thank the witnesses because this is not the first time we have met and I want to thank you for all the energy you have put into trying to get Congress up-to-speed on this issue. Usually we are very much behind, but on this issue, I think with your help, we are almost up-to-speed.

Ms. Haun, I also want to thank you for highlighting the issue of personnel and resources. I was in Bahrain and Dubai, did a little work in the Gulf, and we have one Treasury attache who is responsible for, I think, five different countries. And he is bouncing back and forth with central bankers and totally—he's doing a great job, don't get me wrong, but he's totally overstretched, I think, in terms of our resources. So that is probably something that we can work on.

One of the problems I am trying to grapple with is the asymmetry here of, you know, three guys in a truck and a bunch of steak knives on a bridge in Manchester, and then our sort of—our defense out there talking about cybersecurity and larger systems. There is, I think, an effort by ISIL and others to use this interstitial approach where they hit us where we are not protected. And I don't know how we get at that.

I think this is an emerging issue for us. I know that, Mr. Brito, you have said—you described this as anecdotal, some of the use by terrorists, but I think we have to be prepared. As the use of this becomes more broad, by the general public, then I think, certainly, nefarious elements will capitalize, as well.

On the personnel side, in terms of trying to train people and the money and the time involved in getting people really trained as experts in this, in cybercurrency use and all the other issues involved, when we send our young people to West Point and to the Naval Academy, they go to school and—excuse me?

The Air Force Academy. Oh yes, yes. The Air Force Academy at Colorado Springs, as well. I am just using it as an example, not exclusive. But we commit them—they commit for 5 years beyond that, and so we—for our investment we get the return.

Is there a way that we can sort of—do you think it would be wise for us to set up some similar system where we have a lot of bright people who will be all over this stuff; I think it really appeals to some of the skills and ability of our young people—create a system like that: scholarships, maybe identify a handful of universities who would love to, I think, offer this type of instruction and education. Is that something that you have seen anywhere in our university systems? MIT, any places like that?

Ms. HAUN. I could speak to that.

I taught a cybercrime and digital currency class at Stanford and it was cross-registration from a number of departments—law, business school, computer scientists, engineers. And I am pleased to say that a number of those students actually ended up going to serve across the government in national security capacities, and our U.S. attorneys' offices. So I think the interest is there still in serving in those capacities, albeit in this new, emerging field.

Mr. LYNCH. Yes.

That is good to hear. I think we just need to do more of it.

On the other side, trying to build a system, an agency ourselves, and keep it up-to-speed, we haven't done a very good job of that internally with our government. We have legacy systems that are a problem.

I just want your feedback, any of you, wouldn't it be better to buy the system in terms—purchase the system on the private side and have cutting-edge technology rather than trying to construct it ourselves? Because Congress is subject to appropriations and, dear Lord, we are terribly slow in keeping up. I am just—like your own thoughts on that.

Anybody?

Mr. BRITO. I agree with you, and I think Mr. Levin and Mr. Wilson are being too modest to say that their companies are building exactly the system that allows law enforcement, and not just law enforcement but digital currency firms and banks who deal with these networks, to have greater visibility into the network.

Mr. LYNCH. Great.

I see my time has expired. Mr. Chairman, I would just ask unanimous consent to enter into the record this report: "Terrorist Use of Virtual Currencies," by the Center for a New American Security, by Goldman, Maruyama, Rosenberg, Saravalle, and Solomon-Strauss.

Chairman PEARCE. Without objection, it is so ordered.

Mr. LYNCH. Thank you.

Chairman PEARCE. The gentleman's time has expired, and just by way of kind of updating the subcommittee, after our meeting we asked Mr. Budd and Mr. Davidson and Mr. Lynch and Mr. Foster to come together and really address this idea of adjusting a protocol and the reactiveness of our team, our governmental team, to sort of keep up and see if we can think of a new approach to this.

So again, I thank the gentleman. And it looks like we have five really good people here that you all can work with.

I now recognize Mr. Pittenger for 5 minutes.

Mr. PITTENGER. Thank you, Mr. Chairman.

And again, I thank each of you for your participation with us and for the many times that you have come to address us and engage in this dialogue.

Certainly something that, as you pointed out, Ms. Haun, it is a growing sphere of engagement by those who seek illicit transfer of payments—$90 billion, I had never heard that figure before today, and that will certainly continue to increase. And I think we have found in the past that those with nefarious interests look for—like water going downhill. If they get blocked one way they are going to go somewhere else, and I think we should be anticipating—not

waiting, but anticipating that they will enter into this arena in greater dimension.

To that end, I think the points have been well made in terms of personnel and training. I would like to get your thoughts, just for clarification. If somebody has sophisticated cyber training, they have been certified by SAS or some company like that, is that a strong foundation for being able to move over to address these blockchain types of transactions?

Ms. HAUN. Is that question to me, Mr. Pittenger?

Mr. PITTENGER. Sure, or any of you who would like to answer, but just go ahead.

Ms. HAUN. All right.

I think the answer is it is not necessary. I think it would provide a good foundation, but I founded a digital currency task force out in San Francisco comprised of numerous agencies and none of them had that SAS training. All of them, however, were very interested in this new field and they were looking for something new in their career; perhaps they had done cartel cases before. And so everyone brought something different.

And actually, the technology, a bit counterintuitively, is not that hard to get up to speed on. I really do think that if you watch a few webinars, you go to a few training sessions, and all of a sudden you really know a lot more than you thought possible in a short time.

Mr. PITTENGER. Maybe if I could ask you, then, to that point, you question the merits of bringing on new people. Why would that be a problem if it could be adapted so easily?

Ms. HAUN. Oh, I don't think there would be any problem with bringing on new people. I just, to the chairman's question about do all of our existing people become obsolete, I think that need not be the case either.

Mr. PITTENGER. Okay.

Ms. HAUN. But certainly, of course, I would always say new people—more people are better because we have—dealing with criminals—

Mr. DUEWEKE. It needs to be the right type of people.

Ms. HAUN. The right type of people, but dealing with criminals we have too much business, so yes. Good point.

Mr. DUEWEKE. One of the big problems, though, in this whole conversation is it is overly focused on understanding the blockchain.

Mr. PITTENGER. Okay.

Mr. DUEWEKE. That is a component, and it is actually a fairly small component of the overall virtual currency threat and usage by criminal organizations, et cetera. It is not so much a matter of understanding the technology behind the blockchain; it is having people who understand global payment systems that are on the cutting edge and understand the fintech, the mobile payment systems, the blockchain systems. It is much larger than just, "Hey, let's get some smart kids who understand the blockchain."

You really need to understand the entire payments world, and that is what I have seen in a lot of the training that I have done within U.S. law enforcement and law enforcement around the world. They are just trying to grapple with this one piece, the

bright, shiny bitcoin, I call it; they really need a much broader understanding, and that isn't something that necessarily comes easily from quick training.

And probably what you need to do is foster a better relationship, this public-private partnership, so that the payment processors, the Coinbases, the First Datas, you have a better relationship with them because they are the ones that have this knowledge that takes, frankly, decades to really understand all of these systems globally, and that is what is missing.

Mr. PITTENGER. Yes, sir, Mr. Brito?

Mr. BRITO. I have to agree with Mr. Dueweke. And I think part of what is happening in this conversation is that myself, Ms. Haun, Mr. Levin, and Mr. Wilson are here because we are focused on decentralized digital currencies. Cryptocurrencies is another name for that, bitcoin being the number one example. It was the first cryptocurrency and it is the largest cryptocurrency today.

That said, what Mr. Dueweke is rightly pointing out is that if you think of a pie chart, decentralized cryptocurrencies like bitcoin account for a tiny sliver. You have other digital currencies that are centralized and, as Mr. Dueweke was pointing out, account for a lot of the use by illicit actors.

Mr. PITTENGER. All of your points are well taken. I think we really have our work cut out just getting this on the radar screen to make sure that people see this venue, and so that we can address it in a comprehensive way. I don't think the public at large—in fact, I don't think the Congress fully understands the depth of opportunity that is there for those who seek an illicit transfer of funds.

Thank you. I yield back.

Chairman PEARCE. The gentleman's time has expired.

And just sort of in response to Mr. Dueweke, you are exactly right, but our hearing today is on virtual currencies and so we are trying to get that, and then we had yesterday the meeting that was digging into the actions and the patterns of actions. We will merge these two together in the future, and again, that is our kind of subgroup of four people who are tasked with that. But again, a very accurate observation.

The Chair now recognizes Mr. Kihuen from Nevada for 5 minutes.

Mr. KIHUEN. Thank you, Mr. Chairman, and Ranking Member Perlmutter, for organizing this hearing.

And thank you, to all of you, for testifying this morning.

I just have a couple of quick questions, one regarding mixing. For my colleagues who might not know, since the transactions of some cryptocurrencies that are recorded on the blockchain, mixing is a way to launder payments that may be connected to tainted sources.

Ms. Haun, since you prosecuted some of these cases, are you worried that mixing might become so sophisticated that it might become very hard for law enforcement to track some of these transactions for criminal activity?

Ms. HAUN. Yes, I am.

Right now the technology isn't there to be as sophisticated for the mixers and tumblers, we hear them called tumblers. But, of course, anything that further anonymizes things make it more difficult for

law enforcement authorities to kind of follow the trial, so I am worried about it.

We have heard analogies to—Jonathan mentioned earlier it is like a mask. Think of it, if you are a person who is going in to do some bad acting, and you are wearing a mask, we can't see you because you have disguised yourself. But if you wear that mask again later, we know it is you.

The problem with tumblers and mixers are that let's just say all of those masks that people are wearing get taken off and melted all together and then their different—the masks are reconstituted and put on, so then we don't know that it is you again. I don't know if that analogy makes sense, but that is kind of how we think of them.

So we do think that is a problem, but I think more of a problem right now are the overseas unregulated exchanges. And those are in countries that you might guess at, and we simply see those nefarious actors using these cryptocurrencies are not using these U.S.-regulated exchanges; they are using the ones that are overseas.

Mr. KIHUEN. So do you think that we need to put restrictions on the mixing?

Mr. LEVIN. Yes. If I could also comment, I think that there have been—FinCEN refers to services that transmit virtual currencies on the behalf of other people, and it is—there is a good chance that mixers do come under that jurisdiction, so if it is in the United States there are actually some mechanisms that law enforcement might be able to use to put pressure on those mixers.

Mr. BRITO. If I could add, in some cases you can think of completely legitimate regulated exchanges in this country. You send money to them. At that point it sort of becomes invisible to the software, and then eventually the money goes out. And so in some ways you can think of those as mixers, but it is not a problem because they are complying with FinCEN guidance and with the Bank Secrecy Act.

So the problem is not so much that there is mixing happening, that there is a third party that is keeping funds on behalf of a third party; it is that you have mixers that are completely unregulated and not subject to—or not complying with the BSA regulations, and I suspect, as Ms. Haun was saying, that these are overseas, as well.

Mr. DUEWEKE. And that is a critical part of this, too, the global nature of this and that you have thousands of these unregulated exchanges that are not limited to just that one segment of virtual currencies being centralized—or decentralized, but also the centralized virtual currencies as defined by THADP and acting as a mixer, the best way to mix, actually, is to go to one of these unregulated exchanges and exchange bitcoin for light coin, for dark coin, or for web money or one of the other non-cryptocurrency systems, and then change it back.

You are not following that. It is better than a mixer.

Ms. HAUN. And absolutely, as I alluded to in my written testimony, 100 percent of ransomware campaigns we have seen cashing out through exactly these overseas exchanges, so it is a huge problem.

Mr. BRITO. So I would simply put a point on that by saying mixing is not a problem. Again, mixing is a technology that is neither good nor bad. It is mixing and not complying with the BSA that is a problem.

Ms. HAUN. But to your question about could we regulate these things—and I appreciate Mr. Levin's comment that in the FinCEN guidance it could be construed to regulate—to reach mixers or tumblers. I am not so sure that a prosecutor or FinCEN would take that aggressive of a view. Maybe they would, but certainly if this were included in Section 1960 as explicitly clear, that gives—that statutory authority gives prosecutors a lot more comfort that, oh, no, this technology is absolutely included in a 1960 definition.

So I think that would be important. FinCEN guidance alone is not always enough for us to bring these new cases that are the first cases of first impression.

Mr. KIHUEN. Thank you all so much.

Thank you, Mr. Chairman.

Thank you, Mr. Ranking Member.

Chairman PEARCE. Thank you. The gentleman's time has expired.

The Chair now recognizes the gentleman from Colorado, Mr. Tipton, for 5 minutes.

Mr. TIPTON. Thank you, Mr. Chairman.

And thank you, panel.

Ms. Haun, maybe you would like to follow up a little bit on the last question when you were talking about the 1960 regulation. And listening to Mr. Dueweke describing the mixers, given all of the complexity that is there, even with that authorization, how difficult is it really going to be for law enforcement to be able to track this information even with authorization?

I think there was a RAND report that came out of some of the criminal activity that is going on—RAND National Defense Research Institute—saying that criminals are increasingly gaining access to technology and encryption tools that could allow them to design their own virtual currencies to circumvent the global financial system.

Given that complexity and just your statement, how difficult is it for us really to be on the front end of this curve rather than being reactive trying to catch up?

Ms. HAUN. I think, again, and I hate to keep coming back to it, but the big problem I see are the unregulated and unregistered exchanges. I think we can keep up with more resources and more people and more agents knowing what this is.

I think we can keep up where we have tumblers and mixers or virtual currency exchangers in the United States subject to our jurisdiction, and we have some choice 1960 prosecutions. I think we can keep up.

Where we have a problem is in getting at that information or forcing compliance from these overseas entities. And not surprisingly, the bad actors—the terrorists and the massive cybercriminals—are not using the registered Coinbases of the world that are in San Francisco, that are registered with FinCEN.

So I think that is going to be a problem and we can't keep up with those as the matter currently stands.

Now, one thing I would say is a lot of those businesses or ransomware campaigns, et cetera, or even these unregulated exchanges, they actually rely on a lot of U.S. companies and a lot of presence in the United States. People are always surprised by this. They think, "Why would their servers be in the United States? Why would their infrastructure be in the United States?"

We have a reliable source of energy and power. We have massive companies, like Amazon Web Services or Google, who provide these hosting platforms.

So these big, unregulated, unregistered exchanges do use Google and Gmail; they use Microsoft; they use Amazon. And I think we could use some tools in our toolkit—statutory tools—to more easily chip away at those parts of their businesses that touch on the United States.

Mr. DUEWEKE. Congressman Tipton, I totally agree. The focus should be on the ingress and egress and conversion points. The unregistered, as she put it, exchangers around the world are the point, but I have a very dim view of us being able to cope with them effectively because the barrier to entry for setting up an exchange is so low. It doesn't require you to have a company. It requires you to have a server and some accounts with these different types of payment systems that you want to convert from and to. Very low.

I have done research myself on thousands of these systems, rated them for anonymity, et cetera, and they are incredibly amorphous. They go up and come down regularly. They will change into something else. You won't be able to identify exactly where they are or which systems they might be using in the background.

There might be better signals, intelligence-type things, that you could use to detect that, but we, I believe, are far, far, far behind, as well as law enforcement around the world, in coping with this. And these systems do gravitate towards areas with a relatively low rule of law, and oftentimes they seem to be, according to things I have read and researched, many times they are being protected by local political entities and law enforcement, and there are many stories that you could read about that online.

I also want to make the point that the position that bitcoin is not being used for any terrorist activities might be a bit stretched, as well. It is not reported in the United States but it is well reported in Europe, including Agence France Presse, that four of the automatic weapons that were used in the Paris attacks were purchased with bitcoin from an online dark market seller in Germany. And that was reported in court—open court documents in Stuttgart.

So I agree it is not a huge problem, but there are examples where you have small groups that are using digital currencies, including bitcoin, to anonymously buy what they need to carry out their heinous attacks.

Chairman PEARCE. The gentleman's time has expired.

The Chair recognizes the gentleman from Colorado, Mr. Perlmutter.

Mr. PERLMUTTER. A lot of Coloradans around here.

I want to follow up on Mr. Tipton's line of questions and ask you, Mr. Dueweke, and you, Ms. Haun, and to the rest of the panel, okay, when you say an "unregistered exchange," what is that?

And in your testimony, Mr. Dueweke, you talked about a number of different things—WebMoney, and Perfect Money, and dark money, and Alipay. Do you consider that an exchange or is that a medium of transfer, or—help us understand your terminology.

Mr. DUEWEKE. I teach a 2-day course on this so it is not necessarily that easy, but the terminology—and I would be happy to provide the committee with a topology, a single-page topology that makes sense of these different characteristics.

When you are talking about the large providers like PayPal, WebMoney, Alipay, they do have the ability to act as an exchanger as part of their overall digital payment system. And certainly with systems like WebMoney, that have been shown by other researchers to not be doing strong know-your-customer (KYC), they are suspect and are certainly being used for criminal activities, and a lot of that is they are not doing that good KYC up front.

However, what Ms. Haun is talking about and I have referred to with these other exchangers are entities that set themselves up specifically to exchange one virtual currency for another virtual currency, or for a fiat currency, or for a mobile money system. And all it requires really is a computer, accounts to be set up with these different services, and some level of liquidity, which oftentimes is one of the limiting factors in how effective these exchangers are is how much money they have to buy and sell. They might only have $20,000, $30,000 on hand, whereas the big ones, of course, like Coinbase, have many millions. So—

Mr. PERLMUTTER. All right. And they are kind of the fence in this thing? Are they fencing the stolen goods?

Mr. DUEWEKE. Not so much fencing. It is really—just think of a currency exchanger on the street of some country. You would go and give money—one type of money and they give you another type of money coming back.

It is that, but in a much larger sense for digital payment systems, and the level of anonymity for these unregistered ones can be extremely high because typically they are not doing the KYC; they are not doing the AML.

Mr. PERLMUTTER. They don't care whether it is dirty money or not.

Mr. DUEWEKE. They don't care—

Mr. BRITO. So to answer your question directly, if I want to use bitcoin I need to first acquire some bitcoin.

Mr. PERLMUTTER. Right.

Mr. BRITO. Typically the way you do that is you go to an exchanger and you give them dollars and they give you bitcoin. That exchanger in the United States is a Bank Secrecy Act-regulated entity and has to register with FinCEN, keep records of its customers, and report suspicious activities. So that would be a registered exchange.

And that is who Ms. Haun would go to when she is using Mr. Levin's software and finds a bad guy. She can go to an exchange and say, "Who is this person?" and get the information.

Overseas we see unregistered exchanges—exchanges who, although they are required to, do not comply with the Bank Secrecy Act. And so when Ms. Haun requests information from them I bet

she doesn't hear back from them. That is what an unregistered exchange is.

Ms. HAUN. Or—

Mr. PERLMUTTER. Go ahead.

Ms. HAUN. Or we hear back from them—in a good case scenario I had an MLAT with Japan, for example, where we have an attache on the ground, cooperative partners on the other side, and that even took at least 6 months in a very high-profile case to even get that evidence. So that is in a good case where we have to go to another country, we can get something.

But I think there is another step beyond that, which is an exchange in, say, Russia. Not only could we not go to them, but if we go to them we know what we find back is—and we have actually found this in returns before and evidence before—is the owner of this account is Mickey Mouse who resides at 123 Main Street. That is actually—

Mr. PERLMUTTER. I guess that is what I am worried about, that we have some nation states that are actually fostering making these exchanges impossible to pierce, to understand, to find, whether they are trying to avoid sanctions, whether it is North Korea or Russia avoiding sanctions or helping some criminal enterprise, or underwriting some terrorist organization that is out there doing bad things.

So I am very concerned about how we stretch this globally to get countries that we may be at odds with, like Russia or maybe China, to participate. Are we doing that?

Mr. DUEWEKE. And that is where this—a public-private partnership, having an association where there can be a real mercantile reason for them to want to participate, and where there is a push from the corporations, the companies themselves to want to be part of this. And you have seen this recently in Russia with Kiwi and Yandex.Money have started just in the last year following AML and KYC while WebMoney hasn't. So part of them they want to be integrated in with European payment systems; the other one is kind of remaining off on its own.

But that type of public-private partnership where you can get them to work together with other countries and other companies I think is key because you are not going to be able to do this by dictate from the United States, I don't think.

Mr. PERLMUTTER. All right, thank—

Mr. WILSON. Sir, so this is—

Mr. PERLMUTTER. —you for your—

Mr. WILSON. —normal criminal activity. Criminals are going to go where the path of least resistance is. So if I can go exchange my bitcoin to an exchanger that is not compliant with U.S. laws, that is what I am going to do. That issue there is that they are trying to circumvent our AML procedures and they are using—I mean, all criminals do that all the time.

So that is something else that we need to look out for. It is further down the line. It is happening, but the bigger issue is trying to get these guys trained up to notify, to notice this kind of criminal behavior happening.

Mr. PERLMUTTER. Okay. Thank you.

Chairman PEARCE. The gentleman's time has expired.

The Chair now recognizes the gentleman from Texas, Mr. Williams.

Mr. WILLIAMS. Thank you, Chairman Pearce.

And to all the witnesses today, this has been great.

I want to spend my time this morning focused on money laundering, specifically trade-based money laundering, which, as you know, is just one method used to launder illicit proceeds, and how that relates to virtual currency. According to the FATF report of virtual currencies, two major themes have developed: one, virtual currencies are the wave of the future for payment systems; and two, virtual currencies provide a powerful new tool for criminals, terrorist financers, and other sanction evaders to move and store illicit funds out of reach of the law enforcement or other authorities.

So let me start with you, Mr. Dueweke. In your testimony you spoke about the capability to move unlimited amounts of funds completely outside the Western financial system. You also mentioned transfers to and from terrorist organizations, especially as part of a trade-based money laundering scheme to cause the investigators to lose their money trail.

As we have heard many times during our previous hearing, these schemes can be highly complicated, so virtual currencies just add another layer. So my question is, can you expand on the steps we need to take to help all of the stakeholders involved, whether that be local law enforcement or financial regulators or private companies—I am a private sector guy—and to understand the scope and scale of these schemes?

Mr. DUEWEKE. I think the key is education. I have participated in some investigations where people have had information on different bad actors and had it sitting there for a year because they didn't know what WebMoney was. They didn't know what these systems were or how they could interact with other components of the trade-based money laundering schema.

And all it really takes is one leg of maybe—a lot of these trade-based money laundering schemes can include four or five different hops, cars for drugs for whatever, and all you need is one component to jump in and out of one of these virtual currencies, whether they be centralized or decentralized—probably more likely to be decentralized than centralized like bitcoin, or decentralized—I am sorry, more likely to be centralized than decentralized because when you are using a system like bitcoin, a large transaction is going to stand out and it will be tracked by Elliptic or Chainalysis.

But if you are bringing it in and out of a centralized system and perhaps you are working with the Russian mob or something like that, it is not going to show up and be detected by anybody and it is going to allow you to basically lose the trail of investigators that are following it through traditional mechanisms.

So I think the first step has to be education. You have to have people start to understand what is possible because when we did that in past training there were huge breakthroughs that resulted almost immediately because they found that, "Oh, wow, these bad guys were using these systems as part of this and we just had no idea what we were looking at."

Mr. WILLIAMS. Okay.

Let me switch topics really quickly, Ms. Haun. Section 13 of the Combating Money Laundering, Terrorist Financing, and Counterfeiting Act of 2017, a bill introduced by Senators Chuck Grassley and Dianne Feinstein, directs the Department of Homeland Security and Customs Border Protection to provide a report detailing the strategy to detect prepaid access devices and digital currency at border crossings and ports of entry.

So my question would be, what are your thoughts on this bill and what are the pros and cons of including prepaid cards regulation—in that regulation?

Ms. HAUN. I think that prepaid cards—we have seen that prepaid cards are used by nefarious actors quite a bit, and so I think that it is sensible to include prepaid cards, if that is your question, in that bill. And I have only just seen reporting of it; I haven't yet had an opportunity to read the bill itself.

But I think this is what I was saying about giving—there is already some regulatory guidance, but giving statutory—making the statutes explicit give prosecutors a lot more of a path, a clear path to bringing cases. And we saw this with 1960 where there was a case in Florida where a judge said, "Well, I don't think 1960 includes virtual currency." So I think this would be getting at remedying something like that.

Mr. WILLIAMS. Okay.

I have a little bit if time left, so let me come back to you, Mr. Dueweke. Can you go into more depth about the Identity and Payments Association you launched and what role they can play?

Mr. DUEWEKE. I had been part of a lot of conferences around the world where I had heard story after story about the de-risking of virtual currency providers, exchangers, remittance companies, mobile payment companies that were basically losing their bank accounts because banks didn't understand it, et cetera.

And I saw that really what was needed was some sort of public-private partnership to take all the regulators, the law enforcement around the world that I had been working with in training, bring them together with industry members to find a common path forward where we could agree on best practices, where we could agree on basically a coda like Visa and Mastercard have—in fact, I have one of their former V.P.s working with me on this—where you basically could set up a rule-set where if you follow all of this, you identify a person given these steps, you are not going to be liable to prosecution, or you will be considered in somewhat of a regulatory compliance.

And that would require this public-private partnership, so that is at the heart of what the Identity and Payments Association (IDPAY) is intended to provide, because there is nothing like that globally. It is all done by individual countries, and not very many of them are tackling this topic.

So because of the global nature of the ecosystem, it needs to be tackled globally and it will require some sort of NGO to do that.

Mr. WILLIAMS. Okay. Thank you all for being here.

Chairman PEARCE. The gentleman's time has expired.

The Chair now recognizes Mr. Rothfus for 5 minutes.

Mr. ROTHFUS. Thank you, Mr. Chairman.

Mr. Levin, as we look at other governments hostile to the United States developing anonymous weaponized cryptocurrencies for use against us by criminal or terror organizations, do you have any thoughts on how the U.S. or the international community could counter those efforts?

Mr. LEVIN. Yes. Thank you very much for the question.

When I think about what this testimony is about, it is about virtual currencies that are truly global and decentralized. If the adversary is choosing to account for trades within its own organization on some sort of ledger, that doesn't really pertain to what Congress or anyone else can do about those types of payments.

What we are talking about is a financial system in which everyone in the world can access virtual currencies, as I understand it, as bitcoin. And for that the U.S. Government can have eyes on those types of transactions and would need to be able to have tools in order to understand the purposes and the actors that are behind those transactions.

So I am less worried, actually, about states producing their own virtual currencies no matter what technology they use because the risk to our society is mostly around being able to fund and send value to anyone in the world to carry out acts like we have seen in the past.

Mr. ROTHFUS. So you are not concerned about any kind of internal—

Mr. LEVIN. Yes, because those types of systems already exist, and while we cannot have eyes on them we have no way to put any pressure on those types of systems.

Mr. ROTHFUS. If I could ask Ms. Haun, the idea that virtual currencies out there, bitcoin, that is going to be an asset that perhaps a bad actor is going to have. What would be the possibility of using our asset forfeitures procedures to go after that virtual currency? Can we do that? How would we do that?

Ms. HAUN. Yes. In fact, we have done that and we have used exactly that authority.

So in a case I had we did, we seized those assets under the asset forfeiture laws upon a proper, of course, judicial order. And right now there are a lot of questions about, how do we auction those off? What does the government—now that we own these because they have been forfeited, what do we do? What does the government do? We are the holders of bitcoin now.

And there is a series of disparate things that have happened. The Marshals Service has auctioned them off, so yes, we can do that, and we should do that.

In fact, in a case against an exchange in the United States that my office did involving Ripple Labs in 2013, we brought the first-ever enforcement action against a virtual currency company. We teamed up with FinCEN to do so, and they had to pay and forfeit a $700,000 penalty. They also had to take a number of remedial steps so now when they collect customer data, they must follow all AML laws, know-your-customers, and they collect customer identity.

But I think that the asset forfeiture laws are an important tool as part of this. That is particularly true if we are ever to get to some of the overseas exchanges because, of course, they have cor-

respondent banking accounts with banks, including in the United States. And I would think that would be an appropriate case to use those laws.

Mr. ROTHFUS. Mr. Brito, do you foresee any widespread acceptance of virtual currencies by small to medium-sized businesses in the future whereby domestic criminals could launder illicit profits into bitcoin or virtual currencies?

Mr. BRITO. It is certainly possible. I think, however, that cryptocurrencies like bitcoin really can't compete in the developed world with our existing financial system. We have credit cards; we have cash; we have access to just our phones can pay for things, and you do it really frictionlessly and very well.

Where digital currencies I think are going to really thrive is going to be in the developing world where they don't have access to those financial systems and there really isn't an incentive for networks to go in and develop those networks. So I think that is where we will see retail payments take up for cryptocurrency.

In the developed world, where I think cryptocurrency has a truly bright future are for really novel uses that our existing financial system really can't accommodate—things like micro transactions, transactions that maybe are trade settlements of sort of other assets.

Mr. ROTHFUS. I yield back.

Chairman PEARCE. The Chair now recognizes the gentleman from Ohio, Mr. Davidson, for 5 minutes.

Mr. DAVIDSON. Thank you, Mr. Chairman.

And thank you, to our guests. I really appreciate the information you are giving us and the tools you are helping us be equipped with to keep our laws current.

I am particularly struck by the analogies to the Internet, but also it seems to me that some of this stuff with blockchain is a little bit like the cell phone. Did criminals gain an advantage when they could communicate by cell phone? Well, of course they did, but so did the rest of the planet.

And I think they are going to be just about as hard to contain, so those of you who have mentioned that, I think people are going to be able to do blockchain transactions of all sorts, including in currencies.

Mr. Wilson, I was particularly struck by your opening remarks where you talked about how we can detect the activity. And it seems that if we have this ability, which we theoretically should, that we would be able to find the missing Mt. Gox coins. Why can't we?

Mr. WILSON. We actually did find those. Chainalysis was the official investigators in the Mt. Gox bankruptcy case and the destination of those coins is definitely known.

Mr. DAVIDSON. Okay. Terrific. So what happens to lost coins in general? If they are stolen and you find them, what happens when people lose them?

If you lose your credit card, you can cancel it. If you lose your key to a car, you can get it re-keyed. What happens when you lose cryptocurrency?

Mr. BRITO. It is the same thing that happens when you drop a dollar bill into a fire. If you lose a dollar and it is at the bottom

of the ocean or something bad happened to it, the Federal Reserve does not replace it for you. It's the same thing with bitcoin. It is gone.

Mr. DAVIDSON. That's a bad password to lose.

Mr. BRITO. Yes. Correct.

Mr. DAVIDSON. Okay.

I guess without compromising trade secrets, how are we doing—and I understand that, Mr. Levin and Mr. Wilson, your organizations are working to track mixers and other tumblers, things like this that are making it hard to find currency. Is that accurate?

Mr. WILSON. Yes, it is. We are tracing those, as well.

Mr. DAVIDSON. Okay. So these are the most complex things. How is this different—so regular currency, foreign exchange is regulated in the United States by the Commodity Futures Trading Commission. They, rightly or wrongly—in my opinion, wrongly—restricted the number of people who can trade currencies by raising the capital requirements. I think it puts the U.S. at a disadvantage in one of the world's most important markets, and I am concerned that our regulatory framework with cryptocurrency is going to further hinder our ability to do it.

Can't currency be regulated by one organization, whether it is physical or virtual?

Mr. LEVIN. I think the answer to that could be yes, and it would definitely allow businesses to be more compliant and put their efforts into one domain. I think that also if that regulator adopts technology that is in line with digital currencies like bitcoin, and has tools and automation that will definitely allow the United States to have a business environment that thrives whilst thwarting bad actors.

Mr. BRITO. Digital currencies are one of the most regulated sectors within fintech.

Mr. DAVIDSON. Yes.

Mr. BRITO. And the reason for that is that they are subject to many different regulators and jurisdictions, and so at the Federal level you have the IRS, you have the CFPB, you have FinCEN, and there have been FTC enforcements. There are many.

But really the largest sort of barrier is State-by-State regulation, because if you are a digital currency exchanger or some other kind of custodian for digital currencies, the consumer protection regulation today is done at the State level. So if you are an exchanger you need to get a license from every State in which you do business.

Mr. DAVIDSON. Right. Yes, so you made that point and it is a good one, but why is digital currency so much different than foreign exchange? Why would it be—what is necessary to be treated differently about this other than you have to have different technology?

Mr. BRITO. Because digital currency exchanges are considered money transmitters, and money transmitters are regulated at the State level.

Mr. DAVIDSON. So are foreign currency exchangers.

Mr. BRITO. So it is kind of the same thing. You have the—

Mr. DAVIDSON. Aren't they essentially involved in the same business? If I want to convert U.S. dollars to pounds sterling or euros or RMB, whatever, you can do that through—

Mr. BRITO. It is similar. The one really different piece is that foreign currency is defined in law, whereas digital currency is defined as basically the other category. But that is as far as money laundering is concerned.

Mr. LEVIN. I think also it is different in the sense that you can operate very—and this is probably too technical for this setting, but there are many different types of business models that can exist built on blockchain technology, which may not have perfect analogies in the existing financial system which require people to actually understand the technology in order to regulate it properly.

Mr. DAVIDSON. All right.

I look forward to working with you all. My time has expired.

Mr. Chairman, I yield back.

Chairman PEARCE. I thank the gentleman. His time has expired.

The Chair now recognizes Mr. Hill for 5 minutes.

Mr. HILL. I thank the chairman very much.

And I appreciate the panel's time. This has been a really interesting discussion about a topic that probably needs more exposure in Congress across a number of committees.

Ms. Haun, I was particularly interested in your testimony because we have had a lot of talk about the currencies and we have had a lot of talk about blockchain, but I am really interested in the ways that we have our laws and our regulations, our oversight structured in such a way that we do a better job in our government of either assessing their need for oversight, regulation at the Federal level, or the interdiction, capture, and discovery of them.

So you referenced extensively in your testimony about our MLATs around the world between the United States and our allies and other countries, and you referenced some, the need to modify our MLATs for this particular purpose. Could you go a little bit more specific and tell the committee just what particularly we ought to amend in our basic MLAT treaty with other countries to capture this discovery and prosecution area? Thanks.

Ms. HAUN. And I should note that this isn't just a problem—I also did a number of cybercrime cases not involving cryptocurrency. This MLAT problem is not unique—

Mr. HILL. Yes, and you can be broad in—

Ms. HAUN. Right. And so it really is a problem. I think if you talk to prosecutors across the country who are dealing with cybercrime and cryptocurrency cases they will tell you one of the biggest problems is the problems of getting MLATs through.

And it is always—we are in a good position where we have an MLAT, because at least then we have a country we can work with.

But the problems are essentially these: the speed—the MLAT process was developed decades ago, in the days where you didn't even have e-mail. These were done maybe by couriered mail, and the problem is that the systems have largely stayed the same.

And I will just give you an example. I had an MLAT going and it was to a receptive country. The actual company in that country wanted to give us the data. They would have e-mailed it to us right

away and it would have let us get the bad guy instead of letting that bad guy keep doing bad acts.

But instead we have to go through the MLAT process, and even to get it out of our own country to theirs took 5 months.

Mr. HILL. So have you seen an effort by the Department of State and the Department of Justice to form a task force between the two and streamline and make recommendations? And is there anything Congress can do particularly on that?

Ms. HAUN. I don't know that it is a State Department issue. I think the Office of International Affairs in the Justice Department is the entity that handles the MLATs.

And one of the things is you go from, like, say—I used to be in headquarters, though I have been out in San Francisco for the last 8 years. I am out in the field; I draft up the MLAT; I have to send it back to the OIA attorney. They have five levels of review.

I think it is off with the country, but no, lo and behold, it comes back to me so we can fill out a budget form so that we can get it translated. In other words, it hasn't even gone to our foreign counterparts who are sitting there waiting to turn over the evidence to us.

The budget form is completed and then we have—

Mr. HILL. The ship is in the dock waiting to transport.

Ms. HAUN. Right. Then we have to go to a certain kind of—not just any translator. Only certain ones are approved.

They have a backlog because they have all the government contracts, so they are not going to be able to translate ours quickly.

Okay, so you already see the point. The problem is even leaving—even a fully baked MLAT to get overseas, it doesn't happen for months. And that is in a good case. That is in a high-priority case where the department is willing to pay to expedite and the rest.

And the problem with that system, Congressman, is that what ends up happening is we even now need to send MLATs to get evidence preserved. If a company overseas has a 3-month—as some of these telecom companies do—preservation period, if we don't get an MLAT request over for 6 months, our evidence is just gone.

So I think part of the problem is internal and the processes by which it goes, and I don't want to upset any of my colleagues in the Justice Department by suggesting that Congress needs to form a task force, but it is something that really needs to be looked at, the process in the age of cybercrime and in the age where—we are moving to a world where more and more evidence in every case is electronic, right, no matter the type of case.

I don't know if that illustrates—

Mr. HILL. I appreciate your passion on the answer. This has come up in previous testimonies in the last Congress, not quite with the passion and the direct answer that you have given today, and I appreciate your service in criminal prosecutions, your service to the people of the United States

And, Mr. Chairman, thank you for the opportunity to question.

Ms. HAUN. Thank you.

Chairman PEARCE. The gentleman's time has expired.

The Chair now recognizes Mr. Budd for 5 minutes.

Mr. BUDD. Thank you, Mr. Chairman.

And I thank the panel, as well, for your time.

I think it was Mr. Brito—you mentioned earlier that you would lose—as you lost a dollar bill in a fire, you could lose virtual currency. Isn't there some sort of a virtual wallet that is recommended or a best practice? And if so, could you—if that does exist can you explain what that is and how it works?

Mr. BRITO. Yes. Sure.

So there are essentially two ways in which you can hold digital currency—kind of the same as cash. You can hold it on your person the way you might hold a $100 bill with you, or you can deposit it with a custodial institution. So if you deposit it with them and they are regulated and you trust them and they have good security measures, that is pretty safe.

If you decide to hold the digital currency yourself it has one advantage that a dollar doesn't, which is you can make a backup copy. Of course, you have to keep that backup copy safe.

But that is essentially it. You want to use some good, reputable wallet software, something that is open-sourced and that has been audited by the community; and you want to make sure that you have good backups in safe keeping, in safe places and that you never forget your password.

Mr. BUDD. Okay. Very good.

There was a great interview recently—I think it is a good 101 for a lot of us in here who are new to this—on The Tim Ferriss Show with Nick Szabo. I don't know if he is a recognized name in your industry, but it was a great primer earlier this week for me.

I went to Seoul, Korea, last week and to the DMZ, and as we looked over into North Korea you could see that there is not much of an economy there, and yet it is a country that we have seen is very strong in cyber offense, and that is—they have doubled down on that, as we know, moving towards a nuclear state, as well.

But with their cyber, what do we see—and this is—I will open this up to the whole panel—what do we see a country like North Korea doing with illicit uses of virtual currencies?

Mr. BRITO. I have seen media reports that some of the ransomware that we have seen attack different private companies and public sector organizations could be traced back to North Korea.

Mr. BUDD. Right.

Mr. BRITO. And you can imagine that North Korea, if this is true, would see ransomware as a revenue-generating activity. Of course, if they acquire bitcoin or some other digital currency they need to offload that and so they would need to go through an exchange. I bet they would go through an unregulated, unregistered exchange.

Mr. LEVIN. So I have seen the same sort of reports, although, as Ms. Haun will know, the attribution in cybercrime cases is very, very difficult to attain the identity of people who do them. What I have seen is—and I mentioned it in my written testimony—ransomware campaigns run in domains that I would consider hotbeds potentially for a terrorist activity, and it is about making a profit out of this type of activity in order to fund operations, so I think that risk does exist.

We actually have seen that there are very limited exchanges in a lot of these places, so we monitor for, is there liquidity in those

local markets to cash out for virtual currency activity? For example, there is no domestic North Korean exchange that you can cash virtual currencies into local currency; however, there are virtual currency exchanges in other parts of the Middle East, although liquidity is fairly limited. I know of two exchanges where the joint liquidity in their existence has been $2 million.

Mr. BUDD. Wouldn't you say, Mr. Levin, that it would be better for a country like North Korea to stay in virtual currency rather than egress or come out of it?

Mr. LEVIN. I would say the most likely thing that would happen is that they would use the virtual currency in order to pay for potentially incident infrastructure that actually exists, maybe even in the United States or off shore.

Mr. BUDD. And for the panel—I'm sorry, Ms. Haun, did you have a comment?

Ms. HAUN. Oh, no. Thank you.

Mr. BUDD. For the whole panel, as well—sorry, I had another question there—do you have any idea as to the total volume that you would see North Korea doing through virtual currencies?

Mr. LEVIN. Geographic identification of virtual currency transactions is somewhat difficult, especially where there is no exchanger present in that local market. So companies like mine can identify the services that are providing virtual currency services like exchange, like merchant processing, but if there are no sort of North Korean exchanges it is very difficult for us to be able to assess how much volume is in North Korea.

Mr. BUDD. Thank you.

I yield back.

Chairman PEARCE. The gentleman's time has expired.

The Chair now recognizes Mr. Lynch for 5 minutes.

Mr. LYNCH. Thank you.

I know the last time we spoke, we discussed the committee members perhaps taking advantage of the webinars or any other training opportunities to educate the Members, so committee staff will be reaching out to each of you on that.

Let me give you an extreme example: Somalia: We are having problems—a highly insecure environment, very low capacity among the government there, a fair amount of corruption. All of the banks have basically pulled out of that area. They won't even set up ATMs anymore. Al-Shabaab is very active.

The secure district is actually limited to a small sub-district in Mogadishu around the airport, and when we fly in it is tough to get out of the airport until really recently. And again, they get this aversion by regular banks, so remittances can't get in there. So we have a real problem.

How could this system, cryptocurrencies—I know we are sort of war-gaming this on the fly, but how could this help in an area like that where we have had such—so there is so much reputational risk on the part of the banks that they won't go in there because of our—ironically, because of our antiterrorist financing laws—Bank Secrecy Act and all those. So the banks won't go near it because they will say, "We don't want to be prosecuted in case Al-Shabaab gets the resources."

Is there an opportunity here that, on payment systems, is there some way we might help the people who just want to send money back to their families?

Mr. DUEWEKE. Absolutely. Yes, and I think that is one of the keys cases that drove me to create the Identity and Payments Association, where you have a community that is cut off from the banking world that is relying on remittance systems like Impesa or WorldRemit or a few others, that have been impacted by AML and CFT efforts that have cut them off in some instances from Somali populations in Minneapolis or wherever.

And while they are relying on those systems now, they are prone to disruption, and certainly having an enhanced, in this case, cryptocurrency or decentralized virtual currency connection point with those systems, if done in concert with somebody like WorldRemit who is a very responsible player and tries very hard to identify the users of its system, then you would have an even more reliable, more transparent component where you would have bitcoin or a blockchain-based system be able to interface with those last-mile mobile payment remittance providers.

So yes, I think it would be able to extend the secure paradigm further out into the Somali populations to allow them to get money to those people who need it the most, and do it in a responsible, transparent way. But you are going to have to have some sort of relationship with a lot of different players because there a lot of Somali populations around the world.

Mr. BRITO. And if I can address that, so the—

Mr. LYNCH. Sure.

Mr. BRITO. If I could just say that—

Mr. LYNCH. Please, yes.

Mr. BRITO. —the Charity and Security Network is a nonprofit that represents other nonprofits—

Mr. LYNCH. What is the name of it again?

Mr. BRITO. Charity and Security Network.

Mr. LYNCH. Okay.

Mr. BRITO. And they published a report recently that looked at exactly the problem you are describing, and it is not just conflict areas like Somalia or Syria where they are having trouble getting payments in. It is Latin America; it is Europe, even.

And we are actually going to be—the Coin Center will be working with the Charity and Security Network to develop a pilot program to potentially send grant money from the United States to Mexico, to nonprofits in Mexico who are running grant programs using bitcoin.

Mr. LYNCH. Wow. That is great.

Mr. LEVIN. I could also add—

Mr. LYNCH. Mr. Levin?

Mr. LEVIN. —I think the interesting thing about having a cryptocurrency on the underlayer of this is that the traditional financial system relies, when money goes from a bank to a money transmitter and then gets sent to Somalia, the bank gets very nervous because it has no ability to have any insight into the underlying transaction to the customer's—their customer's customer.

What bitcoin allows—and I have actually implemented this with Barclay's and Circle Financial, which are two sort of well-known

fintech companies—is that the bank is actually able in real time to know what is the underlying activity of its customer, not on an individual who is the identity of the person, but potentially what is the exposure to underground market activity, or ransomware, or the terrorist financing activity that we are interested in.

So I would like to point to that case, and I'm happy to go further in more detail.

Mr. LYNCH. That is great. Thank you.

My time has expired.

Chairman PEARCE. The gentleman's time has expired, and the Chair now recognizes Mr. Pittenger for 5 minutes.

Mr. PITTENGER. Thank you, Mr. Chairman.

Again, I thank each of you for being here to give us your sound advice.

We are dealing with very sophisticated people, as we have found in the past. And this is not a backyard gang of hoodlums. They look for every possible avenue to complete their efforts.

I would like to say that as we consider the cryptocurrencies, while they are not well-known to the public at large and they are growing, certainly to these folks it is on—they are on the radar screen and we, as I said earlier, should anticipate that they will be more engaged, more likely in—outside of the United States, as you said, where there is—we don't have the capacity for oversight that we have here.

I would welcome your involvement, particularly with the media. I think you play a role there and I think you could help define what you are doing in terms of defensive postures, and offensively, and to mitigate this concern.

I think we need, each of us, to speak to this more to let the public and, as well, that the Congress be more adept in these concerns. So on your radar screen I hope that you will consider a more aggressive outreach to try to work with the media and to help tell your story.

Thank you very much. I yield back.

Chairman PEARCE. The gentleman yields back.

The Chair yields himself another 5 minutes.

Mr. Wilson and Mr. Levin, as we discussed the WorldRemit and the retroactive nature of it, in the current system can we assure the same way that Western Union might be able to assure that crypto going into Syria or Somalia could be traced and may be stopped before the incident is—discuss that just a bit if you can.

Mr. LEVIN. Mr. Chairman, so when you send virtual currency transactions outwards you may not know the geographic distribution of that—where the person you are about to send it to, because if you consider bitcoin it is—transfers within bitcoin are not sent to routing numbers or account numbers that have any real-world identification system. Instead, what you need to do is then look after the fact in order to understand what is the activity potentially for that transaction.

If we go back to the analogy of the masks, if you are sending it to someone that you have seen before then you might know that this is, yes, this bitcoin address does belong to a virtual currency exchange in Iran, for example, and you would be able to block that at the time of transaction if you are sort of an exchange here in

the United States. However, if someone is using a new virtual currency address, which are quite easy to create, there is no way to know that at the time, and instead these companies are forced to retrospectively look at all of their transactions in order to identify what was the activity maybe after the fact.

Chairman PEARCE. Mr. Wilson?

Mr. WILSON. Exactly what Jonathan said. What we do is after the fact look at the transaction and we can tell, again, if this is something that is masked. And we have already tagged it to be a nefarious exchanger or a nefarious entity we can then alert the institution that is making this transaction and say, "Hey, this is a possible place that you don't want to send money." So that is kind of how it works right now.

Chairman PEARCE. Ms. Haun, I would appreciate your observation on the same question if you can, because really looking at Western Union and their—I guess that they know both parties, that we have some understanding of who is on the other end, and they have been—will maybe even blacklist entire regions because of the risk, but it is not anonymous sites either.

Do you have an observation?

Ms. HAUN. I am not sure. I also know that Western Union has actually been paying some hefty fines and I think was just the subject of a FinCEN enforcement action about a year ago—

Mr. DUEWEKE. $800,000.

Ms. HAUN. $800,000, yes.

Mr. DUEWEKE. Or $800 million, I am sorry.

Ms. HAUN. $800 million. That sounds—for not always following the things that they are supposed to do under the law.

But I think I agree entirely with what Mr. Wilson and Mr. Levin said. I don't have much to add beyond that other than to say it is much more difficult where you don't know where this is going to unless you have a way of—if they haven't used a mixer or a tumbler and they are using the same virtual currency address, but they rarely do. The sophisticated people who are moving money use sophisticated mechanisms and they create new addresses.

Chairman PEARCE. Okay.

I would like to thank each one of you today for your testimony.

The Chair notes that some Members may have additional questions for this panel, which they may wish to submit in writing. Without objection, the hearing record will remain open for 5 legislative days for Members to submit written questions to these witnesses and to place their responses in the record. Also, without objection, Members will have 5 legislative days to submit extraneous materials to the Chair for inclusion in the record.

I ask our witnesses to respond as promptly as you are able.

I would mention that I think everyone on the subcommittee really appreciates the directness and the depth of your analysis and the substance of your answers. I think that all of you provided very valuable insights into a field that we must be learning a lot more about.

With that, the hearing is adjourned.

[Whereupon, at 11:54 a.m., the hearing was adjourned.]

A P P E N D I X

June 8, 2017

TESTIMONY OF

Jerry Brito

Executive Director of Coin Center

BEFORE THE

United States House of Representatives Committee on Financial Services
Subcommittee on Terrorism and Illicit Finance

"Financial Innovation and National Security Implications"

June 8, 2017

Chairman Pearce, Ranking Member Perlmutter, and Members of the Subcommittee:

My name is Jerry Brito and I am the executive director of Coin Center, an independent non-profit focused on the public policy questions raised by digital currency technology.

I'd like to thank you for the opportunity to speak to you today. What I'd like to do is explain to you what is Bitcoin, why it is a groundbreaking innovation perhaps as important as the web, and why, like the web, illicit actors are attracted to it. I'll then briefly offer some thoughts about what can be done to prevent that.

Before the invention of Bitcoin, for two parties to transact online always required a third-party intermediary; someone like PayPal or a bank. Unlike cash in the "real world," which I can hand to you in person without anyone else between us, electronic payments required a third party, trusted by each of us, to verify and guarantee the transfer. Introduced in 2008, Bitcoin overcame a longstanding computer science conundrum known as the "double spending problem" and for the first time allowed the secure and verifiable transfer of digital assets between individuals without the need for third party intermediaries—just like in the physical world. Among other things, Bitcoin created true digital cash.[1]

---

[1] *See* Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, October 2008, *available at* https://bitcoin.org/bitcoin.pdf; Jerry Brito & Andrea Castillo, Bitcoin: A Primer for Policymakers, 2nd ed., Mercatus Center, May 2016, *available at* https://www.mercatus.org/system/files/GMU_Bitcoin_042516_WEBv2_0.pdf

The innovation of peer to peer transfers unlocked an incredible array of socially beneficial and economically important uses. Not only are fast and inexpensive global money transfers and payments now possible, this technology is being used to make possible previously uneconomic micro-transactions, copyright registries and global rights management systems, faster and more efficient trade settlement, more secure land title and other property record systems, internet of things networks, self-sovereign identity, and much more.[2]

What gives this technology its innovative potential is that, because there are no third-party gatekeepers from which to seek access, it is an open and permissionless network—just like the internet. When Mark Zuckerberg decided to launch Facebook in his dorm room at Harvard, he didn't have to first clear it with the management of Internet, Inc. He simply wrote the Facebook application and launched it on the web. It's the permissionless and open nature of the internet that fosters the awesome pace of innovation from which we all benefit. And it is Bitcoin's open nature that also makes it an awesome platform for innovation.[3]

Unfortunately, this also means that, like the internet, it is open to bad actors who take advantage of it. Criminals certainly use it today, and we have begun to see some nascent interest from terrorist groups. According to a recent report on the potential of terrorist use of digital currencies by the Center for a New American Security, however, "Currently there is no more than anecdotal evidence that terrorist groups have used virtual currencies to support themselves."[4]

This means there is time to develop an appropriate response to the possibility; a reasoned response that targets the threat while preserving the freedom to innovate.

The blockchain and digital currency community has been working for some time now to face this threat. Almost two years ago Coin Center helped co-found the Blockchain Alliance, a public-private forum that serves as an information sharing conduit between law enforcement and industry.[5] Today the Alliance is composed of 35 industry members, including the largest

---

[2] *See* Peter Van Valkenburgh, Open Matters: Why Permissionless Blockchains are Essential to the Future of the Internet, Coin Center, December 2016, *available at* https://coincenter.org/entry/open-matters

[3] *See* Adam Thierer, Permissionless Innovation: The Continuing Case for Comprehensive Technological Freedom, Mercatus Center, March 2016, *available at* https://www.mercatus.org/system/files/Thierer-Permissionless-revised.pdf

[4] Zachary K. Goldman *et al.*, Terrorist Use of Virtual Currencies: Containing the Potential Threat, Center for a New American Security, May 2017, at page 2, *available at* https://www.cnas.org/publications/reports/terrorist-use-of-virtual-currencies

[5] *See* Jason Weinstein & Alan Cohn, After eight months, an update on the Blockchain Alliance, Coin Center, July 2016, *available at* https://coincenter.org/entry/after-eight-months-an-update-on-the-blockchain-alliance

exchanges and digital wallet companies, and over 36 government members, including DOJ, FBI, DHS, IRS, Secret Service, Interpol, Europol, and many others. Thanks to the cooperative work of the Blockchain Alliance, law enforcement today is better equipped than ever to take on this emerging threat.

I'd also like to highlight one very interesting conclusion from the CNAS report I mentioned earlier. They found that the "current policy and regulatory framework impede[s] law enforcement and intelligence officials, as well as the private sector, from collaborating more nimbly to weed out illicit actors."[6]

"One particular challenge in this area," they found, "is the requirement for a virtual currency firm to obtain licenses in all states in which it operates and maintain compliance consistent with both federal and applicable state standards where they are licensed to operate. With only a single federal registration for virtual currency firms, compliance costs would be more manageable for smaller firms, and regulators would be better able to oversee firms."[7]

Inconsistent and unclear state-by-state licensing of innovative fintech firms is preposterous in the 21st Century. It is even more preposterous that modest attempts to offer a federal alternative to state-by-state licensing like the Office of the Comptroller of the Currency's special purpose bank charter initiative would be opposed in court by the New York Department of Financial Services and the Conference of State Bank Supervisors.[8] By making it more difficult for legitimate firms to operate, they will only succeed in ceding the networks to illicit use into which they will have little visibility.

To promote a more uniform approach, Congress should encourage the Office of the Comptroller of the Currency to offer federal "fintech charters" to custodial digital currency firms, and Congress should also consider the creation of a new federal money transmission license that can be an alternative to state by state licensing.[9]

---

[6] Goldman, *supra* note 4, at page 30.

[7] *Id.*

[8] Peter Van Valkenburgh, The CSBS is suing the OCC to stop the new special purpose national bank charter for fintech firm, Coin Center, April 2017, available at https://coincenter.org/link/the-csbs-is-suing-the-occ-to-stop-the-new-special-purpose-national-bank-charter-for-fintech-firms

[9] The OCC has moved apace with its responsible innovation initiative and appears ready to begin entertaining charter applications, however several questions regarding the charter's potential application with respect to digital currency companies remain unresolved. *See* Peter Van Valkenburgh, Comments to the Office of the Comptroller of the Currency on Exploring Special Purpose National Bank Charters for Fintech Companies, Coin Center, May 2016, *available at*

As we discuss these questions today, I hope you will keep in mind a few things:

1. Bitcoin, the most widely used digital currency, is not anonymous as you sometimes read in the press, and it can be traced by law enforcement.[10]
2. This is a technology like the internet, or indeed like fire, that can be used for good or bad. Its inherent nature is neutral.
3. This technology can't be put back in the bottle. Encouraging its legitimate use gives us more and better visibility into the network, while discouraging its use only cedes the network to bad actors.
4. While there is substantial criminal use, terrorist use is nascent and experimental, so there is time to develop a considered response.

Thank you.

---

https://coincenter.org/entry/comments-to-the-office-of-the-comptroller-of-the-currency-on-exploring-special-purpose-national-bank-charters-for-fintech-companies

[10] *See* Adam Ludwin, How Anonymous is Bitcoin?, Coin Center, January 2015, *available at* https://coincenter.org/entry/how-anonymous-is-bitcoin; Jerry Brito, Silk Road corruption case shows how law enforcement uses Bitcoin, Coin Center, April 2015, *availabvle at* https://coincenter.org/entry/silk-road-corruption-case-shows-how-law-enforcement-uses-bitcoin

House Financial Services Committee

Hearing entitled "Virtual Currency: Financial Innovation and National Security Implications"
Thursday, June 8, 2017 10:00 AM in 2128 Rayburn HOB
Terrorism and Illicit Finance

Prepared Testimony
Scott Dueweke
President, The Identity and Payments Association (IDPAY)
President, Zebryx Consulting

Esteemed members of the House Financial Services Committee,

I am honored to be testifying before you today on the important topic of virtual currencies and their role in enabling terrorism and illicit financial transactions.

I have been involved in identifying security concerns of Internet payments and their use by criminals and terrorists since presenting on the topic at the first Internet World conference in 1994. Since that time we have seen the scope and scale of Internet payments grow exponentially and reach every corner of the world. Now, billions of people use virtual currencies and other alternative payment and remittance systems for legitimate purposes and are transforming economies through their use – especially in African and Asia. These systems now represent a major force for the financial inclusion of the more than 3 billion unbanked and underbanked around the world. That is an important point I hope you will remember as you examine the negative uses of these systems.

The Financial Action Task Force (FATF) defines virtual currencies much more broadly than bitcoin, or even cryptocurrencies more generally. In their report "Virtual Currencies: Key Definitions and Potential AML/CFT Risks", June 2014, they define virtual currencies as:

"....a digital representation of a medium of exchange; and/or a unit of account; and/or a store of value, but does not have legal tender status (i.e., when tendered to a creditor, is a valid and legal offer of payment) in any jurisdiction. It is not issued nor guaranteed by any jurisdiction, and fulfills the above functions only by agreement within the community of users of the virtual currency. Virtual currency is distinguished from fiat currency (a.k.a. "real currency," "real money," or "national currency"), which is the coin and paper money of a country that is designated as its legal tender; circulates; and is customarily used and accepted as a medium of exchange in the issuing country."

The report goes on to include many different types of virtual currencies including decentralized systems such as cryptocurrencies (Bitcoin, Litecoin, etc...), as well as centralized systems (Webmoney, Second Life Linden Dollars). There are thousands of these systems, although less than 100 are relevant due to a lack of liquidity. These systems do not stand in isolation but rather are part of a thriving ecosystem of not only virtual currencies but also other digital, mobile and stored value systems that cumulatively number in the thousands. These systems are collectively revolutionizing payments in many parts of the world, especially south Asia and Africa, providing opportunities for financial inclusion and growth. Taken together this alternative payments ecosystem is creating a viable alternative to the traditional western-dominated financial system. Most of these systems adhere to established Know Your Customer (KYC) and Anti-Money Laundering (AML) rules and regulations, but not all. As we saw with the Silk Road case, where Ross Ulbrecht created a Dark Web site which sold drugs online anonymously for bitcoin to more than a million customers around the world, and many other cases including the use of WebMoney for wholesale purchases of stolen Target credit cards and personally identifiable information (PII), criminals find the relative anonymity of these systems to be a boon.

Today's financial technologies (FinTECH), remittance and virtual currency ecosystem is indeed borderless, making them difficult to control simply through national legislation, regulation, and policymaking. The opportunity for the US, due to its size, financial power, and economic influence, to play a leading role in shaping international rulesets. Indeed, this has already occurred with FinCEN's treatment of virtual currency providers as money service businesses (MSBs) that has had a global impact with the establishment or pending establishment of similar regulations. The Committee would do well to set as a goal for itself to maintain and continuously establish the United States as the world's leading advocate of Internet payment systems, virtual currencies, and their use. Doing so would help to ensure that we have the reach to properly manage the growth and uses of these systems and ensure that they remain legal, transparent, and run to internationally-accepted standards of behavior – thus maintaining our position at the heart of a modernizing global financial system.

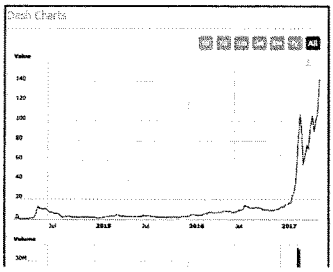
Therefore we are faced with a dilemma. How do we balance the profound benefits of new FinTECH against the criminal use of these systems? It is critical that the entire scope of this ecosystem be considered, it's impact, it's uses, and structure, before making judgments or creating laws and regulations that might have broad unintended consequences. Included in this ecosystem, beyond the virtual and alternative payments providers themselves and the virtual currency exchangers who connect them, I would also recommend understanding the incredible possibilities of the technology which enables bitcoin and other cryptocurrencies – the blockchain.

The impacts of the blockchain are being felt far beyond bitcoin. I am working with St. Luke's University Healthcare Network, for example, to implement the blockchain

to enhance the patient experience and to create a more secure and convenient experience. The blockchain is being implemented in financial institutions to transfer funds, the NYSE to modernize the trading of stocks, and many other applications. It can also be applied to reduce fraud and graft in foreign aid while increasing its reach and impact. In 2012, UN Secretary General Ban ki-Moon said "Last year, corruption prevented 30 per cent of all development assistance from reaching its final destination. This translates into bridges, hospitals and schools that were never built, and people living without the benefit of these services," Mr. Ban said. "This is a failure of accountability and transparency. We cannot let it persist." Accountability and transparency are precisely why the blockchain is being applied in the industries previously mentioned. One example is the Irish start-up Aid:Tech which is trying to work with the UN and the International Red Cross to make aid entirely transparent, using blockchain technology. Aid:Tech has already rolled out a trial project in Lebanon to help Syrian refugees with the Irish Red Cross, using mobile phones and the blockchain to identify people and replace easily falsified vouchers to deliver aid directly. Blockchain could be applied to many foreign aid projects to allow full transparency and accountability.

Mobile phone penetration is also enabling the unbanked and underbanked to be reached throughout the developing world. Global mobile phone penetration in Africa for example is about 60% and about 30% of them use their phones for mobile money transfers. In East Africa the MPesa success is well known, but has grown in the last decade to include more than 30 million users in 10 countries. Through systems like Clam, you can convert digital payment providers like PayPal into MPesa. Focusing only on cryptocurrencies, and not considering mobile payments and stored value systems is a very limiting and misleading mistake.

Although mobile payment systems are not all considered virtual currencies by the FATF definitions, they are part of the same alternative payments ecosystem. Internet-based currency exchanges allow you to convert virtual currencies, mobile payment systems, stored value cards, fiat currencies and even precious metals to and from each other. Actions and regulations against this ecosystem could have broad unintended consequences that could hurt the most vulnerable and derail growing new financial solutions that are meeting their needs where traditional financial systems have failed them. However, the most anonymous of these exchanges are critical nodes in a criminal relationships and transactions exploiting this ecosystem. We must find a way to target these criminal currency exchanges, often sheltered in countries where officials protect and even profit from them.



There are plenty of reasons to be concerned about the enabling effects of virtual currencies on criminal activities. This is not a new trend. It did not begin with bitcoin. Since at least the early 2000s with the use of eGold, anonymous payment systems have been used not only to protect privacy but also to support criminal activities. Child

pornography, money laundering, drug sales, weapon sales, slavery rings, zero day exploits, hackers for hire, murder for hire, mercenaries for hire, credit and debit cards, personally identifiable information, synthetic identities, identity documents such as passports, drivers licenses, and all the components needed to create them, have all been available on the regular internet and the Dark Web as well as much more. The advent of these criminal markets enabled by anonymous virtual currencies have created a global bazaar for criminals and organized crime to reach a mass global market.

While most of the transactions of the Dark Web markets such as Silk Road and those that followed in its footsteps have used bitcoin, this is beginning to change. New, more anonymous cryptocurrencies such as Monero, Dash and Zcash are beginning to gain marketshare. These systems now account for about 1% of cryptocurrency usage on the Dark Web and are increasing rapidly. As these systems increase in usage existing blockchain analysis tools will be challenged to continue to be relevant, as these "dark" cryptocurrencies are designed to avoid the tracking of transactions whereas bitcoin was designed to be transparent.

The Russian central bank on June 3 announced that they will be creating a national cryptocurrency. Considering that a large percentage of the global criminal hackers and many cyber-criminals are Russian or speak Russian, and given Russia's current state of tension with the United States and Europe, this development should be closely monitored. Given current FATF definitions (see the above) will it even be considered a virtual currency since it will likely be tied to the ruble? How this cryptocurrency is set up will be telling. Will it have a publically available and verifiable blockchain like bitcoin, or will it be a private or permissioned blockchain and be opaque to western observers and regulators? If private it could be used to circumvent KYC and AML, and even be used to support proxy "patriotic" hackers, as Vladimir Putin referred to them last week. This possibility already exists with Russian-language centralized systems, especially WebMoney.

WebMoney is a Russian global settlement system established in 1998. In general, this is an e-wallet solution that supports different currencies, including dollars, rubles, bitcoin, gold and many other currencies and forms of value. Currency exchange and asset storage is organized via a network of so-called "guarantors" from various jurisdictions. This system has been implicated many times over the past 19 years in criminal activities. A few examples:

- December 2013 – In the infamous breach of the US retailer Target, which resulted in between 1-3 million credit and debit cards being sold on Dark Web sites including on the carder site Rescator, Russian centralized virtual currency services WebMoney and PerfectMoney, as well as cyrptocurrencies and other payment systems, were used by criminals to make purchases of stolen cards and PII. This resulted in total losses of hundreds of millions of dollars.

- November 2013 - Fraudcheck.cc, an anti-fraud service for criminal spammers exclusively used Webmoney for payment for its services.
- 2004 - Officials with the U.S. Postal Inspection Service worked with Eastern European authorities to shut down two cybergangs, known online as dumpsmarket and carderportal. According to the postal inspectors, the gangs had laundered proceeds from the sale of stolen credit cards through two digital currencies, including WebMoney.

WebMoney in the past several years has become not only ubiquitous in Russian-language speaking countries, but also in countries like Mexico where you can add funds to your WebMoney accounts at over 15,000 OXXO 7/11 stores.

This type of service is not limited to WebMoney. Yandex.Money is a payments solution from Russian search engine giant Yandex. The account can be topped up with cash, bankcard, and virtual currencies. Additionally, every Yandex.Money account can be connected to a bank account. It is also an e-wallet solution similar to Paypal. Yandex.Money can be used to pay for mobile services and Skype, online games and different goods. You can also transfer money between two accounts, for example sending money to friends or business associates.

PerfectMoney is perhaps the most anonymous and is distinctly marketed towards criminals. It is clearly run by Russian language speakers and has a business address in Hong Kong that is an empty office. In my analysis of many thousands of sites and companies and services that are part of the alternative/anonymous payments ecosystem, PerfectMoney is the centralized virtual currency most completely focused on criminal uses.

Taken together, these Russian managed centralized virtual currencies represent a vibrant and growing set of services that are not only serving the ecommerce needs of Russian speaking legitimate customers but also the criminal underground. Why? In 2015 Ed Lowery, U.S. Secret Service Deputy Assistant Director said that criminals are less likely to utilize crypto-currencies like bitcoin. Since bitcoin displays all of its transaction data in the public ledger of the blockchain, making it possible to follow its movement.

"They've been more likely to use digital currency: WebMoney, a Liberty Reserve, or going back a few years to EGold," Lowery said. "It's the anonymity it provides. Most of these currencies have very, very lax 'know your customer' standards. They are specifically built to get around the banking regulations from the various international regulators that are out there."

These centralized virtual currencies, as well as many of the thousands of sites and services that buy and sell and accept decentralized virtual currencies like bitcoin, lie outside of the western financial system's network of detection points. When someone buys WebMoney credits, or PerfectMoney, or AliPay in China, and

identities are not established, or suspicious transactions occur, no Suspicious Activity Report (SAR) is generated like there would be here or in Europe. However, since no SARs are generated, often times there is a lack of appreciation for the scale of the potential, the probable use of these systems for transactions which are criminal, or for transactions for which there is an incentive for nation states to keep hidden from the prying eyes of US law enforcement and regulators.

Hypothetically, what could these virtual currency systems be used for? I'm especially referring now to the centralized virtual currency systems that are not exposed on a public blockchain, and have the capability to move unlimited amounts of funds completely outside of the western financial system and would never be detected by our traditional detection systems:

- Balance of payment transfers between criminal organizations such as organized crime and drug cartels
- Funds transfers between countries doing business with pariah states
- Transfers to and from terrorist organizations, especially as part of a trade-based money laundering scheme to cause investigators to lose their money trail
- Enabling kleptocrats to move funds from their country's coffers off shore – the next "Panama Papers" scandal could well be focused on these systems
- Funding the virtual army of proxy hackers to do their "patriotic" duty

So how do we cope with these daunting law enforcement and regulatory challenges while acknowledging the significant positive role that these systems play in the economy and the potential to use these systems to help connect the unbanked, underbanked and those in need of aid?

Education is of course the first step. Helping regulators and law enforcement understand the scope and scale of these systems outside of those systems they know within the USA is critical, including at the state and local levels. Understanding the role these systems play in the purchase of illicit goods and services, as well as their positive uses in enabling global remittances between foreign workers and their families is important. These systems are not inherently bad, no more so than using cash or credit cards, and should not have a stigma attached to them.

At the Identity and Payments Association (IDPAY) we have launched a global non-profit to attempt to provide a public/private partnership to provide not only education, but a platform to enable a market-driven approach to self regulation. This is of critical importance because of the pressing problem of the "de-risking" of the accounts of virtual currency, FinTECH, and remittance service providers around the world. I will be at the United Nation's Global Family Remittance Day next week at UN headquarters to encourage participation in this NGO. US government agencies need to join us - as well as large US companies such as PayPal, WesternUnion, Bank of America, and others who want to be part of the solution.

Together, public and private entities can work aggressively to promote and coordinate mutually beneficial uniform legal, regulatory, and policy solutions for the management and oversight of virtual currencies and other payments systems. Working with foreign governments and law enforcement, and intelligence community players to create a uniform, level-playing field that ensures that bad actors cannot find and exploit the seams and gaps between the various national regulatory and legal frameworks and policies to undertake and hide their illicit activities. This includes reaching out on multiple levels, on a government to government basis, and through a public/private partnership, to facilitate market conscious policies and regulations which extend beyond national borders which is critical given the new payment ecosystem's transnational nature. Given the rapid pace of development of these systems and the fact that they are almost all developed by private companies and individuals -- not governments (with the exception of the recent Russian central bank's cryptocurrency announcement), it is essential that whatever approaches are made are based on a public/private partnership rather than a government-only approach to the problem.

It is also critical to create transparency regimes and technologies that are publicly sponsored and funded, so that the role of government is not strictly in monitoring illegal, illicit, criminal, and terrorist misapplications of these systems, but also establishing internationally accepted methodologies and transparent solutions that are required for all. Building trust in these systems is critical. This would be a natural and timely development and is an ideal focus for government action as it pertains to payment systems and virtual currencies. This can begin by developing an internationally accepted set of terms and "best practices" and transparency requirements that all governments can agree to adhere to in regulating these systems. Thus, the role of government can be focused where it can both do the most good in encouraging the positive applications of these new technologies as well containing the illicit uses of these systems to more obvious areas of illicit activity, such as the Dark Web. Ultimately, through research grants and contracts, the US Government could enable international transparency in foreign aid, tax payments, government grants, and other payments. Such research should include both great scrutiny of the trajectory of illicit uses, including recognizing the direction that the criminal, terrorist, and illicit users are taking -- and developing an "early warning system" to identify new illicit uses as they gain interest -- while also encouraging the development of digital services and technologies that enable valid uses while improving the tracking of improper uses. This type of approach is needed; it is no less important to the future of the Internet than was the original Advanced Research Projects Agency Network (ARPANET), which created the protocols and packet switching technologies that originally gave birth to the Internet.

Together we can help drive technical innovation, encourage economic growth by helping the disconnected become connected and help themselves. Helping to reduce the de-risking of virtual currency and other alternative payment providers we can spur technical innovation, economic growth, reduce poverty, and allow the US to

stay central to a rapidly morphing world financial system. By enabling the unbanked and underbanked to raise their standard of living while driving economic development organically, not through handouts riddled with corruption, we can undermine one of the key recruiting rationales of terrorist organizations while simultaneously limiting criminal abuse of these systems. This approach cannot be limited only to bitcoin and other cryptocurrencies. There is a shadow financial system that is thriving outside of our control. We need to take strong steps to understand, control and counter it while encouraging the growth of new alternative payment and virtual currency systems that are governed by the rule of law.

Thank You.

Scott Dueweke

TESTIMONY OF

Kathryn Haun Rodriguez

Former Assistant U.S. Attorney, U.S. Department of Justice, Lecturer in Law on Cybercrime and Digital Currency, Stanford University
Current Member of the Board of Directors, Coinbase Global, Inc.[1]

BEFORE THE

U.S. House of Representatives Committee on Financial

Services and Subcommittee on Terrorism and Illicit Finance

"Financial Innovation and National Security Implications"

PRESENTED Rayburn House Office Building, Room 2128
June 8, 2017
10:00 am

[1] The views expressed herein reflect my own personal views and not those of the institutions with which I am affiliated.

Chairman Pearce, Ranking Member Perlmutter, and Members of the Subcommittee: Thank you for inviting me here to testify before you this morning on the role that financial innovation can play in facilitating -- and also in helping curtail -- illicit finance.

Until two weeks ago, I was a federal prosecutor with the U.S. Department of Justice (DOJ), a position I held for over a decade. Most of my time at DOJ was as an Assistant U.S. Attorney in San Francisco, where I also served as the first-ever Digital Currency Coordinator. Previously I worked in the National Security Division at DOJ headquarters and in several other roles. I also taught a course on digital currencies at Stanford. This week, I joined the Board of Directors of Coinbase Global, Inc., the world's largest digital currency platform, and one of the few platforms that has legal authority to operate in all states in which it does business.

In little over a year the market capitalization of bitcoin has gone from $6 billion to $40 billion. Including other cryptocurrencies like Ethereum, the combined market capitalization of digital currencies now exceeds $90 billion. More and more people are buying, selling, trading, transacting in, and using these currencies. They are doing so for all sorts of reasons: as an investment, as an easier way to complete cross-border transactions, for frictionless payments, and also, for some, to conceal and move illicit proceeds because of the perception that virtual currency is untraceable.

I will cover five areas this morning: (1) the intersection of financial innovation and terrorist activity; (2) national security implications of other bad acts that financial technologies facilitate; (3) the ways in which these emerging technologies help make us more resistant to cyberwarfare and make it easier to track those intending to do us harm; (4) the challenge of unregulated and overseas entities; and (5) how industry is helping and the importance of public-private partnerships.

There are plenty of legitimate uses of cryptocurrencies. And those uses are growing by leaps and bounds. I know many small business owners, investors, academics, and even government employees who use cryptocurrency. These are not people engaged in illicit activity but rather people looking to take advantage of a more open and seamless system to transact with one another. They want ease of payments, fewer middlemen, lower fees, and greater privacy. Cryptocurrencies also promote financial inclusion for the unbanked, including in parts of the world that lack stable financial institutions.

But early misuse is a fact of life with many emerging technologies, and cryptocurrency is no exception. We often say that any technology worth adopting is adopted first by bad actors. Although we now all use the Internet every day, in the beginning it was disproportionately used by those engaged in nefarious behavior – for things ranging from child porn to online fraud. With each technological advance, bad actors figure out how to exploit and there is some period where law enforcement plays catch up, a kind of cycle of innovation and adaptation. Digital currencies represent just the latest chapter in this cycle.

(1) I first want to address terrorist use of cryptocurrency. The potential for terrorist use of cryptocurrencies certainly exists, as it exists for cash or any asset. To date we have seen only limited instances of terrorists using cryptocurrency, but these instances are becoming more frequent. Cryptocurrencies may appeal to terrorists because they allow for easier cross-border transactions that can go undetected. Anecdotally, it appears that terrorists and those who finance terror are not using the registered and licensed on-and-off ramps such as wallets or exchanges to acquire and transfer cryptocurrency. Rather, they are using the unregistered overseas ones that do not adhere to U.S. anti-money laundering (AML) and "Know Your Customer" (KYC) requirements. Or they are using anonymous peer-to-peer exchanges such as localbitcoins.com and related sites, which operate similar to Craigslist.

However, none of the recent and horrific terrorist attacks have relied on cryptocurrencies, for the simple reason that they were low tech and inexpensive. Purchasing automatic weapons, renting a truck, making suicide bombs – these are not things that require large sums of money.[2] With the small amounts necessary to inflict massive harm, terrorists overwhelmingly use means to acquire and move funds that are far less traceable. Cash and prepaid cards are two prime examples. There is little reason to use a digital currency account where your IP address may be tracked with each login, there is a permanent record to trace where the funds came from and where they moved to, identity documents are required, etc., when you can simply go to the corner store and buy a few thousand dollars of prepaid cards, or use a peer-to-peer money exchange.

(2) Where we have instead seen more misuse of cryptocurrency is in the areas of cybercrime, money laundering, drug trafficking, and financial fraud. These activities have major national security implications. Ransomware is a particularly compelling example, crippling critical systems and demanding payment of a ransom (upon which, access to data may or may not be restored). The ability to spread ransomware is an obvious tool in any terrorist or cybercriminal's toolkit, because it can target and cripple critical infrastructure: hospitals, first responders, public transit systems, etc. Last month's Wannacry attack infected over 10,000 businesses, hospitals, and public agencies across 153 countries – despite

[2] Darknet marketplaces sell contraband that could facilitate terrorism, including automatic weapons, fraudulent IDs, and explosives. The darknet relies on digital currency and other electronic mechanisms for storing value, so these could be seen to facilitate terrorist access to goods and services that can be used for acts of violence. However, digital currency is not unique in this regard, in that terrorists overwhelmingly use cash, prepaid cards, and other assets to purchase instruments of terror.

some simple errors in the programming. The next, more sophisticated attack could do far worse. And the preferred currency of this generation of ransomware is bitcoin, not just in terms of the ransom but also for purchasing the product (i.e. the malware). The Wannacry malware itself was reportedly auctioned off in bitcoin.

(3) But while some features of cryptocurrencies may facilitate crimes, other features may thwart them. One of the beneficial features of a cryptocurrency such as Bitcoin is the decentralized nature of the technology underlying it, the blockchain. Because the blockchain is decentralized and spread out amongst millions of computers all over the world it is very difficult to hack -- much more so than a centralized database or server. For a nation-state actor wanting to inflict harm on the U.S. economy, a cyberattack using malware on a major financial institution is a natural target. But if large portions of our financial infrastructure ran on such decentralized systems, hackers would have to hack into millions of computers around the world simultaneously. In other words, bitcoin and the blockchain technology underpinning it could bring about more security, and help thwart certain digital attacks.

Moreover, cryptocurrency technology actually helps us solve bad acts. I witnessed this firsthand in prosecutions I brought. One was a case involving the Silk Road darknet marketplace and the agents investigating it. In 2014, we got a tip that there was a rogue agent on the DEA payroll. This agent happened to be on the Silk Road Task Force and was the government's lead undercover agent in communication with Ross Ulbricht, the Silk Road mastermind. Our investigation ultimately revealed that he was using his status as a federal agent to seize the cryptocurrency balances of ordinary citizens at exchanges across the world, and liquidating hundreds of thousands of dollars of bitcoin monthly. He was also selling Mr. Ulbricht information about the government's investigation in exchange for bitcoin, and, through a series of online personas, he was simultaneously defrauding and extorting Mr. Ulbricht for hundreds of thousands of dollars of bitcoin. There is much more to the story, but

what enabled us to solve the crime was this rogue agent's use of cryptocurrency. Because he had used bitcoin, we were able to trace all transactions directly back to him using the blockchain -- a permanent, immutable and public ledger, which can be an invaluable source of evidence. Attached to this written testimony is what was Exhibit 1 in our federal indictment. This shows you the tracing that we were able to do given the subject's use of cryptocurrency. Unlike a series of money orders, a bulk cash transfer, or an anonymous prepaid card, here the criminals left immutable, digital footprints that our team followed.

Before all of this agent's bad conduct had come to light, about 21,000 bitcoins (which would be worth over $52 million today) were stolen overnight from Silk Road vendor accounts. After solving the DEA agent's crimes, we suspected that he was to blame for this theft, too, and not the Silk Road administrator whose login credentials had been used to accomplish the theft. But the blockchain enabled us to see a pattern in the movements of funds, which suggested a second criminal with a different modus operandi. Whoever stole the 21,000 bitcoins had transferred them to Mt. Gox, a digital currency exchange in Japan that had gone bust. The corporate records of Mt. Gox were not all available to us, but, again, we had the blockchain, that permanent record of all bitcoin transactions. Using it, we were able to follow the funds from Mt. Gox to the account where this additional bad actor had cashed out. Our investigation ultimately revealed that the culprit was another federal agent, a Secret Service agent who was also on the Silk Road Task Force. These two agents were particularly savvy criminals, because they knew exactly where we would be looking and they had covered their tracks well. Had these agents not been using bitcoin but other payment methods such as prepaid cards or cash, we would not have caught them. But their Achilles heel – and our most powerful investigative tool – was cryptocurrency. Both these agents are now in federal prison.

This was just one early example. We have since uncovered (and solved) many hacking and major ransomware schemes by looking at the

movement of bitcoin. Many of those cases are not yet public, but I can tell you with confidence that we would not have solved them had cryptocurrencies not been used. Since then, law enforcement around the globe and my former colleagues across the country – from New York to Colorado to Florida to Illinois – have successfully used the fact that criminals used cryptocurrency not only to solve crimes but to prove cases. Investigators like digital footprints and that is exactly what digital currencies provide.

(4) Of course, we can only follow the money to an individual or group if they used a regulated exchange, one that follows basic AML/KYC laws. This is because it does little good to trace funds unless we can tie the wallet or address to a real-world identity. And unfortunately, those who are using these platforms for nefarious purposes are increasingly using the non-compliant exchanges or exchanging on peer-to-peer networks. What we have seen is that the sophisticated criminals – ransomware purveyors, black hat hacking rings, large drug kingpins and serial fraudsters – are now patronizing overseas exchanges that do not follow AML/KYC laws. In fact, nearly 100% of ransomware campaigns cash out through platforms such as these.

When investigators trace illicit funds to a particular wallet or address, they ordinarily subpoena the exchange for information about the customer who owns the account. But several exchanges do not even require full names, let alone identity documents, to open an account. Criminals can open anonymous accounts, or accounts with phony names to fly under the radar of law enforcement. Thus, we have received "Mickey Mouse" who resides at "123 Main Street" in subpoena returns. So even though investigators can follow the funds by analyzing the blockchain, they may not be able to connect those funds to a culprit in the real world.

The question naturally arises, "Why not go after those exchanges?" In 2013, the Digital Currency Task Force I founded, together with the IRS

and U.S. Treasury Department's Financial Crimes Enforcement Network (FinCEN), conducted a criminal investigation into virtual currency company Ripple Labs for failure to follow AML laws and KYC regulations. In 2015, we reached a settlement -- it was the first enforcement ever against a virtual company under the Bank Secrecy Act -- under which Ripple agreed to collect customer data and identity before activating accounts, to enhance their compliance program, and to follow all money laundering laws. Today Ripple has emerged as a major player in this industry.

That was a fairly straightforward case. Ripple was in the U.S. and already had the beginnings of a compliance program. But the majority of the unregulated and non-compliant exchanges are overseas, and they have little to no compliance programs at all. These foreign exchanges pose formidable jurisdictional challenges: Our antiquated Mutual Legal Assistance Treaty (MLAT) process takes months of bureaucratic maneuvering, even in the best-case scenario with cooperative partners on the other side. When we are dealing with an uncooperative country or one not party to an MLAT, we may not get any evidence at all. In less than two minutes, a money launderer with a smartphone can move illicit proceeds halfway across the world. But for the government, it might take months or even years to obtain evidence of the money flows, if ever. This is not a problem unique to cryptocurrency cases. We need more resources and tools to quickly get at electronic evidence overseas: funding more attaché positions, and better systems devoted to processing MLATs. And in the countries not party to an MLAT, we need resources to increase our relationships with local law enforcement. For those exchanges in countries that simply will not cooperate, we need more statutory authority to go after the segments of their businesses that rely upon U.S. companies for support: servers, communications, software, infrastructure, and banking operations. But currently U.S. companies are refusing to even comply with search warrants for data stored overseas.

(5) There are numerous entities in the space who have demonstrated a commitment to abide by U.S. AML laws and regulations and have robust compliance programs. And these platforms are some of the best partners we have had in combatting cybercrime, organized crime, narcotics trafficking, fraud, public corruption, and a host of other crimes. The head of an agency within Treasury told me that the quality of the suspicious activity reports (SARs) from digital currency companies, largely startups, are often far superior to SARs from large financial institutions, despite fewer compliance resources. This is a view shared by many prosecutors and agents around the country. In over a decade as a prosecutor the fastest turnaround on a subpoena I ever got was from a digital currency company: a subpoena sent after 6 pm on a Friday night that called for a three week deadline got returns later that same night. That is unheard of in the subpoena context, and particularly for financial institutions where big banks often take months *past* the deadline to provide law enforcement with returns.

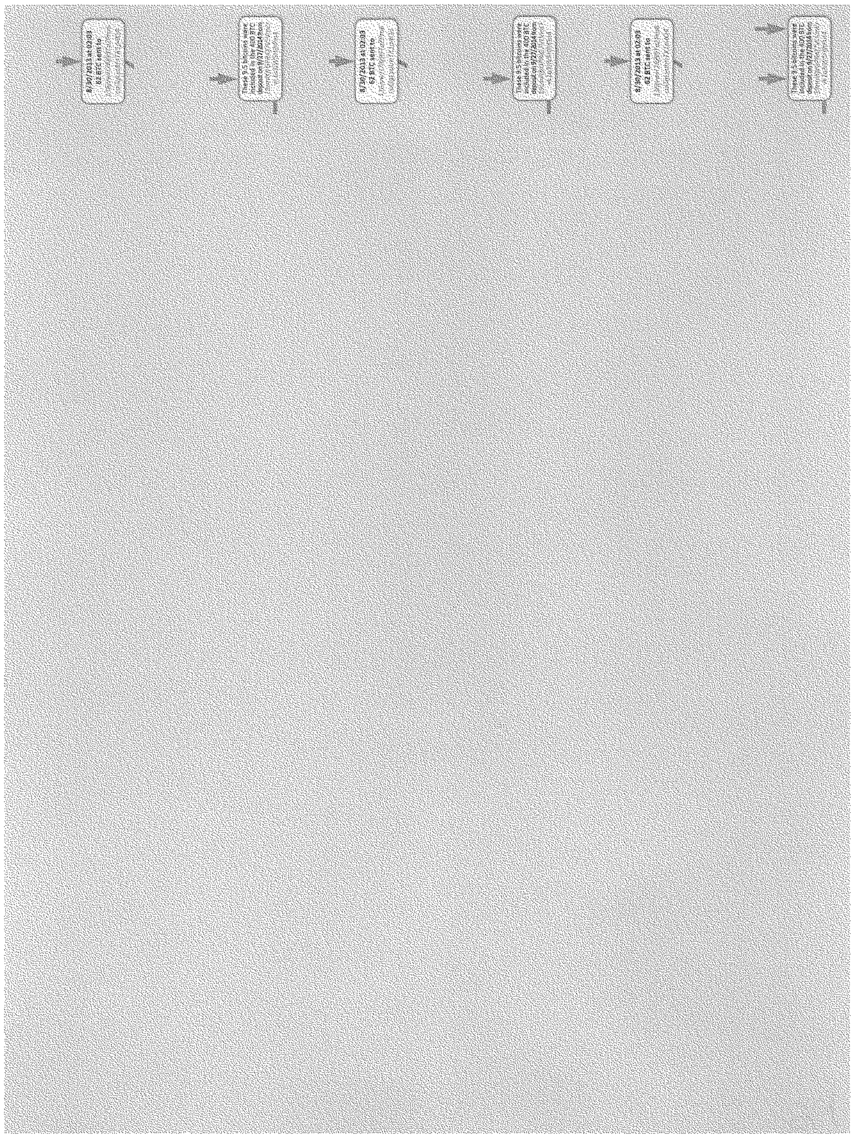
However, with broader adoption of cryptocurrencies, these companies are being stretched from a compliance perspective. They are also subject to having their correspondent banking relationships terminated as banks engage in blanket "de-risking" exercises that can cut these companies off from the rest of the financial system. We want these law-abiding entities to be spending their compliance resources on proactively working to keep bad actors off their platforms or developing tools to spot fraudulent activity, not diverted away from these important tasks to address the vagaries of 50 state regulatory regimes. I know that there is an extensive debate on the FinTech charter the Office of the Comptroller of the Currency (OCC) has proposed, and that others, including the Conference of State Bank Supervisors (CSBS), are challenging that in federal court. And while there are strong views on each side, the idea of a federal solution to harmonize state laws is an area where Congress could help.

The FinTech industry could be a very helpful partner to the government in addressing national security concerns. Analogizing again to the early days of commercial use of the Internet, law enforcement turned to tech companies for help in understanding the then-new technology so they could improve their capacity to go after criminals who misused it. In 1996, DOJ created the first standalone computer crimes section, and tech companies supported that by conducting training, serving as a resource, and partnering together to stop fraud and abuse. This public-private partnership went a long way toward easing the anxiety some law enforcement and regulatory agencies were experiencing about the Internet.

The Blockchain Alliance is trying to accomplish the same thing in the virtual currency space. Industry representatives are working proactively to help law enforcement, regulatory, and national security authorities learn more about cryptocurrency, so they can enhance their ability to follow the money and protect public safety. DOJ was one of the first agencies to join the Blockchain Alliance, and in just one year it has grown to approximately three dozen industry members and three dozen government agencies across the globe, including agencies focused on national security. Partnerships like these are critical to deepening government awareness and understanding of these new technologies and how they actually operate. But we have an urgent need for more resources to be devoted to this emerging space immediately and across the board at all agencies. It is simply not sufficient to have only a handful of people at each federal agency focused on cryptocurrency when it is affecting so many areas that touch upon public security.

Thank you for inviting me to share my thoughts on this important issue.

All times are UTC (Coordinated Universal Time)
9/30/2013 at 1:42
388.4975 BTC sent to
9/27/2013 at 19:40
525 BTC are sent to
9/27/2013 at 19:40
525 BTC are sent to
9/30/2013 at 7:26
54 BTC are sent
from


8/30/2013 at 02:03
62 BTC sent to
These 9.5 bitcoins were included in the 400 BTC deposit on 9/27/2014 from
8/30/2013 at 02:03
62 BTC sent to
These 9.5 bitcoins were included in the 400 BTC deposit on 9/27/2014 from
8/30/2013 at 02:03
62 BTC sent to
These 9.5 bitcoins were included in the 400 BTC deposit on 9/27/2014 from

TRACE OF FRENCHMAID PAYOFF
770 BTC (worth approximately $97,000 on 9/15/2013) Per records obtained from the Silk Road marketplace and Ross Ulbricht's laptop, the 770 bitcoins transaction into bitcoins address 14rE7Jqy4o6P27qWC CangkUfBxtevZhPHB appears to the payment to "frenchmaid". This transaction was a withdrawal made by Ross Ulbricht from Silk Road.
The sum of these 9/15/2013, 2:10 UTC, payments to 14rE7Jqy4o6P27qWC CangkUfBxtevZhPHB is 520 BTC. Total BTC deposited into 14rE7Jqy4o6P27qWC CangkUfBxtevZhPHB = 770 BTC
9/17/2013 20:08
9/17/2013 20:09
9/17/2013 20:11
9/17/2013 20:12
9/17/2013 20:13
9/20/2013, 23:29
48 BTC deposited into
These BTC were also traced to Silk Road wallets
9/22/2013 00:52
sends 154 BTC to
This address received other deposits, for a total of 388.9995 BTC
9/22/2013 00:56
sends 154 BTC to
9/22/2013 1:08
sends 146.9995 BTC to
9/22/2013 1:17
sends 154.0005 BTC to
9/22/2013 1:17
sends 160.9985 BTC to
9/29/2013 18:10
sends 189 BTC to
This is Carl Mark Force's CampBX address
9/29/2013 23:17
sends 154 BTC to
This is Carl Mark Force's CampBX address
9/23/2013, 18:13
sends 194.9995 BTC to
This is Carl Mark Force's CampBX address
9/29/2013, 23:14
sends 154 BTC to
This is Carl Mark Force's CampBX address
9/29/2013, 23:13
sends 160.9985 BTC to
This is Carl Mark Force's CampBX address
All times are UTC (Coordinated Universal Time)

Opening Statement for the House Financial Services Committee's Subcommittee on Terrorism and Illicit Finance

Written Testimony by Jonathan Levin, June 8th 2017

Introductory remarks

Thank you very much for the opportunity to speak to you this morning.

My name is Jonathan Levin and I am one of the Co-Founders of Chainalysis. Chainalysis is the leading provider of investigation software and risk management software for virtual currencies. In this field, we identify illicit use of virtual currencies, including terrorist financing. We provide tools to private industry and law enforcement to mitigate the risks that this activity poses to our society. Prior to my work at Chainalysis, I performed some of the first economic analysis of the incentives that power and secure Bitcoin, the most popular virtual currency.

I wish to prepare my briefing into three significant sections that I believe are worth considering in light of the potential risks that are posed by virtual currencies:

- First, the potential of virtual currencies
- Second, the nature of the technology
- And finally, The current use of virtual currencies

The potential of virtual currencies

The Internet has become the transport layer for all of our communications. It has fundamentally transformed how consumers, producers, friends, families and governments transfer information. The Internet started in the early 1960s but it did not enter the mainstream until the creation of an easy to use consumer layer with the Web and the availability of developer tools in the mid 1990s. Today, we probably almost all used the internet just prior to entering this room and will use it when this analogue session is concluded.

Many of the protocols and infrastructure that we use are now decades old and were pioneered mainly by academia and the government. The US government played an instrumental role in providing these essential layers for private industry to develop business models and products for us as consumers to use. The adoption of the internet by private industry required the use of payments, but these were not baked into the protocol layer of the internet and needed to be built on top.

Famously, value transfer and video streaming over the internet was pioneered by the adult entertainment industry and quickly criminals also saw this venue as a lucrative target for their criminal enterprises. The emergence of PayPal and other internet payment companies have built solutions on top of the internet, but nothing comes close to the native ability to move hypertext seamlessly between two machines anywhere in the world. This motivated the emergence of Bitcoin, which was released to the public in 2009.

Since 2009, the Bitcoin network has bootstrapped itself, and attracting over $1 billion in venture capital for applications being built on top of it. The current value of all virtual currencies exceeds $100 billion with daily liquidity across all the exchanges totaling approximately $4 billion a day. The main driver behind this trade activity is price discovery and speculation that virtual currencies present an opportunity to open completely new markets on the internet that disrupt the incumbent tech giants.

Decentralized internet protocols do not preclude the formation of centralized institutions over the top of them, think of decentralized protocols as providing interoperability between these institutions. It is possible to architect the existing web on top of these protocols and fundamentally new ways of sharing information and data between institutions. As such, we also need to recognize the new institutions that lie on top of these protocols and give them the appropriate regulatory framework and protections to operate within.

The history of virtual currencies is longer than simply Bitcoin, in the years before Bitcoin, there were centralized virtual currencies, such as Linden Dollars, the currency of second life or e-gold. With money laundering risk and financial stabilization concerns, some of these systems have come under regulatory scrutiny. These efforts can be ineffective at curbing demand and may serve to drive the activity underground. In 2007, in China, Tencent came under pressure from the

People's Bank of China to stop conversion between goods and services and Q Coin, a virtual currency issued by Tencent.

In February 2017, the People's Bank of China put pressure on the virtual currency exchanges to stop trading. This led to an uptick in Peer to Peer Bitcoin transactions that are out of the purview of the State. Trading on Local Bitcoins, which is just one of these sites, rose from ¥2.5m a week to over ¥100m. These peer to peer transactions cannot be regulated and diminishes the oversight that can be obtained by the state.

This technology has the potential to create a fundamental new layer for how we interact online where many of the existing institutions have similar roles to play and may benefit from new efficiencies. There is also the space for massively new applications that we haven't yet considered.

The nature of the technology

Bitcoin and other virtual currencies are decentralized and as such are censorship resistant. Receiving Bitcoin can be done by anyone with access to basic computing equipment anywhere in the world. There is no need to register or supply anyone with any identifying information. There is no ability to freeze assets or seize someone's virtual currencies without obtaining access to their private keys, which are their secret keys that only they have access to.

The same benefit that this affords entrepreneurs and software developers around the world to bring revolutionary new business models, it also offers nefarious actors the ability to abuse this technology. Transferring virtual currencies between people is done on a ledger that transcends national borders and current conceptions of identity. Virtual currency are ultimately bearer instruments. The person in control of a private key is the ultimate owner of the virtual currency.

In order to facilitate this system, Bitcoin makes every transaction public. These transactions are recorded in a single transaction ledger, the blockchain. However all of the entries in the ledger are pseudonymous and do not relate to any real world identities. The public broadcast of transactions permits third parties to be able to see certain aspects of these transactions and allow law enforcement armed with the right tools to patrol the virtual currency highways.

The current use of virtual currencies

Chainalysis analyzes the blockchain, to identify which transactions have been performed by the same entity and links these entities to real world services such as exchangers, merchant processors or underground marketplaces. This blockchain analysis can identify the underlying activity behind virtual currency transactions and the on-ramps and off-ramps to the existing financial system.

There are over approximately 10 million virtual currency users in the world today. These users are primarily interested in the long term potential of the technology and are holding on to virtual currency in the hope that it appreciates over time. There are also users who send virtual currencies cross border to avoid high fees associated with traditional money transmitters and banks.

Terrorist organizations are not in the business of speculating on the price of virtual currencies, but rather may be interested to use virtual currencies for the following three cases:

1. Using virtual currencies in cybercriminal activities to fund operations
2. Crowdfunding operations from sympathizers around the world
3. Paying for everyday items and internet infrastructure

Cybercriminals have mainly used Bitcoin to buy and sell capabilities to launch cyber attacks and also to extort their victims. Their use of Bitcoin cannot be attributed to anonymity but rather the speed and finality of payment, its ability to transcend borders and its protection against seizure.

There is some evidence that some terrorist organizations have begun to resort to cybercriminal enterprises to fund activity. In the United Kingdom, in the case against Younis Tsouli, there was evidence of money laundering from stolen credit cards through e-gold online payment accounts. The funds were used both to fund the registration of 180 websites hosting Al-Qaeda propaganda videos and to provide equipment for terrorist activities in several countries. Approximately 1,400 credit cards were used to generate approximately £1.6 million of illicit funds to finance terrorist activity.

There has not been any evidence yet of terrorist organizations running any of the criminal enterprises that are based in virtual currencies. However, I have seen some Ransomware campaigns be associated with high risk jurisdictions in terms of terrorism hotbeds. Recent high profile Ransomware campaigns such as "WannaCry", raise the profile of this type of criminal enterprise but executing in the virtual currency domain successfully requires a level of sophistication. WannaCry despite its massive media presence and disruption to companies, only made $92,000 in victim payments calculated at the time of transaction. Despite lower distribution levels, other Ransomware families have raised over $15 million due to providing better customer service to their victims and gaining better reputation of decrypting files quickly and reliably.

In July 2016, the only verifiable public case of crowdfunding by a known terrorist organization occurred. The campaign itself was not very successful and has only raised a total of $1,000 to date. The nature of virtual currencies meant that Chainalysis was able to size the potential threat and find the ultimate source and destination of funds.

The July 2016 campaign was initiated by an Ibn Taymiyya Media Center (ITMC) online campaign, called Jahezona or "Equip us" in Arabic. The organization started in July 2015 arguing that Muslims donating funds to equip jihadists was equivalent to fulfilling a religious obligation to fight. In late June 2016, the campaign added the option to pay in bitcoin. ITMC began posting infographics on Twitter with QR codes that linked to a Bitcoin address. Due to the lack of success of the campaign, we have not seen any other Bitcoin addresses emerge on the internet to raise funds from sympathizers.

However, even in the ITMC case there is evidence in this case that there are other sources of Bitcoin that are being used to send money around the world. At Chainalysis, we have been able to identify some of the services that the ITMC has been using to purchase anonymity tools and the exchanges used to convert the virtual currency into regular currencies.

Terrorists, like any other person, may use Bitcoin to pay for internet infrastructure or everyday goods and services. There are many merchants around the world that accept virtual currency, some blue chip companies, such as Overstock, as well as internet service providers who offer popular anonymization tools. Using tools these purchases can be useful leads in investigations to

uncover the goods and services purchased and may provide leads to attribution of the individuals involved.

There are still no goods priced in Bitcoin or any other virtual currency. Hence, merchants that accept virtual currencies require Intermediaries to link virtual currencies to the existing financial system. The United States has done a great job at giving clear guidance to these companies about the need to register with FinCEN, as Money Service Businesses, in cases where their businesses facilitates the connection between virtual currencies and US dollars or where they are holding virtual currencies in custody on behalf of their customers. As a result, the Suspicious Activity Reports filed by virtual currency businesses has already led to many successful criminal investigations. Due to the permanence and transparency of Bitcoin transactions many of these cases are solved quickly as evidence of profiting from criminal enterprise is often indisputable.

Concluding remarks

The potential for this virtual currencies to bring radical new business models and ways of organizing social and economic relations around the world remains large. The pace of change in this domain is rapid and the eventual outcomes unpredictable.

The current use of virtual currencies is mainly financial speculation on their eventual impact. The use of virtual currencies by terrorist organizations is still very limited due to the lack of awareness and trust placed in virtual currencies. The use of Bitcoin and other virtual currencies require a level of sophistication that is not often found in terrorist organizations or their supporters. Due to the price volatility, even the use of virtual currencies requires connectivity to the existing financial system to purchase goods and services. The ease by which terrorists access the existing financial system undermines the potential benefits that virtual currencies would afford their organizations.

There is growing awareness among companies and government agencies about the potential threats and their topologies. Outright bans and over-burdening regulation on legitimate businesses pose a large risk to the visibility that we currently have into virtual currencies. Ensuring the financial sector, as a whole, is aware of the technology and has the adequate controls necessary to thwart the potential threat will help realize the potential for this technology.

Virtual currencies continue to evolve rapidly. Private businesses, like Chainalysis, and the public sector should endeavour to mitigate current threats but be cognizant of the future potential of this technology.

The United States House of Representatives
Committee on Financial Services
June 8, 2017

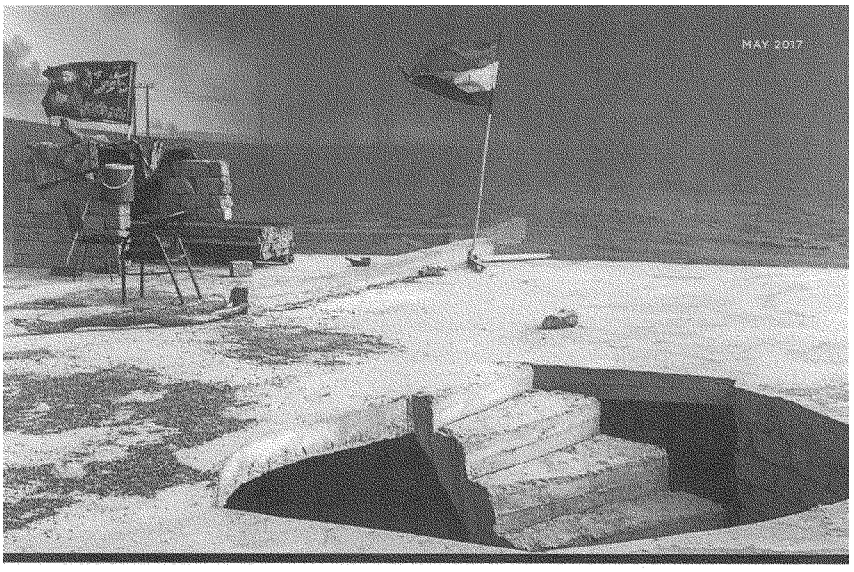
Good Morning, my name is Luke Wilson. I am the Vice President of Business Development - Investigations for Elliptic, with responsibilities for law enforcement engagement and investigations. Elliptic software is used to identify illicit activity on the Bitcoin blockchain and we provide our services to the leading Bitcoin companies and law enforcement agencies globally. We are located in London and Arlington, VA.

I want to thank Chairman, Pearce and fellow members of the Subcommittee on Terrorism and Illicit Finance for the opportunity to speak to you today. My skillset includes a deep understanding of Bitcoin and Blockchain technology, including a Fintech Blockchain Technology certificate from MIT. Prior to Elliptic I was employed by the Federal Bureau of Investigation's Cyber Division and Counterterrorism Division for a total of 7 years. With the assistance of colleagues I constructed the first interagency task force for investigating illicit uses of Bitcoin. Integrating, coordinating, and sharing investigative techniques, tactics, and procedures throughout the task force. I have advised the U.S. government and regulators on digital currencies, with previous employment with the Department of Defense and the United States Intelligence Community, I have over 17 years of law enforcement and intelligence experience.

Today's hearing on "Virtual Currency: Financial Innovation and National Security Implications" is a very good first step forward towards understanding this quickly-evolving technology. My previous employment with the FBI allowed me to investigate several crimes that involved Bitcoin. My experience is that Bitcoin is not, or should not be, alarming to investigators or private companies. Bitcoin is thought to be anonymous by some criminals, in reality it's far from anonymous, and companies like Elliptic have assisted law enforcement and private industry to identify who is behind illicit Bitcoin transactions. Elliptic's software and expertise has assisted in terrorism, ransomware, cyber extortion, and illegal arms trafficking cases, to name a few. In all of these cases we have provided intelligence and leads that help investigators to trace Bitcoin transactions and identify who is transacting. This is all made possible by the record of transactions kept on the blockchain. All Bitcoin transactions are stored on the blockchain, including those performed by criminals. The importance of the blockchain record cannot and should not be undervalued, as it provides a public, permanent and incorruptible record of transactions, the like of which is not available with any other payment method.

My experience in counter-terrorism and virtual-currencies makes me well-placed to evaluate the risks posed by potential terrorist use of Bitcoin My experience is that there have been very few verified terrorism cases in which Bitcoin was used, and that in all of these cases law enforcement was able to trace flows of Bitcoin to subjects and possible co-conspirators. While I cannot say what the future holds for terrorist use of bitcoin/ virtual currencies I can say that it's very small to date and that we have been successful in assisting law enforcement and private institutions combat that threat. Thank you for your time.

Luke Wilson VP Business Development
Elliptic Inc. 300 Clarendon Blvd, Suite 200
Arlington, VA 22201



TERRORIST USE OF VIRTUAL CURRENCIES

Containing the Potential Threat

Zachary K. Goldman, Ellie Maruyama, Elizabeth Rosenberg,
Edoardo Saravalle, and Julia Solomon-Strauss

CNAS
Celebrating 10 Years

About the Authors

ZACHARY K. GOLDMAN is the Executive Director of the Center on Law and Security and an adjunct professor at NYU School of Law. He is also an Adjunct Senior Fellow with the Energy, Economics, and Security Program at the Center for a New American Security (CNAS). Previously Mr. Goldman served as a Special Assistant to the Chairman of the Joint Chiefs of Staff at the U.S. Department of Defense, and as a policy advisor in the U.S. Department of the Treasury's Office of Terrorism and Financial Intelligence, where he was the subject-matter expert on terrorist financing in the Arabian Peninsula and Iran sanctions.

ELLIE MARUYAMA is a Research Associate in the Energy, Economics, and Security Program at CNAS. Previously she worked at the World Bank and interned with the EU Delegation in Washington. She holds a bachelor's degree in international studies from the University of California, San Diego; and a master's in international affairs from Columbia University's School of International and Public Affairs.

ELIZABETH ROSENBERG is a Senior Fellow and Director of the Energy, Economics, and Security Program at CNAS. From May 2009 through September 2013, she served as a Senior Advisor at the Department of the Treasury, helping senior officials formulate anti-money laundering and counterterrorist financing policy and develop financial sanctions. In this capacity she also helped to oversee financial regulatory enforcement activities.

EDOARDO SARAVALLE is a Joseph S. Nye Jr. Research Intern for the Energy, Economics, and Security Program at CNAS. Previously he worked as an investment banker at Moelis & Company.

JULIA SOLOMON-STRAUSS is a Program Associate at the Center on Law and Security at NYU School of Law. Previously she worked at Harvard Business School's Europe Research Center in Paris and the Chicago Council on Global Affairs. She holds a bachelor's degree in social studies from Harvard College and a master's of philosophy (history) from the University of Cambridge.

Cover Photo
Chris McGrath/Getty Images (modified by CNAS)

Acknowledgments

The authors would like to acknowledge Loren DeJonge Schulman, Frederick Reynolds, Cari Stinebower, and Jenny Cieplak for their comments and insights on this paper. They would also like to thank Bogdan Belei for his extraordinary assistance in the initial research for and drafting of this report. The authors thank Kelsey Hallahan, Ushaia Kappen, and Abigail Van Buren for their research support. Finally, they are grateful for the assistance of Melody Cook and Maura McCarthy in producing this report.

TERRORIST USE OF VIRTUAL CURRENCIES

Containing the Potential Threat

02 **Executive Summary**

03 **Chapter 1**
Introduction

09 **Chapter 2**
Setting the Stage: Contemporary Terrorist Financing and the Evolving Virtual Currency Landscape

17 **Chapter 3**
Evaluating the Potential for Terrorists to Abuse Virtual Currencies

25 **Chapter 4**
Virtual Currency Abuse in the Future: Criminals vs. Terrorists

29 **Chapter 5**
Updating the Policy and Regulatory Framework to Address Terrorist Use of Virtual Currencies

35 **Chapter 6**
Recommendations and Conclusion

Executive Summary

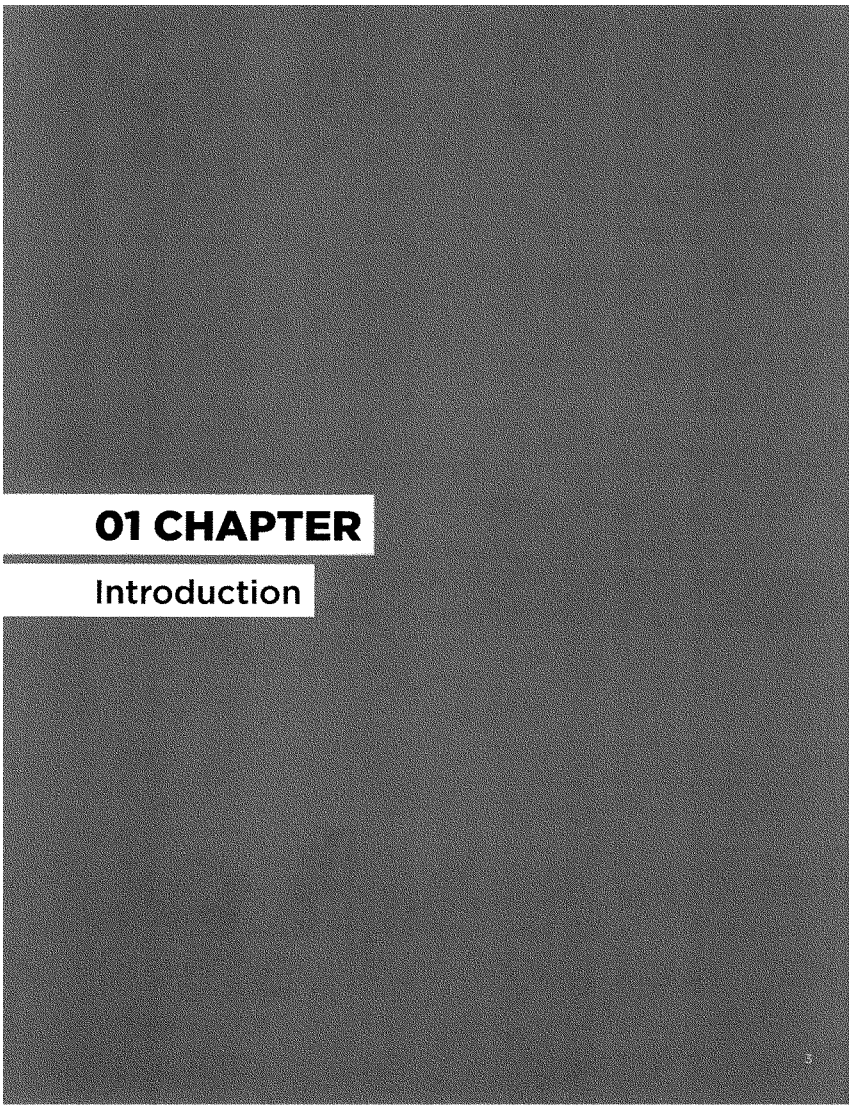
This paper explores the risk that virtual currencies (VCs) may become involved in the financing of terrorism at a significant scale. VCs and associated technologies hold great promise for low cost, high speed, verified transactions that can unite counterparties around the world. For this reason they could appear appealing to terrorist groups (as they are at present to cybercriminals). Currently, however, there is no more than anecdotal evidence that terrorist groups have used virtual currencies to support themselves. Terrorists in the Gaza Strip have used virtual currencies to fund operations, and Islamic State in Iraq and Syria (ISIS) members and supporters have been particularly receptive to the new technology, with recorded uses in Indonesia and the United States.

Most terrorist funding now occurs through traditional methods such as the *hawala* system, an often informal and cash-based money transfer mechanism, and established financial channels.[1] If VCs become sufficiently liquid and easily convertible, however, and if terrorist groups in places such as sub-Saharan Africa, Yemen, and the Horn of Africa obtain the kinds of technical infrastructure needed to support VC activity, then the threat may become more significant.

The task of the law enforcement, intelligence, regulatory, and financial services communities, therefore, must be to prevent terrorist groups from using VCs at scale. The use of VCs by "lone wolf" terrorists—a much bigger potential threat because of the small scales of funding needed to execute an attack—represents the kind of problem in intelligence and digital forensics that law enforcement agencies are well equipped to handle, even if they tax existing resources.

Attacking terrorists' use of virtual currency at scale is a challenging task for many stakeholders. New financial technology firms often lack the resources to comply effectively with oversight obligations, while regulators have tended to devote few resources to non-bank institutions. At the same time, different countries have adopted varying approaches to the regulation of virtual currencies, posing an enforcement challenge in a globalized field that requires a unified response. Finally, the privileging of prevention over management of illicit finance risk in the compliance world has created an incentive structure for banks that does not, ironically, push them toward innovative approaches to countering terrorist financing, including via virtual currencies.

The counterterrorist financing community should adopt three guiding principles that will provide the foundation for policies aimed at countering both the new virtual currency threat and the broader illicit finance danger. First, policy leaders should prioritize the countering of terrorist financing over other kinds of financial crime. Second, the policy and regulatory posture should be oriented toward rewarding and incentivizing innovation. Third, policymakers should emphasize and create a practical basis for strengthening coordination between the public and private sectors on terrorist financing. These approaches form the foundation of an effective response to existing and emerging terrorist financing threats and will balance the burden of regulatory compliance with the policy need to support innovative new virtual currency technologies.


01 CHAPTER
Introduction

In the past several years, terrorist groups in Gaza have solicited support in Bitcoin; there are isolated reports that ISIS has used the cryptocurrency; and cybercriminals use it and other virtual currencies in a range of circumstances. We cannot yet know whether the uses of virtual currencies by terrorist groups amount to isolated incidents or foretell a broader and more pernicious trend.[2] Individual incidents in which lone terrorists or terrorist groups use VCs of course pose a challenge. This is particularly so because the funding requirements for disruptive lone wolf acts of terror are small enough to pose a risk because they may slip through a counterterrorism financing system that struggles to stop small-scale acts of such financing regardless of the medium. But VCs become a strategic threat in the counterterrorism context only when they can compete with cash and other readily available means of financing and achieve "scale," which in this paper signifies a combination of market capitalization, liquidity, convertibility, and network effects that add up to ease of use. Scaled use of VCs by illicit actors poses a particular challenge and exacerbates the underlying threat posed by criminal or terrorist activity because it makes illicit funding networks harder to disrupt. And the larger the stable funding supply for terrorist groups, the greater the scale at which the groups themselves can operate and the more they can engage in acts of violence.

While VCs have many very important legitimate uses, certain characteristics also make them susceptible to abuse. Many, especially cryptocurrencies, protect or obscure identities, thereby making it more difficult for law enforcement to reveal and track those identities than traditional mechanisms of value transfer. Should terrorists adopt VCs at scale, therefore, it could become much more difficult to track and disrupt them.

A second reason it is important to understand the circumstances in which terrorist groups may wish to use VCs at scale is the global reach of such currencies. With certain virtual currencies, it is possible to transfer money instantly around the world without making use of institutions like banks, which require more transparency and have obligations to report suspicious transactions. Even centralized VCs may be accessible online anywhere in the world, so terrorists and criminals can take advantage of these currencies that have been set up in jurisdictions with less scrutiny. Potentially, such characteristics could effectively build a digital platform on top of established systems that currently allows terrorists, and others, to transfer cash on an international scale. Such an architecture would make it easier for terrorist groups to amass larger amounts of money than has generally been possible previously.

Finally, the novelty and some particular attributes of VCs, such as decentralization, make them a particular regulatory challenge. Decentralized cryptocurrencies such as Bitcoin lack concentrated repositories of identifying information on account-holders, which law enforcement agencies typically use in financial crimes and counterterrorism investigations, but which are unavailable when dealing with many VCs. A more precise understanding of the threats and risks posed by VCs will help regulators to develop an effective and efficient governance framework to monitor for potential abuse. In turn, a successful framework will ultimately strengthen the global fight against terrorist financing and terrorism as a whole.

In the post-9/11 era, the international community has made significant progress in the struggle against terrorism generally, and in the struggle against terrorist financing specifically. In the counterterrorism context, "following the money" has been a particularly effective component of an overall strategy to degrade the capabilities of terrorist groups.[3] One of the most significant victories has been the establishment of a global legal and policy framework—grounded in U.N. Security Council Resolutions, national legislation, and global standards—that, by blocking terrorist groups' access to the formal financial system, has made it significantly more difficult for them to raise, move, store, and use funds.

However, recent evolutions in the terrorist threat, including the rise of ISIS and the continued importance of al Qaeda and its affiliates, have led the Financial Action Task Force (FATF), the intergovernmental standard-setting body for combating money laundering,

The hawala system of person-to-person money transfer, pictured above, allows terrorists to transfer cash on a global scale outside the regulated financial system, escaping anti-money laundering and combating the financing of terrorism oversight. (Institute for Money, Technology and Financial Inclusion/Flickr)

terrorist financing, and other threats to the integrity of the international financial system,[4] to note that "further concerted action urgently needs to be taken . . . to combat the financing of . . . serious terrorist threats" that have "globally intensified."[5]

Specifically, a number of challenges regarding terrorism and its financing remain. First, terrorist groups that control territory pose one of the most difficult strategic challenges that the counterterrorism community faces. When groups control territory, it is easier for them to plan and train without disruption. It is also easier for them to derive financial and material support from the local population (through taxation, extortion, or the extraction of natural resources) without having to rely on transfers of funds from external sources that are inherently more vulnerable to disruption.

A second strategic challenge pertains to individual lone wolf terrorists or cells that lack formal ties to any established group. This dynamic makes it more difficult to anticipate attacks with intelligence, because it is difficult to determine which unaffiliated individuals will perpetrate attacks. And because these attacks are relatively inexpensive to execute, it is more difficult to identify and choke off their sources of support. Terrorists such as those who carried out attacks in Orlando, Florida; San Bernardino, California; or Nice, France do not rely on associations with larger groups that require significant funds to sustain themselves. Therefore, they leave only trace financing "signatures" and are not easy to detect and disrupt under a global framework built for more established and less nimble threats.[6] Addressing lone wolf attacks is a significant intelligence challenge for the counterterrorism community. And identifying the ways in which such attackers may use VCs to fund themselves is similarly a significant forensic and intelligence issue that may require the government to invest in new capabilities and to work more closely than it has in the past with private entities.

Despite significant progress in the global counterterrorist financing regime, gaps remain in implementation and coverage. The charitable sector, for example, is still vulnerable to abuse, and unlicensed money transmitters, cash smugglers, and criminal activity of all kinds are a source of support for terrorist groups, both in the United States and abroad.[7] Furthermore, the global counterterrorism financing regime is more oriented toward identifying and degrading the ability of organized groups to function than toward the rising threat of independent attacks. When a terrorist in Nice, for example, can kill 86 people simply by renting a truck and driving it through crowds of revelers on Bastille Day, policy leaders must rethink the approach to counterterrorism that has been oriented primarily toward well-defined groups, as al Qaeda was before the 9/11 attacks.

Looking specifically at the counterterrorist financing risk for VCs, it does not appear that terrorist groups have yet used these currencies at scale, even while other criminal groups (specifically cybercriminals) have done so. Indeed, the U.S. government's 2015 "National Terrorist Financing Risk Assessment" cited cash and the banking system as two of the most significant terrorist financing risks that the United States faces.[8] The assessment described virtual currencies only as a "potential emerging TF [terrorist financing] threat,"[9] and noted that "the possibility exists that terrorist groups may use these new payment systems to transfer funds collected in the United States to terrorist groups and their supporters located outside of the United States."[10] At the same time, the European Banking Authority classified as a high priority risk terrorist use of VC remittance systems and accounts.[11] More troubling is the potential for virtual currencies to "democratize" the funding of terrorism, allowing far-flung, disconnected individual donors to participate in TF networks.[12] So while terrorist groups are not yet using VCs at scale, a key goal of the policy and financial regulatory communities is to prevent that from happening by adapting measures to better track and prevent this threat. A more forward-leaning posture on financial information sharing and disclosure would benefit all stakeholders involved in addressing terrorists' use of VCs and illicit financial activity more broadly.

While terrorist groups are not yet using VCs at scale, a key goal of the policy and financial regulatory communities is to prevent that from happening.

Terrorist groups have not yet adopted VCs at scale, but cybercriminal networks have. There are several reasons criminal and terrorist groups have behaved differently with respect to the adoption of virtual currencies. One important factor surely is the degree of technological sophistication needed to use such currencies at scale. The criminal enterprises that have made extensive use of VCs are generally engaged in technically complex crimes such as the remote theft and sale of data (or significant narcotics trafficking), and they operate in areas that have at least reasonably well-developed financial and telecommunications infrastructures.

Many terrorist groups, by contrast, operate in areas with poor infrastructure and low penetration of modern technical and telecommunications tools. This is true, for example, of al Qaeda in the Islamic Maghreb (AQIM) in the Sahel, al Qaeda in the Arabian Peninsula (AQAP) in Yemen, and, in some measure, ISIS in Iraq and Syria. And this dynamic illuminates a major obstacle to the adoption of VCs, even while terrorist groups take advantage of sophisticated technology in non-financial contexts. ISIS's use of social media to recruit and propagandize[13] and Hezbollah's use of drones stand out as two prominent examples.[14] Technologies like drones do not rely on network effects to be useful and can be provided (nearly) off the shelf and ready to use. Similarly, social media is available on the kinds of smartphones and websites that have been commoditized. Virtual currencies, by contrast, are more difficult to create (should a terrorist group try to do so), employ, and maintain.

Of course, not all terrorist groups or their supporters contend with limited Internet access, computing capabilities, or knowledge of sophisticated tactics to evade regulatory detection of electronic money movements. This is one reason for the instances of terrorist groups using VCs, albeit in more limited ways.

Terrorist networks, by contrast, have a different "business model." They often seek to move money from places outside the locations where they operate to the areas in which they plan and from which they launch attacks. Often they use many layers of intermediaries so that donors and ultimate recipients may not be known to one other. Or, in the case of lone wolf attackers, they scrape together funding from a wide range of sources. In either case, terrorists use the funds to buy things they need to sustain the group or to conduct attacks. And because they do so from the general economy, they often would need to reconvert the VCs they receive into fiat currency. This final step introduces both an unnecessary layer of complexity and an increased vulnerability to the disruption of their operations by adding additional actors and entities into the fundraising matrix.

Moreover, the virtual currency that has achieved the greatest market capitalization and penetration—Bitcoin—is only pseudonymous, not fully anonymous, as is commonly and incorrectly understood. The cryptographic addresses of the sender and the recipient of transactions are recorded; although they may not be linked to real-life identities, with enough investigative resources it may be possible to uncover the true identity

Many terrorist groups operate in areas with poor infrastructure and low penetration of modern technical and telecommunications tools.

Terrorist networks and criminal groups also have different financial structures in which they do or may take advantage of virtual currencies. Cybercriminals often use VCs to buy or sell stolen data, for their exploits in online "dark web" markets,[15] or for commercial transactions in illegal activities such as drug or weapons trafficking.[16] There is less of a need for VCs to be convertible in that context because their users can simply recycle them for the next purchase. Cybercriminals located in Eastern European countries with poor records of law enforcement cooperation with the West can exchange VCs for fiat currencies in unregulated exchanges.[17] Cybercriminals also often engage in extensive vetting of other purported criminals who wish to join online forums in which cybercrime activities take place; therefore they have some degree of confidence that their transaction counterparties can be trusted.[18] This dynamic stems from the fact that the criminals are often repeat players who depend on the continued operation of the network for their activities.

of senders and recipients of Bitcoin transactions. This of course diminishes the allure of that means of transferring funds to terrorists. Notwithstanding its incomplete anonymity, Bitcoin remains dominant in the space. For example, Monero, a cryptocurrency that is more anonymous than Bitcoin, has a market capitalization of about $340 million; Bitcoin's market cap is $17 billion.[19]

But the final—and most important—reason that terrorist groups have not adopted virtual currencies at scale is that these groups, and individual terrorist operatives, have not yet perceived the need to do so. They still find it possible to circumvent global rules governing terrorist financing with sufficient ease and frequency that using VCs is unnecessary. They exploit incomplete implementation of regulatory requirements and global standards at banks, use unlicensed and undersupervised money services businesses (MSBs), or simply cart around cash. As long as these value transfer methods are readily available, there is no great need to invest in new, complicated techniques to transfer value.

Therefore, the crux of the challenge that financial regulators and the counterterrorism community must confront with regard to virtual currency is one of monitoring and prevention: How will they know if and when terrorists begin to use VCs at scale? And how can they design the financial regulatory framework governing VCs to harness the positive uses to which they can be put while preventing them from abuse?

One of the most important factors in the ability of governments and other stakeholders to manage the risks posed by VCs is effective collaboration and communication. Three main categories of actors make up this ecosystem—financial institutions, the regulatory agencies that supervise them, and the law enforcement and intelligence community that target criminals and security threats.

At present, tension among these constituencies prevents them from optimally monitoring and governing the use of virtual currencies. Fundamentally, law enforcement agencies and bank regulatory agencies have different authorities and use information from the private sector in different ways. They also have different approaches to the terrorist financing challenge. Whereas the mission of law enforcement officials is to halt terrorism, regulators are charged with ensuring that financing does not occur in banks that they supervise. Law enforcement agencies take data that they get from banks (often via the government's financial intelligence unit, the Financial Crimes Enforcement Network, FinCEN, in the United States), combine it with other intelligence or evidence to improve their understanding of the threat landscape, and engage in further intervention—often a prosecution—to address it.[20] Regulatory agencies such as the Federal Reserve Bank or the Office of Comptroller of the Currency (OCC) and state-level regulators such as the New York State Department of Financial Services (NYDFS), by contrast, use information from the private sector to assess compliance with existing rules, and then undertake enforcement actions if necessary. These regulators also use private sector information to inform their view of changes that they or others may need to make to manage risk in the financial sector.

In the past decade, financial regulators responsible for supervising banks have imposed significant fines for violations of laws designed to counter illicit finance.[21] As described later in this paper, these enforcement actions have inhibited the development of effective public-private collaboration in the governance of VCs, because they have generated a significant amount of uncertainty within banks. Such collaboration is critical to prevent virtual currencies from being abused for illicit purposes at greater scale, particularly by terrorist groups.

Two main trends stand in the way of greater incorporation of VCs into the formal financial system, which would help manage the risks inherent in the near-instantaneous and anonymous global transfer of funds. The first trend in the financial sector is the desire of banks to avoid high compliance-cost business activities, including in jurisdictions with poor regulation and a relatively high occurrence of illicit financial activity or sanctions evasion, or in dealings with high-risk types of clients.[22] This trend has led many financial institutions to shed expensive-to-service accounts, correspondent relationships, and clients, and is commonly referred to as "de-risking."[23] Virtual currencies have been caught in this trend. Businesses that deal extensively in VCs have found it difficult to establish relationships with the largest global banks because the businesses are often perceived as relatively risky and therefore too costly to take on.[24] As a result, VC businesses have had to conduct their banking operations at smaller financial institutions that do not devote as many resources to compliance as do large global banks, and that are less well regulated than large money center banks. This dynamic, in turn, increases the likelihood that VCs will be used for the conduct of illicit activity at a scale, posing a security threat.

Businesses that deal extensively in VCs have found it difficult to establish relationships with the largest global banks.

Virtual currency firms are also stepping into lines of business—such as cross-border remittances—that some large global banks are abandoning because of the perceived risk.[25] And the anti–money laundering (AML), combating-the-financing-of-terrorism (CFT) and sanctions-compliance system requires companies to establish customer identification programs, screen for sanctions compliance, and establish suspicious activity reporting systems. This rigor may be too expensive for small VC startup companies, which may therefore either collapse before they get off the ground or operate in an unregulated manner, thereby increasing the risk that bad actors may use VCs without detection.

The second broad trend that has made it more difficult to govern virtual currencies is the libertarian ethos that animates many of the individuals and entities involved in the creation and growth of the VC movement.[26] For many people, the most attractive dimension of VCs such as Bitcoin is the same one that makes it most difficult to

govern—it serves as a store of value, unit of account, and medium of exchange that does not require the involvement of any large centralized government institutions or banks.[17] That means these kinds of VCs lack many of the features of national currencies that make them secure and trusted, and it makes them susceptible to abuse by criminals, terrorists, and fraudsters who want their financial transactions to be opaque. It also makes the currency volatile. A recent dispute among developers about one of the technical characteristics of the virtual currency led to a 20 percent decline in the value of Bitcoin over a single weekend.[18] Any system of regulation and governance for virtual currencies must contend with the fact that the developers who create many VCs do so in a manner designed to avoid control by centralized institutions of authority.

So what is the way forward for the governance of virtual currencies? How do policy leaders ensure that terrorist groups do not migrate to them and simultaneously support their innovative contributions to the financial system? Part of the answer requires changes to the current AML regulatory system—reforms to be discussed in greater detail in this paper. Another path is to create incentives for VC businesses themselves to see that preventing abuse is in their commercial interests. This is because a greater number of people will participate in a market in which they have confidence—which, in turn, requires that the public perception of VCs be positive. It also requires ordinary people to feel as though VC exchanges—the gateways between the fiat

What is the way forward for the governance of virtual currencies?

currency systems and new systems—will protect them against fraud. As described in this paper, this dynamic is what ultimately induced PayPal to develop one of the most sophisticated fraud prevention systems available. Ultimately it is the way in which any disruptive new technology may achieve scale.

The paper first describes contemporary methods of terrorist financing and the emerging virtual currency marketplace. Against this backdrop, the paper lays out strategies to better monitor terrorist use of VCs and adapt policies and regulations to guard against broader use. It concludes with specific policy recommendations to stakeholders.

02 CHAPTER

Setting the Stage: Contemporary Terrorist Financing and the Evolving Virtual Currency Landscape

Tracking and disrupting terrorists' financial networks is an important way to follow and impede their overall operations. Intelligence agencies, financial intelligence units including FinCEN, and law enforcement officials work to stay ahead of the evolving threat of terrorist financing, which is influenced by changes in the global financial system and the emergence of new financial technologies, among other factors. This chapter briefly summarizes the vulnerability of VCs to abuse by terrorists, and how terrorists have used this value transfer method in the past. To provide context, the chapter describes the general landscape of contemporary terrorist financing, as well as some of the important innovative uses to which VCs are being put. This framing underlies the challenge and need for financial policymakers to support innovation in VCs and new payment technologies while simultaneously guarding against their abuse.

Contemporary Terrorist Financing

Although terrorist financing requirements vary depending on the organization, they generally consist of funding specific operations and/or providing for the broader costs needed to maintain the viability of the terrorist organization and promote its ideology and objectives.[29] Large organizations require significant funding. Al Qaeda's pre-9/11 annual budget was an estimated $30 million,[30] while ISIS approved a $2 billion budget for 2015.[31] These large organizations often support operatives, some with dependents, who require income, training, and travel support.[32] Costs of specific attacks can vary greatly, from an estimated $10,000 for the 2015 Paris attacks to $400,000–500,000 for the 9/11 attacks.[33] Terrorist groups exhibit a great deal of variation, adaptability, and opportunism when it comes to their funding and are essentially willing to raise and move money any way they can.[34] Although traditional methods of doing this are still in use, including through criminal activities and by relying on banks, MSBs, and cash couriers, innovations unfolding in the 21st century digital economy are introducing changes.

SOLICITING AND RAISING MONEY

Terrorist groups' sources of revenue and fundraising activities combine traditional and new methods. According to FATF, these organizations depend on numerous sources of income derived from both criminal activities and the abuse of legitimate activities.[35] Examples of criminal activities include arms trafficking, kidnapping for ransom, extortion, racketeering, and drug trafficking.[36] Terrorist organizations and their associates also divert funds from legitimate sources such as charities and businesses.[37]

ISIS, described by senior U.S. officials as one of the world's best-funded terrorist organizations,[38] counts on a diverse array of sources.[39] According to U.S. Department of the Treasury estimates, ISIS earned approximately $1 billion in total revenue in 2015, $500 million of which came from the sale of oil and about $350 million from extortion.[40] Unlike most terrorist organizations, ISIS controls tracts of territory across Syria and Iraq.[41] It derives the most significant portion of its revenue from a range of illicit proceeds generated in areas where it operates.[42] This includes theft of cash, as well as assets stolen from banks, black market sale of natural resources such as oil and agriculture, and sale of stolen antiquities from within its controlled territory.[43] In 2014 and early 2015, ISIS obtained a windfall of between $500 million and $1 billion in Iraqi currency from bank vaults, while it made less than $10 million in trafficking antiquities.[44]

Apart from funding derived from the territory under its control, ISIS also has other prominent sources of funding. In 2014, ISIS earned between $20 and $45 million from kidnapping-for-ransom (this figure has since declined substantially, due to the reduced presence of potential Western hostages in or near ISIS-controlled territories).[45] The organization has received funding from wealthy, private, regional donors as well as foreign terrorist fighters who collect money for travel, travel

Unlike most terrorist organizations, ISIS controls tracts of territory across Syria and Iraq. It derives the most significant portion of its revenue from areas where it operates.

with funds, and/or receive funding from external supporters.[46] ISIS's financial picture is dynamic, depending on the availability of resources and the status of coalition military operations.[47] For instance, oil and gas sales to the Assad regime have recently been an important source of the group's funds.[48] In fact, despite the Syrian regime's insistence that it is fighting ISIS with the cooperation of Russia and Iran, it purchases oil from the terrorist group, which sustains it in the face of military pressure.[49]

Terrorist groups have begun to view social media and crowdfunding networks as innovative and expansive new mechanisms for soliciting funds. In one case, a user placed a call for funds for a fighter in Syria on a Facebook page that provided recipes. The fighter supposedly needed "equipment, food, and pharmaceuticals," and the

user gave details of an account with a German bank.[50] This illustrates the ease with which anyone with access to the Internet can fundraise for a terrorism-related cause outside of traditional platforms.

Similarly, crowdfunding websites enable terrorists to set up a page and collect donations.[51] While these crowdfunding platforms have cooperated with investigations in the past, FATF has called for further study about their role in terrorist financing activity.[52] ISIS has made effective use of crowdfunding campaigns to garner support.[53] The group—along with other terrorist organizations in the area—has provided a menu of options for prospective crowdfunding donors to choose from, ranging from covering the cost of a weapon to financing an entire operation.[54] In some instances, the true purpose of a crowdfunding campaign is masked, so an individual may end up inadvertently contributing to a terrorist organization that claims to be engaging in charitable or humanitarian activities.[55]

MOVEMENT OF TERRORIST FUNDS

Traditionally, to move money terrorist groups relied on banks, money transfer systems, and cash couriers. These methods are still in use today. However, terrorist organizations continue to adapt to the pressure placed on their financial networks since 9/11, and they rely on means and resources that are now more varied and localized.[56] New, alternative methods to move money include the use of prepaid cards and digital payment systems.[57] These new methods facilitate transactions that are faster, more anonymous, and capable of global movements.

The formal financial sector remains attractive to terrorist organizations due to its reliability, vast size, and the speed and ease with which money can be moved.[58] To orchestrate the 9/11 attacks, al Qaeda extensively used banks in the United States.[59] Hijackers opened accounts in their own names and conducted small transactions that could pass unnoticed amid billions of dollars flowing through the formal financial sector.[60]

In 2010, for example, St. Louis resident Mohamud Abdi Yusuf was indicted and arrested for sending funds to al Shabaab supporters in Somalia from licensed MSBs, using fictitious names and phone numbers to conceal the purpose of his activities.[62] He was also charged with structuring financial transactions to avoid record-keeping requirements.[63]

Some terrorist organizations resort to physically moving cash across international borders.[64] This method is particularly common in regions where the electronic banking system is nascent or little used by the population.[65] An October 2016 FATF report noted that large, informal, cash-based economies in countries of West and Central Africa with porous borders and lack of financial controls create opportunities for the anonymous movement of money that leaves no paper trail.[66] According to captured internal al Qaeda in Iraq documents, between 2006 and 2007, funds brought by foreign fighters were estimated to make up more than 70 percent of the budget in the group's Border Sector 1 near Sinjar.[67]

Digital payment services such as PayPal, Amazon Pay, and Google Wallet may also be susceptible to abuse.[68] In 2015, Mohamed Elshinawy of Maryland was arrested and charged with attempting to aid ISIS. According to a criminal complaint filed by the Federal Bureau of Investigation (FBI), he received about $8,700 through Western Union and PayPal accounts from individuals abroad he believed had connections to ISIS, and the money was intended for "nefarious purposes."[69] Terrorism suspects have used multiple online payment accounts—both verified and guest accounts—to purchase equipment and clothing before traveling to conflict zones.[70] Some online payments companies such as Venmo have deployed scanning technologies to flag words and symbols associated with terrorism.[71] The prevalence of online payment services and purchases, of low-value transactions often involved, and the ease with which one is able to create accounts are the basis of the difficulty involved in definitively linking to terrorism transactions on these new payment platforms.

Large, informal, cash-based economies in countries of West and Central Africa with porous borders and lack of financial controls create opportunities for the anonymous movement of money that leaves no paper trail.

Terrorist organizations have also used MSBs and alternative remittance systems, financial services providers that often do not register themselves in order to avoid oversight within the regulated financial system.[61]

Counterterrorism officials are also focused on prepaid cards. Following the November 2015 Paris attacks, French government officials reinvigorated their scrutiny of prepaid cards because of their involvement in

financing the terror attacks.[72] Searches of the homes of individuals belonging to terrorist networks have turned up prepaid cards.[73] Last year the European Commission proposed stricter rules on the use of prepaid cards, including reducing the threshold for making anonymous payments from 250 to 150 euros.[74] Although policymakers struggle to know the full extent of terrorists' use of prepaid cards, the amount of money each card can carry as well as its ease of use pose a significant threat in the terrorist financing context.

Terrorist Groups' Use of Virtual Currency

Virtual currencies may be appealing to terrorist groups for the same reason they appeal to legitimate actors. VCs are mainly distinguished by their global reach, often a decentralized structure, varying degrees of anonymity, rapid transactions, and minimal costs. The rapid, efficient, and less costly financial transactions that VCs enable account for their appeal to an array of actors.

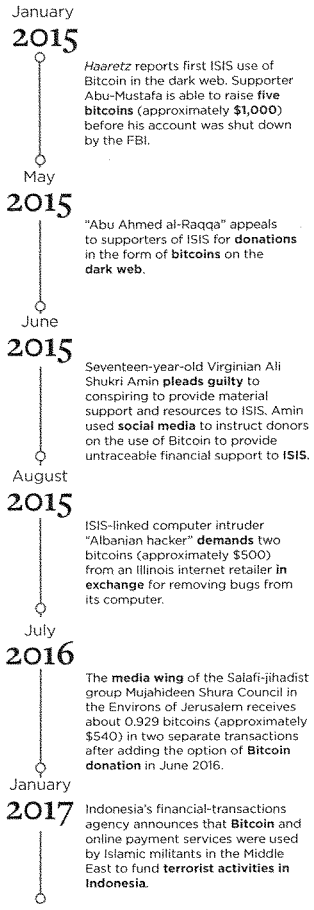
The detection of illicit transactions conducted via VC rather than fiat currency is inherently challenging. Law enforcement officials and regulators may have difficulty accessing customer and transaction records that are distributed across different jurisdictions,[75] or that do not exist at all. Centralized VC systems may deliberately be located in jurisdictions with weak AML/CFT regimes.[76] The diffusion of infrastructures, entities, and services involved in transferring or executing payments in these currencies makes it challenging to assign jurisdictional responsibility for compliance and enforcement, while the evolving nature of VC technology and business models compounds the difficulty of tracking their use.[77]

Amid these forces, anecdotal evidence points to episodic terrorist use of VCs. According to Yaya Fanusie, the first publicly verifiable instance of a terrorist group using Bitcoin entailed a social media fundraising campaign run by the media wing of the Mujahideen Shura Council in the Environs of Jerusalem, a collection of Salafi-jihadist groups in Gaza designated by the U.S. State Department as a foreign terrorist organization. The campaign began in July 2015, and it added the option for donors to pay in Bitcoin in June 2016. As of August 2016, the campaign had received roughly 0.929 bitcoins (around $540) through two transactions that occurred six days apart in July 2016, despite seeking at least $2,500 per fighter. The identity of those responsible for making the deposits is unclear, but Fanusie suggests they are proficient Bitcoin users and employed techniques to preserve their anonymity.[78]

ISIS supporters' activities have also shown the potential for terrorist groups to use virtual currencies on a global scale. Most recently, Indonesia's financial-transactions agency announced that Bitcoin and online payment services had been used by Islamic militants in the Middle East to fund terrorist activities in Indonesia.[79] In August 2015, a computer intruder with ties to ISIS who went by the user name "Albanian hacker" demanded payment of two bitcoins from an Illinois Internet retailer in exchange for removing bugs from their computer. Using data extracted from the server, the Albanian hacker put together a "kill list" for ISIS with identities of 1,351 U.S. government and military personnel.[80] In June 2015, Ali Shukri Amin, a 17-year-old in Virginia, pled guilty to conspiring to provide material support and resources to ISIS. Among other wrongdoings, including facilitating the travel of ISIS supporters to Syria, he used social media to instruct donors on the use of Bitcoin to provide untraceable financial support to the group.[81] In May 2015, "Abu Ahmed al-Raqqa" appealed to supporters of ISIS for donations in the form of Bitcoin on the dark web.[82] In January 2015, *Haaretz* reported on the first instance of an ISIS cell fundraising using Bitcoin on the dark web. The fundraiser was a man identified as Abu-Mustafa, and his Bitcoin account number indicated that he had managed to raise five bitcoins (approximately $1,000) before the FBI shut down his account.[83] More broadly, a number of forum discussions on websites affiliated with the group show efforts by more technical members to educate their peers on the use of virtual currencies.[84] Participants have also referenced using VCs to transfer money to countries where traditional transactions are difficult due to lack of network capacity or surveillance and regulation.[85]

Participants have also referenced using VCs to transfer money to countries where traditional transactions are difficult due to lack of network capacity or surveillance and regulation.

Selected Episodes of Terrorists Using VCs[86]



These instances of terrorist groups using virtual currency indicate that the phenomenon is, at the moment, episodic and not widespread. The "firsts" of terrorist groups using VCs are fairly recent; they appear to still be familiarizing themselves with this new form of value transfer. Where the amount of virtual currency involved has been reported, it has tended to be small. The U.S. government is not inordinately concerned about this threat; David Cohen, former Undersecretary of the Treasury for Terrorism and Financial Intelligence, noted in 2014 that terrorists generally need "real" currency to pay their expenses, rather than employing VCs.[87] A 2015 RAND report posited that there was little evidence terrorists were developing their own VCs.[88] According to a January 2016 Europol report, "Despite third party reporting suggesting the use of anonymous currencies like Bitcoin by terrorists to finance their activities, this has not been confirmed by law enforcement."[89] Scholars generally agree that while virtual currencies have gained in popularity, their expansion among terrorist organizations has been slow and has lagged behind transnational criminal uses of the technology.[90] The following chapter explores some of the reasons for which terrorist groups have been slow to adopt virtual currencies.

Scholars generally agree that while virtual currencies have gained in popularity, their expansion among terrorist organizations has been slow and has lagged behind transnational criminal uses.

The Evolving Virtual Currency Landscape

Information technology and the spread of the Internet have revolutionized the financial system. Populations previously excluded from financial markets can now save, transfer, and exchange money with more ease, at greater speed, and with fewer costs. A 2015 U.S. study found that Internet access reduced the probability of not having a bank account by 9.8 percent for individuals in the lowest income decile and by 7.1 percent for the whole population.[91]

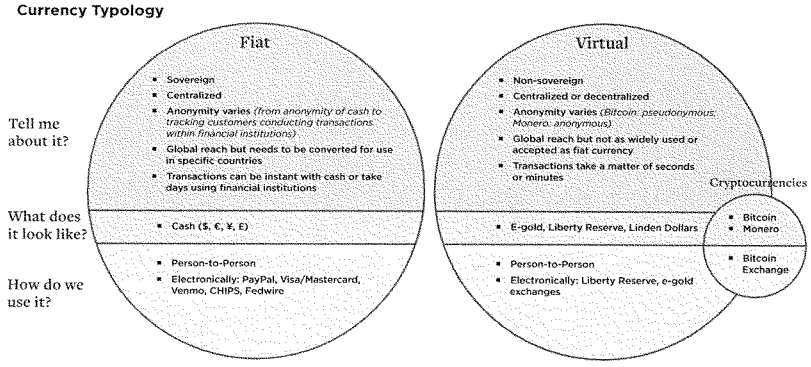
Mobile technologies allow people in developing economies to make small-value electronic payments from mobile phones. Kenya's M-Pesa and similar mobile money systems—used by 86 percent of Kenyans[92]—show how mobile technology makes financial services accessible in a country with almost 25 times fewer ATMs per person than in the United States.[93] Although this mechanism of transferring money does not serve as a primary medium of illicit finance,[94] some experts believe it is simply a matter of time and proper regulatory oversight before violations are discovered.[95] These technologies are more prolific, and therefore potentially more of an immediate security threat, than virtual or cryptocurrency technology such as Bitcoin. According to a study tracking growth during the months since their respective releases, Bitcoin grew at about 5 percent of M-Pesa's rate.[96] The widespread nature of M-Pesa, combined with limited oversight, has led some experts to be concerned. One analyst argued that SMS systems "fail to provide the protections needed by financial services."[97] Another explained, "Simply put, mobile payment systems can be considered the 'Wild West' for savvy criminal organizations."[98]

Online and peer-to-peer money transfer services such as Xoom Corp. and Venmo are disrupting not only the remittance market,[99] one of the slowest and most expensive subsectors of consumer finance, but also traditional payment forms, for example cash and checks.[100]

VIRTUAL CURRENCY TYPOLOGY

Virtual currencies, and especially cryptocurrencies, are at the leading edge of this financial revolution. While they vary along three main axes, VCs lack sovereign backing. First, these currencies can be non-convertible or convertible. Non-convertible currencies operate within a closed virtual platform. Examples include currencies used in massively multiplayer online role-playing games, where no sanctioned mechanism exists to translate the virtual unit into fiat currency. In these systems, however, black market exchanges may spring up, effectively offering some degree of convertibility.[101] Convertible currencies, by contrast, have a defined equivalent value in fiat currency and can be exchanged, through either floating or pegged rates.[102] Second, VCs vary in their degree of anonymity. Generally they fall between the almost total anonymity of cash exchanges and the traceability and disclosure of online payments through the traditional banking system, making them appealing to legitimate users concerned about privacy.[103]

Currency Typology



Recently, new entrants in the VC space have focused on complete anonymity by developing techniques to obfuscate the true origins of Bitcoin transactions.[104] Cybercriminals are making use of new cryptocurrencies such as Monero, which has been called the "drug dealer's cryptocurrency of choice,"[105] because of its enhanced anonymity properties. In August 2016, Monero rose to prominence after AlphaBay, the dark web market, started accepting it as a Bitcoin alternative.[106] It attempts to ensure users' privacy by combining multiple transactions, hiding the amount of each transaction, and obscuring the recipient of the funds.[107] By January 2017, it had become 27 times more valuable due to its adoption in online criminal markets.[108] It is already drawing the attention of law enforcement for its facility of use by criminals on the dark web.[109] Similarly, Dark Wallet, which seeks to make de-anonymizing Bitcoin transactions impossible, disrupts the blockchain's potentially identifying aspects by combining random contemporaneous transactions and then encrypting recipients' information so it does not appear on the blockchain.[110] This method explicitly seeks to enable illicit finance; as one of its founders stated, "It's just money laundering software."[111] Dark Wallet has been commended on blogs supportive of ISIS.[112]

Decentralized VCs have no central administrator or oversight, and trust is based on consensus validation.

Finally, VCs may be centralized or decentralized. Fundamental to this distinction is the question of how to engender trust without government or central bank backing. For centralized VCs, an administrator issues the currency, maintains a unified central payment ledger, and retains the power to withdraw currency from circulation.[113] This central institution acts as the ultimate repository and guarantor of trust. Examples include Linden Dollars, available in the Second Life virtual reality world; Perfect Money; units of the now-defunct e-gold; and LRs, units used on Liberty Reserve.

As discussed above, decentralized VCs have no central administrator or oversight, and trust is based on consensus validation. They often rely on cryptography for their operations and use distributed ledger technologies to record transactions. As the most widespread decentralized VC, Bitcoin has also faced the most real-world vetting. It survived a software glitch in 2013 and a security breach and bankruptcy of its largest exchange in 2014. It has found acceptance as a currency among retailers including popular websites, for example Expedia and Overstock.com.[114] As circulation broadens and trading volume increases, it may become more stable.[115]

KEY ADVANTAGES OF VIRTUAL CURRENCIES

Virtual currencies such as Bitcoin offer two primary benefits compared with legacy financial technology—lower costs and faster transaction speeds.[116] Lower transaction costs were an important goal identified by an anonymous founder—or team of founders— known as Satoshi Nakamoto when conceptualizing Bitcoin.[117] As Nakamoto noted, requiring financial institutions to act as trusted third parties in transfers raises the overall costs.[118] In 2015 the global average cost of sending a $200 remittance, for example, was close to 8 percent.[119] Although diminished from the 9.7 percent average in 2009, this cost remains far above the 1 percent average fee, per Goldman Sachs estimates,[120] and even above the 3 percent fees associated with Bitcoin transfer systems popular in East Asia.[121]

VCs allow for improved speed of transactions by adapting the method of recording the value transfers with very low latency periods.[122] Increased transaction speeds unlock ancillary advantages as well. Faster transfers reduce settlement and credit risks involved in waiting for funds to transfer, and they enable parties to use capital more effectively.[123] Greater speed also reduces a user's exposure to exchange rate fluctuations, a source of concern given the volatility of many early-stage VCs.[124] The current concern over the scalability of Bitcoin highlights how important speed is to virtual currencies. As the scale and use of these currencies has increased, the time to validate each transaction has grown as well, leading supporters to search for technical solutions and skeptics to wonder whether the inability to process a growing number of transactions at sufficient speeds will impose a ceiling to the technology.[125]

The potential of VCs to bring about benefits can be seen in the remittance market. Payphil, Sentbe, and similar Bitcoin transfer services have halved remittance costs between South Korea and the Philippines, and they account for 20 percent of the total remittance flows between the two countries.[126] Circle Internet Financial, for example, provides free remittance services using blockchain. Circle is also registered as an MSB, enabling the company to provide many other financial services. The company is licensed in the United Kingdom and has partnered with Barclays Bank.[127] This partnership allows customers to exchange the British pound and U.S. dollar immediately for free.[128] It is worth noting, though, that unlike direct Bitcoin transfers, many Bitcoin remittance services and exchanges are more akin to payment systems,[129] benefiting from the ease of exchange of VCs without the risks of anonymity or pseudonymity.[130]

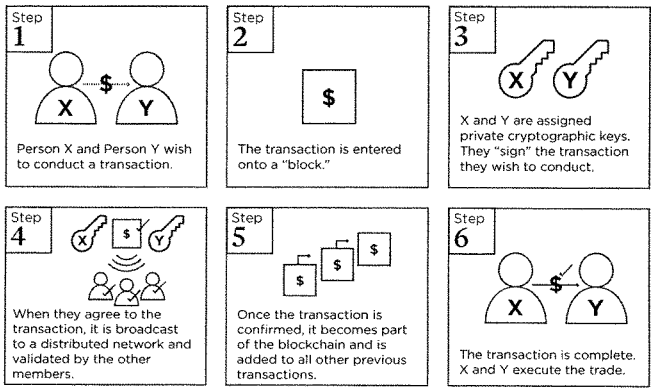
BLOCKCHAIN

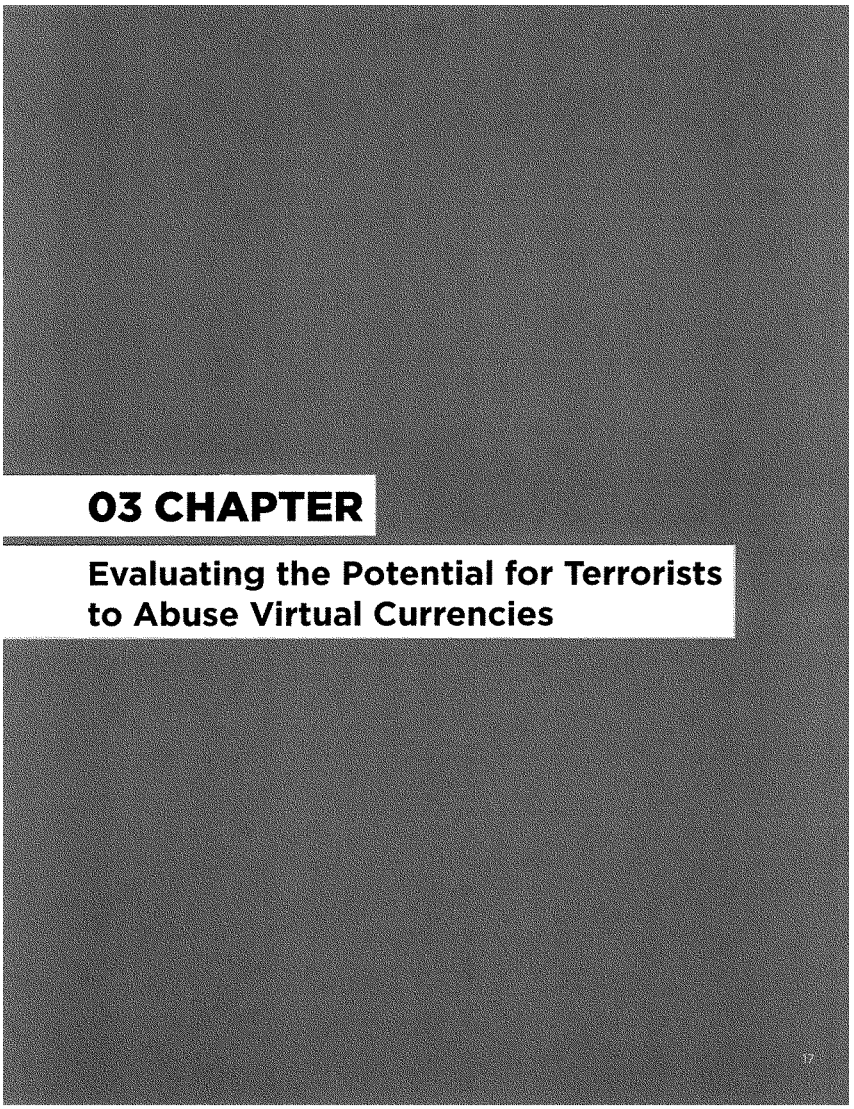
A blockchain is a type of distributed ledger, a copy of which is stored on each instance of a distributed system. Each new entry (known as a block) is certified through the creation of a unique fingerprint that incorporates the previous block, forming a "chain" and cryptographically creating an indelible record of previous transactions.[131] All copies of the blockchain are updated with changes that take place. In the case of Bitcoin, the blockchain is public, records transactions, and enables the cryptocurrency to be decentralized.[132]

The blockchain's appeal as a secure, decentralized database has provoked speculation about its potential for applications across a range of fields. Blockchains can potentially be used to streamline financial transactions;[133] track the origins and legitimacy of precious gems;[134] improve the insurance industry;[135] create secure patient records across healthcare systems;[136] maintain accurate international customs, shipping, and distribution records;[137] secure voting;[138] and help protect property in unstable markets by creating a more stable non-state ownership record network.[139]

But potential obstacles remain to the blockchain's expansion, including because of its indelibility and irreversibility. Human error, hacks, and laws governing consumer rights to data deletion or correction pose challenges for the broad adoption of the blockchain. For example, after fraudulent Bitcoin transactions lost customers tens of millions of dollars in August 2016, the blockchain's irreversibility hindered the amelioration of the breach.[140] And in most of the blockchain's potential applications, the database would only be viewable by a select audience, unlike the public Bitcoin blockchain.

What Is a Blockchain?[141]




03 CHAPTER
Evaluating the Potential for Terrorists to Abuse Virtual Currencies
17

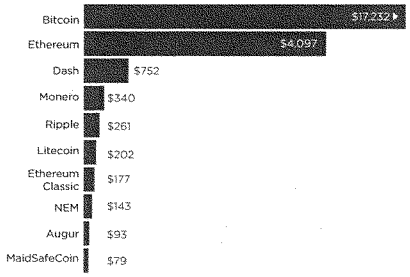
For policy and security leaders focused on countering terrorism, the core question about VCs is when they will reach the kind of scale at which both terrorist groups and their funders can use them with sufficient ease that it becomes a value transfer mechanism of choice. As the previous chapter demonstrates, there is anecdotal evidence that terrorist groups or terrorists working independently have used Bitcoin or have solicited donations in Bitcoin, although there is not yet public evidence that they have begun to do so at scale. Setting aside these more limited instances of terrorists' use of Bitcoin, as a general matter such cryptocurrencies have only really begun to achieve significant scale in a limited fashion, and not yet in the terrorist financing realm. Although scholars and experts are just beginning to rigorously study how and why VCs and payment systems grow and achieve scale and sustainability, policymakers must prioritize these questions to assess potential illicit finance threats prospectively.

To illustrate the importance of scale, Bitcoin, the largest and most widely used cryptocurrency, has an approximate market capitalization of $17 billion as of March 20, 2017.[142] Newer cryptocurrencies are far smaller; Monero's market capitalization for example, is approximately $340 million,[143] and that of ZCash about $22 million (as of early 2017).[144] By contrasting this to the scale of terrorist financing specifically and illicit financing more generally, it is clear that at present, the role that cryptocurrencies can play in illicit activities is structurally limited, especially in comparison with more common means of financing illicit activity. In 2014, in ISIS's most flush period, it brought in $2 billion.[145] The U.S. government estimates that illicit financing generates $300 billion per year,[146] while more than a trillion dollars' worth of illicit financing is raised and moved globally.[147]

Scholars and experts are just beginning to rigorously study how and why VCs and payment systems grow and achieve scale and sustainability.

Studying previous instances in which new payment methods and VCs have scaled, and the ways in which they have been abused by criminal groups, offers a sense of the conditions that may be necessary for VCs to become vulnerable to abuse by terrorists. Such an analysis is useful even though there are fundamental differences between criminal groups and terrorists in the volume of money they move and their ultimate aims. This is because previously new payment technologies such as PayPal were trying to solve the same problems that VCs aim to address today—namely, moving money more quickly and more cheaply in an increasingly globalized environment, often with a commitment to escaping the control of centralized institutions. It also gives a sense of how the characteristics of VCs might change as the currencies grow in users and size, and how those changes may affect their potential for abuse by illicit actors. Thus, notwithstanding the important differences between how criminals have used new payment technologies and VCs in the past and the concerns about terrorist financing today, previous examples are instructive.

Virtual Currencies Market Capitalization ***(in millions)***



"CryptoCurrency Market Capitalizations," CoinMarketCap.com, March 20, 2017, https://coinmarketcap.com/.

How New Payment Technologies Grow and Scale

Three of the key characteristics that determine the scale that virtual currencies can reach are their degree of centralization, their liquidity and convertibility, and the network effects—whereby a service becomes more useful to all users the more people use it.

CENTRALIZATION

As virtual currencies and payment systems expand, it is likely that they will become increasingly de facto centralized, even though they began as a deliberately decentralized system. Experts have observed that online peer production projects (e.g., Wikipedia) likely conform to the so-called iron law of oligarchy, which holds that even organizations set up in a distributed fashion will increasingly converge around a few institutions as they grow.[148] This is in part because as more people begin to use VCs and cryptocurrencies, investments in necessary infrastructure (such as exchanges) will become less expensive as economies of scale take hold. Additionally, users will have more confidence that a transaction will go through, which will reduce volatility and make currencies more consumer-friendly.

Bitcoin, for instance, shows incipient signs of behaving in a manner consistent with the iron law of oligarchy. As scholars have observed, although Bitcoin's founders emphasized its decentralized characteristics, this does not accurately describe how it functions today. Specifically, although the "Bitcoin protocol supports complete decentralization, . . . significant economic forces push towards de facto centralization and concentration" throughout the system.[149] This centralization manifests in several ways. For example, Bitcoin exchanges in well-supervised jurisdictions such as the United States are highly centralized because of regulatory requirements and the technical security requirements necessary to maintain the integrity of a Bitcoin exchange. Moreover, Bitcoin is generated by "mining," in which computers solve mathematically challenging problems (requiring more computing power) to create new bitcoins. These problems become more difficult over time, and miners have brought together their resources into large mining pools, threatening Bitcoin's decentralization.[150]

LIQUIDITY AND CONVERTIBILITY

Liquidity and convertibility are essential components for any currency, including virtual currencies, to become usable by large groups of people. A currency needs to be useful for purchasing a variety of goods or it will be challenging for that system to scale and gain prominence. It also needs to feature easy convertibility to fiat currency. Some liquid, highly convertible, nearly anonymous stores of value do exist and are extremely common. For example, gift cards to Amazon.com approach the liquidity of cash, are easy to obtain—and represent a growing money laundering threat.[151] In March 2016, the U.S. Department of Homeland Security filed a warrant application in which it alleged that 5dimes, an offshore gambling site, used Amazon gift cards to launder almost $2 million. The site offered incentives for gamblers to use Amazon gift cards over other methods of funding their accounts.[152]

For similar reasons, online gift cards are becoming increasingly appealing to terrorists. In January 2017, a Washington transit police officer was arrested for attempting to provide financial support to ISIS by using Google Play gift cards (he gave them to an FBI informant rather than a true supporter of ISIS).[153] Because online gift cards illustrate the kinds of characteristics—liquidity and convertibility—that are needed for a payment mechanism to be used by a large number of people, it is necessary to develop a strategy to avoid their becoming vehicles for illicit finance.

Bitcoin shows incipient signs of behaving in a manner consistent with the iron law of oligarchy.

Case Studies: Abuse of New Financial Technology by Illicit Actors

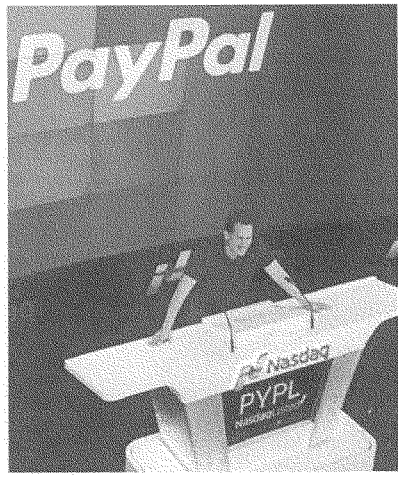
Exploring several case studies demonstrating how criminals and other illicit actors have employed new payment systems illustrates a number of the dynamics outlined above. Criminals may precede terrorists in abuse of VCs as they seek new pathways to avoid the restrictions of the formal financial system. Understanding how this may occur, and some of the methodologies that could be used, will help supervisors and regulators contemplate adequate protections against such abuse. With this information, they can better avoid the use by illicit actors of new financial technologies as they connect a larger network of people, and as the currencies themselves become easier to use.

PAYPAL

This payment technology met an important market need for easier payment methods and improved user interfaces. It achieved scale and broad market penetration while simultaneously protecting against illicit activity. PayPal was officially launched on October 22, 1999.[154] By April 2000, it had 1 million users,[155] and it developed a niche as a credit-card processing service.[156] In August 2002, eBay announced plans to buy PayPal after finding that the service was vastly preferred among eBay customers.[157] This is a prominent example of how network effects can contribute to exponential growth of a business, particularly in the payments space. As more eBay customers used PayPal, it was more advantageous for non-PayPal users to adopt the method, and PayPal was able to push out other competitors. This eventually led to a partnership with an enormous e-commerce merchant. In 2015, eBay spun off PayPal with a second initial public offering.[158] By the end of 2016, its revenue was $10.84 billion, processing 6.1 billion individual transactions, with 197 million active accounts.[159] Its early market strength allowed it to make acquisitions and engage in product development to retain a presence in the now-competitive new payments space.[160]

Importantly for regulatory purposes, PayPal has classified itself as an electronic money transmitter rather than a bank, although it performs bank-like functions, providing accounts, facilitating payments, and even giving loans to customers.[161]At this time, only 20 banks in the country hold more money than PayPal—as of March 2016, it held about $13 billion, just behind TD Bank and Capital One, in accounts that clients could use to buy things online or link to another account, for example a credit card or bank account.[162] Rather than competing with cash the way some virtual currencies do, it instead competes with credit cards, banks, and other payment transfer systems. This distinguishes PayPal from the VCs that are now emerging, which self-consciously seek to circumvent the formal financial system.

PayPal's early market strength allowed it to make acquisitions and engage in product development to retain a presence in the now-competitive new payments space.



PayPal's focus on fighting fraud was fundamental to its success because it allowed the service to distinguish itself from peers. As a major player in the payment space, PayPal's continued focus on fighting fraud must keep pace with evolving tactics used by terrorists. (Guruofsales/Flickr)

Because PayPal allowed (and continues to allow) chargebacks,[163] fraud had the potential to derail the business from the outset.[164] As a result, its founders deliberately focused on how to manage the fraud and crime risk attendant to an online, international payment system.[165] In the summer of 2000, when systematic fraud attacks from organized crime and cybercriminals hit PayPal, company executives realized they needed to tackle fraud head-on or risk significant harm.[166]

Immediately the company invested significant resources in detecting and preventing fraud. Among the most important tools they developed was a machine learning system named Igor, which used advanced analytical techniques to evaluate and understand patterns of fraud across the company. Igor would later become the basis for a new company, Palantir Technologies, spun off by one of PayPal's founders.[167]

Thus PayPal's fraud problem, instead of spelling doom for the company or becoming an inflection point into an illicit finance service, allowed it to distinguish itself from its competitors in a way that became a permanent

advantage. An early commentator noted that "the backbone of PayPal's success is its fraud squad."[168] This led to a cascade of business advantages, including charging customers a low transaction fee relative to credit card companies, which was only possible because of the aggressive and successful fraud detection and mitigation system.[169]

PayPal had other innovations that gave it its foothold in the digital payment market. It debuted novel Know Your Customer (KYC) techniques; for example, when a user requested that PayPal have direct access to an account to deposit or withdraw money, the company would make two small test deposits (a few or several cents each). The user would then have to confirm the exact amounts of the deposits with PayPal.[170] The company is also based around email; each account is limited to one email, and recipients are known by their email rather than name, physical location, or bank account information.[171] This was much easier than asking users to download software or employ complicated security systems, as competitors were doing at the time. PayPal solved both a convenience and a security challenge through this method. Payments themselves were not sent over email; only notifications of payments were transmitted over the Internet, while the money flowed between PayPal servers disconnected from the Internet.[172]

PayPal's fraud problem allowed it to distinguish itself from its competitors in a way that became a permanent advantage.

Instead of seeing counter-illicit finance protections as a burden and an obstacle to effective commerce, PayPal saw them as indispensable to the viability of its business. Yet although PayPal is generally a success story of corporate growth and sustainability without compromising integrity or ability to innovate, no system is perfect. In 2009, PayPal admitted to violating aspects of Australia's AML-CTF law and made an arrangement with the government to address its policies and avoid further issues.[173] More recently, in March 2015, PayPal agreed to pay the U.S. Treasury $7.7 million for violating sanctions by transacting with Cuba, Sudan, Iran, and Turkish nationals blacklisted for proliferation of weapons of mass destruction.[174] At the time of the settlement, the U.S. government explained that PayPal had failed to "implement . . . effective compliance procedures and processes to identify, interdict, and prevent transactions" that violated sanctions, "despite processing a high volume of transactions and maintaining an international presence."[175] In response, PayPal settled with the government and adapted its compliance system.[176]

Even after PayPal instituted procedures designed to ensure adherence to sanctions and anti-fraud measures, in December 2015, the cybersecurity journalist Brian Krebs detailed an incident in which his account information was involuntarily reset by hackers, and money from his account was transferred to terrorist-linked groups.[177] So while PayPal's early success in scaling could largely be attributed to its innovative anti-fraud tactics, now that it is a giant in the payment space, it needs to continue evolving as cybercriminals and terrorists become ever-more technologically advanced. Key for the purposes of evaluating the vulnerability of this technology to terrorist financing is that PayPal initially viewed investment in sophisticated anti-fraud techiques as the foundation of its business success.

E-GOLD

In contrast to PayPal's successful evolution, e-gold, a virtual currency and bespoke money movement system, failed as a business enterprise because it did not do enough to keep out illicit activity. Continued investigations by law enforcement ultimately made it non-viable. E-gold was created in 1996 as a monetary system based around a VC backed up by gold, independent from any government.[178] The founder of e-gold sought to create a "private, international currency," isolated from the market swings of ordinary currencies and instead linked to gold.[179] Other VCs that started around the same time failed, mainly because of customers' reluctance to pay fees to convert fiat currency into virtual currency.[180] But by 1999, commentators deemed e-gold "the only electronic currency that has achieved critical mass."[181] In 2001, an article argued that the "ideal e-currency might even be backed by gold," and praised e-gold's transparency to customers.[182] A 2002 profile in *Wired* lauded it for "quietly thriving" while other VCs and similar systems failed, describing its mission as "not simply better money but the best."[183]

To use e-gold, one had to open an account online; convert a fiat currency into e-gold by using an e-gold exchanger who facilitated getting money into and out of the system; use e-gold to transfer funds or purchase or sell a good or a service; and then exchange e-gold back into fiat currency through the same system of exchangers.[184] These elements of the system—its intentional self-containment, limited connections to the formal financial system, and creation of a novel way to

store and transfer value—would reappear in later financial networks. For example, Liberty Reserve and Silk Road were systematically abused by criminals.

E-gold differentiated itself from its competitors in a few ways, all of which contributed to its ability to scale. First, it was the first virtual currency to be backed by gold,[185] which gave customers a confidence that most VCs could not and appealed to customers who had concerns about the formal banking system.[186] This innovation was so appealing that it spurred the development of several similar currencies.[187] Such a use of gold meant the service was grounded in a formal, inherently trusted institution. Second, it was extremely cheap, at a cost of 1 percent per transaction up to $5 and 50 cents for every transaction after that.[188] Third, it intentionally did not have any identification verification procedures, purporting to protect the privacy of customers.[189] It differentiated itself from PayPal by having no consumer verification procedures.[190] Fourth, it also distinguished itself from PayPal by being irreversible: once transactions were made, there were no chargebacks.[191] A libertarian philosophy supported both its use of gold as backing and its refusal to request identification from its users.[192] Its founder, Douglas Jackson, argued that e-gold was not subject to regulation as a payment system distinct from a money transmitter and a bank, though it had qualities of both.[193]

E-gold's anonymity, ease of use, and inexpensiveness made it appealing to illicit actors.

E-gold became quite successful—in its prime, it had more than 8 million accounts open and $85 million in cash assets.[194] But a few years after it began to build a following, the criminal activity taking place on e-gold drew scrutiny. Experts noted the similarities of systems such as e-gold to hawala services, and argued that it was only a matter of time before terrorists started using e-gold to finance their activities. They pointed to one case where the U.S. and Russian governments requested information about a potential terrorist using the system; the user had threatened an attack if a ransom was not paid into his or her e-gold account.[195] In December 2005—after a year in which transactions worth $1.5 billion were conducted through e-gold, generating $2 million in revenue—the FBI and Secret Service raided the offices of e-gold's parent company.[196] A year later, in 2006, Douglas Jackson made a public show of helping law enforcement find violations in his service, searching user records and transaction history, compromising his libertarian beliefs in an effort to save himself and his company.[197]

Although Jackson worked with the government, providing information that led to arrests, and was working on making e-gold a "clean" service, such efforts were too little too late.[198] In April 2007, e-gold was charged by the U.S. Department of Justice and U.S. Attorney for the District of Columbia with violating money transmission laws and knowingly providing fund transfers to criminals.[199] The indictment identified concerns about VCs continuing to be used by criminals and becoming appealing to terrorists as well.[200] Prosecutors asserted that more than 70 percent of the 65 most valuable e-gold accounts were associated with criminal activity.[201] As a result, the assets of e-gold were seized, including what the defendants claimed were all of their assets in related bank accounts.[202] At the time, though, government officials admitted that e-gold fell into a regulatory blind spot where it was not required to self-report suspicious activity.[203] The three defendants were spared jail time after pleading guilty to money laundering and running an unlicensed money transmitting business. Although the company initially attempted to reform its customer verification processes and register appropriately with regulators, the service did not survive these legal proceedings.[204]

Considering the lessons from e-gold's growth and demise for the development of future systems that might finance terrorism, e-gold's anonymity, ease of use, and inexpensiveness were the attributes that made it appealing to illicit actors. In particular, e-gold's commitment to anonymity was correctly perceived as a clear advantage for criminal and terrorist financiers. Other aspects, including its backing by gold, would be less necessary and more incidental for terrorist groups seeking to finance their operations. Finally, its operations in the United States gave U.S. law enforcement the reach and power needed to deal a serious blow to the business. Terrorists seeking to avoid exposure to U.S. law enforcement may have learned from this example, among others, to avoid financial avenues and technology in U.S. jurisdiction.

LIBERTY RESERVE

Liberty Reserve, created in 2006, promptly and deliberately filled the gap that e-gold left in the illicit finance space; two of its founders had run a company that was an exchanger for e-gold.[205] It served as a bank, money transmitter, and virtual currency to the criminal underground until it was shut down in 2013.[206] To put money into a Liberty Reserve account, any money transfer service, including postal money orders, credit cards, and bank wires, could be used to convert funds into one of

Liberty Reserve's two currencies, which were pegged to the euro and dollar, respectively.[207] An LR, as the unit of currency was called, could be sent to anyone else with a Liberty Reserve account, who could then withdraw it in exchange for fiat currency.[208]

Liberty Reserve emphasized anonymity, which was a large part of why it grew. Although it nominally required a name, address, and birthday, investigators were able to create accounts with obviously fake information.[209] As investigators noted, Liberty Reserve did not validate the information, and the same user could open multiple accounts; a valid email address was the only technical requirement to establish a Liberty Reserve account.[210] Its structure facilitated money laundering in a fashion similar to the e-gold system, and it drew on many of the same techniques. To deposit or withdraw currency into or from an account on the site, one had to pass the money through exchangers, who bought LRs in large quantities and charged a transaction fee. This way, an account on Liberty Reserve would have no identifying information about its customer.[211] For an additional small fee (75 cents per transaction), Liberty Reserve hid users' account numbers when they sent money to others, thereby making their transactions untraceable.[212] In addition, the company offered a private messaging system that it advertised as "much more private and secure than email or instant messenger."[213] Finally, although it was slightly more expensive than e-gold, it still had a nominal transaction fee. The company charged a 1 percent commission on every transaction within its system up to $2.99,[214] though there were additional fees to convert currency in and out of the system. These fees could become substantial for larger transaction amounts.[215]

Liberty Reserve, like e-gold, became a hugely important part of the VC ecosystem during its seven-year lifespan, because it made communications and transactions with criminals easy and inexpensive. From 2009 to 2013, it processed $300 million per month in transactions and about 78 million separate financial transactions.[216] When it was shut down in 2013, it had 5.1 million users, 600,000 of whom claimed to be based in the United States.[217] The website's founder, Arthur Budovsky, maintained that he originally created it for people without bank accounts to buy and sell goods on the Internet, playing an equivalent role to PayPal for people without bank accounts.[218] Indeed, there is reason to believe that not all of the transactions conducted on Liberty Reserve were illegal.[219] But at its heart, Liberty Reserve was driven by criminal activity; the 500 biggest accounts on its service created 44 percent of its business, and of those, 32 belonged to credit card thieves and 117 to Ponzi scheme operators.[220]

This criminal activity drew law enforcement to Liberty Reserve. In 2010, the U.S. Secret Service began investigating the company; by 2011, the Global Illicit Financial Team took over the investigation.[221] Although Liberty Reserve's main operation in Costa Rica was shut down between November 2011 and May 2013, the company continued to run through Budovsky's other businesses.[222] Finally, in May 2013, Liberty Reserve was permanently shut down as the United States brought charges against several key persons in the operation. Budovsky was sentenced to 20 years in prison and was extradited from Spain to serve his sentence; his co-founder, Vladimir Kats, was sentenced to 10 years.[223]

After Liberty Reserve was taken down, much of its customer base went to a centralized virtual currency platform called WebMoney.[224] Europol's 2016 "Internet Organised Crime Threat Assessment" cited WebMoney as a common centralized service for criminals, especially for payments between criminals, although its popularity has decreased compared to currencies like Bitcoin.[225] WebMoney does not allow U.S. citizens to open accounts, thus attempting to seal itself off from U.S. jurisdiction.[226]

Liberty Reserve demonstrated that a niche market exists for a trusted illicit finance network on the dark web.

The example of Liberty Reserve is relevant to the threat of terrorist financing in a few ways. Like e-gold, this system innovated through using exchangers, creating another layer of anonymity and obfuscation between the system and potential criminals, in addition to offering further privacy-enhancing services for a fee. Arguably, any system used by terrorists in the future would entail this as well as potentially additional anonymity innovations. Liberty Reserve also demonstrated that a niche market exists for a trusted illicit finance network on the dark web. Finally, like e-gold, Liberty Reserve was shut down by the U.S. government, a lesson from which future systems for terrorist financing might learn by developing systems with limited or protected access to the U.S. financial system.

BITCOIN

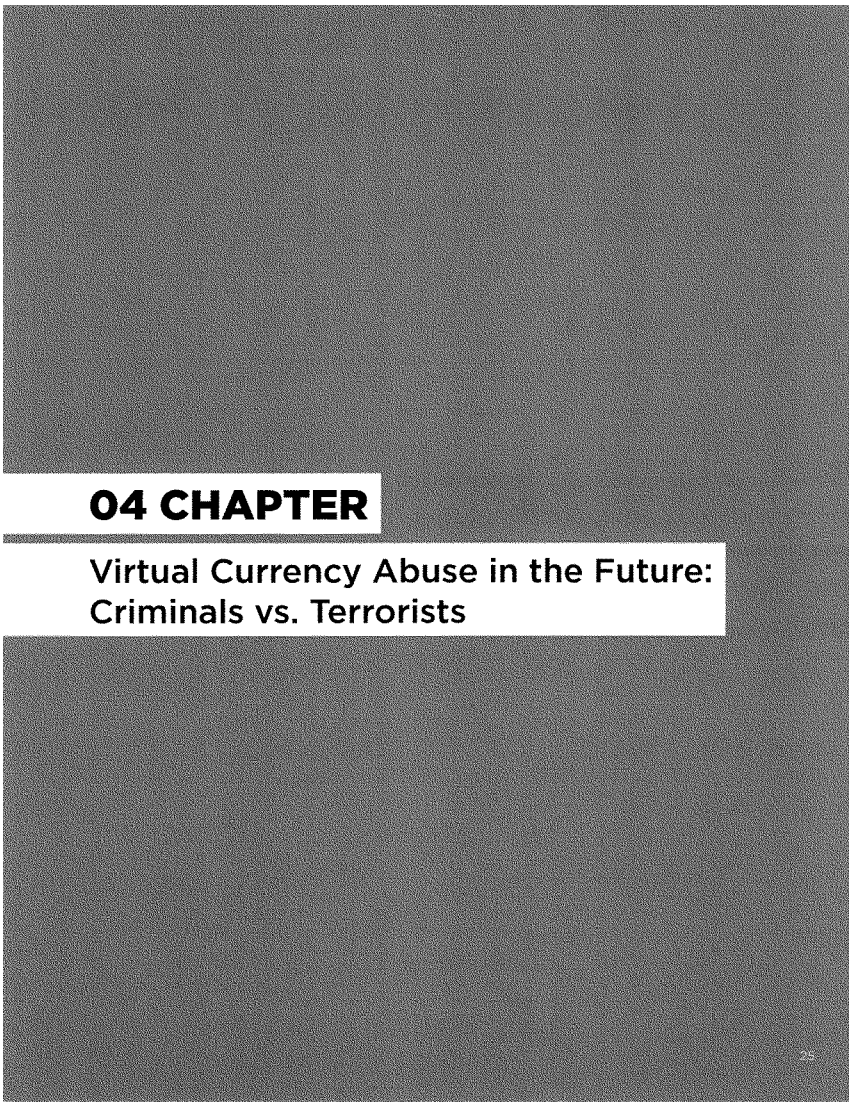
Bitcoin's characteristics—including its irreversibility, use of the blockchain, pseudonymity, and decentralization—make it "more flexible, more private, and less amenable to regulatory oversight," as experts have explained.[227] As has been noted, although no more than anecdotal evidence exists indicating that Bitcoin is being directly used to finance terrorism, it has proven to be a useful tool for illicit financial activity more broadly. Early users bought narcotics on Silk Road, an illegal online marketplace, and gambled.[228] These types of crimes are increasing in sophistication and complexity. More recently, in January 2016, 10 people were arrested in the Netherlands on charges related to money laundering through Bitcoin.[229] According to Europol, Bitcoin is becoming more prominent in investigations of payments between criminals, and was estimated to be responsible for more than 40 percent of these payments in the European Union in 2015.[230]

A major obstacle to Bitcoin scaling as a tool for terrorism finance is the blockchain, the publicly accessible ledger that records all transactions that take place through Bitcoin. Thus while Bitcoin wallets are not necessarily linked to real identities (though exchanges in well-regulated jurisdictions do establish these links), it will always be possible to unravel a chain of transactions. Experts including Aaron Brantly have explained that cryptocurrencies are part of the arms race of cryptography: "As one person develops a cryptographic algorithm allowing transactions to be more anonymous, another person immediately begins work on solving it to peel back the anonymity."[231] Once the sequence of transaction is revealed, Bitcoin addresses can be linked to real-life identities through forensic techniques, after which one's entire transaction history becomes visible.

Bitcoin is often used in ransomware attacks, a threatening development that connects cybercrime to financial crime.

Even so, cybercriminals and narcotics traffickers have made and continue to make extensive use of cryptocurrencies such as Bitcoin. Bitcoin is often used in ransomware attacks, a threatening development that connects cybercrime to financial crime. Online criminals conducting ransomware attacks deploy malware to encrypt data and demand a ransom before providing the decryption key. In February 2016, for example, a hacker seized control of Hollywood Presbyterian Medical Center's computer systems, and the hospital had to pay a $17,000 ransom in bitcoins to regain control.[232] Recently, ransomware attacks have spiked in frequency and significance. In April 2016, the FBI told CNN that in the first three months of 2016 alone, ransomware reaped $209 million from affected consumers.[233] From January to September 2016, the rate of ransomware attacks on businesses increased from one every two minutes to one every 40 seconds, with 62 new variants emerging.[234] Experts have also observed that there has been a 3,500 percent increase in criminals' use of the net infrastructure that supports ransomware.[235] Similarly, Symantec estimates that global losses to ransomware are in the hundreds of millions of dollars.[236] Ransomware attackers, mostly from Eastern Europe and China, target businesses and local governments; as a result, companies are stockpiling bitcoins in the event that they should be hit.[237] Hospitals are a particular target for ransomware, because in order to function, they have an absolute and immediate need for their data, including patient records and drug histories.[238]

Ransomware is so closely linked to Bitcoin because of the anonymity required to launch successful ransomware attacks, which Bitcoin readily provides.[239] Suggestions for ways to impede Bitcoin's irreversibility, immediacy, or decentralization have been dismissed because of how it could compromise the essential nature of the virtual currency.[240] Thus far, because Bitcoin has been adopted by this brand of criminal, there is reason to believe terrorists may take advantage of it more fully as well, as examples discussed in Chapter 2 evince. But without securing anonymity and increasing technological sophistication, systematic use of Bitcoin by terrorists remains unlikely.



04 CHAPTER

Virtual Currency Abuse in the Future: Criminals vs. Terrorists

Policymakers studying whether and how virtual currency may become a central pathway for terrorist financing must continuously examine two main characteristics of evolving virtual currency. First, as discussed in the previous chapter, they must examine how financial technologies with the same goals as virtual currencies have successfully prevented illicit financial activity generally and terrorist financing specifically. Second, they must understand the reasons for which criminal groups today are attracted to virtual currencies to determine whether terrorists, by contrast to other criminals, may seek to use them in the same way in the future.

Several of the reasons for which terrorists have not turned to virtual currencies at scale, while criminals have done so, are described in this section. Because Bitcoin is not completely anonymous, potential terrorist financiers, particularly those operating in the United States and Europe, may be reluctant to use this most liquid, convertible cryptocurrency. But as new cryptocurrencies become more anonymous, and if terrorist groups develop more of the characteristics of criminal enterprises, such as broader person-to-person networks of trust, technical sophistication, and the need for a wider funding base, virtual currencies might become more attractive.

In examining the use of virtual currencies, the U.S. government has assessed that criminal groups will adopt them when doing so offers certain perceived advantages. The U.S. Secret Service, which has jurisdiction over significant financial crimes, has identified five advantages in particular that have motivated criminal groups to adopt virtual currencies. Specifically, they are:

1. The greatest degree of anonymity for both users and transactions.
2. The ability to quickly and confidently move illicit proceeds from one country to another.
3. Low volatility, which results in lower exchange risk, increasing the virtual currency's ability to be an efficient means to transmit and store wealth.
4. Widespread adoption in the criminal underground.
5. Trustworthiness.[241]

Conscious of these advantages, criminal groups have embraced virtual currencies in self-contained online marketplaces like AlphaBay, and ecosystems like Liberty Reserve, described above, and Silk Road.[242]

In these circumstances virtual currencies are used in a number of ways, and because of their broad utility—in particular their convertibility—criminals are incentivized to adopt them at scale. This is perhaps the most important point of distinction between terrorist groups and criminals—terrorists mostly need fiat currency to fulfill the funding requirements described above, and so there is no reason to introduce the complications involved in using virtual currencies if they would rapidly need to be reconverted back to fiat currency. One common way, for example, that criminal groups use virtual currencies is to purchase and sell technical tools required to conduct cyberattacks—such as exploits designed to take advantage of particular software vulnerabilities.[243] Another common way virtual currencies are used is to purchase stolen data, monetized on the dark web.[244] Ransomware is another example of how these currencies enable cybercrime. Such uses of Bitcoin and other cryptocurrencies are consistent with the criteria identified above. Most important, they facilitate anonymous transactions or make available, for a fee, extra steps to ensure anonymity. Enterprises such as Liberty Reserve and Silk Road also operated on a global basis. And the fact that they were relatively self-contained ecosystems (albeit criminal ones) meant there was some level of trust among the participants in the marketplace.

Terrorists mostly need fiat currency to fulfill their funding requirements, so there is no reason to introduce the complications involved in using virtual currencies.

Liberty Reserve, Silk Road, and similar entities achieved scale because they filled a particular niche in the criminal ecosystem: they enabled criminals to buy and sell services *from one another* in a self-contained network. Until they were infiltrated and taken down, two of the most successful adoptions of virtual currencies facilitated global transactions among criminal groups that were able to scale because marketplaces facilitated trusted interactions. Because the groups that took advantage of virtual currencies were already engaged in sophisticated cybercrime, one of the biggest obstacles to adoption—broad comfort with sophisticated technology—had already been surmounted.

In contrast to criminal groups, terrorists have not yet adopted virtual currencies at scale.[245] One basic problem is limited adoption of the technical systems and sophistication needed for a virtual currency ecosystem to

Terrorists have been slow to adopt virtual currencies in part because of a lack of the needed technological and telecommunications infrastructure—including basic internet service—in the areas where they operate. (avlxyz/Flickr)

flourish. As noted, terrorist groups such as Boko Haram, AQIM, AQAP, ISIS, and others often operate in inhospitable environments where telecommunications networks and other Internet services are not reliable, and where broad adoption of technology is limited.[246] If the areas in which these groups operate lack the basic technical and telecommunications infrastructure for their ecosystems to support the use of Bitcoin, then there is no reason for terrorist groups to accept value from outside donors in that form. After all, if the group cannot easily exchange Bitcoin for large quantities of hard currency or cannot use it easily to purchase weapons, other materiel, food, and housing in the areas where they operate, it does not do them much good.

This dynamic stands in stark contrast with that of criminal groups which, at present, make the most extensive use of virtual currencies. These tend to be either cybercriminal groups or others, for example narcotraffickers engaged in large (often cross-border) enterprises that invest in technically sophisticated tools. Since the people with whom cybercriminals and narcotraffickers exchange goods and services also use Bitcoin, the barriers to adoption for their use are low. Terrorist groups, therefore, face significant challenges of technological adoption in comparison with these criminal networks.

But there are also significant differences in the types of trust that characterize the networks of organized criminal groups using cryptocurrencies and the terrorist ecosystems that might have a desire to use them. The significant factor that unites members of ecosystems like Liberty Reserve, Silk Road, and other online marketplaces where tools of cybercrime are bought and sold is their common engagement in criminal activity. This generates a form of trust in the system, derived from a shared interest in preserving the illicit marketplace. Even though participants in these marketplaces may not personally know each other, they use cryptocurrencies to transfer value because they trust that, as repeat players with a shared interest in not getting caught, everyone will play by the same basic rules. As Lillian Ablon, Martin Libicki, and Andrea Golay explain, "The harder-to-access tiers [of dark web markets] where participants are highly vetted . . . are often well structured and policed, with their own constitution-like rules and guidelines to follow."[247] Reputation is paramount—"The black market has several tiers of access, with the higher tiers requiring lots of vetting before they can be entered, or even revealed."[248] Publicly accessible, low-tier channels have more fraudulent goods than the upper echelons, which are, in turn, continually getting more difficult to access without establishing mutual confidence with other criminals, including by "reputation, personal relationships, middlemen, or intermediaries," or, for example, by giving samples of goods (including stolen data or cyber exploits).[249]

Fundamentally, by contrast, terrorist financing for groups such as Hamas, Hezbollah, and al Qaeda has entailed the movement of funds from an external source to the areas where the terrorist groups operate. The role of trust is therefore very different, because terrorist financing networks operate over extended geographies with the involvement of many parties. This means there might be several steps between the sender of the funds and the ultimate recipients, attenuating the trust needed for cryptocurrency networks to scale. Al Qaeda received funds from Gulf-based donors;[250] Hamas received support from charities and state sponsors including Iran;[251] and Hezbollah received funds from Iran,[252] but also from complicated global money laundering schemes.[253] At some point in the transaction chain, the ultimate recipients of funds must know and trust the

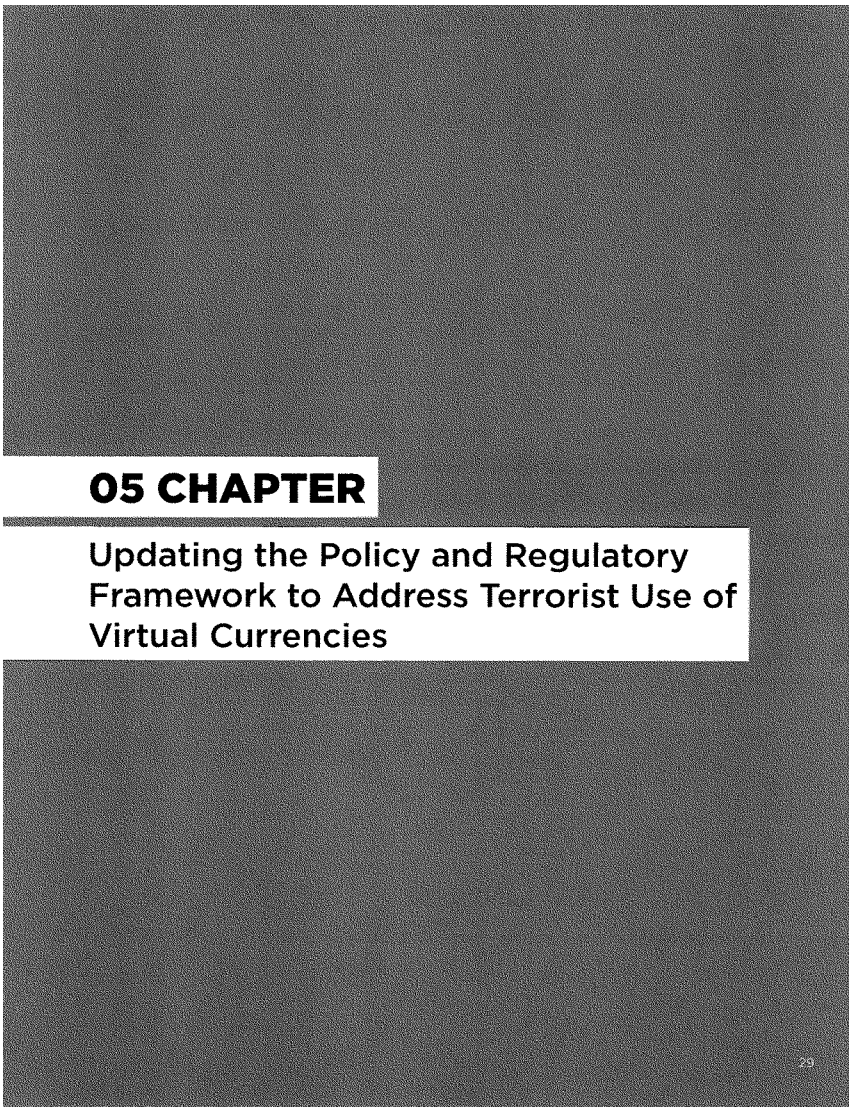
Common engagement in criminal activity generates a form of trust in the system, derived from a shared interest in preserving the illicit marketplace.

facilitators who bundle money for transmission to terrorist groups,[254] but the initial donors might not even be witting (for example in the case of redirected charitable gifts), and often do not know the identities of the recipients. For now, because of the incomplete anonymity of many cryptocurrencies, coupled with the fact that terrorist groups are often interacting with people outside their community, it is difficult to achieve the kind of trust necessary for cryptocurrency networks to scale in the terrorism context.

Perhaps the most important reason for which terrorist groups have not adopted virtual currencies at scale is that they have not needed to do so. Other means of transferring value—cash, prepaid cards, or unlicensed money transmitters and hawalas—have served their needs reliably.[255] And those methods of transferring value can achieve scale in a way that Bitcoin cannot, at present. In 2009 alone, there were 6 billion prepaid card transactions with an aggregate value of more than $140 billion.[256] Prepaid cards are regulated in the United States and in the EU,[257] but criminals are finding enterprising ways to circumvent those rules and use repositories such as gift cards to launder funds.[258] As those other forms of transferring value come under regulatory and law enforcement pressure, terrorist groups may try to diversify their mechanisms of moving money.

Other means of transferring value—cash, prepaid cards, or unlicensed money transmitters and hawalas—have served the needs of terrorist groups reliably.

In this chapter, the discussion of illicit use of virtual currencies indicates that terrorist use of the financial technology is not an imminent or systemic threat. But this could change. Given the gravity of the terrorism threat to U.S. national interests more broadly, staying ahead of evolving trends in terrorist financing is a worthy goal. Therefore, the project for financial policy officials and regulators is insulating the system from terrorist abuse and adapting an approach to regulatory oversight that keeps it closely focused on innovation, adaptation, and contemporary vulnerabilities.


05 CHAPTER
Updating the Policy and Regulatory Framework to Address Terrorist Use of Virtual Currencies
29

The risk that terrorists will increasingly use virtual currencies to move and store money in the future indicates a need to consider whether our current financial regulatory architecture is up to the task of preventing this eventuality. Observers and policymakers have highlighted a need for vigilance to prevent this from occurring, which in practice translates into adaptations to financial regulation and compliance. Additionally, it means a policy posture on financial technology oversight that is designed to both protect the benefits that can be afforded by virtual currencies and prevent their abuse.

In the United States, the core policy framework for monitoring and halting criminal financial activity and bulk cash movement, including for terrorist financing, is the Bank Secrecy Act (BSA), first adopted in 1970 and amended several times thereafter. The BSA reflected the fundamental insight that law enforcement needed an established mechanism to obtain information from banks about the illicit funds transfers that underlie criminal activity. It focuses on banks and MSBs as the core regulatory targets, because these institutions are the gateways through which all money, including the proceeds of crime and terrorist financing, pass. Trying to track illicit dollars in any currency occurs most effectively at these nodes in the financial system. Additional authorities enacted in the USA Patriot Act offer policymakers more legal mechanisms to compel financial information from banks about illicit activity, and they require financial institutions to stay away from the jurisdictions, institutions, and types of activity that criminals and money launderers use to avoid detection.

These statutes require financial institutions, the gateways, to be the first line of defense against illicit activity moving around the financial system. They are charged with blocking the movement of dirty money that transits their systems and keeping out bad actors, and with adopting broader risk management approaches that will make it harder for abuse to take place in the first place.

Fundamental Challenges to Countering Terrorist Financing in the Era of Virtual Currencies

A few basic challenges in the current policy and regulatory framework impede law enforcement and intelligence officials, as well as the private sector, from collaborating more nimbly to weed out illicit actors. The first general challenge is that, in a dynamic technology environment with a large number of new entrants, companies are sometimes unaware of the regulatory requirements to which they are subject, and they are often unable to afford sophisticated legal counsel to help them navigate the compliance process. Thus, even when some financial technology startup companies that deal with virtual currencies do realize that they are, in fact, MSBs for purposes of financial regulation, they may lack the institutional resources to build the requisite compliance systems and sustain viable businesses. One particular challenge in this area is the requirement for a virtual currency firm to obtain licenses in all states in which it operates and maintain compliance consistent with both federal and applicable state standards where they are licensed to operate. With only a single federal registration for virtual currency firms, compliance costs would be more manageable for smaller firms, and regulators would be better able to oversee firms. In the case of Ripple Labs Inc., the company was assessed a $700,000 penalty by FinCEN for willfully violating requirements of the BSA by failing to implement an anti–money laundering program.[259] Ripple acted as an MSB and sold virtual currencies without registering with FinCEN, and failed to implement and maintain an adequate AML program to guard against use of its products by terrorist financiers.[260]

Financial regulatory officials have not devoted the same or, arguably, adequate resources to regulating and examining non-bank financial institutions, by comparison with banks.

Financial regulatory officials have not devoted the same or, arguably, adequate resources to regulating and examining non-bank financial institutions, by comparison with banks.[261] This has been the case even while non-bank institutions present a demonstrated illicit-finance risk. This problem, along with the ignorance of many virtual currency firms about their exposure to financial regulation, likely will diminish over time, as the broader financial technology industry, specifically including exchanges dealing with virtual currencies, matures. This will occur as firms undergo more audits and gain greater familiarity with financial regulators and regulatory frameworks, and as financial regulators simultaneously learn more about the functioning of virtual currencies. Such activities will ideally include, for example, collaboratively exploring some of the enhanced customer verification and due diligence practices that may be available to virtual currencies.[262]

The second and related challenge is that regulators in different jurisdictions (and even in the same jurisdiction) are taking a variety of approaches to the oversight of new payment technologies and virtual currencies. For example, some of the regulators in some jurisdictions have moved faster than others to clarify that certain financial payment technologies, such as virtual currency exchanges, are a new kind of MSB, subject to exams, and must have AML programs. In 2013, FinCEN issued guidance indicating that Bitcoin exchanges were MSBs and subject to regulation as such.[263] Other regulators in other jurisdictions have not offered similar guidance—or have gone so as far as imposing limits on the use of virtual currencies.[264] This uneven outreach to virtual currency companies has sometimes resulted in conflicting regulatory approaches.[265] Even when regulators clarify that certain new payment technologies are "covered entities" subject to regulation, the ability of banking regulators to supervise and of law enforcement officials to take action is nascent.

Finally, the regulation of virtual currencies is highly dynamic, shifting both within and across jurisdictions at a rapid pace. This makes achieving a stable compliance architecture exceedingly difficult.

The Culture of Compliance and Virtual Currencies

In addition to the regulatory challenges in countering terrorist financing that may occur via virtual currency, as discussed above, a further impediment is linked particularly to the culture of compliance. The current rules-based bank supervisory structure entails a fundamental tension between regulatory and compliance approaches to illicit financial activity. Specifically, supervision focuses strictly on the failure of banks to prevent illicit activity, rather than being more oriented toward detecting and monitoring it. The latter approach is often favored by law enforcement officials.

The current structure and requirements for U.S. supervision of major banks in its jurisdiction (which in practice includes the preponderance of all global banks) places overwhelming emphasis on prevention rather than detection. While it is indeed important for financial institutions not to facilitate illicit financial activity, the work of shutting it out has become an elaborate, expensive compliance exercise.[266] This has involved an emphasis on shedding, rather than managing, risky clients. The result has been that risky activity is often pushed to less well-regulated institutions.[267] Compliance activity has become relatively rote, if expensive, and the fact that banks get no "credit" with regulators for adopting innovative approaches to detecting illicit activity does not incentivize the development of novel strategies to track the evolving terrorist financing threat. But the problem may actually be even more significant. When banks do create novel strategies to counter terrorist financing, they are expected by their examiners to maintain both the novel and the conventional strategies, thereby creating a disincentive for banks to innovate and bear the financial burden of parallel counterterrorist financing programs.[268]

It is easier, less expensive, and less problematic for banks to completely avoid any risk and limit scrutiny for terrorist financing to basic compliance with the rules, while avoiding risky clients.

Moreover, the recent record of expensive civil and criminal penalties for sanctions and AML violations has raised the stakes for banks, making them more willing to refrain from engaging entire geographic areas or lines of business because of perceptions of excessive risk.[269] Banking officials report that when they have disclosed evidence of terrorist financing found at their banks, they have been criticized or penalized by federal supervisors for failing to report similar transactions previously, subsequently, or with regularity.[270] Additionally, they say that, perversely, the compliance incentives in this environment do not encourage them to try to detect terrorist financing or other criminal activity. It is simply technically easier, less expensive, and less problematic for their relationship with bank supervisors to completely avoid any risk and limit their scrutiny for terrorist financing to basic compliance with the rules, while avoiding risky clients.

By extension, this also discourages banks from taking on new payment technology firms, or virtual currency platforms, given the risks of assimilating such new and unknown customers. Banks therefore do not have as much insight as they could into illicit financial flows in virtual currencies. Thus it is harder for law enforcement and intelligence officials to track and halt such activity. A more holistic and effective approach to countering terrorist financing would encourage and incentivize banks to take on new payment technologies and virtual currency firms while managing the potential risks of abuse.

From a public policy standpoint, it is concerning that banks do not appear to be incentivized to be as proactive as possible in detecting terrorist financing and adopting innovative strategies for information sharing and coordination with law enforcement and intelligence officials. They should be working in coordination with both to sustain and manage certain risky clients. In the present environment of extensive social media connectivity and ease of moving funds electronically, including through relatively anonymous platforms or currencies, there are growing new aspects to terrorist threats. Moreover, the growing trends of Internet-based radicalization, lone wolf terrorist plotters, and anonymous virtual currencies make it significantly more important that there be much more active multi-sectoral collaboration to identify and halt terrorist activities. In order to arrest such activities, virtual currency exchanges, along with banks, technology providers, merchants, and national security and law enforcement officials, must have powerful incentives and easier pathways to collect and share terrorist threat information.

Regulatory Treatment of Virtual Currencies

It may be tempting to assume that new financial regulation is needed to address these various challenges, particularly given how novel virtual currencies are compared with conventional fiat currency and banks. However, this should not necessarily be the operating assumption of stakeholders. An appropriate approach to regulating virtual currencies should include an emphasis on understanding the applicability of the existing financial regulatory architecture to payment systems that service virtual currencies. While conducting this analysis, policymakers should appropriately balance the burden of compliance for virtual currencies with the need to support the innovative value of new, efficient financial technology. Policymakers may, in this framework, consider only moderate adaptations. This should be the case notwithstanding the fact that new financial technology may, in fact, present an enhanced risk of abuse by terrorists and other financial criminals.[271]

The need for new regulation is also diminished because many financial industry watchers believe that traditional, highly regulated global banks will remain the pillars of the global financial system for the foreseeable future, given the essential security, liquidity, longevity, efficiency, and creditworthiness that they provide. The vast majority of commercial and retail financial activity is legitimate.[272] Those conducting this activity seek reliability and stability, as do those who conduct some illicit financial activity. Both types of actors generally only select new financial technologies that guarantee payment and provide an assured counterparty, credit, and credibility. This may in practice limit their exposure to virtual currencies. But to the extent that banks offer services to virtual currencies, financial regulators generally will continue the practice of applying traditional financial regulatory categorizations and requirements to new payment systems. By extension, this means that banks will pioneer and model customer due diligence and anti–money laundering programs for new financial technology and virtual currencies. There are likely many creative new opportunities to synthesize large amounts of financial and other data to identify the financing of terrorism.

Regulators must constantly evaluate what new payment platforms and virtual currencies should fall under their regulation, and develop innovative new skills and methods to supervise them. It is possible that new regulation to apply to virtual currencies and new payment technologies will eventually be necessary. If at some point the ecosystem of anonymous and distributed financial technology is so expansive, and the virtual currencies exchanged in this ecosystem so stable, that it provides a true alternative at scale to the conventional financial system, new regulatory techniques may be needed to supervise these technological platforms. In this instance, the traditional framework of the BSA may need significant reevaluation.

Any virtual currency regulatory regime should aim to have each entity satisfy the fundamental requirements of a rigorous counterterrorist financing and AML compliance program. This includes following KYC procedures, wherever possible extending to users of virtual currency; maintaining certain transactional records; and reporting suspicious transactions of various types. Regulators and regulated entities could consider including new types of electronic data in suspicious activity and "cash" transaction filings. Among the obvious challenges involved with this innovation would be the need for them to understand where relatively anonymous transactions originate, where they are going, and with whom beneficial ownership resides, as well as how much anonymity is feasible while still adequately managing risk, and at what point in the transaction process anonymity is possible.[273]

There are likely many creative new opportunities to synthesize large amounts of financial and other data to identify the financing of terrorism.

Principles for Improving Financial Supervision and Enforcement to Counter Terrorist Use of Virtual Currencies

It is possible to adopt new strategies to better identify and halt terrorist financing through virtual currencies in the current digital financial era. Not all of these strategies are directly linked to the technical specifications of emerging virtual currencies; rather, they are somewhat more methodological from a regulatory oversight and compliance perspective. Nevertheless, they can all help to capture illicit conduct using new kinds of decentralized and anonymous virtual currencies. First and foremost, however, policy leaders must consider several basic principles that will, if embraced, undergird an ability to successfully adopt policy change to promote a greater ability to counter terrorist use of virtual currency.

National security leaders must embrace three basic principles at the highest levels and clarify them to the private sector. These will serve as the front line to identifying terrorist financing using virtual currencies. Concomitantly, supervisory agencies must recognize and embrace these priorities and regulatory agencies must enforce them. They are:

1. Policy leader prioritization of countering terrorist financing and other financial crimes, including through new virtual currencies
2. A policy and regulatory posture that encourages innovation
3. New strategies and legal means for coordination, particularly between the public and private sectors.

These priorities are beneficial for the task of countering terrorist use of virtual currencies; they are also essential to ensure that the current policy and regulatory framework to counter terrorist financing does not become truly antiquated. Financial connectivity, along with new payment technologies and virtual currencies, is already reorganizing ways in which all financial actors raise, store, and move money.

In line with the first principle, to more effectively counter terrorist use of virtual currencies, and indeed to counter terrorist financing more broadly, banks and MSBs must place much greater emphasis on tracking and reporting suspected terrorist financing. Currently, banks, MSBs, and other actors are asked to report on a wide array of suspicious and threatening activities, including money laundering, narcotics, weapons, human trafficking, securities fraud, and cybersecurity. Policymakers and law enforcement officials do not effectively communicate their priorities to private sector entities with limited resources; they must do so and must coordinate to the extent possible with independent regulators to align supervision and enforcement priorities. As a result, banks have no official policy guidance on how to prioritize risks. Therefore, they place no special emphasis on areas of greatest concern to policymakers, law enforcement, and the intelligence community. For the same reasons, they do not necessarily prioritize creative investigative tactics or information sharing.

Intelligence and law enforcement officials are the ultimate beneficiaries of banks' suspicious activity reporting, so it is particularly incongruous that they are not involved in establishing criteria for threat reporting. Nor do they provide feedback on what banks report as being of value for law enforcement activities. This stands in contrast to the fact that the law enforcement and national security communities do establish investigative and enforcement priorities for themselves regularly. The financial sector's perception of threats may be different from those identified by national leaders, as well as being different from those identified by bank supervisors. Additionally, each individual financial institution's perception may differ depending on its geographic footprint and specific array of business activities. These varying perceptions add to the problematic nature of the lack of policymaker and law enforcement priority-setting for private financial reporting on threats. The policy community must establish a hierarchy of financial crime threats on which they expect the financial sector to focus its activities. Terrorist financing, specifically including its occurrence via virtual currency, should be first among such crimes.

The policy community must establish a hierarchy of financial crime threats. Terrorist financing, specifically including its occurrence via virtual currency, should be first.

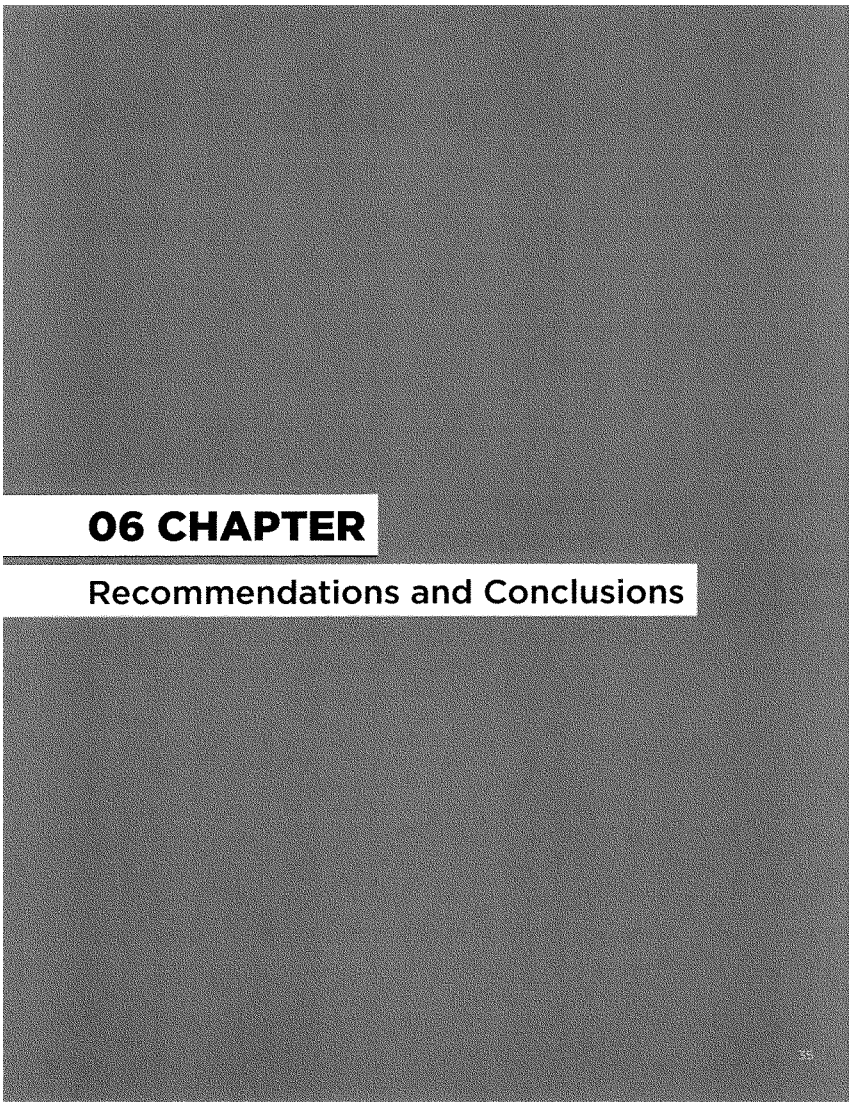
The second principle, aggressively encouraging innovation in strategies to identify and counter terrorist financing, may involve what some financial sector experts have called a "sandbox" approach. Used in the United Kingdom, this approach urges regulators to give financial sector participants and technology entrepreneurs the regulatory running room to experiment with their technology and see how it interacts with customers

and their data without having the relevant—potentially onerous—regulations applied immediately.[274] Necessarily, this running room involves regulators' tolerance of potential failures. In practice, and for compliance professionals and legal officials, this tolerance takes the form of liability shields.

The final principle calls for more extensive cooperation, specifically among private sector entities and between the public and private sectors. Current U.S. statutes allow for financial information sharing among and between public and private sector actors. In some instances this can be a fruitful means of establishing information flow, including during active investigations to track suspected terrorists. The FBI Terrorist Financing Operations Section has publicly expressed the view that financial institutions have been rapidly and extremely responsive to requests for information to all terrorist incidents.[275] But many private sector representatives embrace a legal interpretation of national financial information sharing laws, data privacy rules, and other regulations. In practice, this has enshrined powerful limitations on data sharing and cooperation—acutely, when it comes to sharing information and cooperating across national boundaries, even among branches or subsidiaries of the same bank.[276] When coupled with a libertarian ethos among technology firms, especially those pioneering new ways to send money around the world outside the reach of traditional financial institutions, information flow regarding illicit finance may be particularly poor.

It is more important than ever for law enforcement and intelligence officials to coordinate closely and with the private sector to map threat networks and plots, including terrorist activity.

In a financial ecosystem where payment anonymity is easier to achieve and social media provides for more anonymous communication, it is more important than ever for law enforcement and intelligence officials to coordinate closely and with the private sector to map threat networks and plots, including terrorist activity. It is crucial that policy authorities signal to stakeholders working to counter terrorism that they must radically broaden their coordination, including through expanded legal pathways and liability protection for information sharing and regulatory or enforcement benefits for cooperation. This approach will help to better address terrorist use of virtual currencies, and terrorist financing in general. It is also fundamental to the development of creative strategies to unite private sector entities and government intelligence and regulatory officials in better understanding the identities and patterns of virtual currency users. Moreover, and of significance to the entire financial regulatory and national security establishment, this approach will meaningfully contribute to a more robust ability to fight all manner of criminal financial activity. Applied together, these three principles are the foundation to better fighting the broad array of threat finance.



06 CHAPTER

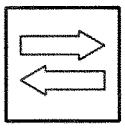
Recommendations and Conclusions

As discussed, anecdotal evidence indicates that terrorists have used virtual currency to move and store money. Policymakers and regulators have the ability, and would be well served, to adapt their approach to supervision and enforcement to better track this illicit finance and work to prevent the threat from achieving scale. Such changes would likely have the beneficial effect of countering terrorist financing more broadly. Additionally, they may also help to address the pernicious and more widespread use of virtual currencies by various types of criminals, including traffickers of drugs, child or other illegal pornography, counterfeit goods, and others. Counterterrorism, national security, and law enforcement officials would all be better off with an invigorated policy focus on preventing terrorist use of virtual currencies.

For now, the most effective strategy for accomplishing this goal is to focus legal and regulatory adaptations on the gateway financial institutions, whether banks, MSBs, or virtual currency exchanges that process virtual currency transactions. As noted, these nodes in the financial system can be effective for identifying suspicious customers or activity. They are relatively centralized and regulated, and therefore require at least a basic degree of transparency and lawfulness. To the extent that such institutions can be encouraged and offered incentives to host virtual currency money movements and exchanges, they can increase their transparency and lawfulness. The more this happens, the more it will benefit the financial system's security and integrity. If virtual currencies scale to a point where they are more broadly used and exchanges themselves become less relevant, this approach might need to change. But for the moment, the most effective governance technique is to focus on exchanges.

The following series of recommendations offers steps to various stakeholders in the counterterrorism and financial technology realm designed to help them better understand terrorist use of virtual currencies, prioritize the issue along with a broader focus on terrorist financing, and refine strategies for preventing such activity from scaling. The recommendations seek to assist regulatory and financial supervisors in protecting valuable financial sector innovation in the virtual currency domain. They also suggest strategies to protect and encourage an innovative approach by financial institutions in detecting illicit financial activity via virtual currencies. Finally, they offer suggestions for more forward-leaning financial information sharing and disclosure, in the service of an improved intelligence, law enforcement, and industry ability to hold terrorist threats at bay. These recommendations, if implemented, will help to mitigate the degree to which terrorists can use virtual currencies, as well as more conventional methods of terrorist financing.

Policy Recommendations



1. Better understand the evolving threat of virtual currencies financing terrorism

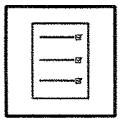
Perhaps the most significant change that policy leaders can implement to more ably counter terrorist use of virtual currency is improving the ability of intelligence and oversight officials to understand the phenomenon. This demands an ongoing investigation of terrorist financing and a novel approach to gaining insight into new financial technologies that terrorists can use. It also demands an ongoing analysis into when, and in what fashion, new regulation is needed to govern evolving and expanding technology.

Expand regulation and guidance to foster greater financial information disclosure and sharing. Congress should move forward with proposals for enhancing requirements for the collection and disclosure of beneficial ownership information in the corporate formation process.[277] Additionally, FinCEN should consider offering new guidance or regulations on sections 314(a) and 314(b) of the USA Patriot Act, to facilitate greater information flow within and among global banks. Federal officials could also consider a rule on cross-border financial flows for exchanges regulated in the United States, contemplating the documentation of virtual currency transactions with FinCEN or another appropriate agency. Given the decentralization of certain virtual currencies, it might be difficult to do this directly after they have achieved a certain scale, but for the moment, virtual currency exchanges remain the subject of regulation. In well-supervised jurisdictions, this remains a viable approach. Information from more traditional banks, when disclosed and exchanged pursuant to these various changes, will help intelligence officials and the law enforcement community to better track terrorist use of virtual currencies, as well as the illicit financial activity of a host of other financial criminals.

Formalize the congressional focus on terrorist financing and financial technology. Relevant congressional committees, including the House Financial Services Committee and Senate Banking Committee, should formally add terrorist financing and financial technology, including virtual currency, into their oversight mandate. The committees can fold this into existing work to investigate terrorist financing, and they should draw upon the Congressional Research Service to gather information on the threat. Congressional staff may also consider establishing a congressional study group to further advance oversight and the consideration of updated financial oversight statutes, as appropriate.

Call for an independent task force to advise federal officials. The Treasury Department, Department of Justice (DOJ), intelligence community, and other agencies should work with financial services trade associations, such as the American Bankers Association and the Association of Certified Anti-Money Laundering Specialists, as well as think tanks with a special focus on illicit finance and counterterrorism, to conduct independent research on terrorist use of new financial technology, including virtual currencies.

Expand regulator outreach to financial technology firms and developers. Given the new entry of technology firms into the business of moving and storing value, as well as the rapid pace of innovation and change in this area, financial regulators and policy officials should focus unique attention on outreach to the technology sector, including the developers of virtual currency and new payment technologies. Regulators and officials should seek to foster encounters that are constructive and oriented toward mutual information flow and collaboration. This will help all parties to understand new developments in financial technology and terrorist financing threats.



2. Prioritize terrorist financing as a matter of public policy and law enforcement significance

Policy and law enforcement leaders must jointly signal to the public and private sectors the importance of countering terrorist financing, including through virtual currencies and other new technologies. This will be meaningful if the prioritization is clearly linked to incentives and the likelihood of enforcement and regulatory examinations in certain high priority areas, with a clearly diminished emphasis in other areas. That is, regulators should reward innovative and effective efforts to counter terrorist financing, while increasing their focus on these areas. Similarly, they should decrease attention and examination or enforcement in other lower priority areas such as structured payments for relatively small-scale money laundering. At present, there is no process by which policy and law enforcement officials can prioritize areas of illicit financial activity for private sector scrutiny and reporting, while the private sector receives regulatory assent for reallocating assets in accordance with these priorities. The effect of all this is that everything becomes a priority, but in fact nothing is a priority. This is surely not the case from a national threat-assessment perspective. A real prioritization will appropriately signal to stakeholders a more enhanced level of significance and resources that they should devote to the challenge. In turn, this will contribute to the effectiveness of counterterrorist financing efforts, in the interest of national security.

Initiate an intelligence prioritization process to highlight counterterrorism finance information. FinCEN or the DOJ should initiate a process, modeled on the National Intelligence Priorities Framework, to rank the counter–illicit finance priorities of the U.S. government. This methodology can elevate terrorism as a priority, signaling to policymakers, law enforcement officials, and financial institution supervisors the need to focus on the topic in enforcement and targeting activities. Financial officials will need to contemplate a strategy for how to grade banks on how well they direct resources to these priority areas.

Prioritize terrorist financing. Recognizing that many bank supervisory agencies are statutorily independent, Congress and the executive branch should emphasize the importance of TF. These priorities should translate into supervision and enforcement approaches.

Expand outreach to the private sector on countering terrorist financing. The Treasury Secretary, or an appropriate deputy in the Treasury Department from the Office of Terrorism and Financial Intelligence, should conduct outreach to the private sector to communicate a priority focus on countering TF. This will signal to banks and MSBs the need to devote appropriate resources to this area.

3. Prioritize terrorist financing as a compliance matter within private institutions

Banks should expand their focus on terrorist financing, including via the use of virtual currencies, as an area of illicit finance in response to the articulated government prioritization of this issue. This work must be undergirded by enhanced efforts to share information on terrorist threats with appropriate law enforcement agencies, including the FBI, and peer institutions. Additionally, in practice the prioritization should be demonstrated by a desire to lead regulators in the establishment of innovative models to counter terrorist financing.

Invest further resources in financial intelligence units (FIUs). Banks should expand their investigative capacity to conduct proactive and targeted monitoring initiatives to identify terrorist threats, as well as to conduct reactive work when an incident occurs. They can usefully model such efforts after federal FIUs, and are well placed to

gather enterprise-wide information about illicit finance threats. Additionally, these initiatives should be coordinated with federal counterparts.

Propose specific legal changes to improve counterterrorist financing efforts. Banks and private sector leaders should identify and propose specific changes to statute, regulations, and policy that would allow them to overcome some of the impediments to tracking terrorist financing activity, including via virtual currencies. As discussed throughout this paper and in some of the remaining recommendations, these changes should include ideas for improved information sharing and legal liability protection. Banks are uniquely placed to play a leadership role in articulating the current challenges and in undertaking the intellectual and technical work involved in adopting new rules and culture. Again, all of this should be coordinated with policymakers.

4. Offer protection and incentives for private initiatives to halt terrorist financing, including through virtual currency

Federal policymakers, including at the FBI, DOJ, Secret Service, and IRS; as well as banking regulatory authorities such as the Federal Reserve, the OCC, and FinCEN, should contemplate and craft guidance for banks and other regulated financial entities to spur them to collaborate more closely with governmental authorities to track and halt terrorist financing. State level bank supervisors, particularly New York's Department of Financial Services, should participate in this process as well. It could ultimately include adaptation of regulation and enforcement guidance, as well as liability protection to protect financial institutions' innovative strategies. Moving toward this approach would mean the creation of a regulatory "sandbox," an environment that fosters collaborative approaches to compliance in order to best advance the ultimate policy goals.

Consider a "laboratory" approach for pioneering new counterterrorist financing strategies. Regulators should contemplate strategies for stimulating specific private sector initiatives and mechanisms whereby banks and other MSBs can pilot or work to institutionalize new ways to identify and halt TF, including via virtual currencies. This will require limited liability protection, possibly including a safe harbor, comfort letters or regulatory guidance from banking supervisors, and close, ongoing coordination with law enforcement officials. It might also include special licensing for unique industry collaborative investigatory efforts to address TF and share information with law enforcement.

Recognize successful models and best practices, including with incentives. Regulators should consider publicly sharing examples of successful strategies to track terrorist financing, including financing via new technological means. Such sharing could include accolades for the quality over quantity of Suspicious Activity Reports (SARs) filed, or a strong record of sharing SARs with high value to the law enforcement community. Such forms of recognition could offer a reputational benefit to the firm that implemented the strategy and signal to financial overseers the value and prioritization placed on innovative, successful strategies to address TF. Additionally, financial policy officials could offer positive inducements such as investment incentives to firms and foreign official counterparts that make a special effort to share information and coordinate in addressing TF. These measures would not, strictly speaking, constitute rewarding activity that is expected of all financial institutions, but rather highlight extraordinary and aspirational behavior.

5. Make financial technology innovation more sustainable

Financial regulators should consider strategies to limit the regulatory "tax" on development of financial technology, including virtual currency technology. Financial technology companies must shoulder the compliance burden of financial system operators, and policies to limit this strain for virtual currency companies—which may not necessarily be inherently risky—would appropriately underscore a risk-based approach to financial regulation. It would also have the effect of stimulating financial technology innovation. Financial policymakers should consider how to actively support beneficial financial technology development, particularly when it can bring virtual currency and new payment technology platforms successfully into the regulated financial sphere.

Explore a risk-based approach to anti-money laundering program requirements. Policymakers should adapt the current oversight regime for new financial technology firms. Oversight would be moved to a more risk-based approach toward countering TF. This could entail a greater focus on some elements of the programs (for example, a risk-based prioritization of firms engaging in cross-border payments or more tailored SAR filing requirements based on services offered), and on liquidity providers and exchanges in particular, in line with guidance offered by policymakers on national security and law enforcement priorities. Ultimately, if virtual

currencies scale in a significant way, then exchanges will become less relevant, and regulators will need to engage in significant adaptation in how they supervise for AML and CTF compliance in the virtual currency space. Promotion of this kind of innovation will help to prepare the groundwork for a future regulatory architecture.

Explore the idea of a common compliance architecture. In coordination with financial industry representatives, policymakers should consider establishing industry-wide mechanisms to aid regulated firms with compliance activities, including with explicit regulatory permission. This could be particularly useful for new financial technology firms that may be both small and relatively unfamiliar with financial sector regulation. One promising idea is the development of a global KYC registry established through blockchain technology. This would dramatically reduce the cost of establishing an effective AML compliance architecture for new firms with limited resources. Other possibilities would be to offer alternative safe channels for permitting financial flows, or alternative ways to validate the transparency of financial platforms or certain ecosystems that conform with international best practices.

Consider adopting unique regulations for financial technology startups. Financial regulators should consider alternative regulatory schemes for small market capitalization or startup financial technology firms with a path to more conventional regulation after they achieve scale and sustainability. This could include enhanced beneficial disclosure requirements in the initial regulatory stage, to avoid the incentive that such a model would create for evading regulation altogether, along with the subsequent formation of shell companies.

Expand the geographic range of financial technology licensing. At present, certain kinds of financial technology companies must seek separate licenses in each state in which they operate. State and federal banking regulators should think about ways to harmonize the financial supervision landscape.

Conclusion

Terrorists' use of virtual currencies has thus far been episodic and relatively uneven, given the greater accessibility to virtual currencies by groups with relatively more technical sophistication. However, even if terrorist use of virtual currency has not yet achieved scale or become a more systemic security threat, it has the potential to grow. For the policymaking community, the true concern when it comes to terrorist use of virtual currencies and other new payment technologies is what may happen in the future, and their ability to track developments.

As this paper has pointed out, regulatory and legal adaptations can improve the ability of regulators, intelligence and law enforcement officials, and the banks and MSBs abused by terrorists to better detect and halt terrorist use of virtual currencies. However, it will be extremely difficult to make such adaptations, in particular due to the confluence of dynamic financial technology innovation and an AML compliance culture that is significantly focused on completely avoiding risk. In order to get ahead of terrorists' ability to manipulate the features of decentralization and anonymity offered by virtual currency, policymakers will have to, in the first instance, encourage financial institutions to manage—not shun—the risks of this and other new financial technologies. To arrive at this point, the government will have to take on enormous dual challenges: assume greater risk and set a tone of collaboration.

The rewards of achieving a more constructive and collaborative industry-government partnership around countering terrorist use of virtual currencies, and indeed all terrorist financing activity, are tremendous. A true partnership in this domain will help policy leaders to better fight terrorism and encourage valuable financial innovation. It will also better protect financial institutions from abuse and preserve their reputation, while contributing to shareholder value. Particularly given the potential for lone wolf terrorist activity, along with the challenge of detecting, through financial data, terrorist attacks before they occur, it will be impossible to keep terrorists out of the financial system entirely and away from electronic currency, whether virtual or fiat. Additionally, the highly dynamic nature of financial innovation means that regulators and policymakers may not be able to avoid some tension as they strive to keep regulations and compliance benchmarks up to speed with technology, and as they conduct proper outreach to the technology sector.

Notwithstanding these risks and regulatory tensions, the strongest defense against terrorist use of virtual currency is an approach to financial policy and regulatory oversight that seeks to embrace and manage, not avoid, risk. This also corresponds with an effective strategy for stimulating financial technology innovation, and the many benefits that new payment systems and new currencies or financial ecosystems can offer. Ultimately, then, the greatest challenge for policymakers is an acculturation to the reality of significant risk and the difficult work of truly prioritizing. For banks, the greatest challenge is to make detection and insight more important than the avoidance of risk. Successfully addressing these challenges will have a direct and meaningful benefit for U.S. national security, as well as for our economic competitiveness and leadership in innovation.

Endnotes

1. For a similar definition of hawala, see: "Letter dated 4 September 2012 from the Chair of the Security Council Committee pursuant to resolution 1988 (2011) addressed to the President of the Security Council," (United Nations Security Council, September 5, 2012), http://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_2012_683.pdf, 15.

2. The terms used in this paper to describe types of emerging financial technology have contested definitions. There is no single commonly agreed-upon definition of a "virtual currency." But the definition used by the Financial Action Task Force (FATF) has perhaps the broadest adherence. The FATF describes a virtual currency as "a digital representation of value that can be digitally traded and functions as (1) a medium of exchange and/or (2) a unit of account and/or (3) a store of value, but does not have legal tender status (i.e., when tendered to a creditor, is a valid and legal offer of payment) in any jurisdiction." A virtual currency, according to the FATF, fulfills its functions "by agreement within the community of users of the virtual currency." FATF does not use the term "digital currency," in order to avoid confusion with virtual currencies and with "e-money," which refers to fiat currency being transferred through electronic means. See "Virtual Currencies: Key Definitions and Potential AML/CFT Risks" (FATF/OECD, June 2014), 4, http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf. Domestically, the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) defines virtual currency as having many characteristics of real currency but as lacking legal tender status in any jurisdiction. See FinCEN's memo "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies," March 18, 2013, https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering. The IRS, which has a tax policy for virtual currency, defines it as "a digital representation of value that functions as a medium of exchange, a unit of account, and/or a store of value." In some instances, it functions like real currency, but it does not have legal tender status in any jurisdiction. See Internal Revenue Service, "IRS Virtual Currency Guidance," April 14, 2014, https://www.irs.gov/irb/2014-16_IRB/ar12.html. The Commodity Futures Trading Commission, which also regulates virtual currencies, uses but does not quote the FATF's definition. Both the FATF and FinCEN definitions differ from that of the European Central Bank in 2012, which was limited to centralized virtual currencies (issued and controlled by a group of developers). See "Virtual Currency Schemes" (European Central Bank, October 2012), 6, https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf. This paper will apply the specific parameters that the FATF lays out to define a virtual currency and avoid using the term "digital currency" for the sake of clarity. Furthermore, this paper also analyzes "cryptocurrencies," a subset of virtual currencies that uses cryptographic techniques for security, including to verify currency ownership and transactions made using the currency. A new payment technology, by contrast to virtual currencies and the systems that enable them, leverages technology to facilitate banking or financial transactions between people using currency.

3. Stuart Levey, Under Secretary, Terrorism and Financial Intelligence, Department of the Treasury, testimony to the Subcommittee on Oversight and Investigations, Financial Services Committee, U.S. House of Representatives, July 11, 2006, 1–2. http://financialservices.house.gov/media/pdf/071106sl.pdf.

4. "Who We Are," FATF, http://www.fatf-gafi.org/about/.

5. "Consolidated FATF Strategy on Combatting Terrorist Financing" (FATF, February 19, 2016), 1, http://www.fatf-gafi.org/media/fatf/documents/reports/FATF-Terrorist-Financing-Strategy.pdf.

6. James Freis, Tom Keatinge, Troels Oerting, and Karen Walter, "Trends in Counter Terrorist Financing: Panel Summary," *SIBOS 2016 in Review* (SWIFT: October 2016), 4.

7. "2015 National Terrorist Financing Risk Assessment"(Department of the Treasury, June 2015), 3, https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/National%20Terrorist%20Financing%20Risk%20Assessment%20%E2%80%93%2006-12-2015.pdf.

8. Ibid., 47.

9. Ibid., 56, 57.

10. Ibid., 58.

11. "EBA Opinion on 'Virtual Currencies,'" EBA/Op/2014/08 (European Banking Authority, July 4, 2014), 33, https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf.

12. Liana Rosen (specialist in international crime and narcotics, foreign affairs, Defense and Trade Division of the Congressional Research Service), "Task Force on Anti-Terrorism and Proliferation Financing Briefing" (United States Congress, March 3, 2017). Discussion with author.

13. Brendan I. Koerner, "#jihad: Why ISIS Is Winning the Social Media War," *Wired*, April 2016, https://www.wired.com/2016/03/isis-winning-social-media-war-heres-beat/.

14. Nicholas Blanford, "How Off-the-Shelf Drones Are Changing War in Syria and Lebanon," *Christian Science Monitor*, August 16, 2016, http://www.csmonitor.com/World/Middle-East/2016/0816/How-off-the-shelf-drones-are-changing-war-in-Syria-and-Lebanon.

15. Andy Greenberg, "New Dark-Web Market Is Selling Zero-Day Exploits to Hackers," *Wired*, April 17, 2015, https://www.wired.com/2015/04/therealdeal-zero-day-exploits/; Lillian Ablon, Martin C. Libicki, and Andrea A. Golay, "Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar" (RAND, 2014), 11–12, http://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf.

16. "Combining an anonymous interface with traceless payments in the digital currency bitcoin, the site allowed thousands of drug dealers and nearly 1 million eager worldwide customers to find each other—and their drugs of choice—in the familiar realm of ecommerce," quoted from Joshuah Bearman and Tomer Hanuka, "The Untold Story of Silk Road, Part 1," *Wired*, May 2015, https://www.wired.com/2015/04/silk-road-1/. See also "Part 2: The Fall," *Wired*, June 2015, https://www.wired.com/2015/05/silk-road-2/; Thomas Fox-Brewster, "Life after Evolution: Meet the Dark Web Drug and Gun Entrepreneurs Succeeding Solo," *Forbes*, April 9, 2015, https://www.forbes.com/sites/thomasbrewster/2015/04/09/drug-and-gun-vendors-thriving-on-their-own/#6574c57535f6.

17. Ransomware, in which cybercriminals encrypt a victim's files and decrypt those files only after receipt of a ransom, generally paid in Bitcoin, is a notable exception.

18. Ablon, Libicki, and Golay, "Markets for Cybercrime Tools and Stolen Data," 15.

19. "Bitcoin," CryptoCurrency Market Capitalizations , https://coinmarketcap.com/currencies/bitcoin/; "Monero," CryptoCurrency Market Capitalizations, https://coinmarketcap.com/currencies/monero/.

20. See "FinCEN Awards Recognize Partnership between Law Enforcement and Financial Institutions to Fight Financial Crime," Financial Crimes Enforcement Network, May 10, 2016, https://www.fincen.gov/news/news-releases/fincen-awards-recognize-partnership-between-law-enforcement-and-financial.

21. Government Accountability Office, *Financial Institutions: Fines, Penalties, and Forfeitures for Violations of Financial Crimes and Sanctions Requirements*, GAO-16-297, March 22, 2016, 11, http://www.gao.gov/assets/680/675987.pdf.

22. Paul Taylor, "How Banks Can Avoid the De-Risking Trap," *American Banker*, July 19, 2016, https://www.americanbanker.com/opinion/how-banks-can-avoid-the-de-risking-trap.

23. For examples of this trend, see Rob Barry and Rachel Louise Ensign, "Cautious Banks Hinder Charity Financing," *The Wall Street Journal*, March 30, 2016, https://www.wsj.com/articles/cautious-banks-hinder-charity-financing-1459349551; Rob Barry and Rachel Louise Ensign, "Losing Count: U.S. Terror Rules Drive Money Underground," *The Wall Street Journal*, March 30, 2016, https://www.wsj.com/articles/losing-count-u-s-terror-rules-drive-money-underground-1459349211; Lanier Saperstein and Geoffrey Sant, "Account Closed: How Bank 'De-Risking' Hurts Legitimate Customers," *The Wall Street Journal*, August 12, 2015, https://www.wsj.com/articles/account-closed-how-bank-de-risking-hurts-legitimate-customers-1439419093. Federal financial supervisors recently released a paper that attempted to assuage the concerns of banks about this trend. See Office of the Comptroller of the Currency, Department of the Treasury, "Risk Management Guidance on Periodic Reevaluation of Foreign Correspondent Banking," October 5, 2016, https://www.occ.gov/news-issuances/bulletins/2016/bulletin-2016-32.html.

24. Virtual currency professional conversation with author, 2016; Pratin Vallabhaneni, David Fauvre, and Andrew Shipe, "Overcoming Obstacles to Banking Virtual Currency Businesses," Coin Center, May 2016, 4–6, https://coincenter.org/wp-content/uploads/2016/05/banking-obstacles.pdf; Paul Vigna and Michael J. Casey, *The Age of Cryptocurrency: How Bitcoin and Digital Money Are Challenging the Global Economic Order* (New York: St Martin's Press, 2015), 117.

25. Luis Buenaventura, "There's a $500 Billion Remittance Market, and Bitcoin Startups Want In on It," Quartz, September 11, 2016, https://qz.com/775159/theres-a-500-billion-remittance-market-and-bitcoin-startups-want-in-on-it/; Swati Pandey, "Australian Bank Exit from Remittances Sends Money Transfers Underground," Reuters, February 25, 2016, http://www.reuters.com/article/australia-remittances-banks-idUSL3N1632JD; Jamila Trindle, "Bank Crackdown Threatens Remittances to Somalia," *Foreign Policy*, January 30, 2015, http://foreignpolicy.com/2015/01/30/bank-crackdown-threatens-remittances-to-somalia/.

26. Vigna and Casey, *The Age of Cryptocurrency*, 160.

27. Mark Garrison, "Regulation May Be Coming for Bitcoin," Marketplace, September 18, 2015, https://www.marketplace.org/2015/09/18/tech/regulation-may-be-coming-bitcoin.

28. Paul Vigna, "Bitcoin Price Plunges on Fears of a Currency Split," *The Wall Street Journal*, March 19, 2017, https://www.wsj.com/articles/bitcoin-price-plunges-on-fears-of-a-currency-split-1489949541.

29. "Terrorist Financing" (FATF/OECD, February 29, 2008), 7, http://www.fatf-gafi.org/media/fatf/documents/reports/FATF%20Terrorist%20Financing%20Typologies%20Report.pdf.

30. Thomas H. Kean, and Lee Hamilton, "The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States Executive Summary," (Washington, D.C.: National Commission on Terrorist Attacks upon the United States, 2004), 14, http://govinfo.library.unt.edu/911/report/911Report_Exec.pdf.

31. Carla E. Humud, Robert Pirog, and Liana Rosen, "Islamic State Financing and U.S. Policy Approaches," Report No. 43980 (Congressional Research Service, April 10, 2015), 13.

32. "Terrorist Financing," 7–10; "Emerging Terrorist Financing Risks" (FATF/OECD, October 2015), 9–10, http://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf

33. Robert Windrem, "Terror on a Shoestring: Paris Attacks Likely Cost $10,000 or Less," NBC News, November 18, 2015, http://www.nbcnews.com/storyline/paris-terror-attacks/terror-shoestring-paris-attacks-likely-cost-10-000-or-less-n465711; National Commission on Terrorist Attacks upon the United States et al., "The 9/11 Commission Report," 14.

34. "Terrorist Financing," 21.

35. "Emerging Terrorist Financing Risks," 13.

36. "Terrorist Financing," 15.

37. Ibid., 11.

38. Kristina Wong, "Senators: ISIS Is 'Best Funded' Terror Group Ever," *The Hill*, August 26, 2014, http://thehill.com/policy/defense/216023-senators-isis-is-best-funded-terrorist-group-in-history.

39. Humud, Pirog, and Rosen, "Islamic State Financing," 1.

40. "Testimony of A/S for Terrorist Financing Daniel L. Glaser before the House Committee on Foreign Affairs Subcommittee on Terrorism, Nonproliferation, and Trade, and House Committee on Armed Services' Subcommittee on Emerging Threats and Capabilities," Department of the Treasury, press release, June 9, 2016, https://www.treasury.gov/press-center/press-releases/Pages/jl0486.aspx; "Statement of Deputy Assistant Secretary Andrew Keller, U.S. Department of State, Bureau for Economic and Business Affairs before the United States House of Representatives Committee on Foreign Affairs Subcommittee on Terrorism, Nonproliferation, and Trade, June 9, 2016," Committee on Foreign Affairs, U.S. House of Representatives, statement to the Subcommittee on Terrorism, Nonproliferation, and Trade, 2–3.

41. "Financing of the Terrorist Organization Islamic State in Iraq and the Levant (ISIL)" (FATF/OECD, February 2015), 10, http://www.fatf-gafi.org/media/fatf/documents/reports/Financing-of-the-terrorist-organisation-ISIL.pdf.

42. Ibid., 12.

43. Ibid.

44. "Statement of Deputy Assistant Secretary Andrew Keller," 3.

45. "Testimony of A/S for Terrorist Financing Daniel L. Glaser."

46. "Financing of the Terrorist Organization ISIL," 18, 20.

47. Ibid., 12.

48. Benoit Faucon and Ahmed Al Omran, "Islamic State Steps Up Oil and Gas Sales to Assad Regime," *The Wall Street Journal*, January 19, 2017, https://www.wsj.com/articles/islamic-state-steps-up-oil-and-gas-sales-to-assad-regime-1484835563.

49. Ibid.

50. "Emerging Terrorist Financing Risks," 31.

51. Ibid.

52. Ibid., 34.

53. "Financing of the Terrorist Organization ISIL,", 25–26.

54. Joby Warrick, "Private Donations Give Edge to Islamists in Syria, Officials Say," *The Washington Post*, September 21, 2013, https://www.washingtonpost.com/world/national-security/private-donations-give-edge-to-islamists-in-syria-officials-say/2013/09/21/a6c783d2-2207-11e3-a358-1144dee636dd_story.html.

55. "Emerging Terrorist Financing Risks," 31.

56. Juan C. Zarate, chairman and co-founder, Financial Integrity Network, "The Next Terrorist Financiers: Stopping Them Before They Start," Statement to the Financial Services Committee, Task Force to Investigate Terrorism Financing, U.S. House of Representatives, June 23, 2016, 2.

57. Ibid., 7–8.

58. "Emerging Terrorist Financing Risks," 20–21.

59. National Commission on Terrorist Attacks upon the United States et al."The 9/11 Commission Report," 14.

60. Ibid.

61. "Combating the Abuse of Alternative Remittance Systems: International Best Practices" (FATF, June 20, 2003), 5, http://www.fatf-gafi.org/media/fatf/BPP%20SRVI%20June%202003%202012.pdf.

62. "Two Indicted in Missouri on Charges of Providing Material Support to a Terrorist Organization; A Third Defendant Is Charged with Structuring Violations," FBI, November 3, 2010, https://archives.fbi.gov/archives/stlouis/press-releases/2010/sl110310.htm.

63. Ibid.

64. "Money Laundering Through the Physical Transportation of Cash" (FATF, October 2015), 3, http://www.fatf-gafi.org/media/fatf/documents/reports/money-laundering-through-transportation-cash.pdf.

65. "Terrorist Financing," 23.

66. "Terrorist Financing in West and Central Africa" (FATF/GIABA/GABAC, October 2016), 27.

67. Jacob Shapiro, "Bureaucratic Terrorists: al-Qaida in Iraq's Management and Finances," in Brian Fishman, ed., "Bomber, Bank Accounts, and Bleedout," Harmony Project report (Combating Terrorism Center at West Point, July 22, 2008), 8, 73, https://www.ctc.usma.edu/posts/bombers-bank-accounts-and-bleedout-al-qaidas-road-in-and-out-of-iraq.

68. "Emerging Terrorist Financing Risks," 37–38.

69. Ralph Ellis, "Maryland Man Charged with Trying to Aid ISIS," CNN, December 14, 2015, http://www.cnn.com/2015/12/14/us/maryland-terror-arrest/.

70. "Emerging Terrorist Financing Risks," 38.

71. J. E. Reich, "Using Internet Slang on Venmo Might Get You Flagged As a Terrorist," Tech Times, March 11, 2016, http://www.techtimes.com/articles/140422/20160311/using-internet-slang-on-venmo-might-get-you-flagged-as-a-terrorist.htm.

72. Alexandra Starr, "In Wake of Attacks, France Moves to Regulate Prepaid Bank Cards," NPR, the Two-Way, November 23, 2015, http://www.npr.org/sections/thetwo-way/2015/11/23/457090827/in-wake-of-attacks-france-moves-to-regulate-prepaid-bank-cards.

73. French Ministry for the Economy and Finance, "France's Contribution: New Efforts to Combat Terrorist Financing at European Level," Paris, November 27, 2015, 7, http://www.economie.gouv.fr/files/files/PDF/20151127_France's_contribution_-_New_efforts_to_combat_terrorist_financing_at_European_level.pdf.

74. Foo Yun Chee, "EU Proposes Stricter Rules on Bitcoin, Prepaid Cards in Terrorism Fight," Reuters, July 5, 2016, http://www.reuters.com/article/us-eu-security-financing-idUSKCN0ZL1RH.

75. "Virtual Currencies: Key Definitions," 9–10.

76. Ibid., 10.

77. Ibid., 9–10.

78. Yaya J. Fanusie, "The New Frontier in Terror Fundraising: Bitcoin," The Cipher Brief, August 24, 2016, https://www.thecipherbrief.com/column/private-sector/new-frontier-terror-fundraising-bitcoin-1089.

79. Resty Woro Yuniar, "Bitcoin, PayPal Used to Finance Terrorism, Indonesian Agency Says," *The Wall Street Journal*, January 10, 2017, http://www.wsj.com/articles/bitcoin-paypal-used-to-finance-terrorism-indonesian-agency-says-1483964198.

80. Tim Johnson, "Computer Hack Helped Feed an Islamic State Death List," *McClatchy DC Bureau*, July 20, 2016, http://www.mcclatchydc.com/news/nation-world/national/article90782637.html.

81. "Virginia Teen Pleads Guilty to Providing Material Support to ISIL," Department of Justice, press release, June 11, 2015, http://www.justice.gov/opa/pr/virginia-teen-pleads-guilty-providing-material-support-isil.

82. Adam Taylor, "The Islamic State (or Someone Pretending to Be It) Is Trying to Raise Funds Using Bitcoin," *The Washington Post*, June 9, 2015, https://www.washingtonpost.com/news/worldviews/wp/2015/06/09/the-islamic-state-or-someone-pretending-to-be-it-is-trying-to-raise-funds-using-bitcoin/?utm_term=.17ae7b7b7221.

83. Danna Harman, "U.S.-based ISIS Cell Fundraising on the Dark Web, New Evidence Suggests," *Haaretz*, January 29, 2015, http://www.haaretz.com/middle-east-news/.premium-1.639542.

84. Aaron Brantly, "Financing Terror Bit by Bit," *CTC Sentinel* 7, no. 10 (October 2014), 4, https://www.ctc.usma.edu/posts/financing-terror-bit-by-bit.

85. Ibid.

86. Harman, "U.S.-Based ISIS Cell Fundraising on the Dark Web, New Evidence Suggests"; Taylor, "The Islamic State (Or Someone Pretending to Be It) Is Trying to Raise Funds Using Bitcoin"; "Virginia Teen Pleads Guilty to Providing Material Support to ISIL"; Johnson, "Computer Hack Helped Feed an Islamic State Death List"; Fanusie, "The New Frontier in Terror Fundraising: Bitcoin"; Yuniar, "Bitcoin, PayPal Used to Finance Terrorism, Indonesian Agency Says."

87. Carter Dougherty and Greg Farrell, "Treasury's Cohen Sees No Widespread Criminal Bitcoin Use," *Bloomberg*, March 18, 2014, https://www.bloomberg.com/news/articles/2014-03-18/treasury-s-cohen-says-regulation-helps-virtual-currencies.

88. Joshua Baron, Angela O'Mahony, David Manheim, and Cynthia Dion-Schwarz, "National Security Implications of Virtual Currency: Examining the Potential for Non-State Actor Deployment" (RAND, 2015), 19.

89. Europol, "Changes in Modus Operandi of Islamic State Terrorist Attacks," January 18, 2016, 7, http://www.wienerzeitung.at/_em_daten/_wzo/2016/01/25/160125_1356_europol_dokument_aenderungen_in_der_verfahrensweise_mit_is_terroranschlaegen_pdf_englisch.pdf.

90. Brantly, "Financing Terror Bit by Bit," 1; Baron et al., "National Security Implications of Virtual Currency," 19.

91. Nathaniel Karp and Boyd W. Nash-Stacey, "Technology, Opportunity and Access: Understanding Financial Inclusion in the U.S.," Working Paper N. 15 (BBVA Research, July 2015), 33, https://www.bbvaresearch.com/wp-content/uploads/2015/07/WP15-25_FinancialInclusion_MSA.pdf.

92. Dayo Olopade, "Africa's Tech Edge," *The Atlantic*, May 2014, http://www.theatlantic.com/magazine/archive/2014/05/africas-tech-edge/359808/.

93. Ibid.; "Mobile Payments Go Viral: M-PESA in Kenya," World Bank, March 2010, http://web.worldbank.org/WBSITE/EXTERNAL/COUNTRIES/AFRICAEXT/0,,contentMDK:22551641~pagePK:146736~piPK:146830~theSitePK:258644,00.html.

94. Department of the Treasury, "2015 National Terrorist Financing Risk Assessment," 47.

95. Josh Meyer, "How Mobile Payments Might Be the Global Money-Laundering Machine Criminals Have Dreamed About," Quartz, June 17, 2013, https://qz.com/94570/how-mobile-payments-might-be-the-global-money-laundering-machine-criminals-have-dreamed-about/.

96. David S. Evans, "Economic Aspects of Bitcoin and Other Decentralized Public-Ledger Currency Platforms" (University of Chicago Coase-Sandor Institute for Law and Economics, April 15, 2014), 10.

97. Bradley Reaves, Nolen Scaife, Adam Bates, Patrick Traynor, and Kevin R.B. Butler, "Mo(bile) Money, Mo(bile) Problems: Analysis of Branchless Banking Applications in the Developing World," (paper included in the proceedings of the 24th USINEX Security Symposium, Washington, D.C., August 2015), 17.

98. Danielle Camner Lindholm and Celina B. Realuyo, "Threat Finance: A Critical Enabler for Illicit Networks," in *Convergence: Illicit Networks and National Security in the Age of Globalization*, Michael Miklaucic and Jacqueline Brewer, eds. (Washington, DC: National Defense University Press, 2013) 119.

99. "PayPal Completes Acquisition of Xoom," Xoom, November 2015, http://blog.xoom.com/2015/11/paypal-completes-acquisition-of-xoom.html.

100. Robin Sidel and Daisuke Wakabayashi, "Apple, Banks in Talks on Mobile Person-to-Person Payment Service," *The Wall Street Journal*, November 11, 2015, http://www.wsj.com/articles/apple-in-talks-with-u-s-banks-to-develop-mobile-person-to-person-payment-service-1447274074.

101. "Virtual Currencies: Key Definitions," 4–5.

102. Ibid., 5.

103. John Bohannon, "Why Criminals Can't Hide Behind Bitcoin," *Science*, March 9, 2016, http://www.sciencemag.org/news/2016/03/why-criminals-cant-hide-behind-bitcoin.

104. For example, bitcoins can be "tumbled" by having their individual transactions mixed with others, obfuscating the trail of ownership. See Jamie Redman, "Tumbling Bitcoins: A Guide Through the Rinse Cycle," Bitcoin News, July 21, 2016, https://news.bitcoin.com/tumbling-bitcoins-guide-rinse-cycle/.

105. Andy Greenberg, "Monero, the Drug Dealer's Cryptocurrency of Choice, Is on Fire," *Wired*, January 25, 2017, https://www.wired.com/2017/01/monero-drug-dealers-cryptocurrency-choice-fire/.

106. Ibid.

107. Yuji Nakamura, "New Digital Currency Spikes As Drug Dealers Get More Secrecy," *Bloomberg Technology*, August 29, 2016, https://www.bloomberg.com/news/articles/2016-08-29/new-digital-currency-spikes-after-giving-criminals-more-secrecy; Greenberg, "Monero, The Drug Dealer's Cryptocurrency of Choice."

108. Greenberg, "Monero, The Drug Dealer's Cryptocurrency of Choice."

109. Michael del Castillo, "The FBI Is Worried Criminals Might Use the Private Cryptocurrency Monero," CoinDesk, January 31, 2017, http://www.coindesk.com/fbi-concerned-about-criminal-use-of-private-cryptocurrency-monero/.

110. Andy Greenberg, "'Dark Wallet' Is About to Make Bitcoin Money Laundering Easier Than Ever," *Wired*, April 29, 2014, https://www.wired.com/2014/04/dark-wallet/.

111. Ibid.

112. Andy Greenberg, "Waiting for Dark: Inside Two Anarchists' Quest for Untraceable Money," *Wired*, July 11, 2014, https://www.wired.com/2014/07/inside-dark-wallet/.

113. "Virtual Currencies: Key Definitions," 7.

114. Sidney Ember, "Overstock to Allow International Customers to Pay in Bitcoin," *The New York Times*, August 19, 2014, https://dealbook.nytimes.com/2014/08/19/overstock-to-allow-international-customers-to-pay-in-bitcoin/?_r=0.

115. Christopher Langner, "Is Bitcoin Growing Up?" *Bloomberg*, February 12, 2017, https://www.bloomberg.com/gadfly/articles/2017-02-13/bitcoin-might-just-be-growing-up.

116. "Virtual Currencies: Key Definitions," 9. Dong He, Karl Habermeier, Ross Leckow, Vikram Haksar, Yasmin Almeida, Mikari Kashima, Nadim Kyriakos-Saad, Hiroko Oura, Tahsin Saadi Sedik, Natalia Stetsenko, and Concepcion Verdugo-Yepes, "Virtual Currencies and Beyond: Initial Considerations," IMF Staff Discussion Note SDN/16/03 (IMF, January 2016), 6.

117. Nakamoto is a pseudonymous identity. Observers have speculated the name could represent either one individual or a team who invented the technology. See Joshua Davis, "The Crypto-Currency," *The New Yorker*, October 10, 2011, http://www.newyorker.com/magazine/2011/10/10/the-crypto-currency.

118. Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," November 1, 2008, https://bitcoin.org/bitcoin.pdf.

119. World Bank Group, "Migration and Remittances Factbook 2016 Third Edition," (Washington, D.C.: World Bank, May 2, 2016), xii.

120. "Top of Mind: All About Bitcoin," Global Macro Research Issue 21 (Goldman Sachs, March 11, 2014), 18, http://www.paymentlawadvisor.com/files/2014/01/GoldmanSachs-BitCoin.pdf.

121. Buenaventura, "There's a $500 Billion Remittance Market."

122. Andreas Adriano and Hunter Monroe, "The Internet of Trust," *Finance and Development* 53, no. 2 (June 2016).

123. Ibid.

124. He et al., "Virtual Currencies and Beyond," 10, 22.

125. Jon Evans, "The Controversy over Satoshi Nakamoto's True Identity Is Jeopardizing Bitcoin's Future," Quartz, May 19, 2016, https://qz.com/687493/the-controversy-over-satoshi-nakamotos-true-identity-is-jeopardizing-bitcoins-future/.

126. Buenaventura, "There's a $500 Billion Remittance Market."

127. As of December 2016, Circle does not, however, permit the input of new Bitcoins into the system allowing the transfer of Bitcoins converted into *fiat* currencies and using Bitcoin as the back-end technology. See Fitz Tepper, "Circle Removes Ability to Buy and Sell Bitcoin As It Doubles Down on Mobile Payments," TechCrunch, December 7, 2016, https://techcrunch.com/2016/12/07/circle-removes-ability-to-buy-and-sell-bitcoin-as-it-doubles-down-on-mobile-payments/. Adriano and Monroe, "The Internet of Trust."

128. Emma Dunkley, "Santander Pilots Blockchain Payments App," *Financial Times*, May 26, 2016, https://www.ft.com/content/2df2f65c-234f-11e6-9d4d-c11776a5124d.

129. Matt Higginson, "How Blockchain Could Disrupt Cross-Border Payments," *Banking Perspectives* 4, no. 4 (4th quarter, 2016), 56–58, https://www.theclearinghouse.org/-/media/tch/documents/research/banking%20perspectives/2016/q4/2016-q4-bp-issue-web.pdf?la=en.

130. Veem Inc.,"Legal Disclosures: Anti-Money Laundering Policy," Veem.com, March 6, 2017, https://www.veem.com/legal/; Corin Faife, "Why Bitcoin's Remittance Disruption Slowed to a Crawl," CoinDesk, December 11, 2016, http://www.coindesk.com/why-bitcoins-remittance-disruption-slowed-to-a-crawl/.

131. "How Bitcoin Mining Works," CoinDesk, December 22, 2014, http://www.coindesk.com/information/how-bitcoin-mining-works/.

132. "What Is Blockchain Technology?" Blockchain, December 20, 2016, https://support.blockchain.com/hc/en-us/articles/211160223-What-is-blockchain-technology.

133. Mariano Belinky, Emmet Rennick, and Andrew Veitch, "Rebooting Financial Services," *Santander Innoventures*, June 2015, 14–15, http://santanderinnoventures.com/wp-content/uploads/2015/06/The-Fintech-2-0-Paper.pdf.

134. Kevin Maney, "Trust and Verify: The Coming Blockchain Revolution," *Newsweek*, May 23, 2016, http://www.newsweek.com/2016/06/03/blockchain-technology-will-remake-global-financial-system-462537.html?rx=us.

135. Ali Safavi and Kevin Wang, "Blockchain Is Empowering the Future of Insurance," TechCrunch, October 29, 2016, https://techcrunch.com/2016/10/29/blockchain-is-empowering-the-future-of-insurance/.

136. Megan Molteni, "Moving Patient Data Is Messy, But Blockchain Is Here to Help," *Wired*, February 1, 2017, https://www.wired.com/2017/02/moving-patient-data-messy-blockchain-help/.

137. Nathaniel Popper and Steve Lohr, "Blockchain: A Better Way to Track Pork Chops, Bonds, Bad Peanut Butter?" *The New York Times*, March 4, 2017, https://www.nytimes.com/2017/03/04/business/dealbook/blockchain-ibm-bitcoin.html?_r=0.

138. Jackie Burns Koven, "Block the Vote: Could Blockchain Technology Cybersecure Elections?" *Forbes*, August 30, 2016, https://www.forbes.com/sites/realspin/2016/08/30/block-the-vote-could-blockchain-technology-cybersecure-elections/#33cc451d2ab3.

139. Jordan Pearson, "Bitcoin Is Too Libertarian to Save the Developing World, Says UN Paper," Motherboard, February 11, 2016, https://motherboard.vice.com/en_us/article/bitcoin-is-too-libertarian-to-save-the-developing-world-says-un-paper.

140. Joseph Adinolfi, "Bitfinex Hack Shows How Bitcoin's Blockchain Can Be a Liability," MarketWatch, August 4, 2016, http://www.marketwatch.com/story/bitfinex-hack-shows-how-bitcoins-blockchain-can-be-a-liability-2016-08-03.

141. Tanya Andreasyan, "Standard Chartered Explores Blockchain Viability," *Banking Technology*, June 16, 2016, http://www.bankingtech.com/514402/standard-chartered-explores-blockchain-viability/; Brady Porche, "Blockchain Could Spur Credit Card Rewards Revolution," Creditcards.com, November 3, 2016, http://www.creditcards.com/credit-card-news/blockchain-could-spur-credit-card-rewards-revolution.php.

142. "Bitcoin," CryptoCurrency Market Capitalizations, https://coinmarketcap.com/currencies/bitcoin/.

143. "Monero," CryptoCurrency Market Capitalizations, https://coinmarketcap.com/currencies/monero/.

144. "Zcash," Cryptocurrency Market Capitalizations, https://coinmarketcap.com/currencies/zcash/.

145. Jose Pagliery, "Inside the $2 Billion ISIS War Machine," CNN Money, December 11, 2015, http://money.cnn.com/2015/12/06/news/isis-funding/.

146. Department of the Treasury, "2015 National Money Laundering Risk Assessment," 2, https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/National%20Money%20Laundering%20Risk%20Assessment%20%E2%80%93%2006-12-2015.pdf

147. Juan C. Zarate and Chip Poncy, "Designing a New AML System," *Banking Perspectives* 4, no. 3 (3rd quarter, 2016), 27, https://www.theclearinghouse.org/-/media/tch/documents/research/banking%20perspectives/2016/q3/2016-q3-bp-issue-web.pdf?la=en.

148. See Aaron Shaw and Benjamin M. Hill, "Laboratories of Oligarchy? How the Iron Law Extends to Peer Production," *Journal of Communication* 64, no. 2 (April 1, 2014), 215–38.

149. Ranier Böhme, Nicolas Christin, Benjamin Edelman, and Tyler Moore, "Bitcoin: Economics, Technology, and Governance," *Journal of Economic Perspectives* 29, no. 2 (spring 2015), 219–20.

150. Ibid., 220–22.

151. Lauren Gensler, "The Idiot's Guide to Laundering $9 Million," *Forbes*, January 11, 2017, http://www.forbes.com/sites/laurengensler/2017/01/11/gift-cards-money-laundering/.

152. Jason Del Rey, "Offshore Gambling Site Laundered $2 Million in Amazon Gift Cards, Feds Say," Recode, March 15, 2016, http://www.recode.net/2016/3/15/11586972/offshore-gambling-site-laundered-2-million-in-amazon-gift-cards-feds.

153. Eric Lichtblau, "How an American Ended Up Accused of Aiding ISIS with Gift Cards," *The New York Times*, January 28, 2017, https://www.nytimes.com/2017/01/28/us/politics/washington-transit-cop-suspected-isis.html.

154. Leslie Walker, "PayPal.com CEO Peter Thiel," *The Washington Post*, August 2, 2001, http://www.washingtonpost.com/wp-srv/liveonline/01/washtech/walker/washtech_walker080201.htm.

155. Ibid.

156. Brian Grow, "Gold Rush," *Bloomberg*, January 9, 2006, http://www.bloomberg.com/news/articles/2006-01-08/gold-rush.

157. Margaret Kane, "eBay Picks Up PayPal for $1.5 Billion," CNET, August 18, 2002, https://www.cnet.com/news/ebay-picks-up-paypal-for-1-5-billion/.

158. Jessica Menton, "PYPL Stock Price Soars 11 Percent on Wall Street Return Following eBay Inc. Spinoff," *International Business Times*, July 20, 2015, http://www.ibtimes.com/paypal-ipo-2015-pypl-stock-price-soars-11-wall-street-return-following-ebay-inc-2016040.

159. "PayPal Reports Fourth Quarter and Full Year 2016 Results," PayPal, January 26, 2017, https://investor.paypal-corp.com/releasedetail.cfm?releaseid=1009339.

160. Sarah Mishkin, "Innovation Key to PayPal's Successful Independence," *Financial Times*, September 30, 2014, http://www.ft.com/cms/s/0/307d8e56-48b7-11e4-9d04-00144feab7de.html#axzz4Hi2zUmBc.

161. Telis Demos, "PayPal Isn't a Bank, But It May Be the New Face of Banking," *The Wall Street Journal*, June 1, 2016, http://www.wsj.com/articles/as-banking-evolves-fintech-emerges-from-the-branch-1464806411.

162. Ibid.

163. Chargebacks occur when a customer contests an order that was received. PayPal opens a dispute resolution process and places a temporary hold on the funds involved. This enables PayPal to potentially reverse the transaction and restore costs to the customer. For more on PayPal's current procedures and policies, see "Resolving disputes, claims and chargebacks," PayPal, https://www.paypal.com/us/webapps/mpp/security/resolve-disputes.

164. Eric M. Jackson and Christopher Grey, "Bitcoin Is The New PayPal," TechCrunch, February 20, 2014, http://social.techcrunch.com/2014/02/20/bitcoin-is-the-new-paypal/.

165. Gregory J. Millman, "How Paypal Manages Fraud Risk," *The Wall Street Journal*, June 18, 2015, http://blogs.wsj.com/riskandcompliance/2015/06/18/how-paypal-manages-fraud-risk/.

166. Jackson and Grey, "Bitcoin Is The New PayPal"; Walker, "PayPal.com CEO Peter Thiel."

167. Mark Berniker and Matt Hunter, "Semi-Secretive CIA-Backed Data Company to Shun IPO, for Now," CNBC, March 12, 2014, http://www.cnbc.com/2014/03/12/whats-behind-silicon-valleys-most-secretive-company.html.

168. Evan I. Schwartz, "Digital Cash Payoff," *MIT Technology Review*, December 1, 2011, https://www.technologyreview.com/s/401297/digital-cash-payoff/.

169. Ibid.

170. Ibid.

171. Ibid.

172. Ibid.

173. "Undertaking to the Chief Executive Officer of AUSTRAC for the Purposes of Section 197 of the AML/CTF Act by PayPal Australia," Australian Transaction Reports and Analysis Center, 3rd Enforceable Undertaking, November 23, 2009, http://www.austrac.gov.au/sites/default/files/documents/eu_paypal.pdf.

174. Rachel Louise Ensign, "PayPal to Pay $7.7 Million to U.S. over Alleged Sanctions Violations," *The Wall Street Journal*, March 25, 2015, http://www.wsj.com/articles/paypal-to-pay-7-7-million-to-u-s-over-alleged-sanctions-violations-1427312161.

175. Office of Foreign Assets Control, Settlement Agreement between the U.S. Department of the Treasury's Office of Foreign Assets Control and Paypal, Inc. (Department of the Treasury, March 25, 2015), 1, https://www.treasury.gov/resource-center/sanctions/CivPen/Documents/20150325_paypal_settlement.pdf.

176. Ibid.

177. Brian Krebs, "2016 Reality: Lazy Authentication Still the Norm," Krebs on Security, December 28, 2015, http://krebsonsecurity.com/2015/12/2016-reality-lazy-authentication-still-the-norm/.

178. P. Carl Mullan, *A History of Digital Currency in the United States: New Technology in an Unregulated Market* (New York: Palgrave Macmillan, 2016), 19–20.

179. Kim Zetter, "Bullion and Bandits: The Improbable Rise and Fall of E-Gold," *Wired*, June 9, 2009, https://www.wired.com/2009/06/e-gold/.

180. Grow, "Gold Rush."

181. Tim Jackson, "When Gold Makes Cents," *Financial Times*, July 13, 1999.

182. Jack White and Doug Ramsey, "Making New Money," *Barron's*, April 23, 2001.

183. Julian Dibbell, "In Gold We Trust," *Wired*, January 1, 2002, http://www.wired.com/2002/01/egold/.

184. Grow, "Gold Rush."

185. P. Carl Mullen, *The Digital Currency Challenge: Shaping Online Payment Systems through U.S. Financial Regulations* (New York: Palgrave Macmillan, 2014), 20.

186. Michael Mandel, "Money Ain't What It Used to Be," *Business Week*, January 9, 2006.

187. Grow, "Gold Rush."

188. Jackson, "When Gold Makes Cents."

189. Grow, "Gold Rush."

190. Loretta Napoleoni, *Rogue Economics* (New York: Seven Stories Press, 2011), 148.

191. Jackson, "When Gold Makes Cents."

192. Zetter, "Bullion and Bandits."

193. Ibid.

194. Jennifer L. Hesterman, *The Terrorist-Criminal Nexus: An Alliance of International Drug Cartels, Organized Crime, and Terror Groups* (Boca Raton, Fla.: CRC Press, 2013), 236.

195. Grow, "Gold Rush."

196. Ibid.

197. Zetter, "Bullion and Bandits"; Kim Zetter, "E-Gold Gets Tough on Crime," *Wired*, December 11, 2006, https://www.wired.com/2006/12/e-gold-gets-tough-on-crime/.

198. Ibid.

199. "Digital Currency Business E-Gold Indicted for Money Laundering and Illegal Money Transmitting," United States Department of Justice, press release, April 27, 2007, https://www.justice.gov/archive/opa/pr/2007/April/07_crm_301.html.

200. Ibid.

201. Stephanie Condon, "Judge Spares E-Gold Directors Jail Time," CNET, November 20, 2008, http://www.cnet.com/news/judge-spares-e-gold-directors-jail-time/.

202. Sarah Jane Hughes, Stephen T. Middlebrook, and Broox W. Peterson, "Developments in the Law Concerning Stored-Value Cards and Other Electronic Payments," *Business Lawyer*, 63 No. 237 (November 2007), 259.

203. Grow, "Gold Rush."

204. Condon, "Judge Spares E-Gold Directors Jail Time;" Stephen Foley, "E-Gold Founder Backs New Bitcoin Rival," *Financial Times*, November 28, 2013, https://www.ft.com/content/f7488616-561a-11e3-96f5-00144feabdc0.

205. United States of America v. Liberty Reserve S.A., No. USA-33s-274 (Ed. 9-25-58), United States District Court, Southern District of New York, May 2013, 6, https://www.justice.gov/sites/default/files/usao-sdny/legacy/2015/03/25/Liberty%20Reserve%2C%20et%20al.%20Indictment%20-%20Redacted.pdf.

206. Jake Halpern, "Bank of the Underworld," *The Atlantic*, May 2015, http://www.theatlantic.com/magazine/archive/2015/05/bank-of-the-underworld/389555/.

207. "Liberty Reserve Digital Money Service Forced Offline," BBC News, May 27, 2013, http://www.bbc.com/news/technology-22680297.

208. Tim Fernholz, "Liberty Reserve: Legit E-Currency, or 'Bank of Choice for the Criminal Underworld'?" *The Atlantic*, May 28, 2013, https://www.theatlantic.com/business/archive/2013/05/liberty-reserve-legit-e-currency-or-bank-of-choice-for-the-criminal-underworld/276312/.

209. Halpern, "Bank of the Underworld."

210. Financial Crimes Enforcement Network, "Notice of Finding That Liberty Reserve S.A. Is a Financial Institution of Primary Money Laundering Concern" (Department of the Treasury, May 28, 2013), 6.

211. Halpern, "Bank of the Underworld."

212. Ibid.

213. "Liberty Reserve Digital Money Service Forced Offline."

214. Halpern, "Bank of the Underworld"; "Liberty Reserve Digital Money Service Forced Offline."

215. United States of America v. Liberty Reserve S.A., 13.

216. "Liberty Reserve Founder Arthur Budovsky Sentenced in Manhattan Federal Court to 20 Years for Laundering Hundreds of Millions of Dollars Through His Global Digital Currency Business," U.S. Department of Justice, May 6, 2016, https://www.justice.gov/usao-sdny/pr/liberty-reserve-founder-arthur-budovsky-sentenced-manhattan-federal-court-20-years.

217. Halpern, "Bank of the Underworld."

218. Ibid.

219. "Liberty Reserve Digital Money Service Forced Offline."

220. Halpern, "Bank of the Underworld."

221. Ibid.

222. "Liberty Reserve Digital Money Service Forced Offline."

223. Nate Raymond and Brendan Pierson, "Digital Currency Firm Co-Founder Gets 10 Years in Prison in U.S. Case," Reuters, May 13, 2016, http://www.reuters.com/article/us-usa-cyber-libertyreserve-idUSKCN0Y42A2; Joe Palazzolo, "Liberty Reserve Founder Budovsky Extradited to U.S. from Spain," *The Wall Street Journal*, October 10, 2014, https://www.wsj.com/articles/liberty-reserve-founder-budovsky-extradited-to-u-s-from-spain-1412974424.

224. Brian Krebs, "Underweb Payments, Post-Liberty Reserve," Krebs on Security, May 30, 2013, http://krebsonsecurity.com/2013/05/underweb-payments-post-liberty-reserve/.

225. Europol, *The 2016 Internet Organised Crime Threat Assessment* (The Hague: European Policy Office, September 27, 2016) 42, https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016.

226. Krebs, "Underweb Payments, Post-Liberty Reserve."

227. Böhme et al., "Bitcoin: Economics, Technology, and Governance," 213–4.

228. Ibid., 222–4.

229. "Ten Arrested in Netherlands over Bitcoin Money-Laundering Allegations," *The Guardian*, January 20, 2016, https://www.theguardian.com/technology/2016/jan/20/bitcoin-netherlands-arrests-cars-cash-ecstasy.

230. Europol, *The 2015 Internet Organised Crime Threat Assessment* (The Hague: European Policy Office, July 27, 2015) 46, https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2015.

231. Brantly, "Financing Terror Bit by Bit."

232. Richard Winton, "Hollywood Hospital Pays $17,000 in Bitcoin to Hackers; FBI Investigating," *Los Angeles Times*, February 18, 2016, http://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html.

233. David Fitzpatrick and Drew Griffin, "Cyber-Extortion Losses Skyrocket, Says FBI," CNN Money, April 15, 2016 http://money.cnn.com/2016/04/15/technology/ransomware-cyber-security/index.html?section=money_technology.

234. Lucian Constantin, "Ransomware Attacks Against Businesses Increased Threefold in 2016," *PCWorld*, December 9, 2016, http://www.pcworld.com/article/3149106/security/ransomware-attacks-against-businesses-increased-threefold-in-2016.html.

235. Mark Ward, "'Alarming' Rise in Ransomware Tracked," BBC News, June 7, 2016, http://www.bbc.com/news/technology-36459022.

236. Symantec, "Ransomware and Businesses 2016," July 19, 2016, 3, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ISTR2016_Ransomware_and_Businesses.pdf.

237. Matt Zapotosky and Ellen Nakashima, "These Hackers Can Hold a Town Hostage. And They Want Ransom—Paid in Bitcoin," *The Washington Post*, March 21, 2016, https://www.washingtonpost.com/world/national-security/these-hackers-can-hold-a-town-hostage-and-they-want-ransom--paid-in-bitcoin/2016/03/18/1a2e2494-eba9-11e5-bc08-3e03a5b41910_story.html; Tim Simonite, "Companies Are Stockpiling Bitcoin to Pay Off Cybercriminals," *MIT Technology Review*, June 7, 2016, https://www.technologyreview.com/s/601643/companies-are-stockpiling-bitcoin-to-pay-off-cybercriminals/.

238. Kim Zetter, "Why Hospitals Are the Perfect Targets for Ransomware," *Wired*, March 30, 2016, https://www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets/.

239. Josephine Wolff, "The New Economics of Cybercrime," *The Atlantic*, June 7, 2016, http://www.theatlantic.com/business/archive/2016/06/ransomware-new-economics-cybercrime/485888/; Nathaniel Popper, "For Ransom, Bitcoin Replaces the Bag of Bills," *The New York Times*, July 25, 2015, http://www.nytimes.com/2015/07/26/business/dealbook/for-ransom-bitcoin-replaces-the-bag-of-bills.html.

240. Popper, "For Ransom, Bitcoin Replaces the Bag of Bills."

241. "Written testimony of USSS Criminal Investigative Division Special Agent in Charge Edward Lowery III for a Senate Committee on Homeland Security and Governmental Affairs hearing titled 'Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies,'" U.S. Department of Homeland Security, press release, November 18, 2013, https://www.dhs.gov/news/2013/11/18/written-testimony-us-secret-service-senate-committee-homeland-security-and.

242. Bearman and Hanuka, "The Untold Story of Silk Road, Part 1"; Bearman and Hanuka, "The Untold Story of Silk Road, Part 2"; Andy Greenberg, "Prosecutors Trace $13.4M in Bitcoins from the Silk Road to Ulbricht's Laptop," *Wired*, January 29, 2015, https://www.wired.com/2015/01/prosecutors-trace-13-4-million-bitcoins-silk-road-ulbrichts-laptop/.

243. Ablon, Libicki, and Golay, "Markets for Cybercrime Tools and Stolen Data," 25–28; Greenberg, "New Dark-Web Market."

244. See Ablon, Libicki, and Golay, "Markets for Cybercrime Tools and Stolen Data," 8–10; Keith Collins, "Here's What Your Stolen Identity Goes for on the Internet's Black Market," Quartz, July 23, 2015, https://qz.com/460482/heres-what-your-stolen-identity-goes-for-on-the-internets-black-market/.

245. Department of the Treasury, "2015 National Terrorist Financing Risk Assessment," 57–58.

246. Baron et al., "National Security Implications of Virtual Currency," 29.

247. Ablon, Libicki, and Golay, "Markets for Cybercrime Tools and Stolen Data," 4.

248. Ibid., 8.

249. Ibid., x, 8, 15–16.

250. "Remarks of Under Secretary for Terrorism and Financial Intelligence David Cohen before the Center for a New American Security on 'Confronting New Threats in Terrorist Financing,'" Department of the Treasury, press release, March 4, 2014, https://www.treasury.gov/press-center/press-releases/Pages/jl2308.aspx.

251. "Risk of Terrorist Abuse in Non-Profit Organizations" (FATF/OECD, June 2014), 60–64, http://www.fatf-gafi.org/media/fatf/documents/reports/Risk-of-terrorist-abuse-in-non-profit-organisations.pdf; U.S. Department of State, "State Sponsors of Terrorism Overview," Country Reports on Terrorism 2015, June 2016, https://www.state.gov/j/ct/rls/crt/2015/257520.htm.

252. Donna Abu-Nasr, "In War and Now Finance, Losses Mount for Iranian Ally Hezbollah," *Bloomberg*, June 14, 2016, https://www.bloomberg.com/news/articles/2016-06-14/iran-s-return-isn-t-helping-ally-hezbollah-pay-the-bills.

253. "Treasury Sanctions Maritime Network Tied to Joumaa Criminal Organization," Department of the Treasury, press release, October 1, 2015, https://www.treasury.gov/press-center/press-releases/Pages/jl0196.aspx; "Treasury Identifies Lebanese Canadian Bank SAL as a 'Primary Money Laundering Concern,'" Department of the Treasury, press release, February 10, 2011, https://www.treasury.gov/press-center/press-releases/Pages/tg1057.aspx.

254. Conversely, the destruction of the trusted relationships between terrorist groups and their fundraisers/facilitators can have a deleterious effect on their financial stability. See Stuart A. Levey, "Loss of Moneyman a Big Blow for al-Qaeda," *The Washington Post*, June 6, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/06/04/AR2010060404271.html.

255. Lichtblau, "How an American Ended Up Accused of Aiding ISIS"; Jack Moore, "Hawala: The Ancient Banking Practice Used to Finance Terror Groups," *Newsweek*, February 24, 2015, http://www.newsweek.com/underground-european-hawala-network-financing-middle-eastern-terror-groups-307984; Dominic Casciani, "Syria Aid Convoys: Two Guilty Over Terror Funding," BBC News, December 23, 2016, http://www.bbc.com/news/uk-38419488.

256. Stephanie Wilshusen, Robert M. Hunt, James van Opstal, and Rachel Schneider, "Consumers' Use of Prepaid Cards," Federal Reserve Bank of Philadelphia, August 2012, 3.

257. "Final Rule—Definitions and Other Regulations Relating to Prepaid Access," Financial Crimes Enforcement Network, November 2, 2011, https://www.fincen.gov/resources/statutes-regulations/guidance/final-rule-definitions-and-other-regulations-relating; "Directive of the European Parliament and of the Council Amending Directive (EU) 2015/849 on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing and Amending Directive 2009/101/EC" (Strasbourg: European Commission, July 5, 2016), http://ec.europa.eu/justice/criminal/document/files/aml-directive_en.pdf.

258. Claire Groden, "Feds Say This Offshore Gambling Site Used Amazon Gift Cards to Launder Cash," *Fortune*, March 15, 2016, http://fortune.com/2016/03/15/5dimes-amazon-laundering/; Gensler, "The Idiot's Guide To Laundering $9 Million."

259. "FinCEN Fines Ripple Labs Inc. in First Civil Enforcement Action against a Virtual Currency Exchanger," FinCEN, press release, May 5, 2015, https://www.fincen.gov/news/news-releases/fincen-fines-ripple-labs-inc-first-civil-enforcement-action-against-virtual.

260. Ibid.

261. Author phone interview with AML attorney, 2016.

262. Marion Keyes, "Challenges Faced When Auditing a Digital-Currency Financial Institution" ACAMS, February 2015, 5–7.

263. FinCEN, "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies," memo, FIN-2013-G001 (March 18, 2013), 1, https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf.

264. "China Bitcoin Exchanges Halt Withdrawals after PBOC Talks," *Bloomberg*, February 9, 2017 https://www.bloomberg.com/news/articles/2017-02-10/china-bitcoin-exchanges-halt-withdrawals-after-central-.

265. Compare IRS, Notice 2014–21 (March 25, 2014), 2, https://www.irs.gov/pub/irs-drop/n-14-21.pdf; and FinCEN, "Application of FinCEN's Regulations," 1.

266. For example, Western Union spends $200 million a year looking for suspicious activity; this is roughly the annual budget of FinCEN. Barry and Ensign, "Losing Count." Another major bank reported spending three times this much last year. Additionally, author interviews with banking executives, 2016.

267. "A New Paradigm: Redesigning the U.S. AML/CFT Framework to Protect National Security and Aid Law Enforcement" (The Clearing House, February 2017), 8, 22, https://www.theclearinghouse.org/-/media/TCH/Documents/TCH%20WEEKLY/2017/20170216_TCH_Report_AML_CFT_Framework_Redesign.pdf.

268. Author phone interview with bank AML lawyer, 2016.

269. Tracey Durner and Liat Shetret, "Understanding Bank De-Risking and Its Effects on Financial Inclusion: An Exploratory Study," research report (Global Center on Cooperative Security/Oxfam, November 2015), 11; Michaela Erbenova, Yan Liu, Nadim Kyriakos-Saad, Alejandro Lopez-Mejia, Giancarlo Gasha, Emmanuel Mathias, Mohamed Norat, Francisca Fernando, and Yasmin Almeida, "The Withdrawal of Correspondent Banking Relationships: A Case for Policy Action," SDN/16/06 (International Monetary Fund, June 2016), 23–26.

270. Author phone interview with banking industry compliance official, 2016.

271. This enhanced risk stems from substantial use of digital financial technology by relatively high-risk clients, including foreign financial institutions, nonbank financial institutions, third-party payment processors, cash-intensive businesses, nonresident aliens and accounts of foreign individuals, foreign corporations, and entities located in higher-risk geographic locations. See Federal Financial Institutions Examination Council, *Bank Secrecy Act Anti-Money Laundering Examination Manual*, Version 2 (2/27/2015), 19–22.

272. "Estimating Illicit Financial Flows Resulting from Drug Trafficking and Other Transnational Organized Crimes: Research Report" (UNODC, October 2011), 7, http://www.unodc.org/documents/data-and-analysis/Studies/Illicit_financial_flows_2011_web.pdf.

273. Keyes, "Challenges Faced When Auditing a Digital-currency Financial Institution," 7–9.

274. Juan C. Zarate and Chip Poncy, "Designing a New Anti-Money Laundering (AML) System," research memo (Center on Sanctions and Illicit Finance, September 2016), 11, http://www.defenddemocracy.org/content/uploads/documents/AML_System_memo.pdf.

275. Dennis M. Lormel, "How Terrorist Trends Evolve and How Financial Institutions Should Respond," *ACAMSToday*, March 7, 2016, http://www.acamstoday.org/how-terrorist-trends-evolve/.

276. Clare Ellis and Ines Sofie de Oliveira, "Tackling Money Laundering: Toward a New Model for Information Sharing," occasional paper (Royal United Services Institute for Defence and Security Studies, September 2015), 6, https://rusi.org/sites/default/files/201509_op_tackling_money_laundering.pdf.

277. "Stopping Terror Finance: Securing the U.S. Financial Sector," report prepared by the Staff of the Task Force to Investigate Terrorism Financing, Committee on Financial Services, U.S. House of Representatives, December 20, 2016, 36–39.

About the Center for a New American Security

The mission of the Center for a New American Security (CNAS) is to develop strong, pragmatic and principled national security and defense policies. Building on the expertise and experience of its staff and advisors, CNAS engages policymakers, experts and the public with innovative, fact-based research, ideas and analysis to shape and elevate the national security debate. A key part of our mission is to inform and prepare the national security leaders of today and tomorrow.

CNAS is located in Washington, and was established in February 2007 by co-founders Kurt M. Campbell and Michèle A. Flournoy.

CNAS is a 501(c)3 tax-exempt nonprofit organization. Its research is independent and non-partisan. CNAS does not take institutional positions on policy issues. Accordingly, all views, positions, and conclusions expressed in this publication should be understood to be solely those of the authors.

1152 15th Street, NW Suite 950 Washington, DC 20005
t. **202.457.9400** | f. **202.457.9401** | **info@cnas.org** | **cnas.org**