AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. Hrg. 113–516

BEYOND SILK ROAD: POTENTIAL RISKS, THREATS, AND PROMISES OF VIRTUAL CURRENCIES

HEARING

BEFORE THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

ONE HUNDRED THIRTEENTH CONGRESS

FIRST SESSION

NOVEMBER 18, 2013

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

Printed for the use of the
Committee on Homeland Security and Governmental Affairs

U.S. GOVERNMENT PRINTING OFFICE

86–636 PDF WASHINGTON : 2014

For sale by the Superintendent of Documents, U.S. Government Printing 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

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

THOMAS R. CARPER, Delaware *Chairman*

CARL LEVIN, Michigan
MARK L. PRYOR, Arkansas
MARY L. LANDRIEU, Louisiana
CLAIRE MCCASKILL, Missouri
JON TESTER, Montana
MARK BEGICH, Alaska
TAMMY BALDWIN, Wisconsin
HEIDI HEITKAMP, North Dakota

TOM COBURN, Oklahoma
JOHN MCCAIN, Arizona
RON JOHNSON, Wisconsin
ROB PORTMAN, Ohio
RAND PAUL, Kentucky
MICHAEL B. ENZI, Wyoming
KELLY AYOTTE, New Hampshire

RICHARD J. KESSLER, *Staff Director*
JOHN P. KILVINGTON, *Deputy Staff Director*
JOHN G. COLLINS, *Professional Staff Member*
MICHELLE C. TAYLOR, *Federal Bureau of Investigations Detailee*
KEITH B. ASHDOWN, *Minority Staff Director*
CHRISTOPHER J. BARKLEY, *Minority Deputy Staff Director*
WILLIAM H.W. MCKENNA, *Minority Investigative Counsel*
LAURA W. KILBRIDE, *Chief Clerk*
LAUREN M. CORCORAN, *Hearing Clerk*

CONTENTS

	Page
Opening statements:	
Senator Carper	1
Prepared statements:	
Senator Carper	45

WITNESSES

MONDAY, NOVEMBER 18, 2013

Jennifer Shasky Calvery, Director, Financial Crimes Enforcement Network, U.S. Department of the Treasury	4
Mythili Raman, Acting Assistant Attorney General, Criminal Division, U.S. Department of Justice	7
Edward W. Lowery, III, Special Agent in Charge, Criminal Investigative Division, U.S. Secret Service, U.S. Department of Homeland Security	9
Ernie Allen, President and Chief Executive Officer, The International Centre for Missing and Exploited Children	27
Patrick Murck, General Counsel, The Bitcoin Foundation, Inc.	29
Jeremy Allaire, Chairman and Chief Executive Officer, Circle Internet Financial, Inc.	31
Jerry Brito, Senior Research Fellow, The Mercatus Center, George Mason University	33

ALPHABETICAL LIST OF WITNESSES

Allaire, Jeremy:	
Testimony	31
Prepared statement	114
Allen, Ernie:	
Testimony	27
Prepared statement	78
Brito, Jerry:	
Testimony	33
Prepared statement	120
Lowery, Edward W., III:	
Testimony	9
Prepared statement	71
Murck, Patrick:	
Testimony	29
Prepared statement with attachment	90
Raman, Mythili:	
Testimony	7
Prepared statement	63
Shasky Calvery, Jennifer:	
Testimony	4
Prepared statement	48

APPENDIX

Statement submitted for the Record by U.S. Immigration and Customs Enforcement	146
Statement submitted for the Record by Sarah Meiklejohn, Ph.D. Candidate, University of California, San Diego	156
Responses to post-hearing questions for the Record:	
Ms. Shasky Calvery	160
Ms. Raman	165

Page

Responses to post-hearing questions for the Record—Continued
Mr. Lowery 171
Mr. Allen 176
Mr. Murck 184
Mr. Allaire 191
Mr. Brito 195

BEYOND SILK ROAD:
POTENTIAL RISKS, THREATS, AND PROMISES OF VIRTUAL CURRENCIES

MONDAY, NOVEMBER 18, 2013

COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS,
Washington, DC.

The Committee met, pursuant to notice, at 3:02 p.m., in room SD–342, Dirksen Senate Office Building, Hon. Thomas R. Carper, Chairman of the Committee, presiding.

Present: Senator Carper.

OPENING STATEMENT OF CHAIRMAN CARPER

Chairman CARPER. Well, good afternoon, everyone. Thank you for joining us. We especially want to thank our witnesses, panel number one and, somewhere out in the audience, panel number two. Mr. Lowery just lost his name plate there. Somebody just go around and pick it up please and put it where it belongs. That way we will know who you are.

Senator Bill Roth, whom I succeeded here in the U.S. Senate, used to say, many years ago—his advice was, "Wear a big button when you are campaigning so that you will remember your name and so will other people." So we want to make sure people remember your name.

Over the past several months, this Committee has engaged in an investigation into the potential implications of virtual currencies. During the course of this inquiry, we have examined the issues and potential risks and threats that virtual currencies pose, as well as some of the potential promises that some believe they can bring.

In addition, we have explored with several departments and agencies throughout our Federal Government how they are approaching virtual currencies as an emerging technology. This has included looking at how they are coordinating together to develop a "whole of government" approach that is consistent and informed.

Virtual currencies, perhaps most notably Bitcoin, have captured the imagination of some, struck fear among others, and confused the heck out of the rest of us, including me. Indeed, based on conversations that my staff and I have had with dozens—maybe more—of individuals both inside and outside of government, it is clear that the knowledge and expectation gaps are wide. Fundamental questions remain about what a virtual currency actually is, how it should be treated, and what the future holds.

Virtual currency can best be described as digital cash. It is generated by computers, lives on the Internet, and can be used to purchase real and digital goods across the world.

Some proponents believe that digital currencies can prove valuable to those in developing countries without access to stable financial systems. Others believe it could prove to be a next generation payment system for retailers both online and in the real world.

At the same time, however, virtual currencies can be an effective tool for those looking to launder money, for those looking to traffic illegal drugs, for those looking to exploit children around the world, and the list goes on.

While virtual currencies have seen increased attention from regulators, law enforcement, investors, and entrepreneurs in recent months, there are still many unanswered questions and unresolved issues.

This is not the first time that advances in technology have posed challenging questions, challenging issues for policymakers and for society as a whole. As we know, technology is dynamic and changes quickly. Concepts like e-mail and even the Internet itself were once alien and difficult to understand and navigate. Now, most of us can read and respond to e-mail on a device we keep in a purse or coat pocket and search the Web on multiple platforms.

I like to use the example that when I first showed up for duty here in the U.S. Senate in 2001, for every e-mail that came in to us from constituents from Delaware and across the country—for every e-mail we received probably 10 to 15 letters. I asked my staff a couple of months ago to tell me if that ratio had changed, and now for every 12 or 13 e-mails we get, we get 1 letter. And that is probably a pretty good metaphor for the situation.

I will be the first to admit that, like most Americans, I am no technical expert in virtual currencies. I think all of you who are gathered in this room are. We will see. But hopefully some of our panelists are those experts, and we hope to learn a lot from you today. What I do know is that a number of smart people both inside and outside of government view this as a major emerging issue that is deserving of our attention, and that includes this Committee's attention.

The ability to send and receive money over the Internet, nearly anonymously, without a third party, has a lot of wide-ranging implications. Our government needs to pay attention to this technology and to understand and, where appropriate, address these implications.

This was made all the more clear last month when Federal law enforcement took down and seized an online marketplace called the "Silk Road" on which many illegal products and services were bought and sold via Bitcoin. The most popular products for sale were illegal drugs and forged documents, such as identifications (IDs) and passports. Other services were also for sale, including hacking services. We are told that approximately $1.2 billion in transactions were made through the Silk Road.

This site lived on what is often called the "Dark Web," also known as the "Deep Web." The Dark Web consists of web pages and data that are only available via special software that keeps users anonymous. Many sites and data on the Dark Web have been

deliberately built to be untraceable in order to protect the anonymity of the user, and Silk Road was one of those sites.

My understanding is that individuals could navigate to Silk Road anonymously and use Bitcoin, which can be sent to someone nearly anonymously, to make purchases.

The anonymity of the marketplace and near anonymity of the currency made it nearly impossible for law enforcement to track and, therefore, made it an attractive place for criminal activity.

In fact, in the course of our investigation, the Department of Homeland Security (DHS) informed us that the suspect who allegedly sent ricin to President Obama in April of this year was also a vendor on Silk Road.

Law enforcement, including the Federal Bureau of Investigation (FBI), Immigration and Customs Enforcement (ICE), and the Secret Service, should be applauded for their work in taking down a major international criminal enterprise.

But while Silk Road was perhaps the most well known, it is not the only marketplace where illicit goods are bought and sold through Bitcoin transactions. Today a number of similar enterprises that accept Bitcoins are still in business, selling weapons, child pornography, and even murder-for-hire services.

While today I suspect we will talk a lot about the well-known virtual currency Bitcoin, there are numerous other virtual currencies operating on the Internet today, each with its own set of specific features.

That said, whether it is Bitcoin or any of the other virtual currencies, the Federal Government and society as a whole need to come together to figure out how to effectively deal with it.

Whether or not digital currencies prove to be a boom or a bust, I think it is clear that some folks just want a chance to try and play by the rules. That is difficult to do if the rules or proper authorities are not clear or if the future is uncertain. It is also difficult if a large number of bad apples are allowed to spoil the bunch.

With that, normally I would turn to my right, and I would say, "Dr. Coburn, you are recognized for whatever comments you would like to offer." I believe he is traveling back from Oklahoma. I hope he will be able to join us at some point during this hearing, and that others of our colleagues will, too. We start voting at 5:30, and what usually happens on Monday afternoons is Senators are coming in from all over the country, and they will drift in and out of hearings like this one. And my hope is that before we are done, a number of them will be able to join us.

I want to take now just a moment, if I can, to welcome and introduce just very briefly our first panel of distinguished witnesses.

On our first panel, our first witness, in fact, the lead-off hitter, is Jennifer Shasky Calvery, Director of the Financial Crimes Enforcement Network (FinCEN), a bureau of the Treasury Department. As Director of FinCEN, Ms. Shasky Calvery—do you go by both names?

Ms. SHASKY CALVERY. Typically just "Shasky."

Chairman CARPER. OK. All right. As Director of FinCEN, Ms. Shasky oversees the protection of U.S. financial systems from money laundering and other forms of illicit financial activity. Prior

to joining Treasury, Director Shasky, served as the Chief of the Asset Forfeiture and Money Laundering Section at the Department of Justice (DOJ).

Our second witness has a name I have never heard before, and her first name is Mythili, right? Sort of rhymes with "mightily," right? Mythili Raman. Do I have that right? Good. Has your name ever been mispronounced?

Ms. RAMAN. Many times.

Chairman CARPER. Today. [Laughter.]

Ms. RAMAN. Not today.

Chairman CARPER. Oh, good. We will try to keep it that way.

Ms. Raman is Acting Assistant Attorney General for the Department of Justice Criminal Division. As head of the Criminal Division, Ms. Raman oversees nearly 600 attorneys who prosecute Federal criminal cases across our country. Prior to joining the Criminal Division, Ms. Raman served for nearly a decade as an Assistant U.S. Attorney for the District of Columbia, our neighbor.

Our final witness on this panel is Edward Lowery. Mr. Lowery is a Special Agent in Charge of the Criminal Investigative Division at the Secret Service. Mr. Lowery began his career with the Secret Service in 1992 and has been in his current position since February 2012. In this position, Mr. Lowery directs and coordinates all investigative activities of the agency and the daily operation of the Secret Service investigative offices located throughout the world. Previously Mr. Lowery established and ran the Secret Service's Cyber Protective Initiative and coordinated operations of the Cyber Investigations Branch and the Cyber Intelligence Section.

Again, we want to thank all of you for your service. We thank you for your preparation for today, for your testimony, and for your willingness to respond to the questions that will be asked of you here and some that will be asked in writing subsequent to this hearing.

With that, Director Shasky, you are recognized. And I do not know how long they told you you had to give your testimony. What did we say? Seven minutes, but you can go a little longer than that. If you go way beyond that, we will have to draw it to a close. But you are recognized. Just know that for you and the other witnesses, your entire statement will be made a part of the record. Please proceed.

TESTIMONY OF JENNIFER SHASKY CALVERY,[1] DIRECTOR, FINANCIAL CRIMES ENFORCEMENT NETWORK, U.S. DEPARTMENT OF THE TREASURY

Ms. SHASKY. Thank you. Good afternoon, Chairman Carper.

Chairman CARPER. Good afternoon.

Ms. SHASKY. As you mentioned, I am Jennifer Shasky Calvery, the Director of the Financial Crimes Enforcement Network, and I am pleased to be here today to discuss the important regulatory, enforcement, and analytical work we are doing at FinCEN to prevent illicit actors from exploiting the U.S. financial system as technological advances such as virtual currency create new ways to move money.

[1] The prepared statement of Ms. Shasky appears in the Appendix on page 48.

FinCEN's mission is to safeguard the financial system from illicit use, combat money laundering, and promote national security through the collection, analysis, and dissemination of financial intelligence and the strategic use of financial authorities. We work to achieve this mission by administering the Bank Secrecy Act (BSA), this country's primary anti-money laundering/counterterrorist financing (AML/CFT) regulatory regime; by sharing the financial intelligence we collect, as well as our analysis and expertise, with law enforcement and regulatory partners; and, by building global cooperation amongst financial intelligence units throughout the world.

Recognizing the emergence of new payment methods, the potential for abuse by illicit actors, and understanding that AML protections must keep pace with these advancements in technology, FinCEN began working with our partners several years ago to study this issue. Here is what we learned.

Illicit actors might decide to use a virtual currency to store and transfer value for many of the same reasons as legitimate users, but also for some more nefarious ones. Specifically an illicit actor may choose to use virtual currency because it enables the user to remain relatively anonymous, is easy to navigate, may have low fees, is accessible across the globe with a simple Internet connection, can be used to both store and make international transfers of value, does not typically have transaction limits, is generally secure, features irrevocable transactions, and depending on the system may have been created with the intent to facilitate money laundering; and, finally provides a loophole from AML/CFT regulatory safeguards in most countries around the world.

Indeed, the idea that illicit actors might exploit the vulnerabilities of virtual currency to launder money is not merely theoretical. Liberty Reserve—a virtual currency administrator—engaged in a $6 billion money-laundering operation facilitating credit card fraud, identity theft, investment fraud, computer hacking, narcotics trafficking, and child pornography. And just recently, the Department of Justice alleged that customers of Silk Road, the largest illegal drug and contraband marketplace on the Internet, were required to pay in Bitcoins to enable both the operator of Silk Road and its sellers to evade detection and launder hundreds of millions of dollars.

That being said, it is also important to put virtual currency in perspective. It has been publicly reported that Bitcoin processed transactions worth approximately $8 billion over the last year; whereas, the best estimate for the amount of criminal proceeds available for laundering throughout the financial system, at least in 2009, was $1.6 trillion.

By way of comparison, in 2012 PayPal processed $145 billion in online payments, Western Union made remittances totaling $81 billion, and Bank of America made $245 trillion in wire transfers. Thus, while of growing concern, to date virtual currencies have yet to overtake more traditional methods to move funds, whether for legitimate or criminal purposes.

Nonetheless, to address growing concerns, in July 2011, after a public comment period designed to receive feedback from industry, FinCEN released two regulations which update several definitions

and provide the needed flexibility to accommodate innovation in the payment system space, including virtual currencies, under our pre-existing regulatory framework. Then this last March, as a followup to the regulations, FinCEN issued additional guidance to further clarify the compliance obligations for those virtual currency actors covered by our regulations.

In short, they are required to register with FinCEN, put AML controls in place to harden themselves as targets, and provide certain reports to FinCEN on suspicious and other activity. It is in the best interest of virtual currency providers to comply with these regulations for a number of reasons.

First is the idea of corporate responsibility. Legitimate financial institutions do not go into business with the aim of laundering money on behalf of criminals. Any financial institution could be exploited for money-laundering purposes, though. What is important is for institutions to put controls in place to deal with those money-laundering threats and to meet their AML reporting obligations.

At the same time, being a good corporate citizen and complying with regulatory responsibilities is good for a company's bottom line. Every financial institution needs to be concerned about its reputation and show that it is operating with transparency and integrity within the bounds of the law. Legitimate customers will be drawn to a virtual currency or administrator or exchanger where they know their money is safe and where they know the company has a reputation for integrity. And banks will want to provide services to administrators or exchangers that show not only great innovation, but also great integrity and transparency.

The decision to bring virtual currency within the scope of our regulatory framework should be viewed as a positive development for this sector. It recognizes the innovation virtual currencies provide, and the benefits they might offer society. Several new payment methods in the financial sector have proven their capacity to empower customers and expand access to financial services. We want such advances to continue. However, those institutions that choose to act outside of the law will be held accountable. FinCEN will do everything in its regulatory power to stop abuses of the U.S. financial system.

We have proven our willingness to do just that by using our targeted financial measures under Section 311 of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) to name Liberty Reserve as a primary money-laundering concern and entering into rulemaking to terminate its access to the U.S. financial system. We stand ready to take additional regulatory actions as necessary to stop other abuses.

As the financial intelligence unit for the United States, FinCEN must stay current on how money is being laundered in the United States so that we can share this expertise with our many law enforcement, regulatory, industry, and foreign partners and effectively serve as the cornerstone of this country's AML/CFT regime. We are meeting this obligation in the virtual currency space as we continue to deliver cutting-edge analytical products to inform the actions of our many partners. We are committed to remaining at the forefront of developments in the days and years to come.

The administration has made appropriate oversight of the virtual currency industry a priority, and FinCEN is very encouraged by the progress we have made thus far.

Thank you for inviting me to testify before you today. I would be happy to answer any questions that you may have.

Chairman CARPER. Thank you so much for being here, for the meeting you had with our staff and me last week, and for your testimony. Thank you.

Ms. Raman, please proceed.

TESTIMONY OF MYTHILI RAMAN,[1] ACTING ASSISTANT ATTORNEY GENERAL, CRIMINAL DIVISION, U.S. DEPARTMENT OF JUSTICE

Ms. RAMAN. Good afternoon, Chairman Carper, and thank you for the opportunity to appear before the Committee today to discuss the Department of Justice's work regarding virtual currencies.

At the Justice Department, we look at virtual currencies through the lens of criminal law enforcement. We recognize that virtual currency systems can be a legal means of exchange. But we also recognize that criminals will always seek to take advantage of new technologies to commit, further, or hide their crimes.

Our responsibility as prosecutors is to ensure that we continue to enforce the law, even in new technological settings, and to prevent criminals from using those technologies to create zones of impunity.

As I will describe in my testimony today, the Department of Justice has been aware of the threat posed by the criminal use of virtual currencies for several years. We have already brought several important prosecutions involving virtual currencies, and we intend to remain vigilant in ensuring that any criminal use of virtual currency systems is aggressively investigated and prosecuted.

As an initial matter, I should note that virtual currency systems, so long as they comply with applicable anti-money laundering and money transmission laws and regulations, are not inherently illegal, and they can be appealing to consumers because they can provide cheap, efficient, and convenient means to transfer currency.

Many of those same features, however, also make virtual currencies appealing to criminals. We have seen increasing use of such currencies by drug dealers, traffickers of child pornography, and perpetrators of large-scale fraud schemes. Most significantly, we have seen evidence that criminals are drawn to virtual currencies for two main reasons: first, their perception that virtual currencies offer greater anonymity than traditional financial services; and, second, the irreversibility of many virtual currency transactions. These features can significantly complicate our ability to utilize one of the most basic techniques we use in criminal investigations: following the money.

The Justice Department has long recognized the potential for the criminal misuse of virtual currency and launched our first major prosecution of an illicit virtual currency service in 2007, when we indicted e-Gold and its three principal owners on charges relating

[1] The prepared statement of Ms. Raman appears in the Appendix on page 63.

to money laundering and operating an unlicensed money transmitting business.

As that indictment alleged, the only information a customer had to provide to set up an e-Gold account was a working e-mail address. As a result, e-Gold became a popular payment method for sellers of child pornography, operators of investment scams, and perpetrators of credit card and identity fraud. At its peak, e-Gold reportedly moved over $6 million a day. E-Gold and its owners were convicted in 2008.

Since that time, we have continued to ensure that we aggressively address any criminal misuse of virtual currency systems, especially as those systems evolve and develop. When virtual currency systems fail to live up to their obligations under existing law, we take action. Earlier this year, for example, we unsealed charges against Liberty Reserve, an offshore virtual currency business, for allegedly running a $6 billion money laundering operation, the Justice Department's largest ever money laundering prosecution.

As alleged in the Department's filings, Liberty Reserve became a system of choice for cyber criminals and was used in a wide array of illegal activity, including credit card fraud, identity theft, investment fraud, computer hacking, and the trade of child pornography.

As a result of the Department's actions and the coordination actions taken by law enforcement agencies in 17 countries around the world, Liberty Reserve was effectively put out of business, seven defendants were charged, and numerous assets were seized. One of the defendants pleaded guilty just 2 weeks ago.

More recently, the Department announced significant steps in its investigation of Silk Road, alleged to be one of the largest online marketplaces for illegal goods and services, including large quantities of illicit drugs. Allegedly operated by a U.S. citizen living in California at the time of his arrest, Silk Road accepted Bitcoins exclusively as a payment mechanism on its site. Charges against Silk Road and its administrator were unsealed just last month in two different districts. The charges against Silk Road's operator included drug distribution, attempted witness murder, and attempted murder for hire. As part of that takedown of Silk Road, the Department seized over 170,000 Bitcoins valued as of this past Friday at over $70 million.

The Department recognizes that in order to stay abreast of the rapidly changing technological environment, we must coordinate our enforcement strategy across the Federal Government. For that reason, we are working closely with the Virtual Currency Emerging Threats Working Group, a variety of law enforcement agencies both here and abroad, and, of course, FinCEN.

From the view of law enforcement, FinCEN's recent guidance applying anti-money laundering and Know Your Customer requirements to virtual currency exchanges was an important step in safeguarding our collective ability both to deter criminal activity and to investigate it successfully when it occurs.

While there is much more to do, the Department is encouraged by virtual currency services that are attempting to comply with U.S. law. We will continue to reach out to those services and provide them with training and other opportunities for real discussion

about emerging threats, as we have long done with other financial services industry participants.

As the virtual currency industry grows, we will continue to explore how new strategies or legislation can play a role in ensuring that virtual currency systems do not become a haven for criminal activity. We look forward to working with Congress to ensure that law enforcement continues to have the tools necessary to enforce the law and protect the public.

In the meantime, we will continue to aggressively use our existing authorities to deal with those virtual currency systems that do not comply with the law and to aggressively prosecute criminals who use those systems as part of their criminal schemes. And, of course, we will continue to innovate in how we investigate crime to deal with whatever changes may come.

Thank you for the opportunity to discuss the Department's work in this area, and I look forward to answering any questions you might have.

Chairman CARPER. We look forward to asking some questions. We very much appreciate your testimony and thank you for joining us today.

Ms. RAMAN. Thank you.

Chairman CARPER. Mr. Lowery, you are recognized. Please proceed.

TESTIMONY OF EDWARD W. LOWERY III,[1] SPECIAL AGENT IN CHARGE, CRIMINAL INVESTIGATIVE DIVISION, U.S. SECRET SERVICE, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. LOWERY. Good afternoon, Chairman Carper. Thank you for the opportunity to testify on behalf of the Department of Homeland Security regarding the risks and challenges posed by digital currencies and the role of the United States Secret Service in investigating crimes associated with online payment systems.

Digital currencies have developed and grown over the last 17 years as part of the continuing integration of information technology (IT) into the financial system. As the original guardians of the Nation's financial payment systems since 1865, the Secret Service has continually adapted its investigative methods to keep pace with the evolving use of information technology within the financial system.

Since the founding of e-Gold in 1996, both digital currencies and various Internet-based payment processors and exchangers have grown to be a significant participant in the global financial system, processing tens to hundreds of billions of dollars annually in total transaction volume.

Criminals and other illicit organizations use digital currency. These groups seek out those digital currency exchangers and providers that best enable them to conceal their illicit activities. For example, Liberty Reserve is alleged to have laundered more than $6 billion during its operation before the Secret Service's joint investigation with ICE and the Internal Revenue Service (IRS) Criminal Investigations dismantled it.

[1] The prepared statement of Mr. Lowery appears in the Appendix on page 71.

The growth of digital currencies and Internet-based payment systems is expected to continue for the foreseeable future, along with the use of these systems in the conduct of criminal activity.

DHS law enforcement approaches digital currencies within the context of its authorities to investigate criminal activity. As a result of Secret Service and ICE investigations, exchangers of digital currency have been charged and convicted without operating unlicensed money-transmitting businesses in violation of 18 U.S.C. 1960 and various State laws.

Additionally, as a result of our investigations, digital currency providers have been charged and convicted for money laundering in violation of 18 U.S.C. 1956 and 1957. As FinCEN emphasized in March of this year, digital currency administrators and exchangers have legal responsibilities under various anti-money laundering laws, Title III of the PATRIOT Act, the Bank Secrecy Act, and FinCEN regulations.

DHS law enforcement works closely with interagency, State, local, and international partners in conducting criminal investigations in their respective jurisdictions that may involve the use of digital currencies, including their use for money laundering purposes.

In particular, as one of the two Federal law enforcement agencies with authority to investigate computer intrusions in violation of 18 U.S.C. 1030, one of the Secret Service's strategic priorities is proactively investigating transnational organized cyber crime and defeating these illicit organizations by arresting their members and seizing and dismantling their criminal infrastructure. The Secret Service has successfully investigated and arrested numerous leaders of major cyber crime operations.

For example, the service arrested Vladislav Horohorin, also known as "BadB," in 2010, and earlier this year apprehended five individuals allegedly responsible for the largest data breach ever prosecuted in U.S. history. Over the past 4 years, the Secret Service has arrested more than 4,500 cyber criminals, preventing over $13 billion in losses based on the financial information recovered from those criminals.

Importantly, many of these cyber criminals made extensive use of digital currencies as part of their illicit activities.

As part of its efforts to disrupt and defeat organized cyber crime, the Secret Service strategically prioritizes investigations of exchangers and administrators of digital currency that perform a substantial criminal role in facilitating widespread illicit activity. As part of these efforts, the Secret Service, in cooperation with other law enforcement agencies and interagency partners, has apprehended the providers of both e-Gold and Liberty Reserve, ending their operations.

The Secret Service has also arrested various illicit exchangers of digital currency that facilitated criminal activity such as Western Express, Incorporated, which was prosecuted by the Manhattan district attorney's office, resulting in 16 individuals pleading guilty or being convicted. These cases are discussed more fully in my written testimony, and I welcome future opportunities to further discuss our investigative work with you and your staff.

Digital currencies are a tool used by a wide variety of criminals. Accordingly, numerous law enforcement agencies investigate illicit activity that involves the use of digital currencies. Through the Secret Service's nationwide network of Electronic Crime Task Forces, Federal, State, and local law enforcement collaborate with the private sector and academia to effectively address the challenges that criminals' use of information technology, including digital currency, pose to law enforcement at all levels of government. Additionally, the Secret Service and ICE are participating agencies in FinCEN and work closely with them to ensure regulatory and enforcement activities are coordinated, and like all Federal law enforcement, the success of Secret Service investigations requires partnering with the U.S. Attorneys throughout the country, in addition to the Asset Forfeiture and Money Laundering and Computer Crime and Intellectual Property Sections of the Department of Justice's Criminal Division.

The Secret Service and ICE also partner with other Federal law enforcement for joint investigations and participate in the Virtual Currency Emerging Threats Working Group.

While digital currencies may provide potential benefits, they present real risks through their use by the criminal and terrorist organizations trying to conceal their illicit activity. As such, digital currencies challenge law enforcement's ability to carry out our responsibilities to enforce the law and suppress criminal activity. The Secret Service has a long history of adapting its investigative methods to maintain the integrity of the Nation's financial infrastructure. As a DHS law enforcement agency, we are committed to partnering with law enforcement at all levels of government to increase the security of the Nation while addressing the challenges posed by digital currencies. The Secret Service will continue to conduct effective criminal investigations to keep America safe and prosperous.

Thank you for the opportunity to testify on this important topic, and I look forward to your questions.

Chairman CARPER. Mr. Lowery, thank you so much and, again, our thanks to each of you for your testimony and your preparation today.

In anticipation of this hearing, a week or two ago I was trying to get my head around this subject, and I asked my staff to talk to me about the early days of the Internet, and how there were a number of concerns raised about how it might foster or facilitate illegal activities. But there were some who said there could be a lot of benefit here as well. And I asked them if that was maybe an analogy that was applicable here for virtual currencies.

Just walk us back in time, if you will, to the early days of the Internet when you guys were in middle school, or before that, and talk to us about some of the early concerns that we had with this criminal activity that can flow through the Internet. At that time, we never imagined we would have the kind of commercial activity that we are going to see in the coming month as people celebrate the holiday season and a lot of commerce that takes place over the Internet, a lot of presents sent using the Internet.

We never imagined anything like YouTube, Wikipedia, or Google searches. It is pretty amazing what it has become, the ability to

download a music video, although in the early days I recall hearing a number of concerns about the bad that could flow from the Internet.

Is this a good corollary or not? And if so, how? And if not, why not? And we will just start with you, Ms. Shasky, please.

Ms. SHASKY. Senator, I believe your analogy is an apt one. So often, when there is a new type of financial service or a new player in the financial industry, the first reaction by those of us who are concerned about money laundering or terrorist finance is to think about the gaps and the vulnerabilities that it creates in the financial system and how illicit actors will take advantage of those vulnerabilities or gaps.

But it is also important that we step back and recognize that innovation is a very important part of our economy. It is very important in this country. It is something that we are known for and proud of and want to continue. So I think the challenge, at least at FinCEN, is for us to balance and have smart regulation that both mitigates the concerns of illicit actors operating in our financial system while at the same time minimizing the burden as much as we can. We believe that we have done just that with this rule by clarifying that virtual currency exchangers and administrators fit within our pre-existing regulatory regime.

Chairman CARPER. All right. Thank you.

Ms. Raman, same question. Walk us back in time: early concerns, those that were realized, and then some of the potential that may have come along through the Internet that perhaps we never envisioned. And does that apply here? That example, is that appropriate here?

Ms. RAMAN. I think as I alluded to in my written testimony, as emerging technologies develop and change, as law enforcement we remain attuned to the criminal misuse of those technologies. But, of course, as you describe it, there are many legitimate uses. And as I hope I have also made clear in my testimony, these virtual currency services are not in and of themselves illegal so long as they comply with our applicable money laundering laws and our money transmission laws and regulations.

And so I think it is our duty as law enforcement to stay vigilant about the criminal misuse of those virtual currency systems while recognizing that, of course, there are many legitimate users of those services.

Our experience over the last several years has showed us that there is reason for our vigilance and there is good reason for us to remain vigilant. Liberty Reserve was the largest money laundering case ever brought by the Department of Justice, and that is an important fact. And it reminds us that there is good reason for us to remain watchful, an we intend to do that. But we also intend to balance that against the need for legitimate users to use those virtual currency systems as they were intended to.

Chairman CARPER. All right. Thank you, ma'am.

Mr. Lowery, same question, please.

Mr. LOWERY. Within the confines of the Secret Service investigations, the Secret Service was enacted to fight counterfeiting at the time in 1865. In the Secret Service, the hallmark of our investigations has always been adapting to the changing threat. As I said,

we started with counterfeiting. We moved into fraud, always defending the Nation's financial infrastructure. In the 1980s, it was access to device fraud when credit cards were starting to become a major impact on the financial system, and it naturally segued directly into computer crimes.

In recognition of that fact, as I mentioned in my testimony, the Electronic Crimes Task Force model is widely respected throughout the country, and it is the way that the Service stays in tune with the changing technology and the threats that can come from the Internet.

Chairman CARPER. All right. A couple of years ago, there was a film out called "Dillinger," and my wife, who is usually not a big fan of gangster movies, and I went to a local theater complex in Delaware, and one of films showing was "Dillinger." She said, "Let us go see that." I said, "OK." And I will never forget one of the scenes in the film, Dillinger and his gang, they made their living robbing banks, as you know, shooting people up and getting away with it. Near the latter part of the film, they were on the run, and Dillinger looked up one of his old compadres in the bank-robbing business to see if he could not give him a hand. And I remember they met, and it looked like the top floor of a big old warehouse that had been retrofitted, and he walked in, and there were all these guys, a lot of them wearing shirts and ties, on old phones making phone calls. And Dillinger said, you know, "What is going on here?" And apparently it was a bookie operation, numbers operations and so forth, and the fellow who was running the operation said, "We do not rob banks anymore." And he said, "You are stupid to do that. This is the future." He said, "This is the future for criminal activity, the way to make money."

And I suspect for some people they see this as the future for them to make money through criminal activity, whether it is in pornography, child pornography, whether it is in money laundering, human trafficking, any number of activities.

But we figured out how to deal with those guys in that film, wearing their shirts and ties and doing illegal activities, not robbing banks anymore, not certain people anymore. We figured out how to deal with that.

How confident are you that we are going to be able to deal with the potential criminal behavior, misbehavior, with this new technology that is before us? Mr. Lowery. And the second part, what role does the legislative body—we have three branches of government, but what role does the legislative body—those of us who sit in these seats, what role do we have to play to make sure you have the resources that you need to meet the dark side of this technology?

Mr. LOWERY. Well, again, going back to my testimony, the Secret Service has investigated many first-of-their-kind investigations. We specialize currently in the transnational cyber criminal, the professional criminal that is targeting our financial infrastructure. We operate within the confines of the laws that we are entrusted to enforce, predominantly 1028, 1029, and 1030, which would be access to the device fraud, identity theft, and computer hacking.

You spoke earlier about the change, how the crimes have changed. I believe that one of the largest changes is the reach of

the criminal. It used to be that we had to worry about—back in the days of early access to device fraud, we had to worry about someone dumpster diving or trying to get an actual image of your credit card. Today anyone in the world can reach anyone else in the world, and that has changed how we have to enforce our laws.

Again, we are consistently, aggressively, and strategically investigating, trying to direct our investigations to the highest impact within the confines of the existing laws, which I believe there are plenty of cyber criminals in prison right now who would agree we are pretty effective.

Chairman CARPER. The second half of my question, and I would ask you to respond to it, and then we will turn to Ms. Raman. But the three branches of government—Judicial, Executive, Legislative—the role that we are attempting to play today on this Committee is not just an oversight role, although this is a Homeland Security and Governmental Affairs Committee, we historically do oversight and have for many decades. The Homeland Security piece of this Committee is actually newer. It is only about 10 years old. But we have a role for oversight. We also have, I think, an obligation or an opportunity here to try to make sure that the Administration is working, maybe with local law enforcement agencies across the country, but that they are working in a cohesive, collaborative manner. And I am encouraged to see that that might be the case. But what advice would you have for us on the legislative side? How can we be supportive and better enable you to do your very difficult work as this new technology appears before us?

Mr. LOWERY. Well, I believe it goes back to—the most important part of being able to do this job is the hiring, developing, and retaining of a highly qualified workforce. Obviously you need a technically gifted investigator to follow the trail and to run these international criminals down. So that is always a challenge, especially given the current fiscal environment. Any support in that realm is definitely appreciated.

Chairman CARPER. All right. Thank you. Ms. Raman.

Ms. RAMAN. Your first question was whether we can keep up with the changing technology, and I do think that law enforcement has proven itself to be nimble and aggressive and willing to work together, and not only with agencies here in the United States but abroad, in order to effectively combat the threat.

I mentioned Liberty Reserve before, but it is an excellent example of how our agencies have worked together to take down an enormous money laundering operation. We worked together with FinCEN and Treasury. They took coordinated action. At the same time that law enforcement made arrests here and abroad, we had 17 other countries working with us for coordinated arrests and takedowns. We seized assets on the same day that arrests were made, and we took down domain names on the same day that arrests were made.

So I do think we are nimble enough and creative enough and aggressive enough to be able to combat the threat. That does not mean that we are not unaware of the challenges that are posed by virtual currency, and there are specific challenges that are inherent to virtual currencies that we are remaining attuned to. Anonymity is certainly one that we are paying attention to. The fact that some

virtual currency services may be based in countries that have laxer regulatory oversight is of concern to us. There are issues with difficulty in obtaining customer records and a host of other difficulties and challenges that go along with investigating global organizations, but I think as our track record shows, we are up to the challenge, and we are continuing to work together to ensure that we are innovating as criminals are innovating, and that we stay one step ahead of them.

As for what the Legislative Branch can do, I think as for our criminal statutes, we feel confident that the statutes that we have available to us, our money laundering statutes, our money transmitter statutes, are broad enough to encompass the activity that we have been talking about this afternoon, and, in fact, those statutes are the ones that we used in e-Gold and Liberty Reserve, for example. And, of course, to the extent that criminals are using virtual currencies as part of their criminal enterprises, the actual substantive criminal statutes are also applicable. For example, if a child exploitation enterprise is trading child pornographic images in virtual currency, we should be able to charge that under traditional child exploitation statutes. And so we feel confident that the statutes that we have on the books are flexible enough to meet our needs.

That having been said, we are always looking for ways to close any gaps that might arise or to close any gaps that we might see that we are not seeing right now. And we would be happy to work, continue to work with you and your staff to ensure that we let you know whenever we need those legislative tools.

Chairman CARPER. All right. Thank you.

Ms. Shasky, would you respond to that question as well, please?

Ms. SHASKY. Sure.

Chairman CARPER. Actually, the two questions.

Ms. SHASKY. Thankfully, Congress' actions in passing the Bank Secrecy Act and the USA PATRIOT Act have already given us a strong platform to meet the challenge. So we are confident that we can meet this challenge, at least in the first instance, using that platform. So the Bank Secrecy Act, of course, is this country's anti-money laundering and counterterrorist financing backbone, which we administer at FinCEN. We issue the regulations under that.

In 2011, when we expanded some of our definitions to enable us to have flexibility in going after new payment systems, our hope was that these regulations would live with changes in the market. What we found is that it has done just that. So as virtual currency has come more strongly to the forefront over the last year or 2 years, that definition has been broad enough for us to encompass virtual currency administrators and exchangers in our pre-existing regulations under the Bank Secrecy Act.

And then with the USA PATRIOT Act, Section 311 of that, that is the section that gives us the authority at FinCEN to name a foreign financial institution as being of primary money laundering concern and to cut it off from the U.S. financial system, and that is exactly the provision we used to confront Liberty Exchange, that targeted financial authority provided to us by Congress.

So we feel like we have a pretty good basis on which to act already, but it is hard to predict where the financial system is going

to go and what tools we might need next, and we would be very thankful to continue that conversation with Congress to see if any additional tools might be better.

Chairman CARPER. OK. Thank you. In your testimony, Ms. Shasky, you said on page 11, I think, of your original testimony—I will just read a couple of sentences from it, if I could. You said, "Several new payment methods in the financial sector have proven their capacity to empower customers, encourage the development of innovative financial products, and expand access to financial services." And you went on to say, "We want these advances to continue."

And then you said, "However, those institutions that choose to act outside of their AML obligations and outside of the law have and will continue to be held accountable. FinCEN will do everything in its regulatory power to stop such abuses of the U.S. financial system."

Now, when you talked about several new payment methods in the financial sector that have proven their capacity to empower customers and encourage the development of innovative financial products, maybe expand access to financial services, this is the bright line in this technology of virtual currencies. Just maybe give us some examples, some concrete examples, if you will, of how those have worked out for the good.

Ms. SHASKY. Sure. I think the one that comes first to mind is prepaid access cards. Another area where we have thought not only about the illicit—the risks from illicit actors but also the benefits that it can offer to consumers. And we have seen many of the unbanked use prepaid cards to gain their initial access to the U.S. financial system, and many might argue that that has been a positive for society.

In my own personal experience, I think of online banking and the changes that has brought about for me as a consumer and the idea of automated clearing house (ACH) where I can now take a picture of a check and deposit it into my account. Some of these technological advances make things easier for the consumer, and so those would be examples that come to mind.

But with each of these, we needed to think in the early days as they came to market how might criminals use these systems, how might they exploit systems, because the fact is any financial service, any type of financial institution can be exploited. Cash is probably still the best medium for laundering money, but the important thing is to put measures in place that mitigate that risk.

Chairman CARPER. All right. I am going to ask each of you to take a shot at this question. We have already addressed it to some extent, but I want to come back and dive a little deeper, if we could.

The question that I want to get to and I want to come back to is whether or not you think that virtual currencies, that would include Bitcoin—fit into our current legal and regulatory framework. And we talked a little bit about this and explored it in the last question, but come back to me, if you will, with some further thoughts on whether you see any gaps in our statutes, any gaps in our regulations regarding virtual currencies. So that is part of the question.

The second half of the question, is which agencies do you believe need to be at the forefront of the Federal Government's work on virtual currencies? Two questions. And, Mr. Lowery, if you feel up to taking this one first, that would be fine.

Mr. LOWERY. Thank you. So is virtual currency within the existing legal framework? I know obviously, Bitcoin is the currency that is part of this discussion today. I can speak within the framework of the Secret Service investigations and what we see out there, and I think it is important to recognize that within what we see in our investigations, that the online cyber criminals, the high-level international cyber criminals that we are talking about have not, by and large, gravitated toward the peer-to-peer crypto-currencies such as Bitcoin. Again, this is within the confines of what we have dealt with.

The Eastern European cyber criminals that we have developed a specialty in have, by and large, gravitated toward a centralized digital currency that is, as my colleague discussed earlier, based in a locale that may have less regulatory guidelines, and may have less aggressive law enforcement. So that is a distinction that I think needs to be made.

Is the virtual currency within the existing laws? I believe there are plenty of opportunities for digital currencies to operate within the existing laws and regulations, and as far as the Secret Service investigations are concerned, as long as they fit within the laws and they comply with existing FinCEN guidance, there would be no violation and no reason for the Secret Service to look into it.

Chairman CARPER. All right. Ms. Raman, would you respond to the same question, especially the second half of the question: Which agencies do you believe need to be at the forefront of the Federal Government's work on virtual currencies?

Ms. RAMAN. Starting with that question then first, I think the Department of Justice recognized a few years ago that a joint effort was needed, and the FBI set up and led the Virtual Currency Emerging Threats Working Group, which is now the working group that my colleagues here and many other agencies participate in. It has borne out to be very fruitful. It is a forum that allows all of the agencies that you would want to be at the table—the Treasury Department, our law enforcement agencies, even within the Department of Justice, the FBI, the Drug Enforcement Administration (DEA), and other agencies within the Department of Justice, prosecutors, we have U.S. Attorney's Offices, and two sections of the Criminal Division, the Asset Forfeiture and Money Laundering Section and the Computer Crime and Intellectual Property Section participating. Office of Foreign Assets Control (OFAC), IRS, and a number of other agencies here in the United States that we think are necessary participants and are, in fact, participants.

We also have foreign law enforcement that participates in that group, including the National Crime Agency in the United Kingdom (U.K.), and these are, I think, the most important agencies to be at the table. That covers the waterfront in terms of regulations and regulatory enforcement and criminal law enforcement.

There is, of course, room for improvement, and we are always looking for additional participants. Even, in fact, last week there

were additional participants that were invited to join that working group. I think it is an excellent——

Chairman CARPER. From other countries or from within this country?

Ms. RAMAN. Both, but even last week we thought of an additional domestic agency that should be at the table, and we have invited them to participate. And so I think it is going to be an evolving process. It has proven helpful thus far, and I think we are intending for that to continue to be an important forum in which we can talk jointly about what the emerging threats are, what each of our agencies can do to coordinate across the government, both here and abroad.

As for the regulations and the laws that cover virtual currencies, I feel confident that currently our criminal statutes that we have used in our prosecutions thus far have been effective tools. Our money laundering statutes have been very effective in our ability to prosecute e-Gold and Liberty Reserve, for example. Our substantive criminal statutes, such as our drug trafficking statutes and murder statutes, have been effective thus far in being able to charge the administrator of Silk Road. And our money transmitter statute, which is 18 U.S.C. 1960, has also been used to prosecute Liberty Reserve and some of its principals, for example.

And so I do think that we have the statutory tools, for the most part, that we as prosecutors need to get at this kind of criminal activity. But I will say that the Department of Justice over the last few years has been proposing and pushing updates to our money laundering statutes through the Proceeds of Crime Act and related pieces of legislation, and those changes are ones that we continue to support. Money laundering statutes have been on the books for a long time, and they have been effective. But they can be updated, and we have proposed over the years several updates that we continue to support.

Chairman CARPER. Ms. Shasky.

Ms. SHASKY. Sure. Taking the questions in turn, FinCEN has never opined and still is not opining on whether virtual currency is a real currency or a commodity, as those questions are outside of our purview. We are the anti-money laundering/counterterrorist financing regulator for the Federal Government, and so our regulations spoke to that and only that, and we tried to make that clear in our guidance this last March. But this country, like all countries, has an interest not only in protecting our financial system from money laundering and terrorist finance, but also protecting consumers from fraud, collecting taxes, protecting investors, ensuring economic stability, all things that are a part of our regulatory system, but outside of the purview of FinCEN.

And so, to the extent that this body or others feel that it is appropriate to take those considerations into account with regard to virtual currency, we would look forward to working with them to make sure we are as coordinated as possible in our actions.

Chairman CARPER. All right. Thank you.

You all know about the Government Accountability Office (GAO), and I guess a lot of people in this country, most people probably have no idea what GAO is or what they do, but they are, as we know, a watchdog and sort of the congressional watchdog to make

sure that we are minding our P's and Q's in the Federal Government in a lot of different ways—in the way we run our operations, trying to do it in a cost-effective way, broad operations, widely diverse operations.

Every other year, GAO comes up with something they call their high-risk list, and when I first heard about the high-risk list, I said, "What is that?" And they said that the high-risk list is a whole list of activities designated by or identified by the General Accountability Office that waste money. Every now and then I talk to constituents, and we talk about what we are doing to try to reduce the budget deficit. And I have people say, "I do not want to pay any more taxes, but if I am going to, I just do not want you to waste my money." And one of the things that GAO does, working with the Congress, is to identify ways to spend money more effectively, and also to collect monies that are owed to the Treasury more effectively. And it is the second half of that function I want to talk about.

The GAO every other year reports to us, along with the help of the IRS, on something called the "tax gap"—monies that are owed, hundreds of billions of dollars that are owed to the Treasury, but that are not being collected. In some cases, we have a pretty good idea who owes the money, the entities that owe the money. But it is a lot of money that goes uncollected. And I would like to say that number is going down, but, unfortunately, to my knowledge, it is not, at least not yet.

But what I want to do is, with that as background, just ask you this: When I think about the new types of currencies, I wonder how they fit into the tax system here in our country. And as you know—we just talked about the GAO, but they issued a report, I think it was earlier this year, maybe it was in May of this year, which follows my line of thinking, and that is that virtual currencies could present a real vulnerability and actually make worse what is already a difficult situation.

They recommended that the IRS find relatively low-cost ways to provide guidance to taxpayers on the basic tax reporting requirements for virtual currencies.

Let me just ask, do you know the current status of that guidance? And what could we expect it to include? And when can we expect it to be released? And I would say, either Ms. Shasky or Ms. Raman, if you could tackle that one, I would be grateful.

Ms. SHASKY. I would be happy to begin with that one.

First of all, as the financial intelligence unit for the United States, one thing FinCEN does, after it collects all of the information that our financial institutions provide to us, is we make that available to our partners in law enforcement, not only for the purpose of enforcing our criminal laws but also for the collection of taxes. And so we have a very close and longstanding relationship with the IRS, both on the criminal side and the civil side, to help them do just that.

In fact, this very last week, we were meeting with them on this very topic, virtual currencies, and how to think of that in our joint work. So it is something that I know they are taking very seriously.

When it comes to guidance on virtual currency for taxpayers, I know there was the GAO report that suggested that IRS come out

with some guidance, because there may perhaps be some question as to how to treat different uses of virtual currency for the purposes of our tax regime. And while I do not know the details and would have to refer you to the IRS to get into great detail, what I can tell you and what I do know is that they are working diligently on such guidance, and that——

Chairman CARPER. Any idea when we might expect to see it?

Ms. SHASKY. My understanding is that the GAO report may have set forth some deadlines. I think it is usually 60 to 90 days. I can tell you they are actively working on it, and it is at the forefront of their minds. And I think it will be very useful guidance for the taxpayers when it comes out.

Chairman CARPER. Thank you.

Ms. Raman, do you want to add or take away anything from what Ms. Shasky said?

Ms. RAMAN. Certainly not take away anything. I would defer to the IRS on the status of the guidance, and I am not personally aware of the status of the guidance. I will say that the Department of Justice was very aware of the GAO report. We took an interest in its findings, and we have been in discussions with the IRS about some of the findings in the GAO report.

Chairman CARPER. OK. Thank you.

Ms. Shasky, I think you said earlier that FinCEN did not opine on whether or not virtual currencies are currencies or commodities. I would just ask of you, who do you think should be making that decision? And a second question would be, beyond who do you think should be making that decision, do we need that definition to be made in order to enforce the laws and regulations?

Ms. SHASKY. I am not sure I know who should ultimately make that decision. I do know it is outside of the——

Chairman CARPER. Do you think it should be Mr. Lowery? [Laughter.]

Ms. SHASKY. I am guessing it should not be Mr. Lowery. In terms of the legality of various things, I am sure that Congress has a role in determining that. When we start talking about commodities, the Commodity Futures Trading Commission (CFTC) comes to mind; when we talk about securities, the Securities and Exchange Commission (SEC).

Regardless of who should be making those determinations, our focus at FinCEN was that we know that virtual currency currently exists; we know that it is being used to transact payments; we know that it has been exploited by some pretty serious criminal organizations. And we want to protect the U.S. financial system, as we are mandated to do, from those illicit actors, from laundering or moving money for the purposes of terrorism through our U.S. financial system. And so our entire focus has been on how can we best do that under our current regulatory scheme, and the nice thing is that the regulatory scheme that we have in place has the flexibility in it to change as the landscape changes. So, in other words, if some part of the industry were to ultimately be defined to come under the SEC or the CFTC, our anti-money laundering regulations also apply to those areas of the industry. And so, regardless, we are going to make sure that we are taking every miti-

gating step we can to prevent illicit actors from operating through the U.S. financial system.

Chairman CARPER. OK. Mr. Lowery, let me focus a question on you, and maybe, if you would like, Ms. Raman. As I think you both are probably aware, a few weeks after the Silk Road website was taken down by Federal law enforcement, a new Silk Road website popped up in its place. And it is hardly alone. Numerous other similar marketplaces exist on the Dark Web selling drugs, selling weapons, selling child pornography, and in some cases murder-for-hire services.

Whether or not these are real marketplaces or simply some scam artist's idea of a sick joke, it obviously makes people worry and it makes people concerned.

How do we develop a strategy to deal with these sites? And are there particular characteristics of these sites that make it more difficult for law enforcement to respond? Would you respond to that, Mr. Lowery? And then maybe Ms. Raman.

Mr. LOWERY. Absolutely. So the online sites. The Secret Service in our investigations, once again, we believe there are three infrastructures in place that facilitate the online crimes:

The Silk Road-type criminal forums, one of the Secret Service specialties are on the criminal forums, Eastern European based predominantly, that specialize in large-scale trafficking, stolen financial data, and what have you. So there are other of these websites that specialize in specific crimes.

The other part of the infrastructure is the digital currencies, the use of digital currencies, predominantly, the digital currencies that fall outside of the guidance of FinCEN or outside of U.S. law or in countries that obviously, as I said earlier, have less regulatory controls.

And the third is what we refer to as "bulletproof hosters."

Chairman CARPER. Refer to as what?

Mr. LOWERY. Bulletproof hosting. It is a criminal organization, a criminal individual who specifically sets up business in a country with very little regulatory or aggressive law enforcement and provides a platform for a tax to be launched against the U.S. critical infrastructure. So the Secret Service attacks the problem strategically. We are always looking to identify the individual behind a specific crime, the intruder, the large-scale vendor, stolen personal data, or what have you. And at times it may be that if we can identify a forum or a digital currency that is within legal reach, within reach of U.S. law enforcement—case in point, Liberty Reserve or e-Gold—then it makes strategic sense to take that out of the equation and disrupt the criminal organization for strategic reasons, quite honestly, usually to facilitate the arrest of other individuals we are looking at.

Chairman CARPER. All right. Thank you.

Ms. Raman, do you want to add anything to that statement?

Ms. RAMAN. I think the challenge that you are pointing to sometimes really results from anonymity, and it results from many criminals migrating to hidden services on the Internet.

Chairman CARPER. Migrating to what?

Ms. RAMAN. To hidden services on the Internet. And that has been a challenge for law enforcement, but as you have seen from

the results that we have been able to achieve in the last several years, I think we have been able to keep pace with that, and we have been able to develop tools and strategies to address it. I think, as you mentioned, it can be frustrating to the public to see another website pop up after one that seemed similar to it was just taken down, I do think, as Mr. Lowery said, that it is incredibly important for us to be taking those steps, not just to disrupt that particular organization but to send a message to the users of those websites that they cannot trust those types of websites, that law enforcement is watching, and it is not, in fact, anonymous, and it is not, in fact, immune from investigation. And that is an important message to send. All of us in law enforcement who pay attention to the results of these takedowns know that the community is aware, the criminal community is aware when we take these actions. It is important that we do so. It is important that we put the wrongdoers in prison when they deserve it. And it is important for us to put these organizations out of business, and I think we have been able to do that.

Chairman CARPER. All right. Well, that was a very encouraging addition to Mr. Lowery's response. Thank you.

I have another question on domestic job creation that I am going to direct to Ms. Shasky. But before I do, my last question will probably fall right after that, and then we will take maybe a short recess and introduce our second panel after that. But sometimes I ask a panel that is before us, when we are trying to figure out how to develop some consensus to address a significant challenge to our country, one of the things I will do—you were very kind to present an opening statement, and I appreciate very much your clear, straightforward responses to the questions I ask. But I want to ask each of you to take a minute or two to maybe give a closing statement and to just reflect on what you said, what others have said, some of the questions that we have asked, and some of what you heard your colleagues on the panel say. So just be thinking about that.

And while they are thinking about that, Ms. Shasky, I am going to ask you this question about domestic job creation. As you know, there has been some concern that virtual currency businesses might leave the United States and move overseas to jurisdictions with a less strict regulatory framework. What, if anything, can the United States do to try to keep businesses in this country? What are we doing that seems to make sense? What maybe more should we do? And along those same lines, is FinCEN engaging with international partners on regulation of virtual currencies? It sounds like we are, but if you could expand on that, I would be grateful. So those two questions, please.

Ms. SHASKY. Sure. So, first, in terms of keeping business in the United States, I guess I would say that if business is going to leave the United States based on perceived or actual regulatory burden, I at least believe that they are going to find that gain short-lived. Every country, as I mentioned earlier, has an interest in protecting its financial system from illicit actors who would launder money or move money on behalf of terrorist organizations, in collecting taxes, in protecting investors, in protecting consumers from fraud, in ensuring a stable economy.

And so if this payment system, this virtual currency payment system about which we are talking today, is going to survive and be a real player, a significant player in the financial system, regulation both at home and abroad is going to catch up, because it has to. And so our challenge here is to have smart regulation that both mitigates the risks while at the same time minimizing the burdens. I feel confident that, at least in the AML/CFT——

Chairman CARPER. What does that stand for?

Ms. SHASKY. Anti-money laundering/counterterrorist financing realm, we have managed to do that and met that challenge, and I think that is going to be borne out over time. So I think the innovation and the jobs will stay in the United States or at least come back to the United States.

In terms of working with our international partners to ensure that we have a kind of consistent regulatory framework on the anti-money laundering side worldwide, the Financial Action Task Force (FATF) is the international standard-setting body and does a good job of ensuring that countries around the world have the laws and the regulations in place. My understanding is that they are interested in taking up this issue at the FATF, as it is known. What I can tell you for sure is that our counterparts abroad have been reaching out to us quite a bit to find out what we are doing in this regulatory space.

We managed in this country to be able to act a bit quicker than some of our colleagues because we had the broad definitions and were able to fit virtual currency within our pre-existing regime. Germany was able to do the same thing, so they, too, already have regulations on the books. Other countries are trying to figure out how they can catch up.

Chairman CARPER. All right. Thank you.

Now, while you think about the answer to this last question, I am going to let Mr. Lowery and Ms. Raman go ahead and give us just a brief closing statement. Ms. Raman, do you want to go first?

Ms. RAMAN. Well, first of all, I want to thank you for holding this hearing. It is encouraging from the law enforcement standpoint to have interest in these kinds of issues because they are not easy. Although we have had many successes, we have clearly had challenges, too, and it is helpful when we have interest from people like yourself and it is helpful when we have questions asked of us like, "What can we do to help?" There is always something that we can do better, and it is helpful to have these dialogues.

I also think it is encouraging that I have colleagues like the ones that are sitting next to me who have been willing to work together on these emerging threats. I think we have all approached it in the same way, which is that virtual currencies in and of themselves are not illegal. We have all recognized that innovation is important, and we have all recognized that, like criminals have done for ages, this will be another vehicle through which criminals may try to launder proceeds or commit additional crimes.

I feel confident that we have the tools that we need to address those threats, and I feel confident that we have the will to address those threats. But we need to keep pace with what is going to come, and we will remain vigilant. We intend to be as aggressive in the years to come as we have been in the last several years. Vir-

tual currencies did not just sneak up on us. As I said in my opening statement, we brought our first indictment in 2007, and so we assume that these kinds of threats will continue to emerge and change and evolve, and we intend to keep pace.

Chairman CARPER. All right. Thank you. That was a pretty good closing statement. You should do this for a living.

Ms. RAMAN. It just so happens I do. [Laughter.]

Chairman CARPER. That is good. I think you found the right job. Mr. Lowery.

Mr. LOWERY. I would echo those statements——

Chairman CARPER. In fact, I think each of you have.

Mr. LOWERY. In closing, as a DHS law enforcement agency and a longstanding original defender of the U.S. critical infrastructure, I know the Service, working with our partners in law enforcement as well as in the prosecution and FinCEN and our international partners, will continue to work strategically to remove the gravest threats to our infrastructure. It is going to take consistent awareness of the growing threat. We are going to have to adapt, as we always have, and we are going to have to handle the international issues and what have you, working together overseas.

I do know U.S. law enforcement is very aggressive and also very collaborative with our foreign partners, because we realize that this issue cannot be taken care of just by ourselves.

We will continue to work as we respond to these threats. As a part of DHS we will continue to work to disseminate the threats through DHS and through our Electronic Crimes Task Forces, through our various partners to ensure that the remaining 16 Critical Infrastructure and Key Resources (CIKRs) for the countries' infrastructure are provided the greatest level of protection. And we believe firmly that aggressive law enforcement is a strong part of cybersecurity, which will benefit the Nation as a whole.

Chairman CARPER. Thank you.

Ms. Shasky, the last word.

Ms. SHASKY. Thank you, Senator Carper. I would like to thank you, as my colleagues did, for convening this very important hearing. I heard a chief executive officer (CEO) of a fairly large bank, say recently that having the privilege to be a financial institution and be a part of the global financial system is just that—it is a privilege. And there is a reason why countries and jurisdictions ask you to be licensed to be one of those financial institutions, because it also comes with great responsibility. You have greater power in your hands as a part of the financial system, and particularly in this country with the financial system we have in the United States.

And so while innovation is a wonderful thing and innovation in the financial services industry is incredibly important, it does come with obligations to have that entre and be able to be a part of the U.S. financial system. And one of those obligations is helping to protect that system from illicit actors.

So we believe that the regulations in place have met that balance of mitigating the risks while minimizing the burden. In essence, we are asking virtual currency exchangers and administrators to do three things:

Register with FinCEN. It is an online form, and it is free;

Put in place AML protections, controls in place to harden yourself to the likelihood that bad actors will take advantage of your system;

And maintain records and provide certain reports to FinCEN, including suspicious activity reports. It is something that many other players in the financial system already do from the smallest Mom-and-Pop check casher that is on the corner, probably just up the street here, to the biggest of the global financial institutions. They have all found a way to offer their services while maintaining those same protections. And so that is what we are asking of virtual currency providers. We believe it is reasonable given that we have seen that virtual currency has, in fact, been exploited by some pretty serious actors.

That being said, FinCEN is constantly engaged in outreach to industry and have been engaged in outreach with the virtual currency industry. We try to bring different parts of the industry together so that they can learn from each other the best practices, for hardening themselves to illicit finance and to share the information we collect from them back with them, so that they can become even better at protecting the U.S. financial system.

So at the end of the day, we hope we have that balance right. We think we have that balance right, but we are committed to continuing the discussions both with industry to see if that is right as well as our colleagues on the law enforcement side. Thank you.

Chairman CARPER. Thank you. This has been a thought-provoking presentation and discussion. It has been encouraging as well. I am going to use—this is probably a stretch of an analogy, but I want to try to make it fit. I serve on a Committee called Environment and Public Works, and we wrestle all the time with the need to clean up our environment and to put in place the kind of regulatory structure, legislative structure, combination of laws and regulations and enforcement, that enable us to breathe the air and drink the water and do so without fear.

I always like to say we do not have to make false choices, and say: We have to choose between a stronger economy and a clean environment. I think that is a false choice. And one of the questions that has been rattling around in my mind as we drill down on this subject, is it possible to reap the benefits, including the economic benefits, of this virtual currency, but at the same time clean up the kind of misbehavior, criminal behavior, that we all know is out there and is a concern to all of us?

Just as I have become convinced over the years it is possible to have a strong economy, a stronger economy and a cleaner environment, I am encouraged that maybe it is possible to have the benefits of a virtual currency or virtual currencies, and to actually be able not to facilitate, but to hold down the kind of criminal activity and criminal involvement that we have talked about here today.

So thank you for giving us both sides of the story, and we are going to have, I suspect, a chance to work with you some more, and my hope is that you will feel free to come back and tell us, informally or formally, what the Legislative Branch of our government needs to be doing to make sure that whatever potential there is here for our economy and for consumers is actually realized, while

we tamp down on that illegal behavior, criminal behavior that we all want to eliminate.

So I am going to just call a very short recess while we change up the cards. I am going to need to take a phone call from one of my colleagues, and we will probably resume in about 2 minutes. But thank you all very, very much for joining us.

Now we will just take a short recess.

[Recess.]

Ladies and gentlemen, I am going to ask you to find your seats. It looks like we have our witnesses lined up, and we thank you for joining us today.

I am told that we are still going to start voting at 5:30, so that will probably be a hard stop for this panel. But let me take just a moment, if I could, to introduce each member of this panel, distinguished witnesses, as my notes here say, distinguished witnesses. Thank you.

The first witness is Ernie Allen, who is the President and Chief Executive Officer of the International Centre for Missing & Exploited Children (ICMEC). Mr. Allen also serves as co-chair of the Digital Economy Task Force, which was developed to focus on the benefits and risks surrounding the digital economy and is led jointly by the International Centre for Missing & Exploited Children and Thompson Reuters.

Our next witness is Patrick Murck, General Counsel for Bitcoin Foundation. The Bitcoin Foundation works to standardize, to protect, and promote Bitcoin. Mr. Murck is also the principal and founder of Engage Legal. His expertise extends across the legal and regulatory issues governing the use of Bitcoin, virtual economies, and alternative payment systems. Previously Mr. Murck worked in business and legal affairs at the tech company BigDoor, as an attorney at a D.C.-based law firm, and also as an international investigative journalist.

Our third witness is Jeremy Allaire. Mr. Allaire is the founder and CEO of Circle Internet Financial, a startup company focused on promoting mainstream adoption of virtual currencies. A serial Internet entrepreneur, Mr. Allaire also serves as founder and CEO of Brightcove, one of the largest online video platforms in the United States.

And our final witness is Jerry Brito. Mr. Brito is a senior research fellow at the Mercatus Center at the George Mason University and Director of the Technology Policy Program. Mr. Brito also serves as an adjunct professor of law at George Mason University. His research focuses on technology, Internet policy, copyright, and on the regulatory process.

Good afternoon and welcome to each of you. Your entire testimonies will be made part of the record, and as I said to the first group, you are welcome to summarize, if you would like, and try to keep your comments to about 7 minutes. If you go way beyond that, I will have to rein you in. Otherwise, we will be just fine.

Mr. Allen, why don't you lead us off? Thank you.

TESTIMONY OF ERNIE ALLEN,[1] PRESIDENT AND CHIEF EXECUTIVE OFFICER, THE INTERNATIONAL CENTRE FOR MISSING & EXPLOITED CHILDREN

Mr. ALLEN. Thank you, Chairman Carper. As you mentioned, we have launched a Digital Economy Task Force with Thomson Reuters, the global media and information company. That was created as a result of a conference we brought together in June with private sector leaders and government officials to look at this larger problem. The task force that is working on this issue today includes the Bitcoin Foundation, the Tor Project, the Gates Foundation, the Brookings Institution, the Cato Institute, Vital Voices, law enforcement leaders from around the world, and many others. Our goal is to bring people together and work toward reasonable, balanced, effective solutions that protect the promise of the digital economy while addressing its misuse. And our task force will issue its final report in February.

Let me begin by saying we are enthusiastic about the potential of virtual currencies and the digital economy for social good, particularly in helping to bring about financial inclusion for the 2.5 billion adults on the planet today without access to banks, credit cards, and the mainstream financial system.

However, as you have pointed out today, there are risks. Our primary concern is the migration of child pornography, child sexual exploitation, trafficking, and other criminal enterprises to this new economy, and we believe it is happening for three primary reasons: The first is anonymity; the second is that this is an economy that belongs to no nation and is overseen by no central bank; and, third, we believe that most countries have not yet begun to apply existing law and regulations to virtual currencies at the exchange level, the point at which virtual currencies are traded for dollars, euros, pounds, or yen.

Over the past year, I have consulted with law enforcement experts and financial experts around the world about this issue, and they advise as it relates to our core concern, which is the exploitation of children, that child pornography is currently being created and disseminated using anonymizing technologies and using virtual currencies for payment.

They hasten to add that it is at a lower threshold of volume than drugs and other criminal goods; however, they call the use of these technologies for child pornography significant because they principally involve the actual producers of the content who are producing content using anonymizing technology and using virtual currencies for payment.

In August, the Irish owner of Freedom Hosting, which the FBI had called "the largest facilitator of child pornography on the planet," was arrested. Freedom Hosting maintained servers for a number of the so-called deep web child pornography sites—Lolita City, PedoEmpire, the Love Zone, and others—all of which accepted digital currencies for payment.

To shut down Freedom Hosting, law enforcement exploited a vulnerability in the site to penetrate its anonymity and expose the Internet Protocol (IP) addresses of the users.

[1] The prepared statement of Mr. Allen appears in the Appendix on page 78.

Regarding Bitcoin, all the transactions are visible and transparent. The challenge for law enforcement is to go from that transaction to an actual person.

The primary challenge that we have learned in our consultations with global law enforcement today is growing Internet anonymity. A recent headline read, "There's A Secret Internet For Drug Dealers, Assassins and Pedophiles." This so-called deep web includes sites like Silk Road, but it also includes sites for the purchase of weapons and counterfeit currencies and stolen credit cards and assassins and child pornography sites. All of these sites accept digital currencies for payment.

What I hear most from law enforcement today is frustration. The primary investigative technique I have been told that law enforcement around the world is using to investigate these operations is infiltration. But infiltration is expensive, it is time-consuming, and it is often ineffective.

And while there are some arrests, the research indicates that most of the arrests are of those who use the anonymizing technology improperly and leave a trail. They connect to a non-anonymous IP address providing a trail to follow. And even the Silk Road arrest involved an offender who made a series of mistakes that made it possible for him to be identified.

My concern is, with the absence of existing law enforcement tools, we are not catching the truly sophisticated, the most high-risk organized criminal offenders.

Through our task force, one of the things that we are doing is exploring new techniques, including clustering Bitcoin transactions to identify patterns, and we hope to learn from the techniques that were utilized by law enforcement to penetrate Freedom Hosting.

For the future, the pace of innovation will quicken. There will be new technologies, and the intensity of the effort to achieve total Internet anonymity will increase.

You asked, "What can Congress do?" I think there are four things.

First, you can ensure that existing law and regulation focusing on the point at which virtual currencies are being exchanged for conventional currencies are used.

Second, you can press for global cooperation. Digital economy funds flow globally, network to network, not nation to nation. This is a problem that the U.S. Government cannot solve alone.

Third, you can ensure that the response of government to the fragile, emerging, high-risk but high-reward area is not so draconian that the effect is simply to push these enterprises out of the United States into countries where there is little or no regulation.

And, finally, you can help us address the core challenge: Internet anonymity. For all of its importance in protecting political dissidents, journalists, and others, we are very concerned that an environment not be allowed to prosper in which child exploiters and traffickers can operate with no risk unless they make a mistake.

Three years ago, the then-Secretary of State Hillary Clinton in her remarks on a free Internet said, "On the one hand, anonymity protects the exploitation of children. And on the other hand, anonymity protects the free expression of opposition to repressive governments." She added, "We should err on the side of openness

while recognizing there are going to be exceptions." That is our challenge, Mr. Chairman, to determine how anonymous the Internet can be. From the perspective of government and law enforcement around the world, we feel that absolute Internet anonymity is a prescription for catastrophe.

Thank you, sir.

Chairman CARPER. Thank you, Mr. Allen. Very good testimony. Mr. Murck, welcome.

TESTIMONY OF PATRICK MURCK,[1] GENERAL COUNSEL, THE BITCOIN FOUNDATION, INC.

Mr. MURCK. Good afternoon, Chairman Carper. I am pleased to have the opportunity to speak with you today. My name is Patrick Murck. I am general counsel for the Bitcoin Foundation. I am a founding member of the Bitcoin Foundation, and I have been an executive in legal and business development for a number of digital currency companies. Additionally, I serve on the Board of Directors for the BitGive Foundation, a fledgling charitable organization for the Bitcoin community.

The Bitcoin Foundation is a member-driven nonprofit representing a global constituency of businesses and individuals contributing to the overall Bitcoin ecosystem. Our membership is comprised of many of the top companies, entrepreneurs, and technologists working to make Bitcoin a success. The foundation's mission is to promote, protect, and standardize the use of distributed, decentralized currencies and to free people to transact on their own terms in the global economy.

Having said that, there is no Bitcoin company that manages or controls the software or its operation. The software is built and maintained by a community of volunteer open-source software engineers and a distributed network of transaction processing, often referred to as "mining." At its most basic level, Bitcoin is an Internet protocol. It is like e-mail for money.

The Bitcoin protocol operates a decentralized store of value and an open and transparent payment network that is secure, efficient, and low cost. The Bitcoin network can operate without any third-party intermediaries and is a highly innovative global financial system unto itself.

In the near future, the Bitcoin protocol will also facilitate advanced payment services, and experiments are currently underway to provide additional non-financial services, like property management and identity verification.

Open and participatory systems like Bitcoin will produce many economic and social benefits. These systems can reduce exploitation of vulnerable populations the world over and here in the United States by providing a safe and private store of wealth in addition to a global transaction network that cannot be corrupted or abused by those who would seek to exploit or harm others.

Financial exclusion is a U.S. problem. It is not just a problem for the global South. There is a rising tide of unbanked and underbanked people right within our borders. This is important because

[1] The prepared statement of Mr. Murck appears in the Appendix on page 90.

access to financial services directly correlates to increases in dignity, liberty, and self-determination.

Bitcoin can help move people trapped in a cash-based informal economy into a globally connected digital economy. At the same time, we acknowledge that, like any technology, there is a potential for abuse of this system. Bitcoin can be used for illicit purposes, and the law enforcement community may have to develop new methodologies for interdicting and investigating criminal activity on the network. This does not mean that it will be any harder to prevent the misuse of the Bitcoin network than existing financial systems.

As we heard in earlier testimony, in Bitcoin's short history, law enforcement and regulatory agencies have had a string of notable successes already. Rather than belabor the overwrought headlines about misuse of Bitcoin in the digital economy, we should be congratulating the law enforcement community on their hard work and skill in adapting investigative techniques to an increasingly digital and openly networked world. Keeping the Bitcoin network safe is all of our responsibility, and industry-led efforts are underway to help prevent abuse.

Like you, Mr. Chairman, we are looking beyond the Silk Road. When the alleged operator of that black market website was arrested, the markets expressed relief and optimism with a long and sustained rally in the price of Bitcoin.

Decentralized currencies like Bitcoin have a different risk profile from centralized currency systems. Central control of the transaction ledger allows bad actors to shroud their activities. Decentralized systems with open ledgers are inherently transparent and may prove too difficult for use in any large-scale and sustained illicit activity.

As we address law enforcement concerns, we must bear in mind that because of this open and transparent architecture, we need to consider the privacy of law-abiding individuals. As it turns out, the blockchain, which is Bitcoin's public ledger system, may be so revealing that the larger problem with Bitcoin is not anonymity for criminals, but the difficulty law-abiding people have maintaining their own privacy.

Bitcoin is not some magical cloaking device that simply allows criminals free rein, nor does Bitcoin pose a unique or unsolvable threat to the law enforcement and regulatory community. The use of Bitcoin is not unregulated. In fact, Bitcoin service providers operate in heavily regulated business environments with deeply entrenched competitors.

For these potential competitors, be they banks, payment networks, financial service companies, Bitcoin also represents an opportunity for them to start innovating again. These institutions already have a deep understanding of the controls and risk management necessary to safely handle Bitcoin transactions and secure consumer Bitcoin accounts. Instead, what we have seen is a chilling effect through the banking industry as Bitcoin companies try and gain bank accounts.

The United States has a strong interest in maintaining its place as a global leader in developing cutting-edge technology and spreading individual freedom and liberty around the world. The

digital economy is poised to be a driver of significant job creation and economic growth.

Fostering the development of a legitimate Bitcoin business in the United States also is the best preventive measure we can take to keep good actors in the system. Applying consistent rules and regulations that encourage technological experimentation is critical to a vibrant, entrepreneurial community. This Committee's work is undeniably helpful in charting a safe and sane regulatory environment for the digital economy in general and Bitcoin specifically.

As one entrepreneur and member of the Bitcoin Foundation put it succinctly, "If you give us clear rules, we will follow them and we will build jobs." Development of clear rules appears to be happening faster at the Federal level than at the State level.

Having said that, we are encouraged by early signs of leadership from States like California and Georgia. We believe a healthy and respectful dialogue between key stakeholders will help ensure that the substantial benefits of the digital economy are met while mitigating many of the risks.

In particular, we would like to thank FinCEN for opening up a dialogue with the Bitcoin community and for demonstrating leadership on this issue at both the Federal and State level.

The Bitcoin Foundation looks forward to continuing this open dialogue and thanks the Committee for allowing us to participate in this hearing.

Chairman CARPER. Thank you, Mr. Murck. Mr. Allaire.

TESTIMONY OF JEREMY ALLAIRE,[1] CHAIRMAN AND CHIEF EXECUTIVE OFFICER, CIRCLE INTERNET FINANCIAL, INC.

Mr. ALLAIRE. Chairman Carper, thank you for hearing my testimony this afternoon. My name is Jeremy Allaire, and I am the founder and CEO of Circle Internet Financial, a recently launched financial services company aimed at facilitating payments and money transfers using global digital currency such as Bitcoin. I have been building Internet software platforms and online service companies for 20 years, having founded and helped to lead multiple global public companies, with products used by hundreds of millions of consumers and hundreds of thousands of businesses globally.

I am here to testify because I believe that digital currency represents one of the most important technical and economic innovations of our time. Specifically, digital currency introduces advancements in electronic payments and money transfers, potentially materially lowering costs for businesses around the world, decreasing fraud risk for consumers and merchants, increasing consumer privacy, and expanding the market for consumer financial products on a worldwide basis.

As this technology moves from early adopters into mainstream acceptance, it is critical that Federal and State governments understand how Bitcoin fits into existing regulatory guidelines and how to apply them to digital currency. These should uphold consumer protections associated with fraud and privacy risks, ensure that criminals and bad actors find it increasingly difficult to utilize

[1] The prepared statement of Mr. Allaire appears in the Appendix on page 114.

these platforms, and provide income tax clarity to consumers and businesses that conduct business using digital currency.

It is very clear that over the past 20 years the Internet has been at the center of global economic innovation. Open platforms have transformed communications, media, software, education, commerce, and retail, but for a variety of reasons, the technology and business models around finance have been insulated from similar transformations. This same open platform approach in digital currency, specifically Bitcoin, presents an opportunity for the same level of innovation and advancement in forms of currency, trade, and payments that we have seen brought to bear on other industries.

I do not think there is much debate that we need to see innovation and transformation in banking and finance, not just reform and remediation. Specifically, our payment systems are inefficient and very much built upon systems and processes that predate the Internet. The result is higher costs for consumers, lower margins for business, and less efficient economic interaction. And in many cases, our financial systems have excluded enormous bases of consumers who remain unbanked or underbanked. The combination of ubiquitous Internet-connected mobile devices and digital currency presents a tremendous opportunity to expand access to financial services on a worldwide basis.

Payments and money transfers are still operating in the pre-Internet era. Today we can communicate with almost anyone in the world, including in video format, at no cost. We have instant access to an enormous amount of the world's knowledge, also effectively at no cost. We have instant access to more media than we ever imagined was possible, again, almost at no cost. Yet to send money between friends and family, whether across the table or across the planet, takes days and costs a significant amount in transaction fees. To accept payments, merchants must bear significant fraud risk; consumer privacy is often threatened; and likewise it takes days for a merchant to actually receive money from an electronic payment, not to mention the widely perceived high costs of transaction fees.

So what are we at Circle specifically doing about this? At Circle, we are building online services for consumers and businesses to be able to easily use digital currency and specifically Bitcoin. For consumers, we intend to enable them to easily purchase, store, send, receive, and make payments using Bitcoin. And for businesses, we are providing tools to help them easily accept digital currency payments.

We are fully committed to complying with all applicable laws and regulations and establishing comprehensive risk management protocols. We have registered with FinCEN as a money transmitter and are actively seeking appropriate licenses from U.S. State financial authorities. We are developing our platforms to provide very high levels of security for our users and employing industry-leading approaches to customer identity verification, fraud remediation and anti-money laundering, designed in partnership with leading regulatory advisors and experts.

I want to talk for a minute, though, about some of the risks inherent in digital currency platforms such as Bitcoin.

First of all, as has been made amply clear from earlier testimony, I want to emphasize that I believe that U.S. regulators and law enforcement are justifiably focused on the potential use of digital currencies to finance criminal activities, including terrorism. But in addition to FinCEN's guidance and the appropriate requirement that Bitcoin operators implement Bank Secrecy Act provisions, it is also a risk if the government does not support innovative companies gaining access to U.S. banking institutions, which will drive companies offshore and overseas.

Another risk is that businesses' adoption of digital currency will be hampered without clarification from the IRS on income generated from sales denominated in digital currency, and such guidance is also needed to thwart potential tax evaders. Without clear guidance on consumer protections required of Bitcoin operators, consumers and businesses could be defrauded through inadequate systems and risk management procedures around customer funds.

Another risk is that the United States falls behind in this critical emerging economic innovation. Regulatory uncertainty could hold back American companies from participating in driving digital currency innovation. Indeed, today a Bitcoin exchange in China has become the largest single trading exchange in the world, followed by exchanges in Japan and Europe. We need to uphold and support our incredible history in America of supporting technical innovation and entrepreneurship.

In terms of U.S. regulation, it appears to me that Federal and State regulators seem to have ample statutory authority to adopt regulations and take enforcement actions as necessary to protect consumers and ensure responsible conduct in the world of Bitcoin commerce and that enforcement actions to date have been constructive. We stand ready to assist them in their ongoing efforts to adapt their regulatory tools to new digital currency.

I believe we are at the forefront of another 20-year journey of Internet-led transformation, this time in our global financial systems, and there is a real opportunity to foster that economic change while simultaneously putting in place the safeguards that only government can enable.

Mr. Chairman, that concludes my prepared testimony. I would be happy to answer any further questions.

Chairman CARPER. Thank you, sir. That was very helpful testimony. Thanks.

Mr. Brito, please proceed. Welcome. We are delighted that you are here.

TESTIMONY OF JERRY BRITO,[1] SENIOR RESEARCH FELLOW, THE MERCATUS CENTER, GEORGE MASON UNIVERSITY

Mr. BRITO. Mr. Chairman, thank you for having me here today. We are here today to discuss virtual currencies in general, but it is Bitcoin in particular that has so many interested in this topic.

But online virtual currencies are nothing new. They have existed for decades, from World of Warcraft Gold to Facebook Credits to e-Gold. And neither are online payments systems new. PayPal, Visa, and Western Union Pay—these are all examples. So what is it

[1] The prepared statement of Mr. Brito appears in the Appendix on page 120.

about Bitcoin and similar cryptographic currencies that makes them unique?

Whatever one may think about Bitcoin's prospects for enduring value, it is safe to say that it is a remarkable technical achievement. Bitcoin is the world's first completely decentralized digital currency, and it is the decentralized part of that sentence that is really unique. Prior to Bitcoin's invention in 2009, online currencies or payment systems had to be managed by a central authority, whether it was Facebook issuing Facebook Credits or PayPal ensuring that transactions between its customers were reconciled. However, by solving a longstanding conundrum in computer science known as the "double spending" problem, Bitcoin for the first time makes possible transactions online that are person to person, without the need for an intermediary between them, just like cash.

This technical breakthrough presents potential benefits for consumers and the economy as well as challenges to law enforcement. For example, because there is no central authority in Bitcoin transactions, there are little to no fees associated with those transactions, which especially benefits small businesses and price-sensitive consumers. And because Bitcoin is not a proprietary platform run by a single company but instead it is an open network, entrepreneurs need no permission to experiment or to innovate new products and services.

On the flip side, law enforcement has long relied on financial intermediaries to help them detect, prevent, and investigate illegal transactions. Because Bitcoin transactions can have no intermediaries, and because Bitcoin transactions are not necessarily tied to identities, it is not surprising that we have seen Bitcoin employed in criminal transactions. In particular, Bitcoin has been used for the sale of drugs and in malware that holds one's data hostage. It is also not difficult to imagine how the technology could be employed in money laundering.

Emerging technologies often present both great potential benefits as well as real risks. For example, 3D printing can be used to cheaply make prostheses and life-saving medical devices, but also undetectable firearms. Domestic commercial drones have the potential to revolutionize agriculture and shipping, but could also be used for stalking. The challenge for policymakers is to address the risks posed by emerging technologies while doing no harm to the innovative potential of that technology.

In many cases where emerging technologies pose risks, there are already laws and regulations of general applicability that address many of those risks without the need for new laws targeted at the specific technology. This is the case with Bitcoin. While Bitcoin transactions do not require intermediaries, one must still acquire Bitcoins by exchanging dollars, and merchants that accept Bitcoins will very often use Bitcoin payment processors. Indeed, there is a fast-growing ecosystem of startup exchanges, payment processors, and wallet and escrow services that make up Bitcoin's burgeoning infrastructure. Each of these are already subject to regulation as money transmitters, including State licensing and FinCEN registration, as well as Know Your Customer and suspicious activity report requirements.

More to the point, serious criminals looking to hide their tracks are more likely to choose a centralized virtual currency run by an intermediary willing to lie to regulators for a fee, rather than a decentralized currency like Bitcoin that, as a technical matter, must make a record of every transaction, even if pseudonymously. While the online black market Silk Road, which used Bitcoins, is estimated to have generated less than $200 million in drug sales, the centralized digital currency Liberty Reserve is believed to have laundered more than $6 billion related to credit card fraud, identity theft, computer hacking, and child pornography. The reason Liberty Reserve, and not Bitcoin, was the payment system of choice for criminals online is that it was designed and managed by its creators to avoid Know Your Customer and reporting rules and to evade subpoena.

As a result, the path forward that can best confront risks while ensuring that we can reap Bitcoin's beneficial potential is to allow the Bitcoin network and its surrounding infrastructure to develop by making sure that entrepreneurial innovators can easily comply with existing regulation. The alternative, promulgating special regulations for virtual currencies or otherwise making it more costly to operate legitimately in the space, could have two unintended consequences. First, it might mean ceding the network to exclusively illegal use and forgoing any visibility that law enforcement could otherwise gain into the activities of compliant firms. And, second, the United States could lose its head start in what may be the next big breakthrough industry if it establishes a regulatory regime that hampers Bitcoin while other countries, like China, Canada, and Germany look for ways to develop workable regulatory frameworks for Bitcoin.

Finally, as regulatory and law enforcement agencies seek to apply existing laws to Bitcoin, they will face the challenge that Bitcoin is not a company with an easily identifiable executive, but instead it is an open-source project and a community. The Bitcoin Foundation is central to that community, but it does not encompass the whole community. So as new guidelines and procedures are developed, policymakers should make sure to engage the community and solicit comments from the public to ensure that they benefit from a wide range of perspectives.

Thank you for your time, and I look forward to your questions.

Chairman CARPER. Thanks very much for joining us today and for that testimony.

If you were here during the testimony of the first panel, you heard me indicate that one of the things I like to do to address an issue like this, around which there is not a great deal of consensus, is to use these hearings as an opportunity to see if we can develop some. And I thought we made a little progress with the first panel, and I am hopeful that we can replicate that with this second panel of witnesses.

Toward that goal, let me just ask you to reflect on what you have heard from your colleagues on this panel, and just tell me and the staff members that are here and whoever is watching on television here in the Capitol or outside the Capitol, where do you see the agreement among the four of you. The perspectives you shared

with us—the opinions that you shared with us, where do you think there is general agreement?

Second question, where do you think there is not agreement? And how do we go about reconciling that lack of agreement, if we can? Mr. Allen, do you want to go first?

Mr. ALLEN. Senator Carper, I think there is broad-based agreement about the potential of a digital economy and virtual currencies. I think there is absolute agreement that there is enormous potential for social good and that this is an emerging technology that needs to be protected.

I also think there is clear agreement that we cannot just ignore the misuse and that the misuse of a digital economy and virtual currencies jeopardizes the viability of virtual currencies in the longer run. So I do not think there is disagreement at all on those points.

As it relates to area—and I also do not think there is disagreement on the need for basic regulation using the existing tools: the application of AML, the application of money transmitter laws at the exchange level, Know Your Customer, those kinds of provisions.

I think maybe the greatest challenge, the greatest area that we have to grapple with is how do we enforce the enforcement techniques to deal with the misuse while preserving the potential long term and the fact that this truly is a global phenomenon. This is something that we are just beginning to adress—the FinCEN guidance on this was just issued in March of this year. The FATF guidance that Director Shasky talked about, the Financial Action Task Force, their guidance on this issue was just issued this summer, I think in July.

So my sense is that most of the world is not applying money transmitter laws, is not applying any money laundering principles. So I think the question of how we get from here to there regarding an area that there is not great knowledge and understanding about is really the issue that the four of us would have to grapple with.

Chairman CARPER. Thank you.

The same question, Mr. Murck, if you would, please. Where do you see consensus agreement? Where do you see a lack of that? And how do we go about reconciling that lack of agreement or consensus?

Mr. MURCK. I will take the second part first. I do not know that I heard a lot of disagreement or anything that we would generally disagree with from this panel or even really from the first panel. I was heartened by that. I think that Ernie is correct that, as we move forward, I think that an open dialogue is good so that as those disagreements do crop up—and they likely will—we can address them quickly and in a safe and sane way.

As to where we have agreement, I think what I heard from the other panelists is there is a real need to create on-ramps into the traditional financial system, that by creating those on-ramps, especially here in the United States, you help to protect the system from abuse.

The biggest obstacle to that happening today is not from regulation or from law enforcement. It is from the ability of businesses in the space to get bank accounts and to be integrated into the banking system.

There is currently a chill in the banking system and in the banking industry that is preventing businesses from getting just simple—even simple checking accounts. There are stories that if you have the word "Bitcoin" anywhere in your name or your documentation, your application will be immediately placed in the circular file, as it were.

So I think there is a need to create some leadership within the banking industry to make sure that these companies are onboarded into the traditional system where some of the protections are in place already and the illicit activity can be detected and rooted out.

Chairman CARPER. Good. Thank you. Mr. Allaire.

Mr. ALLAIRE. I would like to echo some of the other panelists' comments. Clearly there is consensus here around the innovation that we see the potential for financial inclusion. I think there is consensus that many of the regulatory frameworks and tools are sufficient and being applied appropriately. I think there is consensus that the open nature of this technology, its development, its use, and its oversight, is a very positive framework.

I do think that there is some tension around the question of the balance between anonymity and privacy and whether there are new laws that are required to end the possibility of anonymity on the Internet or to address that in some way. I think, as I stated, in my comments, we are very focused within our business on having very deep levels of identity verification, and so we view that as critical. But others within the digital currency world, particularly within geographies that do not have the same kinds of regulatory regimes, may not. And are there other things that we need to be thinking about, other tools that we need to be thinking about for law enforcement that can address some of those issues? So I think that arena needs additional and careful consideration.

Chairman CARPER. All right. Thank you. Mr. Brito.

Mr. BRITO. So I think there certainly is broad consensus among the panel up here, and I was very heartened to hear the first panel's message, and I think we have a lot of consensus. I will pick two issues just to give you an answer.

First, where is there agreement, I was very interested in listening to the gentleman from the Secret Service who said that, in fact, it is centralized currencies that pose the greatest risk as far as money laundering and other illicit uses, and that decentralized currencies like Bitcoin, because of their nature, were not a greater risk. I think that was a great point of agreement there.

To pick a point of disagreement, Ms. Shasky took issue with the idea that U.S. businesses might move overseas seeking a better regulatory environment, and I think her suggestion was that if somebody leaves the United States seeking lax regulatory treatment, they are going to find it eventually. It is going to catch up with them. And I think the danger is not that somebody who is trying to facilitate an illicit business is going to leave the United States. The danger is that real hard-working entrepreneurs who are looking to comply just do not find a regulatory environment that is amenable here. And that is something that we do not want to let stretch for too much time.

Chairman CARPER. OK. Thank you. I want to go back to Mr. Allen. I think you mentioned the guidance issued earlier this year

by FinCEN, and I am going to probably ask Mr. Allaire to lead off and respond to this question. But they issued their guidance earlier this year, I think back in the spring, and they stated that virtual currency exchangers and administrators would need to register as money service businesses and apply for money transmitter licenses in the 48 States that require such licenses.

I want to ask you just to focus on this with me for a little bit. I am going to ask you—and some of you have already alluded to this guidance and given it some thought, but I just want you to give me your thoughts on this guidance from FinCEN. Do you believe that the approaches are a good fit for virtual currency exchanges or other virtual currency-related businesses? And, Mr. Allaire, I am told that your company has registered with FinCEN and has applied for money transmitter licenses in a couple of States. So could you, if you would, just offer the first response.

Mr. ALLAIRE. Sure. I think a business that is going to handle consumer funds, store and manage those, and is going to interact with the banking system should be compliant with the rules that have been set forth through the Bank Secrecy Act to protect consumers and ensure that bad actors are not able to operate. So I think in general we very much think that these are appropriate guidelines, and I think the digital currency business from an entrepreneurial perspective may be different than other prior Internet businesses. Two guys can build a photo-sharing app and put it up on the Web and get a billion users. I do not think it is appropriate that two guys should be able to build a financial services business and operate that without a sufficient investment to protect consumers and protect society.

And so I do believe that the bar needs to be higher for financial services businesses in the United States, and that it is not realistic, which I think some in the entrepreneurial community would like to see regulation which does not require that level of compliance. I do not think that is realistic.

When I founded the company and sought capital to build this company, we understood that the bar was higher and we raised sufficient capital to be able to launch our product and service in a compliant manner and hire the professionals and staff and put in place the systems and protections that were critical. So we think it is appropriate. There are challenges with how many transmission licenses are granted in the United States, the broad number of States, the divergent approaches that each State might take, and I do think that creates cost and complexity and could be argued to be an unnecessary regulatory burden. But that is the system that we have, and that is the system that we are pursuing and operating within.

Chairman CARPER. Good. Thanks. Others on the same issue, Mr. Allen, do you want to——

Mr. ALLEN. Yes, just briefly, Senator Carper. I agree with Mr. Allaire totally, and what I think is most appropriate about the FinCEN guidance is that it is focused at the exchange level. It does not apply to users, it is an application of basic money transmitter law, and I think it is an appropriate use of the existing law, and I think it is a reasonable approach.

I agree with him that one of the great challenges is creating consistency and uniformity because of our Federal system and the fact that there could be 50 different approaches. But that is not unique to this issue.

Chairman CARPER. OK. Thank you.

Mr. Murck, any thoughts, please?

Mr. MURCK. Yes, the 50-State money transmitter license regime has come up. I do think that States have an interest in protecting their consumers. At the same time, it is a bit burdensome and it has slowed down progress in the United States; I do not know what the answer to that question is. I know in the European Union (EU) they have a system of reciprocity where they have a minimum threshold for each country, and if you attain a license in one country, you can passport it to other countries as well. Perhaps that is a framework that would work here. But that would be best left to the Legislative Branch.

Chairman CARPER. All right. Thanks.

Mr. Brito, any thoughts?

Mr. BRITO. One small point regarding the FinCEN guidance. I think it is very clear as it applies to exchanges and to administrators of centralized virtual currencies. I think it is less clear when it applies to users, for example. The guidance says that you are not required to register with FinCEN if you are acquiring, say, Bitcoin in order to buy goods or services. But let us say, for example, that—my mother is from Spain, and recently I helped her send money back home, and it cost 5 percent of the total amount. What if I was buying Bitcoin simply to remit money overseas as, could be one of the great potential benefits to allow remittances to the Third World and to other countries? That is not covered by the FinCEN guidance.

So I think the guidance could use further explanation, and I think if FinCEN were to put any further clarification up to public comment, they would, I think, get all the wrinkles out.

Chairman CARPER. OK. Thanks.

Let me go back to you, if I could, Mr. Allen. I understand that your organization, International Centre for Missing & Exploited Children, was one of the forerunners in bringing together private and public stakeholders to talk about virtual currencies. If you would, first a couple questions. Who was involved in your working group? And why did you form it?

Mr. ALLEN. Mr. Chairman, we formed it because several years ago we had a very positive experience in bringing together financial industry leaders around the fact that the mainstream financial system, the mainstream payment system, credit cards, were being used for the purchase and distribution of child pornography. I called the chairman of a major credit card company and said, "How is this possible?" And he said, "We do not know what these transactions are for. If you can find for us, show us where the merchant bank is, where the account resides, this is an illegal use of the payment system, we can stop the payments, we can shut down the accounts.

So we brought together coalitions in North America, Europe, and Asia and had enormous positive impact. There was a dramatic decline. But as I began to talk to law enforcement and other leaders

around the world, what we determined was that we did not end it. We just moved it. And we were seeing evidence of a migration of these kinds of illegal operations into this new economy.

And so in an effort simply to try to understand it better and determine if it was a problem, to use that same model to bring leaders together, private sector leaders together to try to develop shared commonsense solutions, that is why we joined with Thomson Reuters to create this task force. And it includes the Bitcoin Foundation, it includes the Tor Project, it includes the Gates Foundation and the Brookings Institution, the Cato Institute, Vital Voices, a human rights group. It includes multiple law enforcement groups and representatives.

The intent was to bring people together, better understand the problem, and search for common ground, and so that has been our process.

Chairman CARPER. Let me just follow that up, and you have partly answered this question, but I want to ask it anyway. But just share with me a bit further what you have been able to learn from the dialogue that you facilitated, especially as it pertains to the exploitation of children around the world.

Mr. ALLEN. I think we have really learned a lot in a short time. One of the challenges is most of the evidence is anecdotal, because relatively few cases are actually being made, as we have talked to law enforcement. I talked about that earlier in terms of the absence of investigative techniques to probe these kinds of things.

But I think we have learned that there is broad-based interest in searching for and finding reasonable solutions that work. We have learned, I think, as was pointed out earlier, that the digital economy is far broader than Bitcoin. So the issues we are focusing on are not just Bitcoin but, for example, there are 22 million users today of Russia's WebMoney. We have talked about Liberty Reserve and the case that was made there, $6 billion in illegal money laundering.

So I think we are discovering it is a complex issue, but I think it is one that is addressable, and I think the most encouraging thing to me is I now believe it is addressable using many of the tools and laws that we already have in place; that one of the biggest challenges for policymakers is simply to increase the level of awareness so that countries around the world will begin to use the tools they already have.

Chairman CARPER. Well, that in part is why we are having this hearing. Good.

I was talking with a fellow who goes to the same church as we do back in Delaware the other day. He is in the auto business, sells a lot of cars. He has dealerships, sells a lot of cars in our State. And he was talking about the work of the Consumer Financial Protection Bureau (CFPB) established a couple of years ago, hopefully to look out for the interests of consumers throughout this country in a lot of different ways. But I want to focus just a little bit on consumers, if we could.

I have been told that virtual currencies pose a number of questions as to their use by consumers, and I have maybe two questions, but the first is—maybe we should go down the panel, or go up the panel. Mr. Brito, we will start with you. And if you will, just

give us some of your thoughts on whether virtual currencies have sufficient protections built into them for consumers. And do virtual currencies raise any additional new issues for consumer protection? For example, do we need to do anything to better protect consumers from fraud or to protect consumer privacy as a result of these virtual currencies?

Mr. BRITO. I think that this is a very nascent industry and is still trying to find its way. As a result, that means that the folks who are, at this point, participating in this economy really have to try hard to participate in it. So these are not your average consumers, just yet, jumping into this space.

So at this point I think it gives regulators some time to learn more about the technology and learn more about what the industry players are doing to address these concerns and whether the existing consumer protection laws are enough.

As far as opportunities, what is interesting about especially decentralized digital currencies is that they provide a new choice for consumers. Today, if you want to use electronic payments, you are probably going to be using a credit card or something like PayPal, and that comes with fees, sometimes high fees, and those fees are important because they provide things like insurance. If your identity is stolen or if something that you receive is not what you ordered, you can always have the charge reversed.

Decentralized digital currencies are alike in that there is nothing to reverse, but that also means that there are very little fees. So this now presents a new choice for consumers. They can choose insured but more expensive or not insured but less expensive. That is a new choice for consumers that was not there before.

Chairman CARPER. OK. Thank you. Mr. Allaire.

Mr. ALLAIRE. I think there are many issues around consumer adoption of digital currency. I will touch on a couple of them.

We emphasize that Bitcoin as a digital currency offers great potential to lower the fraud risk that both consumers and merchants face on a day-to-day basis when we conduct payments. When we go into a restaurant and give our credit card out or when we enter that information online, we are effectively giving out the keys to our bank account to every counterparty that we interact with. And so it should not be a surprise that we have seen dramatic growth in the amount of identity theft and specifically financial information, private financial information being stolen and sold on black markets and used for nefarious reasons.

Protocols like Bitcoin reduce that risk because the keys to your bank account, the keys to your money are never transmitted, and that is one of the brilliant aspects of the design of the system. And so there is real potential to lower occurrences of financial fraud in consumer transactions and increase consumer privacy as a result.

So I think those are really key benefits, but there are risks, clearly, for consumers. I think one risk—and this is one that we take very seriously as we look at this—is increasingly, because of ease of use, consumers that want to take advantage of things like Bitcoin are using online services that essentially host their Bitcoin on servers or on the Internet. And because Bitcoin itself, the mechanism by which funds can be used, is based on keys that we then in turn would store, there is a real risk around the security of

funds, and we have seen occurrences just in the past weeks of startups who did not have appropriate levels of security around those funds, and those funds were effectively stolen.

And so I think there is really critical requirements around the safeguarding of funds, the custodianship of these keys and best practices and methods to employ that. I think industry is driving forward on that, but I think that is a key issue that the CFPB may take a look at.

The flip side, which is this question of what I would call merchant fraud, which is the chargeback scenario—you did not get the product, you got the wrong product, someone had inappropriately used your account—I think that there are methods for addressing that within the technology of Bitcoin today and within improvements that are coming in upcoming versions of Bitcoin, mechanisms to create refunds to consumers, mechanisms to provide greater transparency around what you are paying for. And there are mechanisms even that are not well understood, I think generally, but which will become available where funds can be held in escrow until a product has been delivered to a consumer. So there are ways to address some of that merchant fraud risk as well, and I think you are going to see industry participants pushing forward on that in the coming months and years.

Chairman CARPER. OK. Thanks.

Mr. Murck, any thoughts?

Mr. MURCK. Yes. Thanks for the question. There are consumer protection issues in the Bitcoin space, and I will reserve my comments strictly to Bitcoin and decentralized currencies.

When you look at Bitcoin especially, we have not even released Version 0.9 yet, so we are not on Version 1.0. It is very much still an experimental currency, and it should be considered a high-risk environment for consumers and investors at the moment.

That is changing over time as businesses like Mr. Allaire's and others' are coming into the space and building the service layers on top of the Bitcoin protocol to make it safer for consumers to move in. Those service layers are both technological—Bitcoin has been referred to as "programmable money," so you can build in layers of escrow and dispute mediation and things like that right into your payment structure, which is a very interesting concept as most of the laws that exist for consumer protection in the payment space were built around traditional methods where those were not possible. So potentially you do not need as much regulation on the consumer side in the long term to the mid-term as this system grows up.

In the short term, consumers should be aware that this is a high-risk environment and that potentially it is not quite ready for mass consumer adoption today. That time is coming, but it is not here yet.

Chairman CARPER. Thank you. Mr. Allen.

Mr. ALLEN. The other panelists are the experts, so I do not think I have much to add other than to say one of the groups we met with on this were central bankers and financial industry leaders, and they clearly view, as I think the other panelists do, virtual currencies as akin to cash. So there is no Federal Deposit Insurance Corporation (FDIC), there is not that level of protection. So I think

it has to be viewed as high risk, and I think the points that the other panelists made about the fact that consumer protections are part of a work in progress, but certainly something that we need to be very much aware of.

Chairman CARPER. OK. In anticipation of this hearing, I was asking the members of our staff to tell me a little bit about where did Bitcoin come from, who was the creator, who were the creators; and I am told that the protocol was developed either by maybe a programmer or by a group of programmers that go by the name—I think it is Satoshi Nakamoto. Is that correct?

[No verbal response.]

OK. And with all the money and attention that has been given to Bitcoin, it just seems strange to me that either this individual or this group would choose to remain anonymous.

What do we know about this person or what do we know about this group? Does it matter that his, her, or their identity remains a mystery? Who wants to go first? Mr. Murck, do you want to go first? Go ahead.

Mr. MURCK. I will go ahead and field that one for everybody. [Laughter.]

So, yes, Satoshi Nakamoto is the pseudonym for the creator or creators—he, she, they—who developed the Bitcoin protocol and released the original white paper, the spec for the Bitcoin protocol into the world, in addition to the original code base, that was then open-sourced to the entire community. This person or group of people has since left the scene, as it were. At least, if not more than, half of the code base from that original code has already been rewritten. While I think everybody is grateful for that incredible contribution, at this moment in time, who Satoshi is is largely irrelevant to the story of Bitcoin going forward. And I think that was intentional and possibly why a pseudonym was chosen in the first place.

Chairman CARPER. All right. Anybody want to add to that, please? Mr. Brito.

Mr. BRITO. I just want to address that it is a little strange that, Bitcoin, we do not know who the creator is, and so that often conjures up the idea that there is some risk here that we have not seen.

Chairman CARPER. You do not think it was Al Gore, do you? [Laughter.]

Mr. BRITO. He has never denied it.

But I think the key thing to emphasize is that Bitcoin, especially the code base, is open source. That means it is completely open and auditable and available to anybody to look at. And, in fact, many very smart programmers and cryptopgraphers have looked at it and have given it their seal of approval. And as Mr. Murck said, more than half of the code base has been written by others than Satoshi at this point. So, I am pretty confident that the software is what it says on the tin.

Chairman CARPER. All right. We are just about to start voting over in the Capitol, so I think we will wrap it up. I just want to say—I love to quote Albert Einstein. Not all my colleagues do, but he said some just really memorable things. One of the things he said, "In adversity lies opportunity." God knows there is plenty of

adversity with respect to these virtual currencies that we have talked about. It is not just potential, it is not just possible. It is real. And we need to be not just mindful of that but vigilant to make sure that we contain it and eliminate it where we can.

I only know one quote that is attributable to Mrs. Einstein, and I find it sort of relates to my efforts to try to get my head around this whole issue of virtual currencies and Bitcoin. Mrs. Einstein, who probably was quite brilliant in her own right, was once asked if she understood her husband's theory of relativity, and she allegedly responded, "I understand the words but not the sentences."

When I first started trying to understand what this was all about, I sort of felt like Mrs. Einstein: I understand the words but not the sentences. But with the help of our first panel and all of you on the second panel, and with the help of my staff and a lot of other folks that have come by to brief us, I am starting to understand more than just the words, but a few of the sentences, too. And that is really why we wanted to hold this hearing today, to better understand what is going on here, the pitfalls that come from this technology, but also the potential value toward society, to consumers, and to businesses.

I said earlier I thought the first panel gave us a lot of thought-provoking information. I thought they were very thoughtful. But it is also encouraging. It was encouraging. And I find that that has been true here with this panel as well. So for that, we thank you.

And on behalf of my colleagues who are not here, who are flying in from all over the country right now in order to make this 5:30 vote, I thank you. They do not know I am thanking you, but I will thank you in their absence. Someday they will thank me for thanking you, I hope. But we have a bit of a shared responsibility here in trying to figure out how to make this work so that we minimize the bad that can flow from it and maximize the good.

With that, I think we will wrap it up here, and I am going to just note that the hearing record will remain open for 15 days—that is until December 3 at 5 p.m.—for the submission of statements and questions for the record. I suspect we may have a few from me. When you receive those questions, I would just ask that you respond to them promptly.

Again, to our staffs, especially John Collins, who first brought this to me months ago, I want to thank our staffs, both the majority and minority staff, and for you and for our first panel for joining us today, and for the work that you have done in helping to enlighten us a bit on this subject.

With that, we are adjourned, and thank you so much.

[Whereupon, at 5:30 p.m., the Committee was adjourned.]

APPENDIX

Opening Statement of Chairman Thomas R. Carper
"Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies"
November 18, 2013

As prepared for delivery:

Over the past several months, this Committee has engaged in an investigation into the potential implications of virtual currencies. During the course of this inquiry, we've examined the issues and potential risks and threats that virtual currencies pose, as well as some of the potential promises that some believe they can bring.

In addition, we have explored with several departments and agencies throughout government how they are approaching virtual currencies as an emerging technology. This has included looking at how they are coordinating together to develop a "whole of government" approach that is consistent and informed.

Virtual currencies, perhaps most notably Bitcoin, have captured the imagination of some, struck fear among others, and confused the heck out of many of us. Indeed, based on conversations my staff and I have had with dozens of individuals both inside and outside of government, it is clear that the knowledge and expectation gaps are wide. Fundamental questions remain about what a virtual currency actually is, how it should be treated, and what the future holds.

Virtual currency can best be described as digital cash. It is generated by computers, lives on the internet, and can be used to purchase real and digital goods across the world.

Some proponents believe virtual currencies can prove valuable to those in developing countries without access to stable financial systems. Others believe it could prove to be a next generation payment system for retailers both online and in the real world.

At the same time, however, virtual currencies can be an effective tool for those looking to launder money, traffic illegal drugs, and even further the exploitation of children around the world.

While virtual currencies have seen increased attention from regulators, law enforcement, investors, and entrepreneurs in recent months, there are still many unanswered questions and unresolved issues.

This isn't the first time that advances in technology have posed challenging questions for policy makers and society as a whole. As we all know, technology is dynamic and changes quickly. Concepts like email and even the internet itself were once alien and difficult to understand and navigate. Now, most of us can read and respond to email on a device we keep in a purse or coat pocket and search the web on a multiple.

I'll be the first to admit that, like most Americans, I am no technical expert in virtual currencies. However, what I do know is that a number of smart people both inside and outside of

government view this is as a major emerging issue that is deserving of our attention, including this committee's attention.

The ability to send and receive money over the internet, nearly anonymously, without a third party, has a lot of wide-ranging implications. The government needs to pay attention to this technology and to understand, and where appropriate, address these implications.

This was made all the more clear last month when federal law enforcement took down and seized an online marketplace called "the Silk Road" on which many illegal products and services were bought and sold via bitcoin. The most popular products for sale were illegal drugs and forged documents, such as ID's and passports. Other services were also for sale, including hacking services.

We're told that approximately $1.2 billion dollars in transactions were made through the Silk Road.

This site lived on what is often called the 'Dark Web,' also known as the deep web. The 'Dark Web' consists of web pages and data that are only available via special software that keeps users anonymous. Many sites and data on the "Dark Web" have been deliberately built to be untraceable in order to protect the anonymity of the user. Silk Road was one of those sites.

My understanding is that individuals could navigate to Silk Road anonymously and use Bitcoin – which can be sent to someone nearly anonymously—to make purchases.

The anonymity of the market place and near anonymity of the currency made it nearly impossible for law enforcement to track and, therefore made it an attractive place for criminal activity.

In fact, in the course of our investigation, the Department of Homeland Security informed us that the suspect who allegedly sent ricin to President Obama in April of this year was a vendor on Silk Road.

Law enforcement, including the FBI, Immigrations and Customs Enforcement, and the Secret Service should be applauded for their work in taking down a major international criminal enterprise.

But while Silk Road was perhaps the most well-known, it is not the only marketplace where illicit goods are bought and sold through bitcoin transactions. Today, a number of similar enterprises that accept bitcoins are still in business, selling weapons, child pornography, and even murder-for-hire services.

While today I suspect we will talk a lot about the well-known virtual currency Bitcoin, there are numerous other virtual currencies operating on the internet today, each with its own set of specific features.

That said, whether it is Bitcoin or any of the other virtual currencies, the federal government and society as a whole need to come together to figure out how to effectively deal with it.

Whether or not virtual currencies prove to be a boom or a bust, I think it's clear that some folks just want a chance to try and play by the rules. That's difficult to do if the rules or proper authorities aren't clear or if the future is uncertain. It's also difficult if a large number of bad apples are allowed to spoil the bunch."

###

Statement of Jennifer Shasky Calvery, Director
Financial Crimes Enforcement Network
United States Department of the Treasury

Before the United States Senate
Committee on Homeland Security and Government Affairs

November 18, 2013

Chairman Carper, Ranking Member Coburn, and distinguished Members of the Committee, I am Jennifer Shasky Calvery, Director of the Financial Crimes Enforcement Network (FinCEN), and I appreciate the opportunity to appear before you today to discuss FinCEN's ongoing role in the Administration's efforts to establish a meaningful regulatory framework for virtual currencies that intersect with the U.S. financial system. We appreciate the Committee's interest in this important issue, and your continued support of our efforts to prevent illicit financial activity from exploiting potential gaps in our regulatory structure as technological advances create new and innovative ways to move money. I am also pleased to be testifying with my colleagues from the Departments of Justice and Homeland Security. Both play an important role in the global fight against money laundering and terrorist financing, and our collaboration on these issues greatly enhances the effectiveness of our efforts.

FinCEN's mission is to safeguard the financial system from illicit use, combat money laundering and promote national security through the collection, analysis, and dissemination of financial intelligence and strategic use of financial authorities. FinCEN works to achieve its mission through a broad range of interrelated strategies, including:

- Administering the Bank Secrecy Act (BSA) - the United States' primary anti-money laundering (AML)/counter-terrorist financing (CFT) regulatory regime;
- Sharing the rich financial intelligence we collect, as well as our analysis and expertise, with law enforcement, intelligence, and regulatory partners; and,
- Building global cooperation and technical expertise among financial intelligence units throughout the world.

To accomplish these activities, FinCEN employs a team comprised of approximately 340 dedicated employees with a broad range of expertise in illicit finance, financial intelligence, the financial industry, the AML/CFT regulatory regime, technology, and enforcement. We also leverage our close relationships with regulatory, law enforcement, international, and industry partners to increase our collective insight and better protect the U.S. financial system.

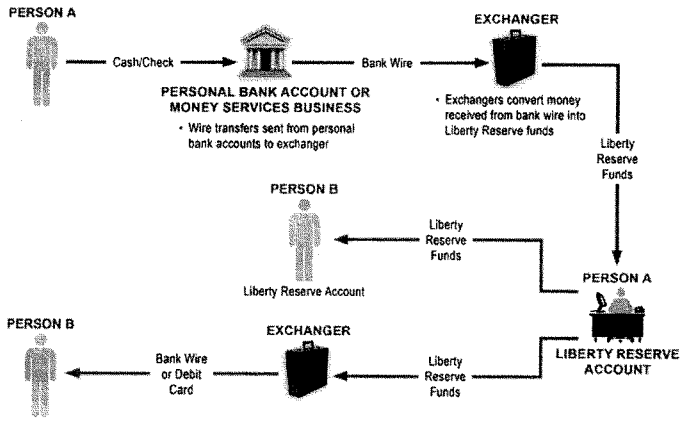
What is Virtual Currency?

Before moving into a discussion of FinCEN's role in ensuring we have smart regulation for virtual currency that is not too burdensome but also protects the U.S. financial system from illicit use, let me set the stage with some of the definitions we are using at FinCEN to understand virtual currency and the various types present in the market today. Virtual currency is a medium of exchange that operates like a currency in some environments but does not have all the

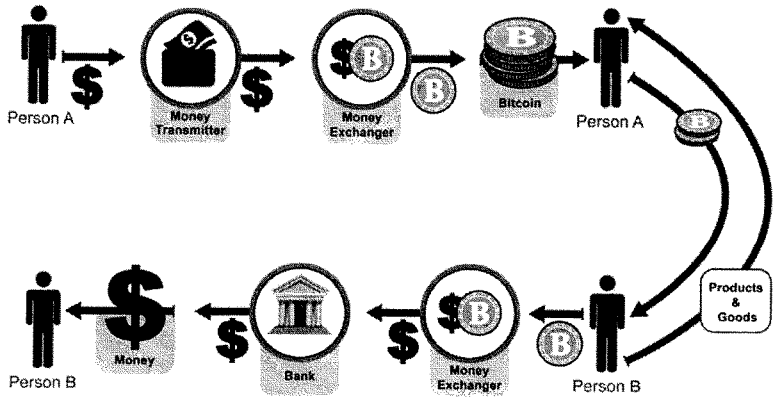
attributes of real currency. In particular, virtual currency does not have legal tender status in any jurisdiction. A *convertible* virtual currency either has an equivalent value in real currency, or acts as a substitute for real currency. In other words, it is a virtual currency that can be exchanged for real currency. At FinCEN, we have focused on two types of convertible virtual currencies: centralized and decentralized.

Centralized virtual currencies have a centralized repository and a single administrator. Liberty Reserve, which FinCEN identified earlier this year as being of primary money laundering concern pursuant to Section 311 of the USA PATRIOT Act, is an example of a centralized virtual currency. Decentralized virtual currencies, on the other hand, and as the name suggests, have no central repository and no single administrator. Instead, value is electronically transmitted between parties without an intermediary. Bitcoin is an example of a decentralized virtual currency. Bitcoin is also known as cryptocurrency, meaning that it relies on cryptographic software protocols to generate the currency and validate transactions

There are a variety of methods an individual user might employ to obtain, spend, and then "cash out" either a centralized or decentralized virtual currency. The following illustration shows a typical series of transactions in a centralized virtual currency, such as Liberty Reserve:



By way of comparison, the next illustration shows a very similar series of transactions in a decentralized virtual currency such as Bitcoin:



From a "follow the money" standpoint, the main difference between these two series of transactions is the absence of an "administrator" serving as intermediary in the case of Bitcoin.

This difference does have significance in FinCEN's regulatory approach to virtual currency, and that approach will be addressed further during the course of my testimony today.

Money Laundering Vulnerabilities in Virtual Currencies

Any financial institution, payment system, or medium of exchange has the potential to be exploited for money laundering or terrorist financing. Virtual currency is not different in this regard. As with all parts of the financial system, though, FinCEN seeks to understand the specific attributes that make virtual currency vulnerable to illicit use, so that we can both employ a smart regulatory approach and encourage industry to develop mitigating features in its products.

Some of the following reasons an illicit actor might decide to use a virtual currency to store and transfer value are the same reasons that legitimate users have, while other reasons are more nefarious. Specifically, an illicit actor may choose to use virtually currency because it:

- Enables the user to remain relatively anonymous;
- Is relatively simple for the user to navigate;
- May have low fees;
- Is accessible across the globe with a simple Internet connection;
- Can be used both to store value and make international transfers of value;
- Does not typically have transaction limits;
- Is generally secure;
- Features irrevocable transactions;

- Depending on the system, may have been created with the intent (and added features) to facilitate money laundering;
- If it is decentralized, has no administrator to maintain information on users and report suspicious activity to governmental authorities;
- Can exploit weaknesses in the anti-money laundering/counter terrorist financing (AML/CFT) regimes of various jurisdictions, including international disparities in, and a general lack of, regulations needed to effectively support the prevention and detection of money laundering and terrorist financing.

Because any financial institution, payment system, or medium of exchange has the potential to be exploited for money laundering, fighting such illicit use requires consistent regulation across the financial system. Virtual currency is not different from other financial products and services in this regard. What is important is that financial institutions that deal in virtual currency put effective AML/CFT controls in place to harden themselves from becoming the targets of illicit actors that would exploit any identified vulnerabilities.

Indeed, the idea that illicit actors might exploit the vulnerabilities of virtual currency to launder money is not merely theoretical. We have seen both centralized and decentralized virtual currencies exploited by illicit actors. Liberty Reserve used its centralized virtual currency as part of an alleged $6 billion money laundering operation purportedly used by criminal organizations engaged in credit card fraud, identity theft, investment fraud, computer hacking, narcotics trafficking, and child pornography. One Liberty Reserve co-founder has already pleaded guilty to money laundering in the scheme. And just recently, the Department of Justice has alleged that

customers of Silk Road, the largest narcotic and contraband marketplace on the Internet to date, were required to pay in bitcoins to enable both the operator of Silk Road and its sellers to evade detection and launder hundreds of millions of dollars. With money laundering activity already valued in the billions of dollars, virtual currency is certainly worthy of FinCEN's attention.

That being said, it is also important to put virtual currency in perspective as a payment system. The U.S. government indictment and proposed special measures against Liberty Reserve allege it was involved in laundering more than $6 billion. Administrators of other major centralized virtual currencies report processing similar transaction volumes to what Liberty Reserve did. In the case of Bitcoin, it has been publicly reported that its users processed transactions worth approximately $8 billion over the twelve-month period preceding October 2013; however, this measure may be artificially high due to the extensive use of automated layering in many Bitcoin transactions. By way of comparison, according to information reported publicly, in 2012 Bank of America processed $244.4 trillion in wire transfers, PayPal processed approximately $145 billion in online payments, Western Union made remittances totaling approximately $81 billion, the Automated Clearing House (ACH) Network processed more than 21 billion transactions with a total dollar value of $36.9 trillion, and Fedwire, which handles large-scale wholesale transfers, processed 132 million transactions for a total of $599 trillion. This relative volume of transactions becomes important when you consider that, according to the United Nations Office on Drugs and Crime (UNODC), the best estimate for the amount of all global criminal proceeds available for laundering through the financial system in 2009 was $1.6 trillion. While of growing concern, to date, virtual currencies have yet to overtake more traditional methods to move funds internationally, whether for legitimate or criminal purposes.

Mitigating Money Laundering Vulnerabilities in Virtual Currencies

FinCEN's main goal in administering the BSA is to ensure the integrity and transparency of the U.S. financial system so that money laundering and terrorist financing can be prevented and, where it does occur, be detected for follow on action. One of our biggest challenges is striking the right balance between the costs and benefits of regulation. One strategy we use to address this challenge is to promote consistency, where possible, in our regulatory framework across different parts of the financial services industry. It ensures a level playing field for industry and minimizes gaps in our AML/CFT coverage.

Recognizing the emergence of new payment methods and the potential for abuse by illicit actors, FinCEN began working with our law enforcement and regulatory partners several years ago to study the issue. We understood that AML protections must keep pace with the emergence of new payment systems, such as virtual currency and prepaid cards, lest those innovations become a favored tool of illicit actors. In July 2011, after a public comment period designed to receive feedback from industry, FinCEN released two rules that update several definitions and provide the needed flexibility to accommodate innovation in the payment systems space under our preexisting regulatory framework. Those rules are: (1) Definitions and Other Regulations Relating to Money Services Businesses; and (2) Definitions and Other Regulations Relating to Prepaid Access.

The updated definitions reflect FinCEN's earlier guidance and rulings, as well as current business operations in the industry. As such, they have been able to accommodate the

development of new payment systems, including virtual currency. Specifically, the new rule on money services businesses added the phrase "other value that substitutes for currency" to the definition of "money transmission services." And since a convertible virtual currency either has an equivalent value in real currency, or acts a substitute for real currency, it qualifies as "other value that substitutes for currency" under the definition of "money transmission services." A person that provides money transmission services is a "money transmitter," a type of money services business already covered by the AML/CFT protections in the BSA.

As a follow-up to the regulations and in an effort to provide additional clarity on the compliance expectations for those actors involved in virtual currency transactions subject to FinCEN oversight, on March 18, 2013, FinCEN supplemented its money services business regulations with interpretive guidance designed to clarify the applicability of the regulations implementing the BSA to persons creating, obtaining, distributing, exchanging, accepting, or transmitting virtual currencies. In the simplest of terms, FinCEN's guidance explains that administrators or exchangers of virtual currencies must register with FinCEN, and institute certain recordkeeping, reporting and AML program control measures, unless an exception to these requirements applies. The guidance also explains that those who use virtual currencies exclusively for common personal transactions like buying goods or services online are users, not subject to regulatory requirements under the BSA. In all cases, FinCEN employs an activity-based test to determine when someone dealing with virtual currency qualifies as a money transmitter. The guidance clarifies definitions and expectations to ensure that businesses engaged in such activities are aware of their regulatory responsibilities, including registering appropriately. Furthermore, FinCEN closely coordinates with its state regulatory counterparts to encourage appropriate

application of FinCEN guidance as part of the states' separate AML compliance oversight of financial institutions.

It is in the best interest of virtual currency providers to comply with these regulations for a number of reasons. First is the idea of corporate responsibility. Legitimate financial institutions, including virtual currency providers, do not go into business with the aim of laundering money on behalf of criminals. Virtual currencies are a financial service, and virtual currency administrators and exchangers are financial institutions. As I stated earlier, any financial institution could be exploited for money laundering purposes. What is important is for institutions to put controls in place to deal with those money laundering threats, and to meet their AML reporting obligations.

At the same time, being a good corporate citizen and complying with regulatory responsibilities is good for a company's bottom line. Every financial institution needs to be concerned about its reputation and show that it is operating with transparency and integrity within the bounds of the law. Legitimate customers will be drawn to a virtual currency or administrator or exchanger where they know their money is safe and where they know the company has a reputation for integrity. And banks will want to provide services to administrators or exchangers that show not only great innovation, but also great integrity and transparency.

The decision to bring virtual currency within the scope of our regulatory framework should be viewed by those who respect and obey the basic rule of law as a positive development for this sector. It recognizes the innovation virtual currencies provide, and the benefits they might offer

society. Several new payment methods in the financial sector have proven their capacity to empower customers, encourage the development of innovative financial products, and expand access to financial services. We want these advances to continue. However, those institutions that choose to act outside of their AML obligations and outside of the law have and will continue to be held accountable. FinCEN will do everything in its regulatory power to stop such abuses of the U.S. financial system.

As previously mentioned, earlier this year, FinCEN identified Liberty Reserve as a financial institution of primary money laundering concern under Section 311 of the USA PATRIOT Act. Liberty Reserve operated as an online, virtual currency, money transfer system conceived and operated specifically to allow – and encourage – illicit use because of the anonymity it offered. It was deliberately designed to avoid regulatory scrutiny and tailored its services to illicit actors looking to launder their ill-gotten gains. According to the allegations contained in a related criminal action brought by the U.S. Department of Justice, those illicit actors included criminal organizations engaged in credit card fraud, identity theft, investment fraud, computer hacking, narcotics trafficking, and child pornography, just to name a few. The 311 action taken by FinCEN was designed to restrict the ability of Liberty Reserve to access the U.S. financial system, publicly notify the international financial community of the risks posed by Liberty Reserve, and to send a resounding message to other offshore money launderers that such abuse of the U.S. financial system will not be tolerated and their activity can be reached through our targeted financial measures.

Sharing Our Knowledge and Expertise on Virtual Currency

As the financial intelligence unit for the United States, FinCEN must stay current on how money is being laundered in the United States, including through new and emerging payment systems, so that we can share this expertise with our many law enforcement, regulatory, industry, and foreign financial intelligence unit partners, and effectively serve as the cornerstone of this country's AML/CFT regime. FinCEN has certainly sought to meet this responsibility with regard to virtual currency and its exploitation by illicit actors. In doing so, we have drawn and continue to draw from the knowledge we have gained through our regulatory efforts, use of targeted financial measures, analysis of the financial intelligence we collect, independent study of virtual currency, outreach to industry, and collaboration with our many partners in law enforcement.

In the same month we issued our guidance on virtual currency, March 2013, FinCEN also issued a Networking Bulletin on crypto-currencies to provide a more granular explanation of this highly complex industry to law enforcement and assist it in following the money as it funnels between virtual currency channels and the U.S. financial system. Among other things, the bulletin addresses the role of traditional banks, money transmitters, and exchangers that come into play as intermediaries by enabling users to fund the purchase of virtual currencies and exchange virtual currencies for other types of currency. It also highlights known records processes associated with virtual currencies and the potential value these records may offer to investigative officials. The bulletin has been in high demand since its publication and the feedback regarding its tremendous value has come from the entire spectrum of our law enforcement partners. In

fact, demand for more detailed information on crypto-currencies has been so high that we have also shared it with several of our regulatory and foreign financial intelligence unit partners.

One feature of a FinCEN Networking Bulletin is that it asks the readers to provide ongoing feedback on what they are learning through their investigations so that we can create a forum to quickly learn of new developments, something particularly important with a new payment method. Based on what we are learning through this forum and other means, FinCEN has issued several analytical products of a tactical nature to inform law enforcement operations.

Equally important to our ongoing efforts to deliver expertise to our law enforcement partners is FinCEN's engagement with our regulatory counterparts to ensure they are kept apprised of the latest trends in virtual currencies and the potential vulnerabilities they pose to traditional financial institutions under their supervision. FinCEN uses its collaboration with the Federal Financial Institutions Examination Council (FFIEC) BSA Working Group as a platform to review and discuss FinCEN's regulations and guidance, and the most recent and relevant trends in virtual currencies. One such example occurred just recently, when several FinCEN virtual currency experts gave a comprehensive presentation on the topic to an audience of Federal and state bank examiners at an FFIEC Payment Systems Risk Conference. The presentation covered an overview of virtual currency operations, FinCEN's guidance on the application of FinCEN regulations to virtual currency, enforcement actions, and ongoing industry outreach efforts.

FinCEN also participates in the FBI-led Virtual Currency Emerging Threats Working Group, the FDIC-led Cyber Fraud Working Group, the Terrorist Financing & Financial Crimes-led Treasury Cyber Working Group, and with a community of other financial intelligence units. We host

speakers, discuss current trends, and provide information on FinCEN resources and authorities as we work with our partners in an effort to foster an open line of communication across the government regarding bad actors involved in virtual currency and cyber-related crime.

Finally, FinCEN has shared its strategic analysis on money laundering through virtual currency with executives at many of our partner law enforcement and regulatory agencies, and foreign financial intelligence units, as well as with U.S. government policy makers.

Outreach to the Virtual Currency Industry

Recognizing that the new, expanded definition of money transmission would bring new financial entities under the purview of FinCEN's regulatory framework, shortly after the publication of the interpretive guidance and as part of FinCEN's ongoing commitment to engage in dialogue with the financial industry and continually learn more about the industries that we regulate, FinCEN announced its interest in holding outreach meetings with representatives from the virtual currency industry. The meetings are designed to hear feedback on the implications of recent regulatory responsibilities imposed on this industry, and to receive industry's input on where additional guidance would be helpful to facilitate compliance.

We held the first such meeting with representatives of the Bitcoin Foundation on August 26, 2013 at FinCEN's Washington, DC offices and included attendees from a cross-section of the law enforcement and regulatory communities. This outreach was part of FinCEN's overall efforts to increase knowledge and understanding of the regulated industry and how its members are impacted by regulations, and thereby help FinCEN most efficiently and effectively work with

regulated entities to further the common goals of the detection and deterrence of financial crime. To further capitalize on this important dialogue and exchange of ideas, FinCEN has invited the Bitcoin Foundation to provide a similar presentation at the next plenary of the Bank Secrecy Act Advisory Group (BSAAG) scheduled for mid-December. The BSAAG is a Congressionally-chartered forum that brings together representatives from the financial industry, law enforcement, and the regulatory community to advise FinCEN on the functioning of our AML/CFT regime.

Conclusion

The Administration has made appropriate oversight of the virtual currency industry a priority, and as a result, FinCEN's efforts in this regard have increased significantly over recent years through targeted regulatory measures, outreach to regulatory and law enforcement counterparts and our partners in the private sector, and the development of expertise. We are very encouraged by the progress we have made thus far. We are dedicated to continuing to build on these accomplishments by remaining focused on future trends in the virtual currency industry and how they may inform potential changes to our regulatory framework for the future. Thank you for inviting me to testify before you today. I would be happy to answer any questions you may have.

Department of Justice

STATEMENT OF

MYTHILI RAMAN
ACTING ASSISTANT ATTORNEY GENERAL
CRIMINAL DIVISION
U.S. DEPARTMENT OF JUSTICE

BEFORE THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS
UNITED STATES SENATE

FOR A HEARING ENTITLED

"BEYOND THE SILK ROAD: POTENTIAL RISKS, THREATS AND PROMISES OF VIRTUAL CURRENCIES"

PRESENTED ON

NOVEMBER 18, 2013

Statement of Mythili Raman
Acting Assistant Attorney General, Criminal Division
Before the United States Senate
Committee on Homeland Security and Governmental Affairs
"Beyond the Silk Road: Potential Risks, Threats and Promises of Virtual Currencies"
November 18, 2013

Chairman Carper, Ranking Member Coburn, and distinguished Members of the Committee: Thank you for the opportunity to appear before the Committee today to discuss the Department of Justice's work regarding virtual currencies. I am honored to represent the Department at this hearing and to describe for you our approach to virtual currencies, our recent successes in prosecuting criminals who use virtual currencies for illicit purposes, and some of the challenges we face as virtual currency systems continue to evolve.

Introduction

The Department of Justice recognizes that many virtual currency systems offer legitimate financial services and have the potential to promote more efficient global commerce. We have also seen, however, that certain aspects of virtual currencies appeal to criminals and present a host of new challenges to law enforcement.

The concept of virtual currencies is not new to the Department and, indeed, the Department has investigated and prosecuted the illicit use of virtual currencies since the late 1990s, when criminals first began using systems such as WebMoney and e-Gold to conduct their business. Over the last 15 years, however, virtual currencies have evolved and diversified significantly, challenging the Department to adapt our capabilities to deal with new systems and threats.

As with all emerging technologies, the Department has aggressively used our existing tools and capabilities to combat illegal activities involving virtual currencies. The Department has two primary law enforcement interests in virtual currency: (1) deterring and prosecuting criminals using virtual currency systems to move or hide money that is used to facilitate, or is derived from, criminal or terrorist acts, *i.e.*, money laundering; and (2) investigating and prosecuting those virtual currency services that themselves violate laws aimed at illegal money transmission and money laundering. As I will describe in my testimony, the Department is committed to using all the tools at our disposal to ensure that those law enforcement interests are met, even as virtual currency systems evolve.

Illicit Use

"Virtual currency" is a medium of exchange circulated over a network, typically the Internet, which is not backed by a government. These systems can be both centralized and decentralized.

Early centralized models, where the currency is controlled by a single private entity, have expanded and now encompass a wide range of business concepts. Some centralized virtual currencies take the form of digital precious metals, such as e-Gold and Pecunix, where users exchange digital currency units ostensibly backed by gold bullion or other precious metals. Others exist within popular online games or virtual worlds, such as Farmville, Second Life, or World of Warcraft. Still others are online payment systems such as WebMoney and Liberty Reserve, which are available generally outside of specific online communities and denominate users' accounts in virtual currency rather than U.S. Dollars, Euros, or some other national currency. Decentralized systems such as Bitcoin, which have no centralized administrating authority and instead operate as peer-to-peer transaction networks, entered the scene relatively recently but are growing rapidly. A network of sites and services, including exchangers who buy and sell virtual currencies in exchange for national currencies or other mediums of value, have developed around virtual currency systems, as well.

Criminals are nearly always early adopters of new technologies and financial systems, and virtual currency is no exception. As virtual currency has grown, it has attracted illicit users along with legitimate ones. Our experience has shown that some criminals have exploited virtual currency systems because of the ability of those systems to conduct transfers quickly, securely, and often with a perceived higher level of anonymity than that afforded by traditional financial services. The irreversibility of many virtual currency transactions additionally appeals to a variety of individuals seeking to engage in illicit activity, as does their ability to send funds cross-border.

Cyber criminals were among the first illicit groups to take widespread advantage of virtual currency. We have seen that many players in the cyber underground rely on virtual currency to conduct financial transactions. Early users of virtual currency also included criminals involved in the trafficking of child pornography, credit card fraud, identity theft, and high-yield investment schemes. As virtual currency became more widespread and criminals became increasingly computer savvy, other criminal groups moved to capitalize on virtual currency, as well. There are now public examples of virtual currency being used by nearly every type of criminal imaginable.

It is not surprising that criminals are drawn to services that allow users to conduct financial transactions while remaining largely anonymous. And, indeed, some of the criminal activity occurs through online black markets, many of which operate as Tor hidden services. Tor hidden services are sites accessible only through Tor, an anonymizing network that masks users' Internet traffic by routing it through a series of volunteer servers, called "nodes," across the globe. Online black markets capitalize on Tor's anonymizing features to offer a wide selection of illicit goods and services, ranging from pornographic images of children to dangerous narcotics to stolen credit card information.

At the same time, we have seen that though virtual currency systems are growing rapidly, few systems currently exist that could easily accommodate the hundreds of millions of dollars often moved in a single large-scale money laundering scheme. Transaction size is limited by the carrying capacity of the virtual currency systems and the exchangers. When taken in the aggregate, however, the relatively small dollar values associated with most illicit virtual currency

transactions quickly add up. At their prime, e-Gold and Liberty Reserve, two virtual currency systems prosecuted by the Department, each moved the equivalent of over $1 billion in illegal proceeds annually. As virtual currencies grow, the capacity for larger single transactions grows, as well.

The Department has prosecuted several of these systems, such as e-Gold, based on evidence that they can be, and often are, intentionally designed to facilitate illegal activity. These services typically do not conduct any meaningful customer due diligence and do not screen for transactions related to money laundering or terrorist financing. At the same time, these complicit and illicit businesses allow users to conceal their identities and maintain high levels of anonymity during transactions.

To be clear, virtual currency is not necessarily synonymous with anonymity. A convertible virtual currency with appropriate anti-money laundering and know-your-customer controls, as required by U.S. law, can safeguard its system from exploitation by criminals and terrorists in the same way any other money services business could. As virtual currency systems develop, it is imperative to law enforcement interests that those systems comply with applicable anti-money laundering and know-your-customer controls.

Department Actions

Exploitation by malicious actors is a problem faced by all types of financial services and is not unique to virtual currency systems. Although malicious actors have utilized emerging technologies to further their criminal schemes, the Department has thus far been able to apply existing tools to ensure vigorous prosecution of these schemes.

The Department relies on money services business, money transmission, and anti-money laundering statutes to curtail this sort of unlawful activity. Many virtual currency systems, exchangers, and related services operate as money transmitters, which are part of a larger class of institutions called money services businesses. Money transmitters are required under 31 U.S.C. § 5330 to register with the Financial Crimes Enforcement Network (FinCEN). Most states also require money transmitters to obtain a state license in order to conduct business in the state. Any money transmitter that fails to register with FinCEN or to obtain the requisite state licensing may be subject to criminal prosecution under 18 U.S.C. § 1960. Additionally, the general money laundering and spending statutes, 18 U.S.C. §§ 1956 and 1957, cover financial transactions involving virtual currencies. Finally, where virtual currencies are used in furtherance of underlying criminal activity, the Department can rely on traditional criminal statutes proscribing that activity, such as narcotics, cybercrime, child exploitation, and firearms laws.

Some of the major prosecutions in recent years involving virtual currency services are as follows.

E-Gold

The Department first took major action against an illicit virtual currency service in 2007, when it indicted e-Gold and its three principal owners on charges related to money laundering

and operating an unlicensed money transmitting business. E-Gold offered digital accounts purportedly backed by physical gold bullion. A valid e-mail address was the only information required to set up an account, allowing users to conduct highly anonymous international transactions over the Internet. As a result, e-Gold became a popular payment method for sellers of child pornography, operators of investment scams, and perpetrators of credit card and identity fraud. At its peak, e-Gold reportedly moved over $6 million each day for more than 2.5 million accounts. In 2008, e-Gold and the three individuals pleaded guilty.

Liberty Reserve

Following the e-Gold indictment, several similar but smaller systems and exchangers were indicted or closed themselves down to evade law enforcement detection. According to publicly filed charging documents, an executive of one of those businesses, Arthur Budovsky, then set out to create Liberty Reserve, an improved centralized virtual currency variation allegedly designed to evade U.S. law enforcement. Among other things, Liberty Reserve operated offshore – it was based in Costa Rica – and purportedly recommended that its customers use money exchangers located in countries without significant governmental money-laundering oversight or regulation. Moreover, Budovsky, the principal founder of Liberty Reserve, was so committed to avoiding the reach of U.S. law that, according to the indictment, in 2011, he formally renounced his U.S. citizenship and became a Costa Rican citizen in order to avoid facing justice in the United States.

Despite Budovsky's alleged efforts, earlier this year, the Department indicted Liberty Reserve and its executives, including Budovsky, for running a $6 billion money laundering operation. In a coordinated action, the Department of the Treasury identified Liberty Reserve as a financial institution of primary money laundering concern under Section 311 of the USA PATRIOT Act, effectively cutting it off from the U.S. financial system.

According to the indictment, Liberty Reserve allowed users to send and receive funds with a high level of anonymity by not requiring users to validate their identities and allowing users to make untraceable fund transfers in exchange for a privacy fee. Many of the transactions were sent to or from users in the United States, but Liberty Reserve never registered with the appropriate U.S. authorities. As revealed in the Department's filings, Liberty Reserve became a system of choice for cyber criminals and was used in a wide array of illegal activity, including credit card fraud, identity theft, investment fraud, computer hacking, and child pornography. As a result of the Department's action, the site was shuttered and effectively put out of business, and seven defendants were charged. One is in custody in the United States, one has entered a guilty plea, three others, including the lead defendant Budovsky, are pending extradition, and two others are at large. The case exemplifies the Department's resolve to pursue purported major money laundering facilitators, even those who hide offshore.

Silk Road

Just last month, the Department took action against one of the most popular online black markets, Silk Road. Allegedly operated by a U.S. citizen living in California at the time of his arrest, Silk Road accepted bitcoins exclusively as a payment mechanism on its site. The

Department's complaint alleges that, in less than three years, Silk Road served as a venue for over 100,000 buyers to purchase hundreds of kilograms of illegal drugs and other illicit goods from several thousand drug dealers and other criminal vendors. The site also purportedly laundered the proceeds of these transactions, amounting to hundreds of millions of dollars in bitcoins. In addition to arresting the site's operator and shutting down the service, the Department to date has seized over 170 thousand bitcoins, valued as of this past Friday, November 15, 2013, at over $70 million.

A separate indictment charges Silk Road's operator with drug distribution conspiracy, attempted witness murder, and using interstate commerce facilities in the commission of murder-for-hire. With regard to the murder-related charges, the indictment alleges that the Silk Road operator paid an undercover federal agent to murder one of the operator's employees.

Unique Challenges

The cases I just described illustrate not only Department successes in combating illicit use of virtual currency, but also many of the challenges investigators face when they encounter these systems, some of which may ultimately require additional legal or regulatory tools.

Virtual currency allows users to send money across the globe without dealing with a traditional financial institution. While this feature provides several benefits for legitimate customers, it can significantly complicate law enforcement efforts to follow the money.

Virtual currency systems have a global reach and clientele. Virtual currency businesses can cater to U.S. clientele while operating on the other side of the world. Investigations into illicit virtual currency businesses therefore often require considerable cooperation from international partners. The Liberty Reserve investigation and takedown, for example, involved coordinated law enforcement action in 17 countries.

The international nature of the transactions poses an additional challenge where the overseas regulatory regime treats virtual currency differently or, as is true in some cases, fails to cover it at all. While this challenge may diminish with the Financial Action Task Force's recent guidance addressing the need for all countries to develop a risk-based approach to new payment products and services, incongruent regulatory regimes will likely remain a challenge when dealing with virtual currency services overseas.

Among the most significant challenges the Department faces in dealing with virtual currency is the difficulty in obtaining customer records. Because decentralized systems lack any sort of administering authority to collect user information or receive legal process, investigators must rely on information collected by other sources, such as exchangers. Even if the target used a centralized system or exchanger, however, accurate customer records may still be difficult to obtain, or may not exist at all. Illicit users are typically attracted to systems with lax anti-money laundering and know-your-customer controls. These services often attempt to evade U.S. action by operating out of countries that have poor regulatory oversight and are less willing to cooperate with U.S. law enforcement. Even if the system at issue operates in a country with effective regulation and a cooperative relationship with the United States, the legal process for

obtaining foreign records is relatively slow when compared to the near-instantaneous speed at which the virtual currency user can send the funds to another jurisdiction.

A final challenge arises from the link between virtual currency and encryption. Decentralized virtual currencies typically rely on an encryption algorithm, rather than a central authority, to administer the currency. These encryption-based currencies, also known as cryptocurrencies, lack a central administering authority that might otherwise possess valuable evidence. In addition, users of these currencies often encrypt their digital wallets, complicating our efforts to seize and forfeit criminal proceeds.

Collaborative Efforts

The Department recognizes that virtual currency's ability to facilitate the global movement of funds by a wide array of illicit actors necessitates a comprehensive and collaborative approach with our domestic and international partners. To promote such coordination, the Department is an active participant in the Virtual Currency Emerging Threats Working Group (VCET). VCET was founded by the Federal Bureau of Investigation (FBI) in early 2012 to mitigate the cross-programmatic threats arising from illicit actors' use of virtual currency systems. The group leverages the collective subject matter expertise of its members to address issues arising from illicit actors' use of virtual currency, and deconflicts and shares information and concerns. VCET members represent an array of U.S. Government agencies, including, within the Department, the FBI, the Drug Enforcement Administration, multiple U.S. Attorney's Offices, and the Criminal Division's Asset Forfeiture and Money Laundering Section and Computer Crime and Intellectual Property Section.

The Department contributes to several additional interagency groups concerning virtual currencies and emerging payment systems, including the New Payment Methods Ad Hoc Working Group, a subgroup of the Terrorist Finance Working Group, led by the State Department. The FBI specifically has issued numerous intelligence products related to virtual currency, many of which were coauthored with other members of the U.S. Intelligence Community.

The Department is committed to working with our regulatory partners to ensure appropriate coordination on regulatory issues related to virtual currency. The Department participated in meetings and discussions with FinCEN regarding the July 2011 Final Rule on Money Services Businesses and its applicability to virtual currencies, as well as the related March 18, 2013, FinCEN guidance. The Department regards FinCEN's regulation of many virtual currency services as money transmitters, as well as the resulting applicability of anti-money laundering and know-your-customer requirements under the Bank Secrecy Act, as crucial tools in preventing malicious actors from exploiting virtual currency systems in furtherance of illicit activity.

The Department works closely with FinCEN and the Department of Treasury to coordinate enforcement actions when appropriate. This relationship allowed the Department to unseal the Liberty Reserve indictment in coordination with Treasury's announcement naming the company as a financial institution of primary money laundering concern under Section 311 of the

USA PATRIOT Act. Such coordinated actions are integral tools in combating illicit finance.

Future Trends

The Department anticipates that virtual currency will continue to evolve and grow in popularity. That growth inevitably will be accompanied by an increase in illicit transactions, which makes it critical that virtual currency services understand their legal obligations and requirements. The Department is encouraged by the increasing prominence of legitimate virtual currency services that are attempting to comply with U.S. law. While a number of services have registered at the federal level, many are still struggling with implementing appropriate anti-money laundering, know-your-customer, and customer due diligence programs, as well as complying with state-level regulations and licensing requirements. As members of the U.S. financial community, virtual currency services can and must safeguard themselves from exploitation by criminals and terrorists by implementing legally required anti-money laundering and know-your-customer controls.

As the Administration's Strategy to Combat Transnational Organized Crime recognizes, transnational organized crime networks are increasingly involved in cybercrime, and can imperil consumers' faith in emerging digital systems. We must also pay close attention to the critical role of facilitators who cross both the licit and illicit worlds and provide services to legitimate customers and criminals alike.

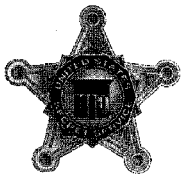
The Department recognizes that malicious actors are often resourceful, and even legitimate virtual currency services can become unwitting conduits for illicit transactions when these actors are able to defeat or circumvent anti-money laundering controls. Outreach to these systems, much as the Department conducts with the formal financial sector, is an important tool in combating the exploitation of the systems for criminal and terrorist purposes. Because centralized payment systems and exchangers often interact with the traditional financial sector and hold bank accounts at major financial institutions, the range of such Department outreach extends to the financial services community at large, complementing the outreach and training efforts of FinCEN, the primary BSA regulator, and the Department of the Treasury. Department of Justice personnel routinely provide trainings to the private sector, as well as to domestic and international law enforcement and intelligence personnel, and specifically address virtual currency.

Law enforcement, Congress, and regulators must remain vigilant to ensure that the U.S. legal and regulatory structure is sufficiently robust to cover decentralized virtual currencies. The Department looks forward to working with Congress to ensure that law enforcement continues to have the tools necessary to combat the use of virtual currency for illicit purposes.

Conclusion

Chairman Carper and Ranking Member Coburn, I thank you for this opportunity to discuss the Department's work on virtual currency.

I look forward to any questions that you may have.



Edward Lowery III

Special Agent in Charge
Criminal Investigative Division,
U.S. Secret Service

Prepared Testimony

Before the
United States Senate Committee on
Homeland Security and Governmental Affairs

November 18, 2013

Good afternoon Chairman Carper, Ranking Member Coburn, and distinguished Members of the Committee. Thank you for the opportunity to testify on behalf of the U.S. Department of Homeland Security (DHS) regarding the risks and challenges posed by digital currencies[1] and the role of the U.S. Secret Service (Secret Service) in investigating crimes associated with online payment systems. Fraudulent schemes and money laundering are the Secret Service's chief concerns with respect to digital currencies and the facilitation of other serious crimes. The Secret Service is committed to adapting to evolving cyber threats by conducting robust investigations of offenses involving digital currencies within its jurisdiction in order to effectively suppress criminal activity.

As the original guardian of the nation's financial payment systems, since 1865 the Secret Service has conducted investigations to protect American consumers, industries, financial institutions, and critical infrastructure from criminal exploit. Accordingly, the Secret Service has extensive authority and responsibility to investigate financial crimes and dismantle the infrastructure that supports these criminal activities, including when these crimes are conducted through cyberspace. In executing our mission, the Secret Service closely partners with Federal, state, local, and international law enforcement agencies and other interagency partners. Notably, the Secret Service and U.S. Immigration and Customs Enforcement's Homeland Security Investigations (ICE/HSI)[2] partner through the Secret Service's Electronic Crimes Task Forces (ECTFs),[3] which leverage the private sector, academia, and state and local law enforcement to support cyber crime investigations. As former Department of Treasury law enforcement agencies, the Secret Service and ICE/HSI partner closely with the Financial Crimes Enforcement Network (FinCEN) and the Department of Treasury in conducting financial crime investigations. In addition, the Secret Service and ICE/HSI participate in the Virtual Currency Threats Working Group and other collaborative efforts with regulators and the national security staff to address the challenges posed by digital currencies and new payment systems.

Over the past decade, in addition to their many legitimate uses, digital currencies—by which I mean digital representations of both real national currencies, or fiat currency, and virtual currencies, which do not constitute the legal tender of any jurisdiction—have attracted malicious actors seeking to hide illicit money transactions. Accordingly, the Secret Service has developed

[1] Digital currencies are a form of electronic money used as alternate currencies. Currently no digital currency serves as legal tender or administered by a national government or central bank; as such digital currencies are a subset of virtual currencies.

[2] ICE/HSI is an investigatory arm of DHS with the jurisdiction and authority to investigate violations involving the illicit importation and exportation of merchandise, bulk cash smuggling, and financial crimes involving a nexus to the border.

[3] Section 105 of the USA PATRIOT Act of 2001 directed the Secret Service to establish a "a national network of electronic crimes task forces, ... for the purpose of preventing, detecting, and investigating various forms of electronic crimes, including potential terrorist attacks against critical infrastructure and financial payment systems." The first Secret Service ECTF was established in New York in 1995; today the Secret Service operates 33 ECTFs, as part of an expanding international network that partners Federal, state, and local law enforcement with the private sector and academia to effectively investigate cyber and cyber-related crimes.

extensive experience in conducting investigations that involve digital currencies. The Secret Service and its interagency partners have investigated and shutdown two major illicit providers of digital currencies that supported extensive criminal activity: e-Gold Ltd. in 2007 and Liberty Reserve earlier this year. Additionally, the Secret Service investigated and shutdown illicit digital currency exchangers, such as Western Express. This successful investigation and prosecution recently concluded with 15 convictions, thanks to the dedicated eight-year effort of the Manhattan District Attorney's Office and the Secret Service's New York/New Jersey ECTF. These and other criminal investigations have provided the Secret Service with a better understanding of the risks and challenges posed by digital currencies.

Criminal Use of Digital Currencies

In recent years, digital currencies have become a preferred form of money for criminals to conduct their illicit activities. Digital currencies provide an efficient means of moving large sums of money globally for both legitimate and criminal purposes. However, as a form of virtual currency,[4] many digital currencies attempt to operate outside the legal and regulatory systems many countries have established to govern legal tender. Additionally, digital currencies often provide a greater anonymity than the traditional banking system. These attributes make digital currencies a preferred tool of transnational criminal organizations for conducting their criminal activities, transmitting their illicit revenue internationally, and laundering their profits.

Based on Secret Service investigations into the criminal use of digital currencies, criminals prefer those they assess to offer:

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 digital currency's ability to be an efficient means to transmit and store wealth.
4) Widespread adoption in the criminal underground.
5) Trustworthiness.

Consequently, as part of its mission to suppress criminal activity, the Secret Service's investigations into digital currency exchangers and administrators have focused on those currencies with the above attributes that play an instrumental role in enabling large-scale criminal activity in violation of laws under Secret Service jurisdiction.[5]

---

[4] FinCEN defines "virtual currency" as those currencies that operates like currency in some environments, but does not have legal tender status in any jurisdiction. Department of Treasury Financial Crimes Enforcement Network, Guidance FIN-2013-G0001 "Application of FinCEN's Regulations to Persons Administrating, Exchanging, or using Virtual Currencies" (March 18, 2013).

[5] Most notably 18 U.S.C. §§ 1028, 1029, 1030, 1343, 1956, 1960, et al.

Digital currencies differ as to their principal criminal uses. Some digital currencies are primarily used to purchase illicit goods and services (e.g., drugs, credit card information, personally identifiable information (PII), and other contraband or criminal services). Other digital currencies are primarily used for money laundering: concealing transactions involving large amounts of money—particularly transnational transfers. The greatest risks are posed by digital currencies that have widespread use for both of these criminal purposes: e-Gold and Liberty Reserve are prime examples of these high-risk digital currencies.

e-Gold

e-Gold was founded in 1996 and offered a pseudonymous digital currency that was originally backed with gold coins stored in a safe deposit box in Florida. A valid email address was the only information that was required to open an e-Gold account. Although other contact information was requested, it was not verified. Thousands of e-Gold users opened their accounts with blatantly false information, such as using the names "Mickey Mouse" or "Donald Duck," among others. Once people opened e-Gold accounts, they could fund them by using exchangers who converted U.S. currency into e-Gold. When these accounts were established and funded, the account holders could gain access through the Internet and conduct anonymous transactions with other e-Gold account holders anywhere in the world.

e-Gold quickly became the preferred financial transaction method of transnational cyber criminals—particularly those involved in the trafficking of stolen financial information and PII of U.S. citizens—and a tool for money laundering by cyber criminals. Criminals' reliance on e-Gold to facilitate certain crimes, including the purchase of child pornography and money laundering, made it the focus of a successful joint investigation by the Secret Service, IRS Criminal Investigations (IRS-CI), the Federal Bureau of Investigation, and the Florida-based St. Cloud Internal Revenue Service-Secret Service Financial Crimes and Money Laundering Task Force. The case was prosecuted by the U.S. Attorney's Office for the District of Columbia, the Department of Justice's Computer Crime and Intellectual Property Section and Asset Forfeiture and Money Laundering Section (AFMLS), with assistance from the Criminal Division's Child Exploitation and Obscenity Section. e-Gold and its corporate affiliate pled guilty to money laundering and operating an unlicensed money transmitting business. The principal director of e-Gold and its corporate affiliate, as well as senior leaders, pled guilty to conspiracy to engage in money laundering and operating an unlicensed money transmitting business. e-Gold's gold reserve was liquidated for $90 million to allow legitimate account holders to claim their assets. As of December 18, 2012, over $10.8 million contained in 12,869 accounts has been forfeited to the Federal Government as part of an on-going asset forfeiture process.

Liberty Reserve[6]

Liberty Reserve was a Costa Rica-based digital currency service that provided what it described as "instant, real-time currency for international commerce" that can be used to "send and receive payments from anyone, anywhere on the globe." Additionally, Liberty Reserve described itself as the Internet's "largest payment processor and money transfer system," serving "millions" of people around the world, including the United States. The alleged principal founder of Liberty Reserve moved to Costa Rica to operate Liberty Reserve after being convicted in the United States in December 2006 for operating "Gold Age, Inc." as an unlicensed money transmitting business.

Liberty Reserve was allegedly designed to make anonymous and untraceable financial transactions to support criminal activity and elude law enforcement. Liberty Reserve quickly became the predominant digital currency used for money laundering by transnational organized cyber crime and other criminals. Before the Secret Service-led investigation shutdown Liberty Reserve, it was estimated to have had more than one million users worldwide, with more than 200,000 users in the United States, and to have processed more than 12 million financial transactions, with a combined value of more than $1.4 billion annually. Overall, from 2006 to May of 2013, Liberty Reserve allegedly processed at least 55 million separate financial transactions and is believed to have laundered more than $6 billion in criminal proceeds.[7]

On May 24, 2013, five individuals were arrested in Costa Rica, Spain, and New York for operating Liberty Reserve under charges for conspiracy to commit money laundering and conspiracy and operation of an unlicensed money transmitting business. At the same time, in close coordination with this law enforcement action, the Department of the Treasury identified Liberty Reserve as a financial institution of primary money laundering concern under Section 311 of the USA PATRIOT Act, effectively cutting it off from the U.S. financial system.

Liberty Reserve's alleged role in supporting criminal activity made its shut down a high priority of numerous law enforcement agencies. The Secret Service worked closely with IRS-CI and ICE/HSI as part of the Global Illicit Financial Team (GIFT) to conduct this investigation, and the Secret Service New York/New Jersey ECTF provided vital assistance. In addition, the cooperation and assistance of international law enforcement partners, including the Judicial Investigation Organization in Costa Rica, the National High Tech Crime Unit in the Netherlands, the Spanish National Police, Financial and Economic Crime Unit, the Cyber Crime Unit at the Swedish National Bureau of Investigation, and the Swiss Federal Prosecutor's Office, was paramount to the apprehension of the defendants.

---

[6] Liberty Reserve is currently under prosecution, the information in this section is based on the documents released by Department of Justice at:
http://www.justice.gov/usao/nys/pressreleases/May13/LibertyReserveetalDocuments.php.

[7] Other estimates of the total volume of transactions and money laundered are substantially higher.

This case is being jointly prosecuted by the U.S. Attorney's Office for the Southern District of New York and AFMLS. The investigation and prosecution of Liberty Reserve is also supported by the Department of Justice's Office of International Affairs and Computer Crime and Intellectual Property Section. Over $40 million in assets, located in numerous countries, have been identified and placed under restraint pending forfeiture, and over 30 Liberty Reserve exchanger domain names have been seized.

Western Express

Western Express International, Inc. was a Manhattan corporation that serviced Eastern European criminals and supported global cybercrime by, among other crimes, acting as a digital currency exchanger, illegal money transmitter, and money launderer. Western Express exchanged conventional currency to e-Gold and WebMoney. It was one of the largest digital currency exchangers to operate within the United States. In total, Western Express exchanged $15 million in WebMoney and $20 million in e-Gold, which supported the global trafficking of stolen account data. To date, sixteen individuals have been found guilty through this case, including three citizens of Eastern European countries who were arrested and extradited with the assistance of the Czech Republic and Greece, with the assistance of the Department of Justice's Office of International Affairs.

This investigation was conducted jointly by the Secret Service and the Manhattan (New York County) District Attorney's Office and was successfully prosecuted by the Manhattan District Attorney's Office. The corporation and its officers ultimately pleaded guilty to laundering about $2 million dollars in connection with the scheme. Nine of Western Express' customers were convicted by guilty plea in the conspiracy, which trafficked nearly 100,000 stolen credit card numbers and was responsible for identity theft resulting in losses of more than $5 million. After a two-and-a-half month jury trial, completed this past June, the remaining three defendants were convicted of every count. This case demonstrates how digital currency has allowed criminals around the globe to do their criminal business together while cloaked in anonymity, and despite never meeting each other in person.

Challenges Posed by Digital Currencies

The growing criminal use of digital currencies challenges the effectiveness of U.S. laws and regulations intended to limit the ability of criminals to profit from their illicit activities and move their criminal proceeds. The key U.S. laws that typically pertain to Secret Service investigations involving the illicit administration or exchange of digital currencies include the Bank Secrecy Act of 1970, the Money Laundering Suppression Act of 1994, and Title III of the USA PATRIOT Act of 2001, and associated Federal regulations. The ability of the Secret Service and

other agencies to enforce current laws and regulations to suppress the use of financial systems by criminal enterprises is complicated by the increasingly transnational nature of the criminal organizations and their continued efforts to circumvent these legal controls.

Digital currencies are particularly well-suited for supporting crime that is transnational in nature, thus requiring close international partnership to conduct investigations, make arrests, and seize criminal assets. Fostering these partnerships and conducting these transnational investigations requires continual investment to maintain effective international law enforcement collaborations, and constant efforts to harmonize anti-money laundering laws and regulations. Investigating crimes involving digital currencies and the transnational organized cyber criminals that use them also requires highly skilled criminal investigators. Hiring, developing, and retaining these special agents is a high priority for the Secret Service, but is challenging in the present fiscal environment. Additionally, while digital currencies may support the activities of transnational criminals who prey upon Americans, the administrators and exchangers of digital currencies are often based in other countries in an effort to minimize their exposure to U.S. regulation and law enforcement.

Conclusion

Digital currencies have the potential to support more efficient and transparent global commerce. However, because digital currencies continue to be used to facilitate illicit activity as well, law enforcement must continually adapt their investigative tools and techniques to dismantle criminal groups that use digital currencies for fraudulent activity or money laundering. Chairman Carper and Ranking Member Coburn, thank you for this opportunity to testify regarding the investigations conducted by the Secret Service and the lessons learned from these investigations on the evolving use of digital currencies by criminal organizations.

TESTIMONY

of

ERNIE ALLEN

PRESIDENT AND CEO

THE INTERNATIONAL CENTRE FOR MISSING & EXPLOITED CHILDREN

for the

UNITED STATES SENATE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

"Beyond Silk Road: Potential Risks, Threats and Promises of Virtual Currencies"

November 18, 2013

Mr. Chairman and distinguished members of the Committee, I welcome the opportunity to appear before you today to discuss the challenges and opportunities associated with the emerging digital economy. We are deeply grateful for the Committee's leadership on these issues and its long-standing commitment to the safety of our children.

The International Centre for Missing & Exploited Children ("ICMEC") is a not-for-profit corporation, supported entirely by private funds and resources. ICMEC leads a global movement to protect children from sexual exploitation and abduction. We have

- Trained law enforcement in 121 countries;
- Reviewed laws in 200 countries and worked with parliaments in 100 countries to enact new law on child pornography.
- Reviewed laws in 200 countries, developed model law on child sexual exploitation, and worked with parliaments and international bodies to change national legislation and international conventions.
- Created a research institute, the Koons Family Institute on International Law & Policy, to examine child abduction and sexual exploitation and launch policy initiatives with world leaders.
- Built a Global Missing Children's Network, now including 22 countries.
- Worked with Belgium, Romania, South Africa, Russia, Belarus and others to establish national centers on missing & exploited children.
- Created a regional center, the Southeastern European Center on Missing and Exploited Children, serving thirteen countries in the Balkan region.
- Entered into formal partnerships with Interpol, the Organization of American States, the Hague Conference on Private International Law, and others.
- Hosted international conferences, including a 2009 meeting of 400 Arab leaders in Cairo which produced "The Cairo Declaration," an agreement on child protection; a 2010 conference of judges from 15 countries at the US State Department to examine cross-border transportation of children, resulting in the "The Washington Declaration," now cited in case law worldwide; and a 2011 forum in Rome in partnership with the Vatican, the Mayo Clinic and Il Telefono Azzurro, which produced "The Declaration of Rome" on children's rights.
- Managed private sector financial industry and technology industry coalitions to address child sexual exploitation.
- Launched a Global Health Coalition of pharmaceutical companies and health care institutions to attack the problem of child sexual abuse and exploitation not just from a legal and law enforcement perspective but as a public health crisis.
- And there is much more.

I am honored to have the opportunity to address the risks and the promise of virtual currencies. We are enthusiastic about the potential of virtual currencies and the digital economy. We believe that the digital economy can achieve social good, particularly in bringing about real financial inclusion for the 2.5 billion adults on the planet today without access to banks, credit cards or the mainstream financial system. In addition, a digital economy is attractive to tech-centric young people, and has particular appeal in light of the global movement to mobile technologies and mobile payment systems.

Nonetheless, the International Centre for Missing & Exploited Children is involved in this issue because there are risks. For the past year I have consulted with law enforcement and financial experts worldwide. While much of the evidence is still anecdotal, there is consensus that commercial child pornography, sexual exploitation, sex trafficking and other criminal enterprises are increasingly moving to a new unregulated, unbanked digital economy. Through voluntary industry coalitions and following the money through the trails and tunnels of the payments system, these enterprises had declined dramatically. Yet, we have concluded that "we didn't end it, we just moved it."

There are three primary reasons for this migration: (1) anonymity; (2) the emergence of new, digital economy that belongs to no nation and is overseen by no central bank; and (3) most countries have not yet begun to apply existing laws and regulations to virtual currencies at the exchange level; i.e., the point at which virtual currencies are traded for dollars, euros, pounds, yen, etc. A US Treasury Department official told us, "the more virtual currencies function like real currencies, the greater the illicit finance threat." Yet, few countries are addressing this emerging threat.

There are positive signs. In March the Financial Crime Enforcement Network, or FinCEN, in the US issued guidance on the legal status of Bitcoin, the best-known digital currency, under the money laundering laws. Bitcoin exchanges, which exchange Bitcoins for conventional currencies, and most Bitcoin miners are required to register as Money Services Businesses and comply with anti-money laundering regulations. FinCEN indicated that a "money transmitter" is anyone that (1) "accepts and transmits a convertible virtual currency" or (2) "buys or sells convertible virtual currency for any reason." However, Bitcoin users who merely use the currency to purchase goods and services are not required to register. We believe that this is not only a positive step for the issues we are concerned about, it is also a positive step for Bitcoin.

In July the Financial Action Task Force (FATF), the 36-member, inter-governmental body based in Paris, issued similar guidance. The FATF focuses on combating money laundering and the financing of terrorism.

We define key elements of the digital economy as including digital currencies; anonymous online payment systems; anonymous Internet tools; and bulletproof hosting. A primary area of focus is digital currencies, particularly those with bidirectional flow; i.e., digital currencies which are bought and sold at prevailing exchange rates and used to purchase both real and virtual goods and services. The best-known example is Bitcoin.

As a result of our consultations with law enforcement leaders worldwide, ICMEC, in partnership with Thomson Reuters, the global media and information company, set out to find a balanced, reasonable response to the problems associated with the misuse of digital currencies for child sexual exploitation and other criminal activity. In June ICMEC and Thomson Reuters convened a conference on this issue and also met with global financial leaders at the World Bank. As a result we created a Digital Economy Task Force, which includes the Bitcoin Foundation, the Tor Project, the Gates Foundation, the Brookings Institution, the Cato Institute, Vital Voices, law enforcement leaders and others. Our goal is to offer recommendations and real solutions for the threats and risks without jeopardizing the promise and potential of the digital economy.

You asked that I address several questions:

(1) The extent to which virtual currencies are being used directly in child-exploitive or related online criminal activities, or in support of such activities;

(2) The unique challenges that virtual currencies bring for law enforcement investigations and prosecutions; and

(3) The work of our Digital Economy Task Force and other collaborative efforts;

(4) Future trends and potential policy considerations for Congress and other policymakers.

1 – The use of virtual currencies in child-exploitive or related online criminal activities, or in support of such activities.

Great progress has been made in addressing the use of the mainstream payments system for commercial child sexual exploitation. Nonetheless, we are concerned about the apparent migration of commercial child sexual exploitation, including sex abuse images, child exploitation and sex trafficking, along with other criminal enterprises to a new unregulated digital economy, made up of digital currencies; anonymous online payment systems; anonymous internet tools; and file hosting companies.

While much of our evidence regarding the use of digital currencies in child exploitation is anecdotal, a leading law enforcement expert advised us that child pornography producers are using Tor hidden services for the creation and dissemination of child pornography and Bitcoin for payment. However, he cautioned that the market to buy/sell child pornography on Tor hidden services using Bitcoins is small in comparison to the market for drugs and other illegal goods. He called the use of Tor and digital currencies for child pornography "significant" because those involved are the actual producers of the content. Thus, these crimes tend to involve new victims whom law enforcement has not seen before, and creates the presumption that the abuse is likely to be on-going.

There is a twofold challenge for law enforcement: the anonymity provided by Tor and the complexities of Bitcoin. The attractiveness of Tor and Bitcoin for child pornography is based upon a perception of anonymity. Those who use Tor and Bitcoin sacrifice speed for anonymity. Thus, if the perception of anonymity diminishes, we believe the criminal use will diminish with it.

In August 2013 the Irish founder/owner/operator of Freedom Hosting, which the FBI called "the largest facilitator of child pornography on the planet," was arrested. Freedom Hosting maintained servers for a number of Tor-based, so-called "deep web" child pornography sites and others. The best –known child pornography sites included Lolita City, the Love Zone and PedoEmpire, all of which accept Bitcoins for payment.

To shut down Freedom Hosting, law enforcement exploited a "java script exploit," a vulnerability in the site, enabling law enforcement to penetrate Tor and expose the IP addresses of the users of Freedom Hosting. Interestingly, in 2011 the hacktivist group, Anonymous, hacked into Tor to shut down Lolita City. However, Lolita City has reemerged with an estimated 15,000 members and 1.5 million child pornography images.

The digital economy of today is centered on peer-to-peer networks. There is clear evidence of the movement of child pornography and other types of exploitation from Internet Service Providers and central servers to peer-to-peer networks. Law enforcement is having some success in identifying individual users through the use of specialized peer-to-peer investigative tools to penetrate p2p-based operations. Yet, the emergence of a p2p-based digital economy is posing enormous challenges.

Much of the current discussion about digital currencies centers on Bitcoin, which can be bought and sold at prevailing exchange rates and then used to purchase both real and virtual goods and services. It is different from other digital currencies which may be purchased at a specific exchange rate, but may not be exchanged back. Examples are Facebook credits, Amazon coins, or frequent flyer points.

Recently, a judge in Texas ruled that Bitcoin is a currency. He compared it to a precious metal. Today, there are Bitcoin exchanges, like Mt. Gox in Japan, where one can exchange Bitcoins for conventional currencies. All Bitcoin transactions are visible and transparent. The challenge for law enforcement is in going from those transactions to an actual person.

It is not my position that Bitcoin or the emergence of a digital economy is negative. Nonetheless, there are challenges.

2 – The unique challenges that virtual currencies bring for law enforcement investigation and prosecution.

The primary challenge facing law enforcement worldwide today is the growing anonymity surrounding internet transactions and the emergence of a so-called "deep web." In its April 24, 2012 Intelligence Estimate focusing on Bitcoin, ("Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity"), the FBI reported, "Bitcoin...provides a venue for individuals to generate, transfer, launder and steal illicit funds with some anonymity. Bitcoin offers many of the same challenges associated with other virtual currencies, such as WebMoney, and adds unique complexities for investigators because of its decentralized nature."

The FBI report adds, "Since Bitcoin does not have a centralized authority, law enforcement faces difficulties detecting suspicious activity, identifying users, and obtaining transaction records – problems that might attract malicious actors to Bitcoin. Bitcoin might also logically attract money launderers and other criminals who avoid traditional financial systems by using the internet to conduct global money transfers."

All of this is exacerbated by the emergence of Tor, The Onion Router, created by the US government to enable political dissidents to use the internet anonymously, avoiding retaliation from repressive regimes. It is a noble, high-minded, laudable purpose, and it protects not only political dissidents, but also journalists in countries where the practice of journalism is dangerous, victims of domestic violence or stalking, and others.

However, there are unintended consequences. Political dissidents, journalists and stalking victims are not the only ones using Tor. A March 6, 2013 headline in Business Insider read, "There's A Secret Internet For Drug Dealers, Assassins and Pedophiles." We are particularly concerned about the emergence of an unregulated "deep web" utilizing anonymizing hidden services and digital currencies for payment.

The so-called "deep web" made possible by anonymizing tools includes sites like Silk Road, but it also includes sites for the purchase of weapons; counterfeit currencies; assassins; stolen credit cards, fake IDs, and fake passports; and of particular concern to ICMEC, sites like Hard Candy, Jailbait, Lolita City, PedoEmpire, Love Zone and others for child abuse images. All of those sites accept digital currencies for payment.

It is important to note that while the so-called "deep web" is most often associated with Tor, Tor is not the only network being used or being developed to guarantee anonymity and untraceable access. In fact, there are indications that efforts are accelerating globally to create even more anonymous, impenetrable technologies.

In addition to Tor, there are the other "darknets," the Invisible Internet Project (I2P) and Freenet, and alternative top-level domains which are also called "rogue TLDs." I2P was designed as an anonymous peer-to-peer distributed communications layer that can run any traditional internet service. It was an evolution of the Freenet network. I2P's exclusive goal is to enable users to host services without being traceable or identifiable.

From consulting with law enforcement worldwide, it is clear there is progress. The recent arrest of the founder of Silk Road, "the Amazon for Drugs," was an important step. Yet, barely one month later the site is back up and is operating again.

There have been other arrests. In February Australian police arrested a cocaine dealer operating on Silk Road and being paid in Bitcoins. In May Israeli police broke up a drug distribution ring operating in Bitcoins. There have been others.

However, what I hear most from law enforcement worldwide is frustration. The primary investigative technique being utilized by police today for addressing anonymous, "deep web," criminal enterprises is infiltration. However, infiltration is expensive, time-consuming and often ineffective.

While there are some arrests, they primarily involve less sophisticated users who make mistakes and leave a trail. Even the Silk Road arrest appears to be largely the result of a series of mistakes by the offender. That doesn't minimize its importance or denigrate the incredible work of law enforcement to make it happen. Law enforcement must be vigilant and positioned to take advantage of the mistakes. It simply illustrates how daunting the challenge is.

In 2013 researchers at the University of Massachusetts reported that "while Tor presents a challenge to investigators, in practice offenders use Tor inconsistently. Over 90% of regular Tor users send traffic from a non-Tor IP at least once after first using Tor." Thus, most cases are currently being made due to mistakes by the offender. Our concern is that most often we are apprehending the less sophisticated offenders, not the serious, sophisticated organized criminals who represent the greatest threat and do not make these kinds of mistakes.

The Tor Project is committed to help train law enforcement in Tor technology, and should be praised for its willingness to help. It has also committed to help law enforcement develop ways to use Tor as part of its investigative arsenal. Nonetheless, it is vital that new investigative tools be developed.

We are also exploring some new techniques. For example, a recent analysis experimented with "clustering" Bitcoin transactions. While it is not possible to go from a transparent Bitcoin transaction to an actual human being, this analysis conducted by Forbes Magazine demonstrated that it is possible to identify patterns in Bitcoin transactions and to move from those patterns to the identification of specific offenders. The Forbes example unmasked the identities behind Bitcoin transactions on Silk Road.

Similarly, the recent investigation that shut down Freedom Hosting appeared to use variations of "hacking" techniques similar to those used by Anonymous in its efforts that shut down the child pornography site, Lolita City. These techniques offer potential for study, but must be examined carefully to ensure that legal and ethical standards are met.

Another concern is that in addition to the major "deep web" marketplaces like Silk Road, there are other sites that allow anonymous trading. According to an analysis by Digital Economy Task Force member, Trend Micro, there are underground message boards where people post and read generic classifieds regarding almost any good or service. There are also privately maintained sites that offer specific types of goods and services. Some are pages with prices and contact information for anonymous orders and others provide a full order and payment management system. Goods and services being offered include drugs, guns, hired assassins, child pornography, and much more.

TrendMicro concluded that the so-called "deep web" in general and Tor in particular offer a secure platform for cybercriminals to support a vast amount of illegal activities – from anonymous marketplaces to secure means of communications to an untraceable and difficult to shutdown infrastructure to deploy malware and botnets. It adds, "it becomes more important...to be able to track and monitor activities that take place in darknets, focusing today on Tor networks but extending in the future to other technologies."

3 – The work of the Digital Economy Task Force –

On June 13, 2013 ICMEC and Thomson Reuters hosted a conference with leaders of the Bitcoin movement, the Tor Project, government and law enforcement experts, private sector leaders, and others. Speakers included the US State Department's Ambassador who heads the Trafficking in Persons Office, an executive from the World Bank, the US Justice Department's Chief of the Child Exploitation & Obscenity Section, the US Department of Homeland Security's head of its Blue Campaign on human trafficking, an official from the State Department's International Narcotics & Law Enforcement (INL) bureau, a Deputy Assistant Attorney General, and the Director of the US Financial Crimes Enforcement Network (FinCEN). The conference also included private sector leaders from Thomson Reuters, General Electric Co., TrendMicro and others.

The representatives of Bitcoin, Tor and other entities explained their systems and indicated a desire to work with ICMEC, Thomson Reuters and others to ensure that their services are not used for child exploitation, human trafficking and other criminal purposes. They argued that the new digital economy represents an historic opportunity to advance financial inclusion and that the use of their systems for child sexual exploitation harms their larger purpose. They committed to work with us to seek solutions.

On June 14, 2013 ICMEC and Thomson Reuters participated in a meeting at the World Bank with officials of the International Monetary Fund, the European Central Bank, the US Federal Reserve, the US Department of Treasury's Office on Terrorist Financing and Financial Crimes, and others. I presented our concerns that digital currencies and the digital economy were becoming safe havens for child pornography, sexual exploitation and sex trafficking, in addition to other criminal enterprises.

The European Central Bank cited four primary conclusions:

(1) that virtual currencies do not yet pose a risk to price stability nor jeopardize financial stability;

(2) that since they are not yet regulated and not closely supervised or overseen by any public authority, they pose a risk for users;

(3) that they fall within the realm of central banks' authority as a result of characteristics shared with payment systems; and

(4) that they represent "a challenge for authorities, as they might be used by criminals, fraudsters, and money launderers."

The ECB committed to monitor developments, set payments security requirements, keep legal frameworks updated and "facilitate a social dialogue."

The US Federal Reserve raised several questions:

(a) Is Bitcoin a more efficient currency for illegal activities than physical currency?

(b) How anonymous is it?

(c) How vulnerable is Bitcoin to theft and counterfeiting? Like cash, there is no recourse for a victim of theft. Is it easier to steal virtual currency or physical currency?

(d) How vulnerable are Bitcoin exchanges to cyber attacks? This introduces volatility to the value of the currency.

(e) Will other virtual currencies emerge to challenge Bitcoin?

(f) Will Bitcoin or another virtual currency become "widespread enough to have implications for central bank currency and monetary policy?"; and

(g) "Will bank-like institutions emerge to take deposits and make loans of virtual currencies?"

The Federal Reserve also committed to monitor the situation.

Thus, as a result of the June conference and subsequent meetings and consultations, in August ICMEC and Thomson Reuters created a Digital Economy Task Force to seek reasonable, constructive solutions, including best practices models to address the challenge of anonymity.

ICMEC also committed to launch a global advocacy effort to urge individual nations and international bodies to begin applying anti-money laundering rules and regulations at the exchange level; to engage international law enforcement partners in an effort to increase awareness of the risks of the digital economy and develop specialized investigative techniques for addressing these kinds of crimes; and initiate discussions with policy makers regarding the use of "money transmitter" laws, which are in place in almost every country but are currently not being used to address this growing problem.

The Digital Economy Task Force created five working groups: Defining the Problem; Regulation; Law Enforcement; Human Rights/Financial Inclusion; and Interagency Cooperation and Coordination. Each group is compiling specific recommendations, which will be reviewed by the full task force. The Task Force is committed to issuing its final report and findings by February 2014.

(4) Future trends and potential policy considerations for Congress and other policymakers.

The digital economy is an evolving field. The pace of innovation will quicken. There will be new technologies and new currencies. The intensity of the effort to achieve total internet anonymity will also increase, posing increasing challenges for law enforcement.

What can Congress do?

You can ensure that we apply and utilize existing law and regulation, and that we focus our regulatory attention at the point at which virtual currencies are being exchanged for conventional currencies.

You can help ensure global cooperation and coordination. Digital economy funds flow globally, network to network, not nation to nation. This is not a problem that the US government can solve alone. An excellent model is the recent US-led investigation that shut down Liberty Reserve, the Costa Rican company indicted for unlicensed money transmissions; i.e., laundering $6 billion in illicit funds, some of which came from the sale of child pornography. Seventeen nations participated in that investigation.

We are gratified by the work of US and international law enforcement in the fight against Internet-based child sexual exploitation. Entities like the Virtual Global Task Force, which brings together national law enforcement agencies in 12 nations including international bodies Interpol and Europol, and the Global Alliance Against Child Sexual Abuse Online, launched recently by the US and Europe which now has nearly 50 member countries, are great models for international cooperation. We need a quick, nimble response system. These are global crimes and require a global solution.

You can ensure that the response of government to this fragile, emerging area is not so draconian that the effect is simply to push these new enterprises outside the United States to countries where there is little or no regulation.

Finally, you can help us address the core challenge, internet anonymity. For all of its importance, we simply cannot create an environment in which child exploiters, traffickers, and other organized criminals can operate on the internet with a complete veil of anonymity and no risk of being identified unless they make a mistake.

In our consultations with law enforcement worldwide, we have heard the argument that there is a difference between privacy and anonymity. Law enforcement leaders embrace the broadest possible privacy protections for individuals, but emphasize that absolute internet anonymity is a prescription for catastrophe.

Our challenge is to find the right balance. Free speech is not absolute. Nearly a century ago, the US Supreme Court articulated the "clear and present danger" test, emphasizing that limits on speech may be appropriate based upon the context in which that speech is exercised.

That determination is much more difficult today in the world of the internet, a medium that is global in scope. We recognize that protecting the rights of political dissidents, journalists and others is incredibly important. We also recognize that all countries are not equally committed to individual freedoms, and that there are countries which will use internet speech as a basis for retaliation.

Nonetheless, the crux of the challenge we face with regard to the use of the digital economy for the exploitation and victimization of children and other criminal purposes is internet anonymity. There have to be some limits, hopefully as minimal as possible. Law enforcement has to have some possibility of tracing evidence of unlawful behavior, with full and appropriate legal processes, to the person responsible for it.

In her "Remarks on Internet Freedom" at the Newseum in Washington, DC in January 2010, former Secretary of State Hillary Clinton said, "On the one hand, anonymity protects the exploitation of children. And on the other hand, anonymity protects the free expression of opposition to repressive governments." That is our challenge.

Secretary Clinton added, "…we must grapple with the issue of anonymous speech. Those who use the internet to recruit terrorists or distribute stolen intellectual property cannot divorce their online actions from their real world identities. But these challenges must not become an excuse for governments to systematically violate the rights and privacy of those who use the internet for peaceful political purposes."

She added, "None of this will be easy…But I think these overriding principles should be our guiding light. We should err on the side of openness and do everything possible to create that, recognizing, as with any rule or any statement of principle, there are going to be exceptions."

She was exactly right. We must develop and implement those limited exceptions.

Bitcoin Foundation

Testimony of Patrick Murck
General Counsel, the Bitcoin Foundation
to the Senate Committee on Homeland Security and Governmental Affairs
"Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies"
November 18, 2013

Executive Summary

Bitcoin is a decentralized store of value and open-ledger payment network that operates securely, efficiently, and at low cost without the need for any third-party intermediaries. The Bitcoin protocol allows individuals or service providers access to a global financial system that will see rapid innovation.

Bitcoin and digital currency alone will not alleviate issues of poverty and financial exclusion that effect vulnerable populations around the world. However, Bitcoin can provide a safe store of wealth and a global transaction network that cannot be corrupted or abused by those who would seek to exploit or harm vulnerable populations. It can help advance liberty and dignity for people worldwide, restore financial privacy for law-abiding people, and provide a stable money supply in countries where the currency may be mismanaged.

The United States has an acute interest in maintaining its place as a global leader in developing this cutting edge technology, fostering financial services innovation, and spreading individual freedom and liberty around the globe. Applying consistent rules and regulations that encourage technological experimentation is critical to a vibrant entrepreneurial community, and this committee's work may help to chart a safe and sane regulatory course for the digital economy in general and Bitcoin specifically.

Though challenges exist, Bitcoin does not pose a unique or unsolvable challenge to law enforcement or existing regulatory structures. Bitcoin service providers enter a highly regulated marketplace with deeply entrenched competitors.

The Bitcoin Foundation looks forward to continuing a dialog with this committee and others, federal and state regulators, law enforcement agencies, financial services firms and banks, and academics. Together, we can help ensure that the substantial benefits of the digital economy are attained while the risks are mitigated.

Introduction

Good afternoon, Chairman Carper, Ranking Member Coburn, and Distinguished Members of the Committee. I am pleased to have the opportunity to speak with you today. My name is Patrick Murck, and I am general counsel of the Bitcoin Foundation.

The Bitcoin Foundation is a member-driven non-profit organization dedicated to serving the business, technology, government relations, and public affairs needs of the Bitcoin community. The Foundation works to standardize and strengthen the Bitcoin protocol and software, to protect the Bitcoin community, and to broaden the use of Bitcoin through public education and by fostering a safe and sane legal and regulatory environment. Incorporated in July of 2012, the foundation is organized under section 501(c)(6) of the Internal Revenue Code.

The Bitcoin Foundation's members include many of the top companies, entrepreneurs, and technologists working to make Bitcoin a success. The Bitcoin Foundation represents an international membership and our focus is global. Currently, about 60% of the foundation's membership is international. The rapid development of Bitcoin is a global phenomenon, and the Bitcoin 2014 conference, successor to our hugely successful Bitcoin 2013 conference in San Jose, California, earlier this year, will be held in Holland May 15-17, 2014. The Bitcoin Foundation is actively developing systems to empower local foundation subsidiaries and chapters in countries around the world with the resources they need to further the Foundation's mission of promoting, protecting and standardizing the Bitcoin protocol and distributed, decentralized digital currency in general.

I am a founding member of the Bitcoin Foundation and have served as General Counsel since its inception. Additionally, I have been an executive in legal and business development for a number of digital currency companies. In private practice, I have represented digital currency clients, and worked as a telecom, media, and technology attorney with a Washington, D.C.-based law firm. I am a native of Washington, D.C., and received my undergraduate degree from American University and my J.D. with honors from Catholic University, Columbus School of Law.

About Bitcoin

Bitcoin was invented in 2008 as a peer-to-peer payment system for use in online transactions.[1] Bitcoin is revolutionary in that, unlike any prior online payment system, Bitcoin is not administered by any central authority. There is no middleman between the sender/buyer and the receiver/seller as there is with, for example, PayPal, traditional payment cards, bank wires, or other payment systems. Bitcoin is thus referred to as a "decentralized" digital currency.

[1] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," http://bitcoin.org/bitcoin.pdf.

The Bitcoin software is also open-source and non-proprietary, developed by a community of volunteers in collaboration with our Chief Scientist, Gavin Andresen. There is no "Bitcoin company" that manages or controls the software or its operation. If the Bitcoin Foundation ceased work on Bitcoin's technical development, the technical development work would continue among the volunteers worldwide who already do so much of the heavy lifting. If the Bitcoin Foundation or any other actor tried to take control of the Bitcoin software, the Bitcoin community would reject that and develop the software on its own, independent of such an interloper.

Instead of a central authority, the Bitcoin transaction network consists of computers around the world running the Bitcoin software, which operates the protocol for administering Bitcoin transactions. That software can be downloaded and run by anyone, and any computer running the software can join the network. Each computer on the network also maintains a copy of the universal public ledger known as the "block chain."

The Block Chain

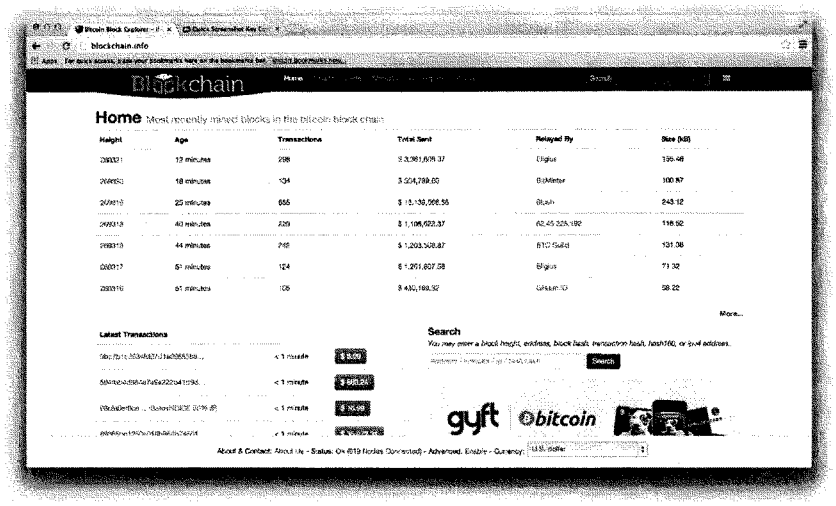
The public ledger is crucial to understand. The heart of the Bitcoin technology is this ledger that records all transactions occurring in the system. The ledger is broken into blocks of transactions, and each new block of transactions is linked to the previous block, forming what is called the "block chain." The newest block at the end of the chain links back to every block that precedes it. Having access to the most recent block allows one to follow the chain backward to observe every Bitcoin transaction ever made.

New blocks are created by "mining." Mining is done by solving a very difficult math problem, which creates the next block incorporating recent transactions. This is costly in terms of computer processing (hardware, electricity, and time). But though the problem is difficult to solve, the solution is easy to verify, so a miner discovering the solution can declare it (Eureka!), and nodes across the network will promptly confirm the new block.

The difficulty of the math problem increases with the amount of effort going into mining across the network. This controls the pace at which new bitcoins are added to the system, and it reduces the chance that any one miner or group will take control of the block chain. The amount of Bitcoin created by mining will drop over time until it ceases altogether in 2140 at just fewer than 21 million bitcoins in existence. In the meantime, mining will increasingly be rewarded by transaction fees.

Critically, the universal ledger prevents anyone from spending the bitcoins they own twice. Because a record of every transaction is available to all, attempts to spend the same bitcoin after it has already been transferred are easily detected using the block chain. This allows there

to be purely digital transactions without any central administrator, who would otherwise manage the ledger and police against double spending of a digital currency.



Source: blockchain.info

How a Bitcoin Transaction Works

Any Bitcoin user can transact directly with any other Bitcoin user. To utilize the Bitcoin network, a user needs a Bitcoin address, or "wallet." A Bitcoin wallet takes the form of a cryptographic "public key," which is a string of numbers and letters roughly 33 digits long. Each public key has a matching "private key," known only to the user. Control of the private keys is what assures one of control of the bitcoins at any Bitcoin address, so collections of private keys must be protected by passwords or other means of securing them. While wallets can be created and maintained using the Bitcoin open-source software, in practice many users have accounts with one or more Bitcoin service providers and store bitcoins at addresses provided through their accounts.

To initiate a transaction, the software or service sends a message to the other computers on the network announcing the transfer of a certain value in bitcoins from the user's public key to the recipient's public key. The sending user's private key is used to "sign" the transaction. The private key is mathematically paired with the public key, and through a standard cryptographic process of the sort used to secure website connections, every computer on the network can verify that the transaction is signed with the correct private key. The private key signature thus

serves to confirm that the transaction originated with, and was approved by, the actual owner of the originating public key, and therefore that the transaction is valid.

While this process sounds complicated, it is handled automatically and invisibly for users by the Bitcoin software. From the user's perspective, sending bitcoins to someone else is no more difficult than sending funds using PayPal or traditional payment systems, or sending an email. Administering a payment or money system is not the only use of a universal public ledger. The Bitcoin protocol may expand over time to facilitate many advanced services such as deposits, escrows, and potentially even distributed stock trading. And the Bitcoin protocol may find many uses beyond payments and money, including proving the existence of documents, establishing and verifying human identities, Internet naming and numbering, and many more.

Bitcoin is a protocol. It is like TCP/IP, which enables all the different uses people around the globe invented for the Internet. And it is like HTML, which enables all the different uses people invented for the World Wide Web without having to ask anyone's permission. We envision Bitcoin as a driver of global change that rivals these other protocols in terms of the benefits it delivers to humankind across the globe.

Bitcoin's Promise

There may be as many reasons to support Bitcoin as there are Bitcoin supporters. But we believe Bitcoin holds out a number of powerfully beneficial social and economic outcomes, including global financial inclusion, enhanced personal liberty and dignity, improved financial privacy, and a stable money supply for people in countries where monetary instability may threaten prosperity and even peace.

Global Financial Inclusion

In April 2012, a World Bank report found that half of adults worldwide are unbanked due to barriers such as high cost, physical distance, and lack of proper documentation.[2] It is hard to believe amid the relative wealth of the United States, but half the world's population lacks access to financial services that are everyday matters to us. These are rungs on the ladder from poverty to prosperity that many people cannot access at all.

A 2001 study confirms in striking terms what common sense suggests: Informal saving methods such as keeping physical money in the home are subject to losses as high as 26% of the

[2] Asli Demirguc-Kunt and Leora Klapper, "Measuring Financial Inclusion: The Global Findex Database," Policy Research Working Paper No. 6025, The World Bank, Development Research Group, Finance and Private Sector Development Team (April 2012) http://www-wds.worldbank.org/servlet/WDSContentServer/WDSP/IB/2012/04/19/000158349_20120419083611/Rendered/PDF/WPS6025.pdf.

amounts saved per year.[3] Around the world, multitudes of hard-working, capable people simply lose wealth that they could use for food, shelter, medical care, and the education of their children because of underdeveloped financial infrastructure.

Bitcoin is an extremely lightweight financial infrastructure because it can exist wherever there is Internet or cell phone access and the requisite computing device, smartphone, or SMS-capable phone. Whether it brings people into existing financial services systems, or if it secures people's wealth better outside of formal systems, we believe Bitcoin has tremendous potential to improve the capacity of people around the world to build and store wealth. That greater access to wealth may produce improved outcomes in the area of food and nutrition, health and longevity, education and child development, family structure, protection of civil and political rights, and even political stability and global security.

It would be a mistake, of course, to think that Bitcoin can simply be sprinkled on longstanding social, economic, and political problems to easily solve them. And it will take time and effort to propagate the infrastructure that is needed to access and use Bitcoin in the far corners of the globe. But the Bitcoin Foundation will be fostering businesses and business environments that allow local merchants everywhere to accept bitcoins and that allow convertibility of Bitcoin to local currencies.

We believe Bitcoin can improve the lot of the world's poor. If these efforts and the underlying genius of the Bitcoin protocol improve the financial situation and wherewithal of millions, hundreds of millions, or perhaps billions of people by even a small fraction, the total quantum of good done by Bitcoin will be quite large.

Liberty and Dignity

Along similar lines, we see potential for Bitcoin to improve people's enjoyment of autonomy, liberty, and dignity everywhere in the world.

Deep running principles—in Western thought, at least—emphasize individuals' ownership of themselves and the things they produce. In varying degrees around the world, though, governments and powerful private actors often encroach on people's rights and their ability to use and dispose of their property as they see fit. This makes people objects of control, denying them the dignity of being autonomous, independent, and responsible moral actors whose well-being and self-worth rise or fall based on their own decisions.

---

[3] Graham A.N. Wright and Leonard Mutesasira, "The Relative Risks to the Savings of Poor People," MicroSave (January 2001) http://www.microfinancegateway.org/gm/document-1.9.28889/26216_file_The_Relative_Risks_.pdf.

Bitcoin can facilitate private and anonymous transactions, which are resistant to oversight and control. Because it can aid people in deploying their property less subject to external impediments, Bitcoin may expand the realm of autonomy, liberty, and dignity for people around the world. This means traveling from market to village without being robbed, it means avoiding official corruption and confiscatory tax regimes, and many more things. It also means that people using Bitcoin can fund controversial speech or causes that governments and powerful private actors may seek to suppress using their control of conventional financial services. Bitcoin is a communications protocol, and it has the Internet virtue of being censorship-resistant, which expands freedom of speech and freedom of action.

This by no means implies that using Bitcoin can or should provide anyone immunity from the law. Though it has sometimes been portrayed as such in careless media stories, Bitcoin is not a magic cloaking device that allows criminal actors free reign. It does offer enhanced privacy protections, however, which is the just desert of hundreds of millions of law-abiding Americans and billions of law-abiding people worldwide.

Financial Privacy

The American people have been reminded this year of reasons to be concerned for their privacy, as have people around the world. We believe that peaceful, law-abiding people are entitled to protections for their privacy.

In the United States, constitutional protections such as the Fourth Amendment should allow people to be secure against unreasonable searches and seizures of their persons, houses, papers, and effects, even when their papers and effects are in digital form. We also believe the International Covenant on Civil and Political Rights bars arbitrary or unlawful interference with one's privacy, family, home, or correspondence, regardless of format.

Privacy is many things to many people. Among other things, it is the individual's bulwark against objectification by governments, corporations, and other individuals. People who have their privacy have more personal power and a richer, more independent life. Privacy is also a means to various ends, including personal security and freedom of speech and action.

Many at the Bitcoin Foundation and in the Bitcoin community are acutely aware that financial transactions in nearly every format are subject to some degree of surveillance. For good and bad, centralized payment systems always include gatekeepers and overseers. Bitcoin can facilitate fully private transactions, which, when legal in the jurisdictions where they occur, are nobody's business but the parties to the transactions.

Privacy can mask wrongful behavior, of course, and governments have a valid interest in information about activities they have made illegal. And there are certainly circumstances when

Bitcoin-based services will require and benefit from collection of personal information about users. So "more privacy" is not the essence of Bitcoin. But the use of Bitcoin should strengthen the hand of individual users to protect their privacy.

Today, privacy in financial services is typically dictated by governments and corporations. The bitcoin ecosystem should be more amenable to what we refer to as "user-defined privacy." Bitcoin may once again allow law-abiding people to have privacy on the terms they want it.

Stable Money Supply

A significant benefit of Bitcoin in the eyes of many in the Bitcoin community is its assurance of a stable base money supply. As I noted earlier, the bitcoin protocol provides for mining of a limited number of bitcoins, and that limit cannot be changed without the consensus of the community. The production of bitcoins will slow according to a schedule until around 2140, when the last new fraction of a bitcoin, known as a satoshi, will be mined just shy of 21 million bitcoins.

The rate of new bitcoin mining is similar to the mining rate of precious metals such as gold or silver. A low rate of new creation relative to the existing base means that added supply does not significantly debase the value of the existing stock. Like these precious metals and unlike fiat currencies, the stock of Bitcoin cannot increase rapidly, causing them to drop in value relative to other goods.

This means that Bitcoin is largely inflation-proof. Time and experience may prove it to be a more stable store of value than many fiat currencies, while it enjoys advantages over precious metals in other respects, such as transferability, divisibility, security in storage, and so on. This makes Bitcoin a potential key to financial well-being for savers and investors worldwide, but particularly in those jurisdictions where fiat currencies may be mismanaged.

Some Bitcoin enthusiasts may crow about the idea of Bitcoin replacing national fiat currencies, and it may be possible in a small country sometime in the future. The way to contemplate Bitcoin in the near term is as a means of making a small central bank or currency bloc accountable if they poorly manage their portfolio, while at the same time ameliorating the economic effects of the central bank's mismanagement. We believe all the world's currency systems are safer if there is a more diverse web of monetary systems with which to work. We believe that Bitcoin can add to monetary stability both directly, by acting as stable money itself, and indirectly, by husbanding the behavior of central bankers.

We are very motivated at the Bitcoin Foundation by the social and economic benefits that we believe Bitcoin has to offer. We are mindful, of course, that Bitcoin is subject to misuse. It would be regrettable if the many benefits Bitcoin offers were denied the world's people, or even delayed, by overreaction to the challenges that come with this emerging new technology. We

share your opinion, Chairman Carper, stated very well in a recent press release, that "we need to develop thoughtful, nimble and sensible federal policies that protect the public without stifling innovation and economic growth."

Beyond Silk Road

As you are likely aware, federal law enforcement recently seized the "Silk Road" website and arrested its alleged controller, Ross Ulbricht. With Silk Road shuttered, it is clear that Bitcoin thrives irrespective of sensationalist stories about a "dark web" of illicit transactions. Silk Road drew attention to Bitcoin, and the attention may have helped Bitcoin go mainstream, but now that it is mainstream, Bitcoin is beyond Silk Road.

Bitcoin and tools like Tor, which the U.S. Navy invented to secure the communications of ships, and which protects journalists and dissidents around the world, can be used for illicit purposes. But, as the Silk Road case makes evident, Bitcoin is not a magic cloak for illicit transactions. Bitcoin is a new and advanced technology, and law enforcement will likely have to develop new methodologies for interdicting and investigating criminal activity. This does not make it harder for law enforcement to do its important job. It simply means that law enforcement will have to learn this protocol and adjust its methods somewhat, something that has been successfully accomplished in many different contexts before.

In any event, the choice for policymakers is not whether Bitcoin will exist, and it is not whether Bitcoin will be used in the United States. The question is whether Bitcoin businesses will be integrated with the U.S. financial services system and become producers of U.S. jobs and economic growth that respond to legitimate U.S. law enforcement inquiries, or whether Bitcoin businesses will move offshore, taking jobs and innovation with them, and making it harder for U.S. law enforcement to gather information for legitimate investigations.

True: Bitcoin Can be Used for Illicit Purposes, Like All Other Forms of Payment

Bitcoin is no different than any other payment system, form of money, or technical infrastructure. It can be used by criminals. Bitcoin was used on the Silk Road website, which was primarily a market for illegal drugs. The less this colors public and policymaker assessments of Bitcoin, the better. Criminals do turn the beneficial instruments of society to their ends. But overreacting to this simple and obvious fact because Bitcoin is exotic and new could delay Americans enjoyment of Bitcoin's benefits, which are vastly greater than its potential costs.

An analysis by digital currency research and data site *The Genesis Block* puts the relationship between Silk Road and Bitcoin in perspective. In a thoroughly researched October 2013 piece entitled, "Analysis of Silk Road's Historical Impact on Bitcoin," writer Jonathan Stacke finds that

"a significant portion of bitcoin's early traction and price gains can be traced directly to Silk Road, with that impact waning over time, most dramatically in the past six months."[4]

In late December 2010 and early 2011, Stacke finds, people acquiring bitcoin for use on Silk Road may have produced a spike in Bitcoin's price against the U.S. dollar from $0.30 to a trading range of $0.65 to $0.80. Mainstream press attention from *The New York Times*, *Time*, and Gawker.com then began a far more significant price spike that reached $30 per Bitcoin before prices settled to a new higher equilibrium of around $5. Succeeding price changes, Stacke finds, correlate to events and news reporting unrelated to Silk Road. But denial-of-service attacks on Silk Road in April and May of 2012 show effects falling to between 25% and 35% of Bitcoin's price. When Silk Road was finally taken down last month, the price of Bitcoin suffered a one-day drop of about 20%, but then began climbing relentlessly, more than doubling since then.

The Bitcoin market is infinitesimal compared to its potential size, so it is subject to relatively high volatility. That volatility will drop over time, as the worldwide use of the Bitcoin protocol grows. Psychology around this new asset probably also drives wider price swings than will occur in the future. But judging by their behavior in the markets, the Bitcoin community seems relieved and optimistic about the falling relevance of Silk Road and illicit markets.

As with every other payment system, criminals will surely and regrettably use bitcoins. That said, law enforcement appears well-equipped to deal with copycat sites to Silk Road. In fact, copycats "Atlantis" and "Project Black Flag" have recently shuttered themselves spontaneously and absconded with their users' bitcoins. Criminals are not reliable business partners, and they will turn on each other when the circumstances are right. Anonymity is also a two-way street. A top dealer on Silk Road was actively working with federal law enforcement, the anonymity of Silk Road making it easier for them to make undercover drug deals and subsequent arrests. A user of "Black Market Reloaded," another Silk Road copycat, was recently arrested.

The document charging Ross Ulbricht noted Bitcoin's legitimate uses, and it shows that solid law enforcement work is effective with respect to Bitcoin and Tor just like other payment and communications systems. Silk Road is gone. The lawful uses of Bitcoin will continue to grow in number and quantity, easily swamping illicit uses and helping to bring the association between Bitcoin and crime into accurate perspective.

---

[4] Jonathan Stacke, "Analysis of Silk Road's Historical Impact on Bitcoin," The Genesis Block, http://thegenesisblock.com/analysis-silk-roads-historical-impact-bitcoin/.

New, Not Necessarily Harder

As I said earlier, Bitcoin is not a magic cloak for illicit transactions. At the same time, it certainly may provide new challenges to law enforcement, who will have to learn about Bitcoin and the block chain to pursue investigations. But we expect the law enforcement challenge to be different, not necessarily harder, in the Bitcoin environment. Law enforcement has and will be able to successfully investigate and prosecute criminals who use bitcoins.

We see the law enforcement paradigm in the Bitcoin ecosystem differing from the status quo in the following way: Law enforcement investigations using payment systems today typically are "parties known/transactions unknown." Having some insight into suspected criminal behavior, law enforcers use warrants, subpoenas, and other legitimate investigative tools to learn from financial services providers what transactions their suspects have engaged in.

If Bitcoin businesses thrive in the United States, investigations may still follow this model, gathering the Bitcoin transactions of existing suspects from U.S.-based providers. But investigations may also follow a "transaction known/parties unknown" model. The block chain—that worldwide public ledger of all transactions—may permit law enforcement to observe transaction flows that they know to be illicit or to use the products of illicit activity. Tracing illicit transactions to transactions that identify the parties will reveal the identities of suspects.

The block chain may be so revealing that the problem with Bitcoin is the difficulty law-abiding people have maintaining privacy. Bitcoin mixing services, which are intended to obscure the source of their users' bitcoins, may become popular if the sense of the Bitcoin community is that the flow of bitcoins is being used for excessive or illegitimate surveillance of private financial activity. Incautious behavior on the part of governments and law enforcement could make the Bitcoin environment harder to work with.

The issues here are complex, and the capacity of mixing services to truly obscure transaction flow will be the subject of much study over time. But a cautious law enforcement approach to Bitcoin is much smarter than trying to convert the Bitcoin block chain and the data held by Bitcoin service providers into a mass surveillance system.

Nimble and sensible interaction with the Bitcoin community will permit law enforcement to protect the public without stifling innovation and economic growth. U.S. law enforcement will have better access to data sought under legitimate legal processes if the U.S. Bitcoin industry is strong. Simply put, U.S. companies will be easier to work with than overseas firms. But some circumstances are already driving Bitcoin businesses offshore.

Bitcoin and the U.S. Financial Services System

While we have been pleased by the solicitous tone of official policy statements coming from U.S. federal government agencies, some factors appear to be driving Bitcoin start-ups away from U.S. shores. To the extent this happens, it comes at the cost of innovation, jobs, and economic growth that Bitcoin promises the United States. Conditions are improving, but initial hostility to Bitcoin in some states may have unnerved U.S. financial services providers, forestalling their adoption of Bitcoin and their provision of service to Bitcoin businesses. We would like to see conditions improve.

Official Policy Recognizes Bitcoin

We have been pleased by federal regulators' recognition of Bitcoin as an exciting and innovative entrant into the field of digital currency and financial services generally. Directly or indirectly a number of federal agencies have recognized Bitcoin and even touted its genius.

In March, for example, the Financial Crimes Enforcement Network (FinCEN) in the U.S. Treasury Department issued guidance on the application of money transmitter rules to Bitcoin businesses. Some interpreted this as official recognition that Bitcoin is valid and legitimate. We believe it signaled that existing regulation covers most of the business activity taking place in the Bitcoin ecosystem.

There are details on which we might quibble, and to the extent FinCEN promulgated new legislative rules, we believe they should have been issued after a notice-and-comment rulemaking. But, the Bitcoin Foundation's successful meeting with financial regulators, which FinCEN hosted in August, shows that the Treasury Department and others recognize the value of dialogue and the capacity of the Bitcoin Foundation to inform their work.

Also in August, at the urging of the Securities and Exchange Commission, a federal judge ruled that Bitcoin is a form of money also fitting the definition of a security under the Securities Exchange Act. A defendant charged with pursuing a Ponzi scheme argued that the SEC did not have jurisdiction over Bitcoin transactions. The judge struck this argument down on the basis that, just like with any other form of payment, it is illegal to use Bitcoin for fraud. This is undeniably sensible and helps to protect the Bitcoin community from similar frauds and scams that may arise in the future.

These are legal questions on which more work will have to be done. Bitcoin's differing characteristics potentially make it a different asset class than what existing regulation recognizes. But it fits well within the legal and regulatory regimes that bar frauds like the Ponzi scheme at issue in that case.

The official reception for Bitcoin among U.S. federal regulators has been essentially welcoming. Even agencies that one might assume to be antagonistic to Bitcoin acknowledge its legitimacy. The Department of Justice, for example, in its charging document for the alleged founder of the Silk Road, Ross Ulbricht, took pains to note that bitcoins are legal "in and of themselves" and "have known legitimate uses." The Federal Reserve Bank of Chicago issued a Bitcoin "primer" two weeks ago in which senior economist François R. Velde called Bitcoin a "remarkable conceptual and technical achievement, which may well be used by existing financial institutions."

We look forward to continuing our dialogue with policymakers and regulators at both the federal and state levels. In addition to the Bitcoin Foundation, there are several industry-led efforts underway to create standards of care and best practices for digital currency exchanges (for example, the committee to explore D.A.T.A.), transaction processing ("mining" in some cases), and digital currency investors. We are equally pleased to support these industry efforts.

We appreciate this committee's inquiries of federal agencies regarding their approaches to Bitcoin. Our belief, supported by the agency activities noted above, is that Bitcoin and Bitcoin businesses largely fit into existing regulatory structures. Where they may not, the framework for analysis we recommend is identifying the few "gaps" in public protection that Bitcoin's unique characteristics may produce and determining how best to fill them. We look forward to ongoing dialogue that your sensibly structured hearing and thoughtful public comments presage.

Improving the Environment for Bitcoin

While official federal policy as developed in the agencies seems clearly to recognize Bitcoin as an innovative source of economic growth and jobs, the early treatment of Bitcoin in some states and in the banking industry has clouded the picture of the United States as a center of innovation and business development. We are optimistic that the environment for Bitcoin in the United States will improve.

As illustration of early antipathy to Bitcoin, some states have issued subpoenas and cease-and-desist letters to Bitcoin businesses and others involved in the Bitcoin community. While most states and federal regulators seem to intuitively understand this, these harsh actions are not conducive to an open and productive dialog. One state regulator issued subpoenas to 22 Bitcoin-related businesses and went on television making unfounded statements relating Bitcoin to "narcoterrorism." Irresponsible public statements like these make it more likely that legitimate Bitcoin businesses will relocate to more welcoming countries.

The Bitcoin Foundation is well prepared to respond to legal inquiries and our membership does not rely on cable television for its information, but startups and small businesses are harder-pressed to respond. They may spend much of their seed capital on lawyers responding to

carelessly founded government inquests. And investors, recognizing the risks of heavy-handed government actions like this, may pull out or never materialize to invest in Bitcoin companies.

We do believe that conditions are right for improvement, and we are open to dialogue with all states, as with the federal government and its agencies, seeking to apply their laws to Bitcoin use and Bitcoin businesses. In fact, we have recently perceived a marked improvement in the tone and tenor taken by both state officials and bank executives. We are optimistic that we can generate greater understanding of the opportunity and potential for this part of the digital economy.

There are certainly risks to serving innovative small businesses, but these are matched by potential profit, and we hope that U.S. financial services providers will integrate with Bitcoin. So far, U.S. banks and other financial services providers have yet to harness Bitcoin's transformative power. As a result, most Bitcoin businesses have been started by technology experts with less experience in the intricacies of federal and state anti-money-laundering laws or know-your-customer rules. Established banks could provide expert counsel and cultivate customer relationships with these companies, and we think they should.

Indeed, banks could brand and offer Bitcoin exchange services themselves, quickly becoming the de facto leaders because of their regulatory status and supreme customer identity procedures. As it stands, a majority of people still prefer banks over trusting Apple, Google, or PayPal with sensitive data. Security at banks and financial institutions usually represents the strongest in the world among private businesses. For those individuals desiring a third-party safe-keeper for their Bitcoin balances, banks would provide several obvious advantages.

Bitcoin is a global protocol that will thrive with or without U.S. government support and with or without U.S. banks, but thoughtful policymakers and businesspeople in the U.S. should work to integrate Bitcoin and banking in the United States. Doing so will bring the benefits of Bitcoin to the United States as quickly as they reach the rest of the world. Innovation, economic growth, and jobs related to Bitcoin should be welcomed by policymakers at every governmental level in the United States.

Conclusion

The horizon is bright for Bitcoin under any circumstance. We at the Bitcoin Foundation believe that this innovative protocol can deliver financial services and improve the lot of people the world over. We see coordinate gains in liberty and human dignity, also spanning the globe. Bitcoin-based financial services can improve the privacy of law-abiding Americans and people around the world. And Bitcoin may provide a stable base money supply in countries where currency is mismanaged.

Bitcoin Foundation

The Bitcoin story goes far beyond Silk Road. Nearly every technology has potential bad uses, but the vast majority of people are law-abiding and hard-working. In their hands, Bitcoin will produce benefits that vastly outstrip the costs of the illegal and wrongful uses.

We are pleased to report that federal agencies across the spectrum are acknowledging Bitcoin and incorporating it into their regulatory regimes. For the most part, Bitcoin fits into existing regulatory structures, and we see little need for new or changed laws, though careful assessment of regulatory "gaps" may reveal where the law requires tweaks to account for Bitcoin.

We see encouraging signs that early skepticism about Bitcoin in some quarters is giving way to interest and support. This bodes well for the United States because the question is not whether Bitcoin will be used here. It is how long Bitcoin's adoption will take and whether the United States will be leaders in the digital economy.

Thank you for the opportunity to share my views with you.

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

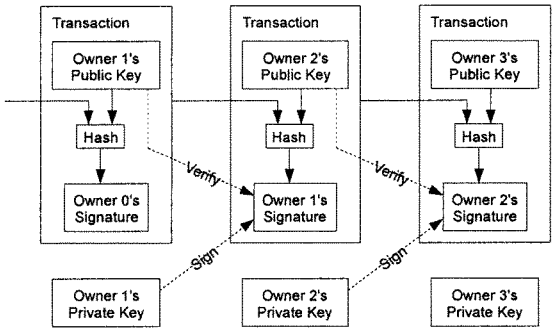
1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

2. Transactions

We define an electronic coin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership.

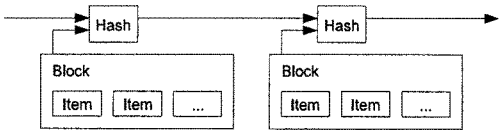


The problem of course is the payee can't verify that one of the owners did not double-spend the coin. A common solution is to introduce a trusted central authority, or mint, that checks every transaction for double spending. After each transaction, the coin must be returned to the mint to issue a new coin, and only coins issued directly from the mint are trusted not to be double-spent. The problem with this solution is that the fate of the entire money system depends on the company running the mint, with every transaction having to go through them, just like a bank.

We need a way for the payee to know that the previous owners did not sign any earlier transactions. For our purposes, the earliest transaction is the one that counts, so we don't care about later attempts to double-spend. The only way to confirm the absence of a transaction is to be aware of all transactions. In the mint based model, the mint was aware of all transactions and decided which arrived first. To accomplish this without a trusted party, transactions must be publicly announced [1], and we need a system for participants to agree on a single history of the order in which they were received. The payee needs proof that at the time of each transaction, the majority of nodes agreed it was the first received.

3. Timestamp Server

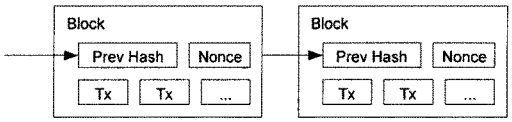
The solution we propose begins with a timestamp server. A timestamp server works by taking a hash of a block of items to be timestamped and widely publishing the hash, such as in a newspaper or Usenet post [2-5]. The timestamp proves that the data must have existed at the time, obviously, in order to get into the hash. Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before it.



4. Proof-of-Work

To implement a distributed timestamp server on a peer-to-peer basis, we will need to use a proof-of-work system similar to Adam Back's Hashcash [6], rather than newspaper or Usenet posts. The proof-of-work involves scanning for a value that when hashed, such as with SHA-256, the hash begins with a number of zero bits. The average work required is exponential in the number of zero bits required and can be verified by executing a single hash.

For our timestamp network, we implement the proof-of-work by incrementing a nonce in the block until a value is found that gives the block's hash the required zero bits. Once the CPU effort has been expended to make it satisfy the proof-of-work, the block cannot be changed without redoing the work. As later blocks are chained after it, the work to change the block would include redoing all the blocks after it.



The proof-of-work also solves the problem of determining representation in majority decision making. If the majority were based on one-IP-address-one-vote, it could be subverted by anyone able to allocate many IPs. Proof-of-work is essentially one-CPU-one-vote. The majority decision is represented by the longest chain, which has the greatest proof-of-work effort invested in it. If a majority of CPU power is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing chains. To modify a past block, an attacker would have to redo the proof-of-work of the block and all blocks after it and then catch up with and surpass the work of the honest nodes. We will show later that the probability of a slower attacker catching up diminishes exponentially as subsequent blocks are added.

To compensate for increasing hardware speed and varying interest in running nodes over time, the proof-of-work difficulty is determined by a moving average targeting an average number of blocks per hour. If they're generated too fast, the difficulty increases.

5. Network

The steps to run the network are as follows:

1) New transactions are broadcast to all nodes.
2) Each node collects new transactions into a block.
3) Each node works on finding a difficult proof-of-work for its block.
4) When a node finds a proof-of-work, it broadcasts the block to all nodes.
5) Nodes accept the block only if all transactions in it are valid and not already spent.
6) Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

Nodes always consider the longest chain to be the correct one and will keep working on extending it. If two nodes broadcast different versions of the next block simultaneously, some nodes may receive one or the other first. In that case, they work on the first one they received, but save the other branch in case it becomes longer. The tie will be broken when the next proof-of-work is found and one branch becomes longer; the nodes that were working on the other branch will then switch to the longer one.

New transaction broadcasts do not necessarily need to reach all nodes. As long as they reach many nodes, they will get into a block before long. Block broadcasts are also tolerant of dropped messages. If a node does not receive a block, it will request it when it receives the next block and realizes it missed one.

6. Incentive

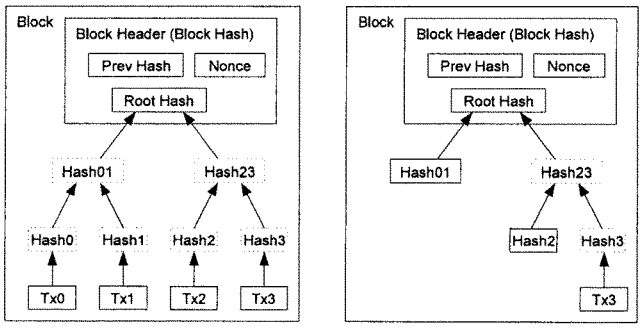
By convention, the first transaction in a block is a special transaction that starts a new coin owned by the creator of the block. This adds an incentive for nodes to support the network, and provides a way to initially distribute coins into circulation, since there is no central authority to issue them. The steady addition of a constant of amount of new coins is analogous to gold miners expending resources to add gold to circulation. In our case, it is CPU time and electricity that is expended.

The incentive can also be funded with transaction fees. If the output value of a transaction is less than its input value, the difference is a transaction fee that is added to the incentive value of the block containing the transaction. Once a predetermined number of coins have entered circulation, the incentive can transition entirely to transaction fees and be completely inflation free.

The incentive may help encourage nodes to stay honest. If a greedy attacker is able to assemble more CPU power than all the honest nodes, he would have to choose between using it to defraud people by stealing back his payments, or using it to generate new coins. He ought to find it more profitable to play by the rules, such rules that favour him with more new coins than everyone else combined, than to undermine the system and the validity of his own wealth.

7. Reclaiming Disk Space

Once the latest transaction in a coin is buried under enough blocks, the spent transactions before it can be discarded to save disk space. To facilitate this without breaking the block's hash, transactions are hashed in a Merkle Tree [7][2][5], with only the root included in the block's hash. Old blocks can then be compacted by stubbing off branches of the tree. The interior hashes do not need to be stored.



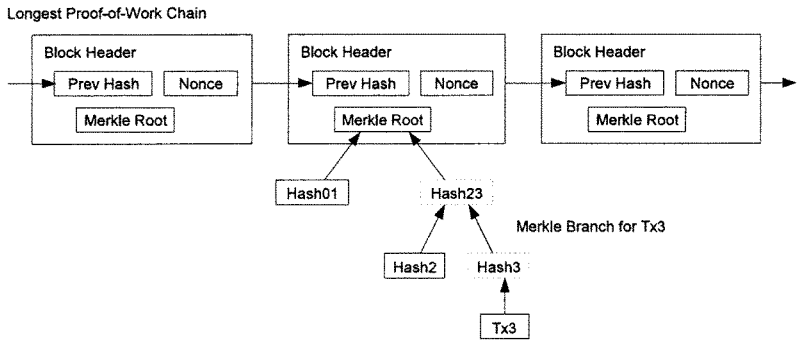
Transactions Hashed in a Merkle Tree

After Pruning Tx0-2 from the Block

A block header with no transactions would be about 80 bytes. If we suppose blocks are generated every 10 minutes, 80 bytes * 6 * 24 * 365 = 4.2MB per year. With computer systems typically selling with 2GB of RAM as of 2008, and Moore's Law predicting current growth of 1.2GB per year, storage should not be a problem even if the block headers must be kept in memory.

8. Simplified Payment Verification

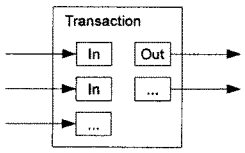
It is possible to verify payments without running a full network node. A user only needs to keep a copy of the block headers of the longest proof-of-work chain, which he can get by querying network nodes until he's convinced he has the longest chain, and obtain the Merkle branch linking the transaction to the block it's timestamped in. He can't check the transaction for himself, but by linking it to a place in the chain, he can see that a network node has accepted it, and blocks added after it further confirm the network has accepted it.



As such, the verification is reliable as long as honest nodes control the network, but is more vulnerable if the network is overpowered by an attacker. While network nodes can verify transactions for themselves, the simplified method can be fooled by an attacker's fabricated transactions for as long as the attacker can continue to overpower the network. One strategy to protect against this would be to accept alerts from network nodes when they detect an invalid block, prompting the user's software to download the full block and alerted transactions to confirm the inconsistency. Businesses that receive frequent payments will probably still want to run their own nodes for more independent security and quicker verification.

9. Combining and Splitting Value

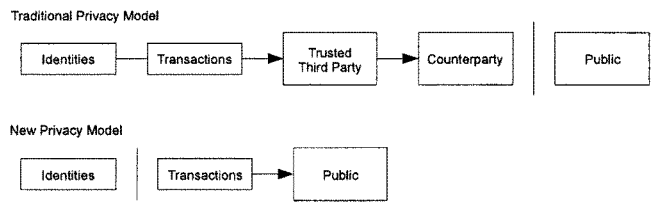
Although it would be possible to handle coins individually, it would be unwieldy to make a separate transaction for every cent in a transfer. To allow value to be split and combined, transactions contain multiple inputs and outputs. Normally there will be either a single input from a larger previous transaction or multiple inputs combining smaller amounts, and at most two outputs: one for the payment, and one returning the change, if any, back to the sender.



It should be noted that fan-out, where a transaction depends on several transactions, and those transactions depend on many more, is not a problem here. There is never the need to extract a complete standalone copy of a transaction's history.

10. Privacy

The traditional banking model achieves a level of privacy by limiting access to information to the parties involved and the trusted third party. The necessity to announce all transactions publicly precludes this method, but privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous. The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone. This is similar to the level of information released by stock exchanges, where the time and size of individual trades, the "tape", is made public, but without telling who the parties were.



As an additional firewall, a new key pair should be used for each transaction to keep them from being linked to a common owner. Some linking is still unavoidable with multi-input transactions, which necessarily reveal that their inputs were owned by the same owner. The risk is that if the owner of a key is revealed, linking could reveal other transactions that belonged to the same owner.

11. Calculations

We consider the scenario of an attacker trying to generate an alternate chain faster than the honest chain. Even if this is accomplished, it does not throw the system open to arbitrary changes, such as creating value out of thin air or taking money that never belonged to the attacker. Nodes are not going to accept an invalid transaction as payment, and honest nodes will never accept a block containing them. An attacker can only try to change one of his own transactions to take back money he recently spent.

The race between the honest chain and an attacker chain can be characterized as a Binomial Random Walk. The success event is the honest chain being extended by one block, increasing its lead by +1, and the failure event is the attacker's chain being extended by one block, reducing the gap by -1.

The probability of an attacker catching up from a given deficit is analogous to a Gambler's Ruin problem. Suppose a gambler with unlimited credit starts at a deficit and plays potentially an infinite number of trials to try to reach breakeven. We can calculate the probability he ever reaches breakeven, or that an attacker ever catches up with the honest chain, as follows [8]:

p = probability an honest node finds the next block
q = probability the attacker finds the next block
q_z = probability the attacker will ever catch up from z blocks behind

$$q_z = \begin{cases} 1 & \text{if } p \le q \\ (q/p)^z & \text{if } p > q \end{cases}$$

Given our assumption that $p > q$, the probability drops exponentially as the number of blocks the attacker has to catch up with increases. With the odds against him, if he doesn't make a lucky lunge forward early on, his chances become vanishingly small as he falls further behind.

We now consider how long the recipient of a new transaction needs to wait before being sufficiently certain the sender can't change the transaction. We assume the sender is an attacker who wants to make the recipient believe he paid him for a while, then switch it to pay back to himself after some time has passed. The receiver will be alerted when that happens, but the sender hopes it will be too late.

The receiver generates a new key pair and gives the public key to the sender shortly before signing. This prevents the sender from preparing a chain of blocks ahead of time by working on it continuously until he is lucky enough to get far enough ahead, then executing the transaction at that moment. Once the transaction is sent, the dishonest sender starts working in secret on a parallel chain containing an alternate version of his transaction.

The recipient waits until the transaction has been added to a block and z blocks have been linked after it. He doesn't know the exact amount of progress the attacker has made, but assuming the honest blocks took the average expected time per block, the attacker's potential progress will be a Poisson distribution with expected value:

$$\lambda = z\frac{q}{p}$$

To get the probability the attacker could still catch up now, we multiply the Poisson density for each amount of progress he could have made by the probability he could catch up from that point:

$$\sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \cdot \begin{Bmatrix} (q/p)^{(z-k)} & if\, k \le z \\ 1 & if\, k > z \end{Bmatrix}$$

Rearranging to avoid summing the infinite tail of the distribution...

$$1 - \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!} \left(1 - (q/p)^{(z-k)}\right)$$

Converting to C code...

```
#include <math.h>
double AttackerSuccessProbability(double q, int z)
{
    double p = 1.0 - q;
    double lambda = z * (q / p);
    double sum = 1.0;
    int i, k;
    for (k = 0; k <= z; k++)
    {
        double poisson = exp(-lambda);
        for (i = 1; i <= k; i++)
            poisson *= lambda / i;
        sum -= poisson * (1 - pow(q / p, z - k));
    }
    return sum;
}
```

Running some results, we can see the probability drop off exponentially with z.

```
q=0.1
z=0     P=1.0000000
z=1     P=0.2045873
z=2     P=0.0509779
z=3     P=0.0131722
z=4     P=0.0034552
z=5     P=0.0009137
z=6     P=0.0002428
z=7     P=0.0000647
z=8     P=0.0000173
z=9     P=0.0000046
z=10    P=0.0000012

q=0.3
z=0     P=1.0000000
z=5     P=0.1773523
z=10    P=0.0416605
z=15    P=0.0101008
z=20    P=0.0024804
z=25    P=0.0006132
z=30    P=0.0001522
z=35    P=0.0000379
z=40    P=0.0000095
z=45    P=0.0000024
z=50    P=0.0000006
```

Solving for P less than 0.1%...

```
P < 0.001
q=0.10    z=5
q=0.15    z=8
q=0.20    z=11
q=0.25    z=15
q=0.30    z=24
q=0.35    z=41
q=0.40    z=89
q=0.45    z=340
```

12. Conclusion

We have proposed a system for electronic transactions without relying on trust. We started with the usual framework of coins made from digital signatures, which provides strong control of ownership, but is incomplete without a way to prevent double-spending. To solve this, we proposed a peer-to-peer network using proof-of-work to record a public history of transactions that quickly becomes computationally impractical for an attacker to change if honest nodes control a majority of CPU power. The network is robust in its unstructured simplicity. Nodes work all at once with little coordination. They do not need to be identified, since messages are not routed to any particular place and only need to be delivered on a best effort basis. Nodes can leave and rejoin the network at will, accepting the proof-of-work chain as proof of what happened while they were gone. They vote with their CPU power, expressing their acceptance of valid blocks by working on extending them and rejecting invalid blocks by refusing to work on them. Any needed rules and incentives can be enforced with this consensus mechanism.

References

[1] W. Dai, "b-money," http://www.weidai.com/bmoney.txt, 1998.

[2] H. Massias, X.S. Avila, and J.-J. Quisquater, "Design of a secure timestamping service with minimal trust requirements," In *20th Symposium on Information Theory in the Benelux*, May 1999.

[3] S. Haber, W.S. Stornetta, "How to time-stamp a digital document," In *Journal of Cryptology*, vol 3, no 2, pages 99-111, 1991.

[4] D. Bayer, S. Haber, W.S. Stornetta, "Improving the efficiency and reliability of digital time-stamping," In *Sequences II: Methods in Communication, Security and Computer Science*, pages 329-334, 1993.

[5] S. Haber, W.S. Stornetta, "Secure names for bit-strings," In *Proceedings of the 4th ACM Conference on Computer and Communications Security*, pages 28-35, April 1997.

[6] A. Back, "Hashcash - a denial of service counter-measure," http://www.hashcash.org/papers/hashcash.pdf, 2002.

[7] R.C. Merkle, "Protocols for public key cryptosystems," In *Proc. 1980 Symposium on Security and Privacy*, IEEE Computer Society, pages 122-133, April 1980.

[8] W. Feller, "An introduction to probability theory and its applications," 1957.

Testimony of

Jeremy Allaire
Chairman and CEO, Circle Internet Financial

Before the

Senate Committee on Homeland Security and Governmental Affairs

Hearing on

"Beyond Silk Road: Potential Risks, Threats and Promises of Virtual Currencies"

November 18, 2013

Introduction

Chairman Carper, Ranking Member Coburn and members of the Committee, my name is Jeremy Allaire and I am the Founder and CEO of Circle Internet Financial, a recently launched financial services company aimed at facilitating payments and money transfers using global digital currency such as Bitcoin. I have been building Internet software platforms and online service companies for twenty years, having founded and helped to lead multiple global public companies. The products that I have conceived and helped to build include software and online services used by hundreds of millions of consumers and hundreds of thousands of businesses around the world.

I am here to testify because I believe that global digital currency represents one of the most important technical and economic innovations of our time. Specifically, digital currency introduces advancements in electronic payments and money transfers, potentially materially lowering costs for businesses around the world, decreasing fraud risk for consumers and merchants, increasing consumer privacy and protection, and expanding the market for consumer financial products on a worldwide basis.

As this technology moves from early adopters into mainstream acceptance, it is critical in my view that Federal and State governments establish policies surrounding digital currency that uphold consumer protections associated with fraud and privacy risks, ensure that criminals and bad actors find it increasingly difficult to utilize these platforms and provide clarity to consumers and businesses that conduct business using digital currency.

The Emergence of Global Digital Currency

Digital currency platforms such as Bitcoin have emerged over the past several years, fostered by a number of significant technical and social advancements, including:

- Continued and broad based adoption of the Internet on a worldwide basis, which has enabled billions of consumers to instantly connect and interact anywhere and anytime.

- Dramatic growth in the adoption of smartphones and mobile devices, now used by nearly 4 billion people, and which enable digital payment applications to be available ubiquitously.

- Advances in distributed and peer-to-peer computing that enable highly efficient, global and low-cost systems and infrastructure, enabling decentralized systems of finance.

- Advances in cryptography and digital signature technology, which provide a tremendous foundation for establishing trust, security and privacy in financial transactions.

- Accelerating globalization of trade and labor, which is driving demand for more efficient, secure and cost-effective cross-border payments.

Finally, it seems clear to me that the global financial crisis shattered the trust of many consumers and businesses around the world. It should not be surprising to anyone that in the midst of what appeared to be an emerging global depression in late 2008 that innovative mathematicians, cryptography experts, and computer scientists designed a system, Bitcoin with the goal of providing a resilient yet decentralized platform for finance.

Open Internet Platforms and Global Economic Innovation

To put all of this in context, I think it's critical to look at the role of the Internet and open platforms in transforming industries and fostering global economic innovation. Today, open Internet-based platforms are at the center of global economic innovation in industries ranging from communications, to media, software, education, commerce and retail. However, for a variety of reasons, the technologies and business models surrounding finance have been relatively insulated from these changes over the past twenty years. Open standards, protocols and formats based on digital currency, and Bitcoin specifically, present an opportunity to transform finance to the same degree that these other industries have been transformed. Indeed, the intense globalization that we are experiencing because of the Internet is in many ways calling out for more efficient forms of currency, trade and payments than existing institutions provide.

The Need for Innovation in Banking and Finance

I don't think there is much debate that we need to see innovation and transformation in banking and finance, and that on a global level we need to be thinking about what new platforms and rules of the road are needed to meet the global economic challenges that we face. Specifically, our payments systems are cumbersome and inefficient, and very much built upon systems and processes that are decades old. The result is that consumers and businesses all around the world are paying an implicit tax in the form of higher costs, lower margins and less efficient economic interaction. And, in many cases, our financial systems have excluded enormous bases of consumers who remain un-banked or under-banked. The combination of ubiquitous Internet-connected mobile devices and digital currency presents a tremendous opportunity to radically expand access to financial services on a worldwide basis.

Payments and money transfers are still operating in the pre-internet era. Today, we can communicate freely and instantly with nearly any human on the planet; we have nearly free and instantaneous access to enormous volumes of human knowledge; we have access to — and collectively create — more media and content than was ever thought possible, also at essentially no cost. Yet, to send money between friends and family, whether across the table or across the planet, it takes days and costs a significant amount in transaction fees. Our cash-based currency systems are very costly to operate and are

easily subject to abuse by criminals and money launderers. To make payments, merchants must bear significant fraud risk, consumer privacy is threatened, and likewise it takes days for a merchant to actually receive money from an electronic payment, not to mention the widely perceived high costs of transaction fees. The costs and complexities rise as we look at these issues on a global basis.

How Circle Is Building on This Innovation

I founded Circle with a vision that open Internet platforms for digital currency could transform and improve financial products to the same degree that Internet platforms have transformed media, communications, commerce, education and so many other industries. Specifically, we are building online services for consumers and businesses to be able to easily use digital currency, and specifically Bitcoin, to send and receive money and make and accept payments. For consumers, we intend to enable them to easily purchase, store, send, receive and make payments using Bitcoin, and for businesses we are providing tools to help them easily accept digital currency payments.

We are fully committed to complying with all applicable laws and regulations and establishing comprehensive risk management protocols. In particular, recognizing that we are subject to regulation as a money services business, we have registered with FinCEN as a money transmitter, and are actively seeking licenses from U.S. State financial authorities to operate as a money transmitter within their jurisdictions. We are developing our platforms to provide very high levels of security for our users, and employing industry-leading approaches to customer identity verification, fraud remediation and anti-money laundering, including a BSA/AML/OFAC compliance program, designed in partnership with leading regulatory advisors and experts.

Risks and Threats Created by Global Digital Currency

As digital currency gains more traction, U.S. regulators and law enforcement are justifiably focused on the potential use of digital currencies to finance criminal activities, including terrorism. As evidenced by Silk Road, and other recent legal and enforcement actions, digital currency, just like cash, can indeed be used for nefarious means. Silk Road also demonstrates the importance of industry players implementing robust fraud and anti-money laundering programs and working closely with law enforcement to prevent and report this type of behavior.

A number of potential risks exist with digital currency that need to be considered by government, including:

- Criminals and terrorists will seek to employ digital currency if it remains unregulated, leaving Bitcoin operators to operate without stringent controls and effective systems to verify identities, monitor transactions, and report suspicious activity.

- Tax cheaters will seek to employ digital currency to evade taxes if the government doesn't issue and enforce clear guidelines and rules on the role of digital currency in accounting for income and taxation in U.S. Dollars, and businesses will be uncertain as to how to account for revenue and income received in digital currency.

- Consumers and businesses could be defrauded if Bitcoin operators are allowed to operate without the highest levels of security when storing digital currency and associated personal information.

- Consumers and businesses could be exposed to financial loss if Bitcoin market prices fluctuate wildly, and central banks and institutional investors are not able to act as market-makers in Bitcoin.

- Because Bitcoin is not centrally controlled and relies upon an open network of computing nodes that provide transaction processing and payment confirmations while securing the network as a whole, it is potentially subject to malicious "51% attacks" that aim to disrupt Bitcoin's records of asset ownership.

At Circle, we are committed to working with key government agencies and policy makers to ensure safeguards are in place to mitigate these risks. These safeguards include the development of strong Know Your Customer ("KYC") standards for customers and counterparties, transaction monitoring, and regulatory reporting. We are encouraged by the ongoing dialogue and the formation of groups, such as the Bitcoin Foundation and the Digital Asset Transfer Authority ("DATA"), which are coordinating to develop best practices within the industry.

Government and Regulatory Regimes Needed for Digital Currency

All of these risks and opportunities require that governments around the world take a proactive stance with regards to guidance around digital currency. It should be noted that digital currency has expanded globally due to different regulatory standards and attitudes overseas, particularly in the European Union and China. Several foreign firms have also refused to accept U.S. customers due to the lack of clear regulatory guidance. We do not think that it is in anyone's best interest for digital currency to become an offshore industry, or an industry dominated by China. No other country in the world has a startup entrepreneurial culture like the United States. We should protect and embolden this spirit that creates economic growth and provides us with a considerable global advantage.

In terms of U.S. regulation, it appears to me that Federal and State regulators generally appear to have ample statutory authority to adopt regulations and take enforcement actions as necessary to protect consumers and ensure responsible conduct in the world of Bitcoin commerce, that their actions to date have been constructive, and that we stand ready to assist them in their ongoing efforts to adapt their regulatory tools to new digital currency.

I believe we are at the forefront of another twenty year journey of Internet-led transformation, this time in our global financial systems, and the opportunity is to foster that economic change while simultaneously putting in place the safeguards that only government can enable.

Mr. Chairman, that concludes my prepared testimony. I would be happy to answer any questions for the Committee.

MERCATUS CENTER
George Mason University
Bridging the gap between academic ideas and real-world problems

TESTIMONY

BEYOND SILK ROAD: POTENTIAL RISKS, THREATS, AND PROMISES OF VIRTUAL CURRENCIES

JERRY BRITO
Senior Research Fellow, Mercatus Center at George Mason University

Senate Committee on Homeland Security and Governmental Affairs

November 18, 2013

Mr. Chairman and members of the Committee, thank you for inviting me here today to comment on the risks and promises of virtual currencies. My name is Jerry Brito and I am a senior research fellow at the Mercatus Center at George Mason University, where I study the regulation of emerging technologies in the Mercatus Center's Technology Policy Program.

We're here today to discuss virtual currencies in general, but it is Bitcoin in particular that has so many interested in this topic.

Online virtual currencies are nothing new. They have existed for decades. From World of Warcraft Gold to Facebook Credits to e-gold. Neither are online payments systems new. PayPal, Visa, and Western Union Pay are all examples. So what is it about Bitcoin and similar cryptocurrencies that makes them unique?

Whatever one may think about Bitcoin's prospects for enduring value, it is safe to say that it is a remarkable technical achievement.[1] Bitcoin is the world's first completely decentralized digital currency, and it's the decentralized part that makes it unique. Prior to Bitcoin's invention in 2009, online currencies or payments systems had to be managed by a central authority, whether it was Facebook issuing Facebook Credits or PayPal ensuring that transactions between its customers were reconciled. However, by solving a longstanding conundrum in computer science known as the "double spend" problem, Bitcoin for the first time makes possible transactions online that are person to person, without the need for an intermediary between them, just like cash.

This technical breakthrough presents both potential benefits for consumers and the economy and challenges to law enforcement. For example, because there is no central intermediary in Bitcoin transactions, there are little to no fees associated with those transactions, which especially benefits small businesses and price-sensitive consumers. And because Bitcoin is not a proprietary platform run by a single company but an open network, entrepreneurs need no permission to experiment and innovate new products and services.

1. The attached appendix is an updated version of *Bitcoin: A Primer for Policymakers* by me and Andrea Castillo, which goes into considerable detail about the technical workings of Bitcoin, as well as a detailed description of the cryptocurrency's potential benefits not just for consumers and the economy, but also for free speech and oppressed minorities around the world. It also looks at Bitcoin's challenges, including the currency's security and volatility, as well as law enforcement concerns and regulatory alternatives.

For more information or to meet with the scholar, contact
Taylor Barkley, (703) 993-8205, tbarkley@mercatus.gmu.edu
Mercatus Center at George Mason University, 3351 Fairfax Drive, 4th Floor, Arlington, VA 22201

The ideas presented in this document do not represent official positions of the Mercatus Center or George Mason University.

On the flip side, law enforcement has long relied on financial intermediaries to help them detect, prevent, and investigate illegal transactions. Because bitcoin transactions can have no intermediaries, and because bitcoin transactions are not necessarily tied to identities, it is not surprising that we have seen Bitcoin employed in criminal transactions. In particular, Bitcoin has been used for the sale of drugs and in malware that holds one's data hostage. It's also not difficult to imagine how the technology could be employed in money laundering.

Emerging technologies often present both great potential benefits as well as real risks. For example, 3D printing can be used to cheaply make prostheses and life-saving medical devices, but also undetectable firearms. Domestic commercial drones have the potential to revolutionize agriculture and shipping, but could also be used for stalking. The challenge for policymakers is to address the risks posed by emerging technologies while doing no harm to the innovative potential of that technology.

In many cases where emerging technologies pose risks, there will already be laws and regulations of general applicability that address many of those risks without the need for new laws targeted at the specific technology. This is the case with Bitcoin. While bitcoin transactions do not require intermediaries, one must still acquire bitcoins by exchanging dollars, and merchants that accept bitcoins will very often use Bitcoin payment processors. Indeed, there is a fast-growing ecosystem of start-up exchanges, payment processors, and wallet and escrow services that make up Bitcoin's burgeoning infrastructure. Each of these are already subject to regulation as money transmitters, including state licensing and FinCEN registration, as well as "know your customer" and "suspicious activity report" requirements.

More to the point, serious criminals looking to hide their tracks are more likely to choose a centralized virtual currency run by an intermediary willing to lie to regulators for a fee, rather than a decentralized currency like Bitcoin that, as a technical matter, must make a record of every transaction, even if pseudonymously. While the online black market Silk Road, which used bitcoins, is estimated to have generated less than $200 million in drug sales,[2] the centralized digital currency Liberty Reserve is believed to have laundered more than $6 billion related to credit card fraud, identity theft, computer hacking, and child pornography.[3] The reason Liberty Reserve, and not Bitcoin, was the payment system of choice for criminals online is that it was designed and managed by its creators to avoid "know your customer" and reporting rules and to evade subpoena.

As a result, the path forward that can best confront risks while ensuring that we can reap Bitcoin's beneficial potential is to allow the Bitcoin network and its surrounding infrastructure to develop by making sure that entrepreneurial innovators can easily comply with existing regulation. The alternative, promulgating special regulations for virtual currencies or otherwise making it more costly to operate legitimately in the space, could have two unintended consequences. First, it might mean ceding the network to exclusively illegal use and forgoing any visibility that law enforcement could otherwise gain into the activities of compliant firms. Second, the United States could lose its head start in what may be the next disruptive industry if it establishes a regulatory regime that hampers Bitcoin while other countries, like China and Canada,[4] look for ways to develop workable regulatory frameworks for Bitcoin.

---

2. The FBI has reported that total revenues generated by Silk Road were 9,519,664 bitcoins. Criminal Complaint against Ross Ulbricht, page 15, available at http://www1.icsi.berkeley.edu/~nweaver/UlbrichtCriminalComplaint.pdf. That has been erroneously reported as the equivalent of over $1 billion in sales. Id. The error lies in simply multiplying the number of bitcoins by the exchange rate at the time of Ulbricht's arrest. This does not take into account the fact that bitcoins fluctuated in value widely from the time of Silk Road's inception to the present, so that the actual sales figure in dollars is much less than $1 billion. Nicolas Christin of Carnegie Mellon University has conducted the most rigorous estimates of Silk Road's revenues prior to its seizure. Nicolas Christin, "Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace," Carnegie Mellon CyLab Technical Reports: CMU-CyLab-12-018, July 30, 2012 (updated November 28, 2012), http://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab12018.pdf. In forthcoming work he estimates that over its life Silk Road actually generated revenues of between $100 and $200 million.

3. *U.S. v. Liberty Reserve, et al.* Indictment at ¶¶ 9 & 12, http://www.justice.gov/usao/nys/pressreleases/May13/LibertyReserveetalDocuments/Liberty%20Reserve,%20et%20al.%20Indictment%20-%20Redacted.pdf.

4. China has emerged as the fastest growing market for Bitcoin, with 33 percent of the world's bitcoins now flowing through a Chinese Bitcoin exchange, BTC China. Robert McMillan, "This Chinese Exchange Just Pushed the Value of Bitcoins over $200," *WIRED*, October 23, 2013, http://www.wired.com/wiredenterprise/2013/10/btc-china/. Canada has pursued a progressive approach toward Bitcoin with FINTRAC, that

Finally, as regulatory and law enforcement agencies seek to apply existing law to Bitcoin, they will face the challenge that Bitcoin is not a company with easily identifiable executives, but instead an open-source project and a community. The Bitcoin Foundation is central to that community, but it does not encompass the whole community. So as new guidelines and procedures are developed, policymakers should make sure to engage the community and solicit comments from the public to ensure that they benefit from a wide range of perspectives.

Thank you for your time and I look forward to your questions.[5]

ABOUT THE AUTHOR

Jerry Brito is a senior research fellow at the Mercatus Center at George Mason University and director of its Technology Policy Program. He also serves as an adjunct professor of law at George Mason University. His research focuses on technology and Internet policy, copyright, and the regulatory process.

ABOUT THE MERCATUS CENTER

The Mercatus Center at George Mason University is the world's premier university source for market-oriented ideas—bridging the gap between academic ideas and real-world problems.

A university-based research center, Mercatus advances knowledge about how markets work to improve people's lives by training graduate students, conducting research, and applying economics to offer solutions to society's most pressing problems.

Our mission is to generate knowledge and understanding of the institutions that affect the freedom to prosper and to find sustainable solutions that overcome the barriers preventing individuals from living free, prosperous, and peaceful lives.

Founded in 1980, the Mercatus Center is located on George Mason University's Arlington campus.

www.mercatus.org

country's equivalent of FinCEN, determining that exchanges and other businesses need not register as money transmitters. Jeremy Kirk, "Canadian Regulator Takes Lighter View of Bitcoin," *PC World*, May 21, 2013, http://www.pcworld.com/article/2039347/canadian-regulator-takes-lighter-view-of-bitcoin.html. As a result, Vancouver (and not San Francisco or New York) boasts the world's first bitcoin ATM. Vivian Luk, "First Ever Bitcoin ATM Goes Live in Vancouver, but Experts Warn of Risks," *Vancouver Sun*, October 30, 2013, http://www.vancouversun.com/business/your-money/First+ever+Bitcoin+goes+live+Vancouver+experts+warn/9099351/story.html.

5. For example, FinCEN issued its March guidance without providing any notice or providing the public an opportunity to comment. While that guidance clarified Bitcoin's regulatory treatment, it also introduced regulatory uncertainty around several specific use cases that would have no doubt been easily spotted by the Bitcoin community had it been given the opportunity. See *infra* 19–21. Since then FinCEN has begun to better engage with the Bitcoin community.

APPENDIX

Bitcoin: A Primer for Policymakers

Jerry Brito[1]
Andrea Castillo[2]

Bitcoin is the world's first completely decentralized digital currency. Four short years ago, knowledge of it was confined to a handful of hobbyists on Internet forums. Today, the bitcoin economy is larger than the economies of some of the world's smaller nations. The value of a bitcoin (or BTC) has grown and fluctuated greatly, from pennies in its early days to over $390 at its peak in November 2013. The current market capitalization of the bitcoin economy is estimated to be over $4 billion.[3] Businesses big and small have shown interest in integrating the Bitcoin platform into their operations and providing new services within the bitcoin economy. Venture capitalists, too, are eager to put their money behind this growing industry.[4] Traditional financial institutions and researchers, too, have taken notice. Noting its rapid development and status as a "remarkable conceptual and technical achievement," the Federal Reserve Bank of Chicago recently released a primer on the cryptocurrency.[5] The development of Bitcoin and its early successes are an exciting testament to the ingenuity of the modern entrepreneur.

Because Bitcoin is decentralized, it can be used pseudonymously, and this has attracted the attention of regulators. The same qualities that make Bitcoin attractive as a payment system could also allow users to evade taxes, launder money, and trade illicit goods. Both the Financial Crimes Enforcement Network (FinCEN) of the US Department of the Treasury[6] and the Department of Justice[7] have released official statements regarding the regulation of virtual currencies, including Bitcoin. A Government Accountability Office report on virtual currencies urged the IRS to reduce tax-compliance risks by issuing a guidance.[8] The appendix of that report contains a letter from IRS Deputy Commissioner Steven T. Miller, who assured the office that the IRS is "working to address these risks." Additionally, a commissioner of the Commodities Futures Trading Commission recently expressed interest in exploring whether Bitcoin falls

---

[1] Jerry Brito is a senior research fellow at the Mercatus Center at George Mason University.
[2] Andrea Castillo is a research assistant at the Mercatus Center at George Mason University.
[3] Financial information provided at bitcoincharts.com estimates total market capitalization to be $4,097,390,850 as of November 12, 2013.
[4] Sarah E. Needleman and Spencer E. Ante, "Bitcoin Startups Begin to Attract Real Cash," *Wall Street Journal*, May 8, 2013, http://online.wsj.com/article/SB10001424127887323687604578469012375269952.html.
[5] François R. Velde, "Bitcoin: A Primer," *Essays On Issues*, Number 317, Federal Reserve Bank of Chicago, December 2013, http://www.chicagofed.org/digital_assets/publications/chicago_fed_letter/2013/cfldecember2013_317.pdf.
[6] US Department of the Treasury, Financial Crimes and Enforcement Network, "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies" (Regulatory Guidance, FIN-2013-G001, US Department of the Treasury, Washington, DC, March 18, 2013), http://fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html.
[7] Jennifer Shasky Calvery, "Combating Transnational Organized Crime: International Money Laundering as a Threat to Our Financial Systems" (Statement for the Record Before the Subcommittee on Crime, Terrorism, and Homeland Security of the House Committee on the Judiciary, February 8, 2012), http://www.justice.gov/ola/testimony/112-2/02-08-12-crm-shasky-calvery-testimony.pdf.
[8] US Government Accountability Office, "Virtual Economies and Currencies: Additional IRS Guidance Could Reduce Compliance Risks" (report to the Senate Committee on Finance, GAO-13-516, May, 2013), http://www.gao.gov/assets/660/654620.pdf.

within the commission's jurisdiction.[9] In considering how to best oversee this still-nascent technology, government regulators should take care that their overlapping directives do not hinder the promising growth potential of this innovative financial platform.

This paper will provide a short introduction to the Bitcoin network, including its properties, operations, and pseudonymous character. It will describe the benefits of allowing the Bitcoin network to develop and innovate, while highlighting issues of concern for consumers, policymakers, and regulators. It will describe the current regulatory landscape and explore other potential regulations that could be promulgated. The paper will conclude by providing policy recommendations that will assuage policymakers' common concerns while allowing for innovation within the Bitcoin network.

WHAT IS BITCOIN?

Bitcoin is an open-source, peer-to-peer digital currency. Among many other things, what makes Bitcoin unique is that it is the world's first completely decentralized digital-payments system. This may sound complicated, but the underlying concepts are not difficult to understand.

Overview

Until Bitcoin's invention in 2008 by the unidentified programmer known as Satoshi Nakamoto, online transactions always required a trusted third-party intermediary. For example, if Alice wanted to send $100 to Bob over the Internet, she would have had to rely on a third-party service like PayPal or MasterCard. Intermediaries like PayPal keep a ledger of account holders' balances. When Alice sends Bob $100, PayPal deducts the amount from her account and adds it to Bob's account.

Without such intermediaries, digital money could be spent twice. Imagine there are no intermediaries with ledgers, and digital cash is simply a computer file, just as digital documents are computer files. Alice could send $100 to Bob by attaching a money file to a message. But just as with email, sending an attachment does not remove it from one's computer. Alice would retain a copy of the money file after she had sent it. She could then easily send the *same* $100 to Charlie. In computer science, this is known as the "double-spending" problem,[10] and until Bitcoin it could only be solved by employing a ledger-keeping trusted third party.

Bitcoin's invention is revolutionary because for the first time the double-spending problem can be solved without the need for a third party. Bitcoin does this by distributing the necessary ledger among all the users of the system via a peer-to-peer network. Every transaction that occurs in the bitcoin economy is registered in a public, distributed ledger, which is called the block chain. New transactions are checked against the block chain to ensure that the same bitcoins haven't been previously spent, thus eliminating the double-spending problem. The global peer-to-peer network, composed of thousands of users, takes the place of an intermediary; Alice and Bob can transact without PayPal.

One thing to note right away is that transactions on the Bitcoin network are not denominated in dollars or euros or yen as they are on PayPal, but are instead denominated in bitcoins. This makes it a virtual currency in addition to a decentralized payments network. The value of the currency is not derived from gold or government fiat, but from the value that people assign to it.

---

[9] Tracy Alloway, Gregory Meyer, and Stephen Foley, "US Regulators Eye Bitcoin Supervision," *Financial Times*, May 6, 2013, http://www.ft.com/intl/cms/s/0/b810157c-b651-11e2-93ba-00144feabdc0.html.
[10] David Chaum, "Achieving Electronic Privacy," *Scientific American*, August 1992, 96–101.

The dollar value of a bitcoin is determined on an open market, just as is the exchange rate between different world currencies.[11]

Operation

So far we have discussed what Bitcoin is: a decentralized peer-to-peer payments network and a virtual currency that essentially operates as online cash. Now we will take a closer look at how Bitcoin works.

Transactions are verified, and double-spending is prevented, through the clever use of public-key cryptography.[12] Public-key cryptography requires that each user be assigned two "keys," one private key that is kept secret like a password, and one public key that can be shared with the world. When Alice decides to transfer bitcoins to Bob, she creates a message, called a "transaction," which contains Bob's public key, and she "signs" it with her private key. By looking at Alice's public key, anyone can verify that the transaction was indeed signed with her private key, that it is an authentic exchange, and that Bob is the new owner of the funds. The transaction—and thus the transfer of ownership of the bitcoins—is recorded, time-stamped, and displayed in one "block" of the block chain. Public-key cryptography ensures that all computers in the network have a constantly updated and *verified* record of all transactions within the Bitcoin network, which prevents double-spending and fraud.

What does it mean when we say that "the network" verifies transactions and reconciles the ledger? And how exactly are new bitcoins created and introduced into the money supply? As we have already seen, because Bitcoin is a peer-to-peer network, there is no central authority charged with either creating currency units or verifying transactions. This network depends on users who provide their computing power to do the logging and reconciling of transactions. These users are called "miners"[13] because they are rewarded for their work with newly created bitcoins. Bitcoins are created, or "mined," as thousands of dispersed computers solve complex math problems that verify the transactions in the block chain. As one commentator has put it,

> The actual mining of Bitcoins is by a purely mathematical process. A useful analogy is with the search for prime numbers: it used to be fairly easy to find the small ones (Eratosthenes in Ancient Greece produced the first algorithm for finding them). But as they were found it got harder to find the larger ones. Nowadays researchers use advanced high-performance computers to find them and their achievements are noted by the mathematical community (for example, the University of Tennessee maintains a list of the highest 5,000).
>
> For Bitcoins the search is not actually for prime numbers but to find a sequence of data (called a "block") that produces a particular pattern when the Bitcoin "hash" algorithm is applied to the data. When a match occurs the miner obtains a bounty of Bitcoins (and also a fee if that block was used to certify a transaction). The size of the bounty reduces as Bitcoins

---

[11] "Markets," Bitcoincharts, accessed July 30, 2013, http://bitcoincharts.com/markets/.

[12] Christof Paar, Jan Pelzl, and Bart Preneel, "Introduction to Public-Key Cryptography," chapter 6 in *Understanding Cryptography: A Textbook for Students and Practitioners*, ed. Christof Paar and Jan Pelzl (New York: Springer, 2010). Sample available at http://wiki.crypto.rub.de/Buch/download/Understanding-Cryptography-Chapter6.pdf.

[13] Miners tend to be ordinary computer enthusiasts, but as mining becomes more difficult and expensive, the activity will likely become somewhat professionalized. For more information, see Alec Liu, "A Guide to Bitcoin Mining," *Motherboard*, March 22, 2013, http://motherboard.vice.com/blog/a-guide-to-bitcoin-mining-why-someone-bought-a-1500-bitcoin-miner-on-ebay-for-20600.

around the world are mined.

The difficulty of the search is also increased so that it becomes computationally more difficult to find a match. These two effects combine to reduce over time the rate at which Bitcoins are produced and mimic the production rate of a commodity like gold. At some point new Bitcoins will not be produced and the only incentive for miners will be transaction fees.[14]

So, the protocol was designed so that each miner contributes a computer's processing power toward maintaining the infrastructure needed to support and authenticate the currency network. Miners are awarded newly created bitcoins for contributing their processing power toward maintaining the network and verifying transactions in the block chain. And as more processing power is dedicated to mining, the protocol will increase the difficulty of the math problem, ensuring that bitcoins are always mined at a predictable and limited rate.

This process of mining bitcoins will not continue forever. Bitcoin was designed to mimic the extraction of gold or other precious metals from the earth—only a limited, known number of bitcoins can ever be mined. The arbitrary number chosen to be the cap is 21 million bitcoins. Miners are projected to painstakingly harvest the last "satoshi," or 0.00000001 of a bitcoin, in the year 2140. If the total mining power scales to a high enough level, the difficulty in mining bitcoins will have increased so much that procuring this last satoshi will be quite a challenging digital undertaking. Once the last satoshi has been mined, miners that contribute their processing power toward verifying transactions will be rewarded through transaction fees rather than mined bitcoins. This ensures that miners still have an incentive to keep the network running after the last bitcoin is mined.

Pseudonymity

A great deal of attention given to Bitcoin in the media centers on the anonymity that the digital currency is supposed to lend its users. This idea stems from a mistaken understanding of the currency, however.

Because online transactions to date have required a third-party intermediary, they have not been anonymous. PayPal, for example, will have a record of every time Alice has sent Bob money. And because Alice's and Bob's PayPal accounts are tied to their respective bank accounts, their identities are likely known. In contrast, if Alice gives Bob a $100 bill in cash, there is no intermediary and no record of the transaction. And if Alice and Bob don't know each other's identities, we can say the transaction is completely anonymous.

Bitcoin falls somewhere between these two extremes. On the one hand, bitcoins are like cash in that once Alice gives bitcoins to Bob, she no longer has them and Bob does, and there is no third-party intermediary between them that knows their respective identities. On the other hand, unlike cash, the fact that a transaction took place between two public keys, the time, the amount, and other information is recorded in the block chain. Indeed, every transaction that has ever occurred in the history of the bitcoin economy is publicly viewable in the block chain.[15]

While the public keys for all transactions—also known as "Bitcoin addresses"[16]—are

---

[14] Ken Tindell, "Geeks Love the Bitcoin Phenomenon Like They Loved the Internet in 1995," *Business Insider*, April 5, 2013, http://www.businessinsider.com/how-bitcoins-are-mined-and-used-2013-4.

[15] Note that this might be a boon to economic researchers.

[16] *Bitcoin wiki*, s.v. "Address," accessed July 30, 2013, https://en.bitcoin.it/wiki/Address.

recorded in the block chain, those public keys are not tied to anyone's identity. Yet if a person's identity were linked to a public key, one could look through the recorded transactions in the block chain and easily see all transactions associated with that key. So, while Bitcoin is very similar to cash in that parties can transact without disclosing their identities to a third party or to each other, it is unlike cash in that all the transactions to and from a particular Bitcoin address can be traced. In this way Bitcoin is not anonymous, but pseudonymous.

Tying a real-world identity to a pseudonymous Bitcoin address is not as difficult as some might imagine. For one thing, a person's identity (or at least identifying information, such as an IP address) is often recorded when the person makes a Bitcoin transaction at a website, or exchanges dollars for bitcoins at a bitcoin exchange. To increase the chances of remaining pseudonymous, one would have to employ anonymizing software like Tor, and take care never to transact with Bitcoin addresses that could be tied back to one's identity.

Finally, it is also possible to glean identities simply by looking at the block chain. One study found that behavior-based clustering techniques could reveal the identities of 40 percent of Bitcoin users in their simulated Bitcoin experiment.[17] An early analysis of the statistical properties of the Bitcoin transaction graph showed how a passive network analysis with the appropriate tools can divulge the financial activity and identities of Bitcoin users.[18] A later analysis of the statistical properties of the Bitcoin transaction graph garnered similar results with a larger dataset.[19] Another analysis of the Bitcoin transaction graph reiterated that observers using "entity merging"[20] can observe structural patterns in user behavior and emphasized that this is "one of the most important challenges to Bitcoin anonymity."[21] In spite of this, Bitcoin users do enjoy a much higher level of privacy than do users of traditional digital-transfer services, who must provide detailed personal information to the third-party financial intermediaries that facilitate the exchange.

Although Bitcoin is frequently referred to as an "anonymous" currency, in reality, it is very difficult to stay anonymous in the Bitcoin network. Pseudonyms tied to transactions recorded in the public ledger can be identified years after an exchange is made. Once Bitcoin intermediaries are fully compliant with the bank-secrecy regulations required of traditional financial intermediaries, anonymity will be even less guaranteed, because Bitcoin intermediaries will be required to collect personal data on their customers.

Benefits

The first question that many people have when they learn about Bitcoin is, Why would I want to use bitcoins when I can use dollars? Bitcoin is still a new and fluctuating currency that is not accepted by many merchants, so the uses for Bitcoin may seem mostly experimental. To better

---

[17] Elli Androulaki et al., "Evaluating User Privacy in Bitcoin," *IACR Cryptology ePrint Archive* 596 (2012), http://fc13.ifca.ai/proc/1-3.pdf.

[18] Fergal Reid and Martin Harrigan, "An Analysis of Anonymity in the Bitcoin System," in *Security and Privacy in Social Networks*, ed. Yaniv Altshuler et al. (New York: Springer, 2013), http://arxiv.org/pdf/1107.4524v2.pdf.

[19] Dorit Ron and Adi Shamir, "Quantitative Analysis of the Full Bitcoin Transaction Graph," *IACR Cryptology ePrint Archive* 584 (2012), http://eprint.iacr.org/2012/584.pdf.

[20] Entity merging is the process of observing two or more public keys used as an input to one transaction at the same time. In this way, even if a user has several different public keys, an observer can gradually link them together and remove the ostensible anonymity that multiple public keys is thought to provide.

[21] Micha Ober, Stefan Katzenbeisser, and Kay Hamacher, "Structure and Anonymity of the Bitcoin Transaction Graph," *Future Internet* 5, no. 2 (2013), http://www.mdpi.com/1999-5903/5/2/237.

understand why people might want to use Bitcoin, it helps to think of it, not necessarily as a replacement for traditional currencies, but rather as a new payments system.

Lower Transaction Costs

Because there is no third-party intermediary, Bitcoin transactions are substantially cheaper and quicker than traditional payment networks. And because transactions are cheaper, Bitcoin makes micropayments and other innovations possible. Additionally, Bitcoin holds much promise as a way to lower transaction costs for small businesses and global remittances, alleviate global poverty by improving access to capital, protect individuals against capital controls and censorship, ensure financial privacy for oppressed groups, and spur innovation (within and on top of the Bitcoin protocol). On the other hand, Bitcoin's decentralized nature also presents opportunities for crime. The challenge, then, is to develop processes that diminish the opportunities for criminality while maintaining the benefits that Bitcoin can provide.

First, Bitcoin is attractive to cost-conscious small businesses looking for ways to lower the transaction costs of doing business. Credit cards have greatly expanded the ease of transacting, but their use comes with considerable costs to merchants. Businesses that wish to offer the option of credit card payments to their customers must first pay for a merchant account with each credit card company. Depending on the terms of agreement with each credit card company, businesses must then pay a variety of authorization fees, transaction fees, statement fees, interchange fees, and customer-service fees, among other charges. These fees quickly add up and significantly increase the cost of doing business. However, if a merchant neglects to accept credit card payments to save on fees, he or she could lose a considerable amount of business from customers who enjoy the ease of credit cards.

Since Bitcoin facilitates direct transactions without a third party, it removes costly charges that accompany credit card transactions. The Founders Fund, the venture capital fund headed by Peter Thiel of PayPal and Facebook fame, recently invested $3 million in the payment-processing company BitPay because of the service's ability to lower the costs of doing online commerce across borders.[22] In fact, small businesses have already started to accept bitcoins as a way to avoid the costs of doing business with credit card companies.[23] Others have adopted the currency for its speed and efficiency in facilitating transactions.[24] Merchants labeled "high risk" by credit card companies have difficulty finding a payment processor willing to work with them, so they have turned to Bitcoin merchant services providers, like BitPay, as an affordable and convenient alternative to credit card services.[25] Bitcoin will likely continue to lower transaction costs for businesses that accept it as more people adopt the currency.

Accepting credit card payments also puts businesses on the hook for charge-back fraud.

---

[22] Tom Simonite, "Bitcoin Hits the Big Time, to the Regret of Some Early Boosters," *MIT Technology Review*, May 22, 2013, http://www.technologyreview.com/news/515061/bitcoin-hits-the-big-time-to-the-regret-of-some-early-boosters/.

[23] Gabrielle Karol, "Small Business Owners Say Bitcoins Better Than Credit Cards," *FOX Business, Small Business Center*, April 12, 2013, http://smallbusiness.foxbusiness.com/entrepreneurs/2013/04/12/small-business-owners-say-bitcoins-better-than-credit-cards/.

[24] Bailey Reutzel, "Why Some Merchants Accept Bitcoin Despite the Risks," *Payments Source*, May 21, 2013, http://www.paymentssource.com/news/why-some-merchants-accept-bitcoin-despite-the-risks-3014183-1.html.

[25] Bailey Reutzel, "Some Risky Merchants Turn to Bitcoin Processor; Others Go It Alone," *Payments Source*, November 8, 2013, http://www.paymentssource.com/news/some-risky-merchants-turn-to-bitcoin-processor-others-go-it-alone-3015974-1.html.

Merchants have long been plagued by fraudulent "charge-backs," or consumer-initiated payment reversals based on a false claim that a product has not been delivered.[26] Merchants therefore can lose the payment for the item and the item itself, and also have to pay a fee for the charge-back. As a nonreversible payment system, Bitcoin eliminates the "friendly fraud" wrought by the misuse of consumer charge-backs. This can be very important for small businesses. As Dan Lee, the manager of a small bodega in Brooklyn, puts it, "[With Bitcoin], there are lower fees, and you don't have to worry about charge-backs, which is beneficial for merchants. It's better than Visa or MasterCard."[27] This property is so valuable to the business that Lee's Greene Avenue Market offers a 10% discount to customers who pay in Bitcoin.

Consumers like charge-backs, however, because that system protects them from unscrupulous merchants or merchant errors. Consumers may also enjoy other benefits that merchant-account fees help fund. Indeed, many consumers and merchants will probably stick to traditional credit card services even if Bitcoin payments become available. Still, the expanded choices in payment options would benefit people of all preferences.

Those who want the protection and perks of using a credit card can continue to do so, even if they pay a little more. Those who are more price- or privacy-conscious can use bitcoins instead. Not having to pay merchant fees means that merchants who accept Bitcoin have the option to pass the savings on to consumers. That is the business model of the Bitcoin Store,[28] which sells thousands of consumer electronics at discounted prices and only accepts bitcoins. The same Samsung Galaxy Note tablet that sells on Amazon for $779 plus shipping[29] sells at the Bitcoin Store for a mere $480.[30] In this way, Bitcoin provides more low-cost options to bargain hunters and small businesses without detracting from the traditional credit card services that some consumers prefer.

As an inexpensive funds-transfer system, Bitcoin also holds promise for the future of low-cost remittances. In 2012, immigrants to developed countries sent at least $401 billion in remittances back to relatives living in developing countries.[31] The amount of remittances is projected to increase to $515 billion by 2015.[32] Most of these remittances are sent using traditional brick-and-mortar wire services such as Western Union and MoneyGram, which

---

[26] Emily Maltby, "Chargebacks Create Business Headaches," *Wall Street Journal*, February 10, 2011, http://online.wsj.com/article/SB10001424052748704698004576104554234202010.html. One such scam involves Alice sending Bob a PayPal payment for a laptop that Bob has listed on Craigslist. Alice comes by Bob's house, picks up the laptop, and soon thereafter initiates a "charge-back" (i.e., reverses the payment). PayPal generally requires proof of shipment before reversing a charge-back, so Bob is out of luck.

[27] Rob Wile, "A Brooklyn Bodega Owner Told Us Why All Merchants Should Start Accepting Bitcoin," *Business Insider*, November 11, 2013, http://www.businessinsider.com/brooklyn-bitcoin-bodega-2013-11.

[28] Vitalik Buterin, "Bitcoin Store Opens: All Your Electronics Cheaper with Bitcoins," *Bitcoin Magazine*, November 5, 2012, http://bitcoinmagazine.com/bitcoin-store-opens-all-your-electronics-cheaper-with-bitcoins/.

[29] Amazon listing for a Samsung Galaxy Note tablet, accessed May 29, 2013, http://amzn.com/B00BJXNGIK.

[30] Bitcoin store listing for a Samsung Galaxy Note tablet, accessed May 29, 2013, https://www.bitcoinstore.com/samsung-galaxy-note-gt-n8013-10-1-32-gb-tablet-wi-fi-1-40-ghz-deep-gray.html. Products on the Bitcoin store are priced in both bitcoins and US dollars. At the point of purchase, Bitpay, a Bitcoin payment processing company, determines the currency conversion rate and holds that price for 15 minutes. See the Bitcoin Store FAQ: https://www.bitcoinstore.com/faq.

[31] World Bank Payment Systems Development Group, *Remittance Prices Worldwide: An Analysis of Trends in the Average Total Cost of Migrant Remittance Services* (Washington, DC: World Bank, 2013), http://remittanceprices.worldbank.org/~/media/FPDKM/Remittances/Documents/RemittancePriceWorldwide-Analysis-Mar2013.pdf.

[32] Ibid.

charge steep fees for the service and can take several business days to transfer the funds.[33] In the first quarter of 2013, the global average fee for sending remittances was 9.05 percent.[34] In contrast, transaction fees on the Bitcoin network tend to be less than 0.0005 BTC,[35] or 1 percent of the transaction.[36] This entrepreneurial opportunity to improve money transfers has attracted investments from big-name venture capitalists.[37] Even MoneyGram and Western Union are contemplating whether to integrate Bitcoin into their business models.[38] Bitcoin allows for instantaneous, inexpensive remittances, and the reduction in the cost of global remittances for consumers could be considerable.

Potential to Combat Poverty and Oppression

Bitcoin also has the potential to improve the quality of life for the world's poorest. Improving access to basic financial services is a promising antipoverty technique.[39] According to one estimate, 64 percent of people living in developing countries lack access to these services, perhaps because it is too costly for traditional financial institutions to serve poor, rural areas.[40] Because of the impediments to developing traditional branch banking in poor areas, people in developing countries have turned to mobile banking services for their financial needs. The closed-system mobile payment service M-Pesa has been particularly successful in countries such as Kenya, Tanzania, and Afghanistan.[41] Entrepreneurs are already moving to this model; the Bitcoin wallet service Kipochi recently developed a product that allows M-Pesa users to exchange bitcoins.[42] Mobile banking services in developing countries can be further augmented by the adoption of Bitcoin.

Other Bitcoin business models seek to streamline Bitcoin use in developing economies. LocalBitcoins.com, a listing and escrow service for individual small Bitcoin traders, publicizes trader information in over 190 countries, including Bangladesh, Zimbabwe, the Democratic Republic of Congo, Pakistan, Venezuela, Romania, India, Libya, and other developing economies.[43] The Google- and YCombinator-backed service provider startup, Buttercoin, aims to spread Bitcoin use in the developing world by partnering with locally licensed exchange

---

[33] Jessica Silver-Greenberg, "New Rules for Money Transfers, but Few Limits," *New York Times*, June 1, 2012, http://www.nytimes.com/2012/06/02/business/new-rules-for-money-transfers-but-few-limits.html?pagewanted=all&_r=0.

[34] World Bank, *Remittance Prices*.

[35] *Bitcoin wiki*, s.v. "Transaction fees," accessed July 30, 2013, https://en.bitcoin.it/wiki/Transaction_fees.

[36] Andrew Paul, "Is Bitcoin the Next Generation of Online Payments?," *Yahoo! Small Business Advisor*, May 24, 2013, http://smallbusiness.yahoo.com/advisor/bitcoin-next-generation-online-payments-213922448--finance.html.

[37] Simonite, "Bitcoin Hits the Big Time."

[38] Andrew R. Johnson, "Money Transfers in Bitcoins? Western Union, MoneyGram Weigh the Option," *Wall Street Journal*, April 18, 2013, http://online.wsj.com/article/SB10001424127887324493704578431000719258048.html.

[39] Muhammad Yunus, *Banker to the Poor: Micro-lending and the Battle against World Poverty* (New York: Public Affairs, 2003).

[40] Oya Pinar Ardic, Maximilien Heimann, and Nataliya Mylenko, "Access to Financial Services and the Financial Inclusion Agenda around the World" (Policy Research Working Paper, World Bank Financial and Private Sector Development Consultative Group to Assist the Poor, 2011), https://openknowledge.worldbank.org/bitstream/handle/10986/3310/WPS5537.pdf.

[41] Jeff Fong, "How Bitcoin Could Help the World's Poorest People," *PolicyMic*, May 2013, http://www.policymic.com/articles/41561/bitcoin-price-2013-how-bitcoin-could-help-the-world-s-poorest-people.

[42] Emily Spaven, "Kipochi launches M-Pesa Integrated Bitcoin Wallet in Africa," *CoinDesk*, July 19, 2013, http://www.coindesk.com/kipochi-launches-m-pesa-integrated-bitcoin-wallet-in-africa/.

[43] "Bitcoin Statistics," LocalBitcoins.com, accessed November 12, 2013, https://localbitcoins.com/statistics.

businesses to trade bitcoins for local currencies. By providing Bitcoin services to already-licensed companies in countries all over the world, Buttercoin can penetrate local markets without sacrificing compliance.[44] The company plans to open services in India by the end of 2013 and extend operations to six different countries in the following six months.[45]

Charities in the United States also have looked to Bitcoin as a promising way to alleviate poverty. Bitcoin's ease and affordability in transferring funds makes it an attractive option to lower operation costs for cash-strapped charities. The Bitcoin100 charity campaign has contributed Bitcoin donations to a number of causes since 2011.[46] Sean's Outpost, a homeless outreach organization located in Pensacola, Florida, has been providing meals and toiletries to Pensacola's neediest solely with bitcoins.[47] The charity's founder, Jason King, plans to open a nine acre homeless sanctuary, fittingly titled "Satoshi Forest," paid for entirely with Bitcoin.[48] According to King, Bitcoin's low costs and ease of transfer make it an ideal currency for his charity. "Anyone being able to send money to us in the world instantaneously is very valuable, and we've gotten donations from over twenty-three different countries," he explains.[49] As an open-system payment service, Bitcoin can provide low-income people in developing and developed countries alike with inexpensive access to financial services on a global scale.

Bitcoin might also provide relief to people living in countries with strict capital controls. The total number of bitcoins that can be mined is capped and cannot be manipulated. There is no central authority that can reverse transactions or prevent the exchange of bitcoins between countries. Bitcoin therefore provides an escape hatch for people who desire an alternative to their country's devalued currencies or frozen capital markets. We have already seen examples of people turning to Bitcoin to evade the harmful effects of capital controls and central-bank mismanagement. Some Argentines, for instance, have adopted Bitcoin in response to the country's dual burdens of a 25 percent inflation rate and strict capital controls.[50] Consumer confidence, too, continues to plunge in Argentina.[51] Demand for bitcoins is so strong in Argentina that one popular bitcoin exchange is planning to open an Argentine office.[52] Argentine Bitcoin use continues to surge in the face of Argentina's capital mismanagement.[53] For example,

---

[44] Bailey Ruetzel, "Buttercoin Takes a Different Path to Handling Virtual Currency," *Payments Source*, September 9, 2013, http://www.paymentssource.com/news/buttercoin-takes-a-different-path-to-handling-virtual-currency-3015366-1.html.

[45] Kim-Mai Cutler, "YC-Backed Buttercoin Uses Bitcoin To Attack the $500B-A-Year Remittances Economy," *Techcrunch*, August 20, 2013, http://techcrunch.com/2013/08/20/buttercoin/.

[46] Vitalik Buterin, "Charity Focus: Sean's Outpost," *Bitcoin Magazine*, April 2013, http://bitcoinmagazine.com/sandbox/seansoutpost.pdf.

[47] Ibid.

[48] Vitalik Buterin, "Sean's Outpost Announces Satoshi Forest, Nine-Acre Sanctuary for the Homeless," *Bitcoin Magazine*, September 9, 2023, http://bitcoinmagazine.com/6939/seans-outpost-announces-satoshi-forest/.

[49] Meghan Lords, "Feeding and Housing the Homeless with Bitcoin," *Bitcoin Not Bombs*, August 16, 2013, http://www.bitcoinnotbombs.com/feeding-and-housing-the-homeless-with-bitcoin/.

[50] Jon Matonis, "Bitcoin's Promise in Argentina," *Forbes*, April 27, 2013, http://www.forbes.com/sites/jonmatonis/2013/04/27/bitcoins-promise-in-argentina/.

[51] Roberto A. Ferdman, "Argentina's Unofficial Consumer Confidence Metric is Free-Falling Again," *Quartz*, October 23, 2013, http://qz.com/138498/argentinas-unofficial-consumer-confidence-metric-is-free-falling-again/.

[52] Camila Russo, "Bitcoin Dreams Endure to Savers Crushed by CPI: Argentina Credit," *Bloomberg*, April 16, 2013, http://www.bloomberg.com/news/2013-04-16/bitcoin-dreams-endure-to-savers-crushed-by-cpi-argentina-credit.html.

[53] Georgia Wells, "Bitcoin Downloads Surge in Argentina," *Wall Street Journal Money Beat*, July 17, 2013, http://blogs.wsj.com/moneybeat/2013/07/17/bitcoin-downloads-surge-in-argentina/.

the Net Party, an Argentine political reform movement, was funded almost entirely with bitcoins. "There you can see the different: the speed of money," says founder Santiago Siri, "[Raising] the money would have taken eight weeks [using the official currency]; it took one hour with Bitcoin."[54]

Individuals in oppressive or emergency situations might also benefit from the financial privacy that Bitcoin can provide. There are many legitimate reasons why people seek privacy in their financial transactions. Spouses fleeing abusive partners need some way to discreetly spend money without being tracked. People seeking controversial health services desire financial privacy from family members, employers, and others who might judge their decisions. Recent experiences with despotic governments suggest that oppressed citizens would benefit greatly from the ability to make private transactions free from the grabbing hands of tyrants. Bitcoin provides some of the privacy that has traditionally been afforded through cash—with the added convenience of digital transfer.

Stimulus for Financial Innovation

One of the most promising applications of Bitcoin is as a platform for financial innovation. The Bitcoin protocol contains the digital blueprints for a number of useful financial and legal services that programmers can easily develop. Since bitcoins are, at their core, simply packets of data, they can be used to transfer, not only currencies, but also stocks, bets, and sensitive information.[55] Some of the features that are built into the Bitcoin protocol include micropayments, dispute mediations, assurance contracts, and smart property.[56] These features would allow for the easy development of Internet translation services, instantaneous processing for small transactions (like automatically metering Wi-Fi access), and Kickstarter-like crowdfunding services. Indeed, early initiatives have already materialized. The crowdfunding platform Pozible now allows project creators to amass microdonations in Bitcoin for minuscule transaction fees.[57] The payment platform Bitmonet provides internet content creators with a way to monetize their blog or portfolio with bitcoins.[58] Similarly, Beatcoin is a music delivery service powered through Bitcoin micropayments.[59] As the Bitcoin economy further matures, more of these innovative applications will continue to materialize.

Additionally, programmers can develop alternative protocols on top of the Bitcoin protocol in the same way that the Web and email are run on top of the Internet's TCP/IP protocol. One

---

[54] Ben Smith and Conz Preti, "Argentina's Net Party Is Ready for the Revolution," *Buzzfeed*, October 24, 2013, http://www.buzzfeed.com/bensmith/argentinas-net-party-is-ready-for-the-revolution.

[55] Jerry Brito, "The Top 3 Things I Learned at the Bitcoin Conference," *Reason*, May 20, 2013, http://reason.com /archives/2013/05/20/the-top-3-things-i-learned-at-the-bitcoi.

[56] Mike Hearn, "Bitcoin 2012 London: Mike Hearn," YouTube video, 28:19, posted by "QueuePolitely," September 27, 2012, http://www.youtube.com/watch?v=mD4L7xDNCmA. Smart property is a concept to control ownership of an item through agreements made in the Bitcoin block chain. Smart property allows people to exchange ownership of a good or service once a condition is met using cryptography. Although smart property is still theoretical, the basic mechanisms are built into the Bitcoin protocol. See *Bitcoin wiki*, s.v., "Smart Property," accessed July 30, 2013, https://en.bitcoin.it/wiki/Smart_Property.

[57] "Pozible Now Accepting Pledges in Bitcoin," *Pozible Blog*, October 2013, http://www.pozible.com/blog/article /index/129.

[58] John Biggs, "Bitmonet Monetizes Your Blog Through the Power of Bitcoin, " *Techcrunch*, August 30, 2013, http://considertechcrunch.com/2013/08/30/bitmonet-monetizes-your-blog-through-the-power-of-bitcoin/.

[59] Romain Dillet, "Beatcoin is a Music Jukebox Hack Powered By Bitcoin Micropayments," *Techcrunch*, October 27, 2013, http://techcrunch.com/2013/10/27/beatcoin-is-a-music-jukebox-hack-powered-by-bitcoin-micropayments/.

programmer has already proposed a new protocol layer to add on top of the Bitcoin protocol that can improve the network's stability and security.[60] Another programmer created a digital notary service to anonymously and securely store a "proof of existence" for private documents on top of the Bitcoin protocol.[61] Other programmers have adopted the Bitcoin model as a way to encrypt email communications.[62] Another group of developers has outlined an add-on protocol that will improve the privacy of the network.[63] Bitcoin is thus the foundation upon which other layers of functionality can be built. The Bitcoin project can be best thought of as a process of financial and communicative experimentation. Policymakers should take care that their directives do not quash the promising innovations developing within and on top of this fledgling protocol.

CHALLENGES

Despite the benefits that it presents, Bitcoin has some downsides for potential users to consider. It has exhibited considerable price volatility throughout its existence. New users are at risk of improperly securing or even accidentally deleting their bitcoins if they are not cautious. Additionally, there are concerns about whether hacking could compromise the bitcoin economy.

Volatility

Bitcoin has weathered at least five significant price adjustments since 2011.[64] These adjustments resemble traditional speculative bubbles: overoptimistic media coverage of Bitcoin prompts waves of novice investors to pump up Bitcoin prices.[65] The exuberance reaches a tipping point, and the value eventually plummets. Newcomer investors eager to participate run the risk of overvaluing the currency and losing their money in a crash. Bitcoin's fluctuating value makes many observers skeptical of the currency's future.

Does this volatility foretell the end of Bitcoin? Some commentators believe so.[66] Others suggest that these fluctuations are stress-testing the currency and might eventually decrease in frequency as mechanisms develop to counteract volatility.[67] If bitcoins were only used as stores of value or units of account, the currency's volatility could indeed endanger its future. It does not make sense to manage business finances or keep savings in bitcoins if the market price swings

---

[60] J. R. Willett, "The Second Bitcoin Whitepaper" (white paper, 2013), https://sites.google.com/site

fradicates the possibility forie hyphens up in here?emerging and another underlying class? If so, leave as is. If not, consider/2ndbtcwpaper/2ndBitcoinWhitepaper.pdf.

[61] Jeremy Kirk, "Could the Bitcoin Network Be Used as an Ultrasecure Notary Service?," *ComputerWorld*, May 23, 2013, http://www.computerworld.com/s/article/9239513/Could_the_Bitcoin_network_be_used_as_an_ultrasecure_notary_service_.

[62] Jonathan Warren, "Bitmessage: A Peer-to-Peer Message Authentication and Delivery System" (white paper, November 27, 2012), https://bitmessage.org/bitmessage.pdf.

[63] Ian Miers et al., "Zerocoin: Anonymous Distributed E-Cash from Bitcoin" (working paper, the Johns Hopkins University Department of Computer Science, Baltimore, MD, 2013), http://spar.isi.jhu.edu/~mgreen/ZerocoinOakland.pdf.

[64] Timothy B. Lee, "An Illustrated History of Bitcoin Crashes," *Forbes*, April 11, 2013, http://www.forbes.com/sites/timothylee/2013/04/11/an-illustrated-history-of-bitcoin-crashes/.

[65] Felix Salmon, "The Bitcoin Bubble and the Future of Currency," *Medium*, April 3, 2013, https://medium.com/money-banking/2b5ef79482cb.

[66] Maureen Farrell, "Strategist Predicts End of Bitcoin," *CNNMoney*, May 14, 2013, http://money.cnn.com/2013/05/14/investing/bremmer-bitcoin/index.html.

[67] Adam Gurri, "Bitcoins, Free Banking, and the Optional Clause," *Ümlaut*, May 6, 2013, http://theumlaut.com/2013/05/06/bitcoins-free-banking-and-the-optional-clause/.

wildly and unpredictably. When Bitcoin is used as a medium of exchange, however, volatility is less of a problem.[68] Merchants can price their wares in terms of a traditional currency and accept the equivalent number of bitcoins. Customers who purchase bitcoins to make a one-time purchase don't care about what the exchange rate will look like tomorrow; they simply care that Bitcoin can lower transaction costs in the present. Bitcoin's usefulness as a medium of exchange might explain why the currency has grown more popular among merchants in spite of its price volatility.[69] It is also possible that the value of bitcoins will become less volatile as more people become familiar with the Bitcoin technology and develop realistic expectations about its future.

Security Breaches

As a digital currency, Bitcoin presents some specific security challenges.[70] If people are not careful, they can inadvertently delete or misplace their bitcoins. Once the digital file is lost, the money is lost, just as with paper cash. If people do not protect their private Bitcoin addresses, they can leave themselves open to theft. Bitcoin wallets can now be protected by encryption, but users must choose to activate the encryption. If a user does not encrypt his or her wallet, bitcoins could be stolen through malware.[71] Bitcoin exchanges, too, have at times struggled with security; hackers successfully stole 24,000 BTC ($250,000) from a bitcoin exchange called Bitfloor in 2012[72] and mounted a massive series of distributed denial-of-service (DDoS) attacks against the most popular bitcoin exchange, Mt.Gox, in 2013.[73] (Bitfloor eventually repaid the stolen funds to its customers, and Mt.Gox ultimately recovered from the DDoS attacks.) More recently, the wallet and mixing service inputs.io lost an equivalent of $1.2 million of their customers' bitcoins to a hacking attack.[74] Unscrupulous exchange stewards have similarly been a problem; in November of 2013, GBL, a Chinese Bitcoin exchange, abruptly closed its website and absconded with $4.1 million worth of their customers' bitcoins.[75] While the accountable operator of inputs.io will compensate his customers with a partial refund, GBL customers are not so lucky. Combined with the GBL operators' duplicity, Bitcoin's irreversibility eradicates the possibility of recourse. Of course, many of the security risks facing Bitcoin are similar to those facing traditional currencies. Dollar bills can be destroyed or lost, personal financial information can be stolen and used by criminals, and banks can be robbed or targeted by DDoS attacks. Bitcoin

---

[68] Jerry Brito, "Why Bitcoin's Valuation Really Doesn't Matter," *Technology Liberation Front*, April 5, 2013, http://techliberation.com/2013/04/05/why-bitcoins-valuation-doesnt-really-matter/.

[69] Today, merchant service providers accept the risk presented by the volatility and nevertheless maintain low fees. It remains to be seen whether this model will be sustainable in the long run.

[70] Most of the security challenges concern wallet services and bitcoin exchanges. The protocol itself has proven to be considerably resilient to hacking and security risks. Renowned security researcher Dan Kaminsky tried, but failed, to hack the Bitcoin protocol in 2011. See Dan Kaminsky, "I Tried Hacking Bitcoin and I Failed," *Business Insider*, April 12, 2013, http://www.businessinsider.com/dan-kaminsky-highlights-flaws-bitcoin-2013-4.

[71] Stephen Doherty, "All Your Bitcoins Are Ours . . . ," *Symantec Blog*, June 16, 2011, http://www.symantec.com/connect/blogs/all-your-bitcoins-are-ours.

[72] Devin Coldewey, "$250,000 Worth of Bitcoins Stolen in Net Heist," *NBC News*, September 5, 2012, http://www.nbcnews.com/technology/250-000-worth-bitcoins-stolen-net-heist-980871.

[73] Meghan Kelly, "Fool Me Once: Bitcoin Exchange Mt.Gox Falls after Third DDoS Attack This Month," *VentureBeat*, April 21, 2013, http://venturebeat.com/2013/04/21/mt-gox-ddos/.

[74] Robert McMillan, "$1.2M Hack Shows Why You Should Never Store Bitcoins on the Internet," *Wired*, November 7, 2013, http://www.wired.com/wiredenterprise/2013/11/inputs/.

[75] Jim Edwards, "A Bitcoin Exchange Holding $4.1 Million for 1,000 Customers Has Simply Vanished," *Business Insider*, November 12, 2013.

users should take care to learn about and prepare for security concerns just as they currently do for other financial activities.

Criminal Uses

There are also reasons for policymakers to be apprehensive about some of Bitcoin's exaptations. Because Bitcoin is pseudonymous, policymakers and journalists have questioned whether criminals can use it to launder money and accept payment for illicit goods and services. Indeed, like cash, it can be used for ill as well as for good.

For one example, we can look at the shuttered Deep Web[76] black-market site known as "Silk Road." While in operation from February 2011 to October 2013, Silk Road took advantage of the anonymizing network Tor and the pseudonymous nature of Bitcoin to make available a vast digital marketplace where one could mail-order drugs and other licit and illicit wares. Although Silk Road administrators did not allow the exchange of any goods that resulted from fraud or harm, like stolen credit card information or photographs of child exploitation, it did allow merchants to sell illegal products like forged identity documents and illicit drugs. The pseudonymous nature of Bitcoin allowed buyers to purchase illegal goods online in the same way that cash has been traditionally used to facilitate illicit purchases in person. One study estimated the total monthly Silk Road transactions amounted to approximately $1.2 million.[77] But the Bitcoin market amassed $770 million in transactions during June 2013; Silk Road sales constituted a small drop in the total bitcoin economy bucket.[78]

Bitcoin's association with Silk Road has tarnished its reputation. Following the publication of an article on Silk Road in 2011,[79] senators Charles Schumer and Joe Manchin sent a letter to Attorney General Eric Holder and the Drug Enforcement Administration's administrator Michele Leonhart calling for a crackdown on Silk Road, the anonymizing software Tor, and Bitcoin.[80] Their concerns were quickly addressed. Following a two year investigation into the Deep Web market, the FBI shut down the Silk Road website on October 2, 2013 and arrested Ross Ulbricht, the man alleged to be its infamous operator known only as the "Dread Pirate Roberts."[81] The FBI confiscated all bitcoins associated with Silk Road, totaling an unprecedented seizure of 26,000 BTC, worth $3.6 million at the time of the transfer.[82] Many of the largest merchants on Silk Road, too, have been indicted since Silk Road's closure.[83] Still, the end of Silk Road has not

---

[76] *Wikipedia*, s.v. "Deep Web," accessed July 30, 2013, http://en.wikipedia.org/wiki/Deep_Web.

[77] Nicolas Christin, "Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace," *Carnegie Mellon CyLab Technical Reports: CMU-CyLab-12-018*, July 30, 2012 (updated November 28, 2012), http://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab12018.pdf.

[78] Jerry Brito, "*National Review* Gets Bitcoin Very Wrong," *Technology Liberation Front*, June 20, 2013, http://techliberation.com/2013/06/20/national-review-gets-bitcoin-very-wrong/.

[79] Adrian Chen, "The Underground Website Where You Can Buy Any Drug Imaginable," *Gizmodo*, June 1, 2011, http://gawker.com/5805928/the-underground-website-where-you-can-buy-any-drug-imaginable.

[80] Brett Wolf, "Senators Seek Crackdown on 'Bitcoin' Currency," *Reuters*, June 8, 2011, http://www.reuters.com/article/2011/06/08/us-financial-bitcoins-idUSTRE7573T320110608.

[81] Emily Flitter, "FBI Shuts Alleged online Drug Marketplace, Silk Road," *Reuters*, October 2, 2013, http://www.reuters.com/article/2013/10/02/us-crime-silkroad-raid-idUSBRE9910TR20131002.

[82] James Ball, Charles Arthur, and Adam Gabbatt, "FBI Claims Largest Bitcoin Seizure After Arrest of Alleged Silk Road Founder," *The Guardian*, October 2, 2013, http://www.theguardian.com/technology/2013/oct/02/alleged-silk-road-website-founder-arrested-bitcoin.

[83] Brian Krebs, "Feds Arrest Alleged Top Silk Road Drug Dealer," *Krebs on Security*, October 7, 2013, http://krebsonsecurity.com/2013/10/feds-arrest-alleged-top-silk-road-drug-seller/.

eliminated the problem of illicit trade. Other Deep Web black markets, like Black Market Reloaded,[84] Sheep Marketplace,[85] and the relaunched Silk Road 2.0,[86] present new challenges for law enforcement.

Another concern is that Bitcoin can be used to launder money for financing terrorism and trafficking in illegal goods. Although these worries are currently more theoretical than evidential, Bitcoin could indeed be an option for those who wish to discreetly move ill-gotten money. Concerns about Bitcoin's potential to facilitate money laundering were stoked after Liberty Reserve, a private, centralized digital-currency service based in Costa Rica, was shut down by authorities on charges of money laundering.[87]

While Liberty Reserve and Bitcoin appear similar because they both provide digital currencies, there are important differences between the two. Liberty Reserve was a centralized currency service created and owned by a private company, allegedly for the express purpose of facilitating money laundering. Bitcoin is not. The transactions within the Liberty Reserve economy were not transparent. Indeed, Liberty Reserve promised its customers anonymity. Bitcoin, on the other hand, is a decentralized open currency that provides a public record of all transactions. Money launderers may attempt to protect their Bitcoin addresses and identities, but their transaction records will always be public and accessible at any time by law enforcement. Laundering money through Bitcoin, then, can be seen as a much riskier undertaking than using a centralized system like Liberty Reserve. Additionally, several bitcoin exchanges have taken steps to comply with anti–money laundering record-keeping and reporting requirements.[88] The combination of a public ledger system and the cooperation of bitcoin exchanges in collecting information on their customers will likely make Bitcoin less attractive to launderers relative to private anonymous virtual currencies.

It is also important to note that many of the potential downsides of Bitcoin are the same as those facing traditional cash. Cash has historically been the vehicle of choice for drug traffickers and money launderers, but policymakers would never seriously consider banning cash. As regulators begin to contemplate Bitcoin, they should be wary of the perils of overregulation. In the worst-case scenario, regulators could prevent legitimate businesses from benefitting from the Bitcoin network without preventing money launderers and drug traffickers from using bitcoins. If bitcoin exchanges are overburdened by regulation and shut down, for instance, money launderers and drug traffickers could still put money into the network by paying a person in cash to transfer his or her bitcoins into their virtual wallets. In this scenario, beneficial transactions are prevented by overregulation while the targeted activities are still able to occur. The challenge for policymakers and regulators is how to develop a system of oversight that assuages their twin

---

[84] Ryan Mac, "False Alarm: Silk Road Competitor Black Market Reloaded Staying Online," *Forbes*, October 18, 2013, http://www.forbes.com/sites/ryanmac/2013/10/18/false-alarm-silk-road-competitor-black-market-reloaded-staying-online/.

[85] Leonid Bershidsky, "Goodbye Silk Road, Hello Sheep Marketplace," *Bloomberg*, October 4, 2013, http://www.bloomberg.com/news/2013-10-04/goodbye-silk-road-hello-sheep-marketplace.html.

[86] Andy Greenberg, "'Silk Road 2.0' Launches, Promising A Resurrected Black Market for the Dark Web," *Forbes*, November 6, 2013, http://www.forbes.com/sites/andygreenberg/2013/11/06/silk-road-2-0-launches-promising-a-resurrected-black-market-for-the-dark-web/.

[87] "Liberty Reserve Digital Money Service Forced Offline," *BBC News—Technology*, May 27, 2013, http://www.bbc.co.uk/news/technology-22680297.

[88] Jeffrey Sparshott, "Bitcoin Exchange Makes Apparent Move to Play by U.S. Money-Laundering Rules," *Wall Street Journal*, June 28, 2013, http://online.wsj.com/article/SB10001424127887323873904578574000957464468.html.

concerns about money laundering and illicit purchases without smothering the benefits that Bitcoin is poised to provide to legitimate users in their everyday lives.

REGULATION

Current law and regulation does not envision a technology like Bitcoin, so it exists in something of a legal gray area. This is largely the case because Bitcoin does not exactly fit existing statutory definitions of currency or other financial instruments or institutions, making it difficult to know which laws apply and how.

This situation is reminiscent of regulatory uncertainty surrounding other new technologies, such as Voice over Internet Protocol (VoIP).[89] When VoIP first emerged, the Communications Act and Federal Communications Commission (FCC) regulations only contemplated voice communications over the traditional public switched telephone network. Like Bitcoin, VoIP competed with a highly regulated legacy network, was less expensive, and was often peer-to-peer. To this day Congress and the FCC continue to grapple with VoIP policy questions, including which public-interest obligations should be required of VoIP providers and whether VoIP providers must comply with law-enforcement wiretap requests.

Luckily, however, Congress and the FCC have charted a path for VoIP that has clarified much of the regulatory ambiguity without saddling the new technology with the legacy regulatory burden intended for monopoly telephone service. As a result, VoIP has flourished as a technology, has introduced competition to a previously stagnant market, and has lowered costs and improved access for consumers. Policymakers should seek to achieve the same with Bitcoin.

Bitcoin has the properties of an electronic payments system, a currency, and a commodity, among other things. As a result, it will likely receive scrutiny from several regulators. Below is an outline of some of the questions confronting these agencies as they prepare to regulate Bitcoin.

Is Private Currency Legal?

One of the most common initial questions about Bitcoin is whether the online currency is legal, given the federal government's monopoly on issuing legal tender. The answer seems to be yes. The Constitution only prohibits the states from coining money.[90] Privately issued currencies are not forbidden, and in fact many local currencies are in circulation.[91] To promote local economies, businesspeople and lawmakers have developed several alternative currencies in recent years, such as the Cascadia Hour Exchange in Portland and Life Dollars in Bellingham, Washington.[92]

What private parties may not do is issue currency that resembles US money.[93] One notorious case is that of Bernard von NotHaus, who was convicted in 2011 after printing and distributing a gold-backed currency called the "Liberty Dollar." His crime was not that he issued an alternative currency, but that it was similar in appearance to the US dollar and that von NotHaus attempted

---

[89] Sam Rozenfeld, "FCC'S VoIP Regulation Dilemma," *Telephony Your Way*, April 30, 2011, http://www.telephonyyourway.com/2011/04/30/fccs-voip-regulation-dilemma/.

[90] U.S. Const. art I § 10.

[91] Reuben Grinberg, "Bitcoin: An Innovative Alternative Digital Currency," *Hastings Science & Technology Law Journal* 4 (2011): 159–208.

[92] Blake Ellis, "Local Currencies: 'In the U.S. We Don't Trust,'" *CNN Money*, January 27, 2012, http://money.cnn.com/2012/01/17/pf/local_currency/index.htm.

[93] 18 U.S.C. §§ 485 and 486.

to spend his currency into circulation as dollars and encouraged others to do so as well.[94] In contrast, Bitcoin is in no danger of being confused with US currency.

Money-Transmission Laws

A business that transmits funds from one person to another is a money transmitter and in 48 states and the District of Columbia must obtain a license to operate.[95] Money transmitters are also subject to the Bank Secrecy Act (BSA) as implemented by regulations from FinCEN. Additionally, the USA PATRIOT Act made it a criminal offense to operate an unlicensed money-transmission business.[96]

The purpose of state licensing of money transmission has traditionally been consumer protection.[97] Because money transmitters (such as money-order issuers) are typically not FDIC-insured banks, consumers can be left holding the bag if a money transmitter does not forward the funds to the intended recipient. Licensing attempts to minimize this risk. Money-transmitter licensing in the States became widespread after the widely publicized defaults of several money-order companies in the 1980s.[98]

The BSA, on the other hand, is intended to prevent or detect money laundering and terrorist financing.[99] It requires money transmitters and other financial institutions to register with FinCEN, implement anti-money-laundering programs, keep records of their customers, and report suspicious transactions and other data.

Because it's not a company or legal entity, but instead a global peer-to-peer network, Bitcoin itself can't be said to be a money transmitter. The question then is, Do any of the actors in the Bitcoin ecosystem fit the statutory definitions of "money transmitter" that would subject them to state and federal regulation?

In March 2013, FinCEN issued guidance on the application of the BSA to virtual currencies, which include Bitcoin. The guidance defines three categories of persons potentially subject to its regulations as money transmitters:

> A *user* is a person that obtains virtual currency to purchase goods or services. An *exchanger* is a person engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency. An *administrator* is a person engaged as a business in issuing (putting into circulation) a virtual currency, and who has the authority to redeem (to withdraw from circulation) such virtual currency.[100]

We can apply each of these definitions to persons in the Bitcoin ecosystem. The clearest

---

[94] Grinberg, "Bitcoin," 193n158.

[95] *Hearing on the Regulation of Non-bank Money Transmitter—Money Services Businesses*, 112th Congress (2012) (statement of Ezra C. Levine), testimony before the Subcommittee on Financial Institutions and Consumer Credit of the House Committee on Financial Services, http://financialservices.house.gov/uploadedfiles/hhrg-112-ba15-wstate-elevine-20120621.pdf.

[96] 18 U.S.C. § 1960.

[97] Aaron Greenspan, *Held Hostage: How the Banking Sector Has Distorted Financial Regulation and Destroyed Technological Progress* (Palo Alto, CA: Think Computer Corporation, 2011), http://www.thinkcomputer.com/corporate/whitepapers/heldhostage.pdf.

[98] Ibid., 3.

[99] 31 U.S.C. § 5311.

[100] FinCEN, *Application of FinCEN's Regulations*.

definition is that of an *exchanger*. If one is in the business of exchanging dollars for bitcoins or vice versa, then we can conclude that one is a money transmitter under this guidance and must register with FinCEN and comply with the relevant record-keeping and reporting requirements. Also, because states often look to FinCEN's determinations about which types of entities are or are not money transmitters, an exchanger likely must obtain state money-transmitter licenses as well.

Less straightforward are the obligations of mere "users" of Bitcoin. The guidance states that if one obtains bitcoins "to purchase real or virtual goods or services," then one is not a money transmitter and not subject to FinCEN's regulations. It does not explain, however, how the law applies if one obtains bitcoins *not* to purchase goods or services. Some other reasons why one might obtain bitcoins include (1) speculation that the price of bitcoins will go up, (2) simply because one trusts a virtual currency's stability more than that of a particular "real currency" (think of Argentina or Zimbabwe), or (3) because one wants to make a remittance to a family member overseas. In none of these cases would Bitcoin users be assured that they are exempted from FinCEN's registration, record-keeping, and reporting requirements. This creates an uncertain regulatory environment that might unduly dampen use of Bitcoin.

Most confusing is how the guidance applies to Bitcoin miners, who create new bitcoins by lending their computing power to the Bitcoin network. The third class of persons that it defines is "administrators," but the definition only applies to centralized virtual currencies in which a central authority creates the currency. For example, Amazon.com is clearly the administrator of its new "Amazon Coins" virtual currency.[101] The guidance, therefore, has a section addressing decentralized virtual currencies such as Bitcoin. According to that section, a miner who mines bitcoins and then uses them "to purchase real or virtual goods and services" is considered a user not subject to the regulations.[102] But if the miner sells the mined bitcoins "to another person for real currency or its equivalent" then the miner qualifies as a money transmitter subject to regulation.[103]

It is not clear how such regulation of miners as money transmitters would further either consumer protection or anti-money-laundering interests. Miners are not transmitting bitcoins from one party to another; they are creating new bitcoins from thin air. If miners sell the bitcoins they mine, there are only two parties to the transaction. As a result, there is neither a consumer to protect nor a potential criminal seeking to convert "dirty money" into clean money.

Finally, the guidance notes that FinCEN regulations define currency as the currency of a state, and so the guidance also refers to this definition as "real currency."[104] It then develops a new concept that it calls "virtual currency" on which all the guidance is predicated.[105] The guidance defines virtual currency as "a medium of exchange that operates like a currency in some environments, but does not have all the attributes of real currency."[106] It goes on to introduce another concept by stating that there are different kinds of "virtual currency" and that the present guidance only extends to "convertible virtual currency," which it defines as one that

---

[101] Ingrid Lunden, "Amazon Now Offers Amazon Coins Virtual Currency on Kindle Fire, Gives $5 in Free Coins to All Users," *TechCrunch*, May 13, 2013, http://techcrunch.com/2013/05/13/amazon-launches-amazon-coins-virtual-currency-on-kindle-fire-gives-5-in-free-coins-to-all-users/.
[102] Ibid.
[103] Ibid.
[104] FinCEN, *Application of FinCEN's Regulations*.
[105] Ibid.
[106] Ibid.

"either has an equivalent value in real currency, or acts as a substitute for real currency."[107] While the definition of currency (aka "real currency") was adopted through rulemaking, the other new and substantive concepts of "virtual currency" and "convertible virtual currency" exist only in the guidance. As a result, the guidance may be seen as encompassing new law and not merely interpretations of existing law or regulations, thus necessitating a rulemaking under the Administrative Procedure Act.

CFTC Regulation

By their nature, bitcoins can be conceived of either as a commodity or as a currency. Indeed, economist George Selgin has called Bitcoin "synthetic-commodity money."[108] This has attracted the attention of the Commodity Futures Trading Commission (CFTC), which has authority to regulate commodity futures and the markets in which they trade, as well as to regulate some foreign-exchange instruments.[109]

Bart Chilton, one of five CFTC commissioners, recently told the *Financial Times* that Bitcoin "is for sure something we need to explore."[110] Other sources confirmed that the CFTC is "seriously" looking at the virtual currency.[111] To the extent it chooses to regulate bitcoin transactions, one obvious question is whether CFTC will do so under its commodity futures or foreign-exchange authority.

While the Commodity Exchange Act defines "foreign-exchange forwards" and "foreign-exchange swaps," it does not define "foreign exchange" or "foreign currency," presumably because Congress considered the meaning of those terms obvious. Therefore, if the CFTC moves to apply its foreign-exchange regulations to Bitcoin transactions, it will have to make the determination that bitcoins are considered "foreign currency." While conceivable, such a determination would be at odds with the common understanding of foreign currency, as the money coined by foreign governments.

To illustrate this, we can look at the 2009 Dodd-Frank Wall Street Reform and Consumer Protection Act, which expands the CFTC's authority to regulate foreign exchange. Title 10 of the act also establishes the Consumer Financial Protection Bureau (CFPB), and for purposes of that title defines "foreign exchange" as "the exchange, for compensation, of currency of the United States or of a foreign government for currency of another government."[112] This definition gives a hint of what Congress's conception of "foreign exchange" is, and bitcoin exchange would clearly fall outside it, because bitcoins are not the currency of any government.

The connection between foreign currency and government issuance is commonplace. For example, the Treasury Department's definition of currency (adopted through rulemaking, as noted earlier) is

> the coin and paper money of the United States or of any other country that is designated as legal tender and that circulates and is customarily used and accepted as a medium of exchange in the country of issuance. Currency includes US silver certificates, US notes and

[107] Ibid.
[108] George Selgin, "Synthetic Commodity Money" (working paper, Department of Economics, University of Georgia, Athens, 2013), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2000118.
[109] 7 U.S.C. §§ 2(C) and 2(E).
[110] Alloway, Meyer, and Foley, "US Regulators Eye Bitcoin."
[111] Ibid.
[112] Dodd-Frank Wall Street Reform and Consumer Protection Act § 1002 (16); 12 U.S.C. § 5481 (16) (2012).

> Federal Reserve notes. Currency also includes official foreign bank notes that are customarily used and accepted as a medium of exchange in a foreign country.[113]

This comports with the Uniform Commercial Code's definition of "money," which is "a medium of exchange authorized or adopted by a domestic or foreign government [including] a monetary unit of account established by an intergovernmental organization or by agreement between two or more nations."[114]

In contrast, the CFTC would have no problem treating bitcoins as commodities. The Commodity Exchange Act defines commodities as all "goods and articles . . . and all services, rights, and interests . . . in which contracts for future delivery are presently or in the future dealt in," except onions and motion-picture box-office receipts.[115] Therefore, bitcoins could certainly qualify as a commodity because they are articles that can be traded and made subject to futures contracts. That said, it is interesting to note that bitcoins are unlike traditional commodities such as gold, corn, or oil, which are tangible and have intrinsically valuable uses. It is also important to note that the CFTC's authority is over, not commodities themselves, but commodity futures. An exchange of bitcoins for dollars or other national currency, however, typically occurs instantaneously, and not as part of a futures contract. Therefore, CFTC regulation of bitcoins *as commodities* may be limited. To the extent bitcoin futures markets develop, however, they will certainly be subject to CFTC supervision.[116]

Electronic Fund Transfer Regulation

The final possible vector for regulation of Bitcoin under existing law that we will consider is regulation under the Electronic Fund Transfer Act (EFTA)[117] and its application through the Federal Reserve's Regulation E.[118] The purpose of the EFTA is to establish the respective rights and responsibilities of consumers and financial institutions in electronic fund transfers.[119] Like the other laws and regulations we have seen, the EFTA does not seem to contemplate a decentralized virtual currency like Bitcoin.

The act defines electronic fund transfers as "any transfer of funds, other than a transaction originated by check, draft, or similar paper instrument, which is initiated through an electronic terminal, telephonic instrument, or computer or magnetic tape so as to order, instruct, or authorize a financial institution to debit or credit an account."[120] It further defines "financial institution" as "a State or National bank, a State or Federal savings and loan association, a mutual savings bank, a State or Federal credit union, or any other person who, directly or indirectly, holds an account belonging to a consumer."[121] These definitions, and the regulations they undergird, assume that electronic fund transfers will necessarily involve "financial

---

[113] 31 C.F.R. § 1010.100(m).
[114] Unif. Commercial Code §§ 1–201.
[115] 7 U.S.C. § 1a (9).
[116] There are, however, emerging Bitcoin futures markets. See Cyrus Farivar, "'Taming the Bubble': Investors Bet on Bitcoin via Derivatives Markets," *Ars Technica*, April 11, 2013, http://arstechnica.com/business/2013/04/taming-the-bubble-investors-bet-on-bitcoin-via-derivatives-markets/.
[117] 15 U.S.C. §§ 1601–1692 (2013).
[118] 12 C.F.R. §§ 205.1–205.20.
[119] 15 U.S.C. § 1693(b).
[120] 15 U.S.C. § 1693a (7).
[121] 15 U.S.C. § 1693a (9).

institutions" and "accounts." Bitcoin, however, runs counter to that notion.

The Bitcoin system itself does not qualify as a "financial institution" because, as noted earlier, it is not a company or legal entity but instead a global peer-to-peer network. As a result, a Bitcoin address with which bitcoins are associated on the network cannot be said to be an account of a financial institution. Furthermore, as noted above in the technical discussion of how bitcoins are transferred between addresses, in the Bitcoin system there is no "financial institution" or other third party of any kind that "debit[s] or credit[s] an account." Electronic fund transfers between addresses are carried out by users alone, who sign a transaction with the private key associated with a Bitcoin address under their control. The Bitcoin network merely confirms that the transaction is legitimate.

While many users keep the "wallet files"[122] containing their private keys on their own computers or other devices,[123] some delegate securing their keys to online wallet services.[124] Such third-party wallet services often also provide greater ease-of-use than desktop Bitcoin software. Users typically create an "account" on such a wallet service, and their Bitcoin addresses are associated with those accounts. It is conceivable that such online services could fit the definition of "financial institution" under the EFTA, and thus be subject to the regulation. An argument could be made, however, that these services are not engaged in electronic fund transfers because they do not initiate transfers.[125] Transfers are made by the users directly and are verified by the Bitcoin network; online wallet services merely provide the software and storage that allows users to interact with the Bitcoin network.

Finally, new rules from the Consumer Financial Protection Bureau (CFPB) amending Regulation E target remittance-transfer providers. The regulations require remittance providers to disclose exchange rates and fees associated with international transfers, and to investigate and remediate processing errors.[126] They also require that consumers be afforded 30 minutes or more to cancel a transfer.[127] This requirement can be seen as incompatible with the Bitcoin protocol, because all bitcoin transactions are irreversible. One way to comply with this regulation might be to delay the execution of transactions. The real problem, though, is that this requirement is fundamentally at odds with the purpose of the technology.

Policy Recommendations

As we have seen, Bitcoin does not easily fit into existing regulatory boxes. That is often the hallmark of a disruptive technology. Indeed Bitcoin is a revolutionary technical achievement that heralds amazing potential benefits to human welfare. However, like any technology that can be used for good, it can also be used for ill. The challenge for policymakers will be to foster Bitcoin's beneficial uses while minimizing its negative consequences. We conclude with some recommendations to help policymakers meet this challenge.

---

[122] *Bitcoin wiki*, s.v. "Wallet," accessed July 30, 2013, https://en.bitcoin.it/wiki/Wallet.

[123] Matthew Sparks, "Winklevoss Twins Back Bitcoin as Bubble Bursts," *Telegraph*, April 12, 2013, http://www.telegraph.co.uk/technology/news/9989610/Winklevoss-twins-back-bitcoin-as-bubble-bursts.html.

[124] *Bitcoin wiki*, "EWallet," accessed July 30, 2013, https://en.bitcoin.it/wiki/EWallet.

[125] Nikolei M. Kaplanov, "Nerdy Money: Bitcoin, the Private Digital Currency, and the Case against Its Regulation," *Loyola Consumer Law Review* 25, no. 1 (2012).

[126] Consumer Financial Protection Bureau, "Summary of the Final Remittance Transfer Rule (Amendment to Regulation E)" (Washington, DC: Consumer Financial Protection Bureau, 2013), http://files.consumerfinance.gov/f/201305_cfpb_remittance-transfer-rule_summary.pdf.

[127] Ibid.

Don't Restrict Bitcoin

Because Bitcoin is essentially online cash, some who trade in drugs and other illicit goods online have found it to be an ideal medium of exchange.[128] Confronted with this fact, the initial impulse of some policymakers will be to call for restrictions on the technology.[129] There are many good reasons, however, to resist such an impulse.

First, as a technology, Bitcoin is neither good nor bad; it is neutral. Paper dollar bills, like bitcoins, can be used in illicit transactions, yet we do not consider outlawing paper bills. We only prohibit their *illicit use*. Furthermore, there is only anecdotal evidence about the extent to which bitcoins are utilized in criminal transactions. It would be wise to put the criminal use of the technology in perspective alongside its legitimate uses. As the bitcoin economy grows, legitimate uses of bitcoins will likely dwarf criminal transactions,[130] just as we see with paper dollar bills.

Second, any attempt to restrict Bitcoin technology will only harm legitimate uses while leaving illicit uses largely unaffected. Because it is a decentralized global network, Bitcoin is virtually impossible to shut down. There is no Bitcoin company or other entity that can be targeted. Instead, Bitcoin and its ledger exist only in the distributed peer-to-peer network created by its users. As with the peer-to-peer file-sharing service BitTorrent, taking down any of the individual computers that make up the peer-to-peer system would have little effect on the rest of the network. Therefore, making the use of Bitcoin illegal would not undermine the network; it would only serve to ensure that law-abiding users are denied access to the technology. As a result, society would forgo enjoying the many potential benefits of Bitcoin without seeing any drop in criminal use.

Third, if Bitcoin were prohibited, the government would forego the opportunity to regulate intermediaries in the bitcoin economy, such as exchangers and money transmitters. The governmental interests in detecting and preventing money laundering and terrorist financing would be better advanced, not by prohibiting the technology, but by requiring intermediaries to keep records and report suspicious activities, just as traditional financial institutions do. Again, restricting the use of Bitcoin will only ensure that criminals alone will use the technology. Any illicit intermediaries that emerge, such as exchanges and payment processors, will be unregulated.

Finally, even if the United States prohibited the use of Bitcoin, it is likely that many other countries would not, recognizing the technology's many potential benefits. The Finnish central bank, for example, has stated that the digital currency is not illegal,[131] and as a result many Finnish businesses have begun to accept bitcoins.[132] By prohibiting Bitcoin use, the United

---

[128] Andy Greenberg, "Founder of Drug Site Silk Road Says Bitcoin Booms and Busts Won't Kill His Black Market," *Forbes*, April 16, 2013, http://www.forbes.com/sites/andygreenberg/2013/04/16/founder-of-drug-site-silk-road-says-bitcoin-booms-and-busts-wont-kill-his-black-market/.

[129] Charles Schumer and Joe Manchin, Letter to Attorney General Eric Holder and Drug Enforcement Administration Administrator Michele Leonhart, June 6, 2011. Available at http://www.manchin.senate.gov/public/index.cfm/press-releases?ID=284ae54a-acf1-4258-be1c-7acee1f7e8b3.

[130] Jan Jahosky, "BitPay Eclipses Silk Road in Bitcoin Sales with Explosive $5.2M March," *BitPay Blog*, April 2, 2013, http://blog.bitpay.com/2013/04/bitpay-eclipses-silk-road-in-bitcoin.html.

[131] Matt Clinch, "Bitcoin Utopia? Interest Is Sky High in This Euro Nation," *CNBC*, April 4, 2013, http://www.cnbc.com/id/100618694.

[132] Jan Jahosky, "BitPay Exceeds 1,000 Merchants Accepting Bitcoin," *BitPay Blog*, September 11, 2012, http://blog.bitpay.com/2012/09/bitpay-exceeds-1000-merchants-accepting.html.

States could put itself at an international competitive disadvantage in the development and use of what may be the next-generation payments system.

Normalize Regulation and Encourage Further Development

Rather than overreact to illicit uses of Bitcoin, policymakers would be wise to take a calm and careful approach to the challenges posed by the new technology. Doing so would allow law enforcement to pursue its interests in detecting and preventing money laundering and terrorist financing while ensuring that society does not forgo Bitcoin's many benefits. Luckily, regulators to date have taken such a cautious approach by slowly integrating Bitcoin into the existing financial regulatory framework. Policymakers can take a few basic steps to maintain the right balance.

In the short term, FinCEN should clarify its recent guidance, especially as it relates to miners and users who do not obtain bitcoins to purchase goods or services, but instead do so for other legal and legitimate purposes. It should do this by welcoming public participation of the Bitcoin community of developers, miners, businesses, and users in formal public notice and comment proceedings. While FinCEN's mission is to safeguard the financial system from illicit use, it also has an obligation not to unduly hinder its technological development. Working with Bitcoin's legitimate users, there is no doubt FinCEN can achieve its goals while minimizing regulatory uncertainty.

In the long term, policymakers should better define Bitcoin's broader regulatory status. As we have seen, the digital currency does not comfortably fit any existing classification or legal definition. It is not a foreign currency, nor a traditional commodity, nor is it simply a payments network. Consequently, applying existing rules to Bitcoin could unduly impede Bitcoin's legitimate development without any attendant gains to law enforcement or consumer welfare. As a result, policymakers may want to consider developing a new category that takes into account the technology's unique nature. They should also carefully consider what regulation, if any, bitcoin exchanges, payment processors, and users should face.

Finally, policymakers should not only allow Bitcoin's development to continue unimpeded, they should help foster its growth by revisiting existing regulatory barriers. One of the greatest obstacles to Bitcoin's legitimate adoption is the requirement that businesses engaging in money transmission acquire a license from each state. This is a duplicative, laborious, and expensive process that presents a barrier to interstate commerce without much benefit to consumers. Federal lawmakers and regulators should consider whether preemption is necessary.

CONCLUSION

Bitcoin is an exciting innovation that has the potential to greatly improve human welfare and jump-start beneficial and potentially revolutionary developments in payments, communications, and business. Bitcoin's clever use of public-key encryption and peer-to-peer networking solves the double-spending problem that had previously made decentralized digital currencies impossible. These properties combine to create a payment system that could lower transactions costs in business and remittances, alleviate poverty, provide an escape from capital controls and monetary mismanagement, allow for legitimate financial privacy online, and spur new financial innovations. On the other hand, as "digital cash," Bitcoin can be used for money laundering and illicit trade. Banning Bitcoin is not the solution to ending money laundering and illicit trade, just as banning cash is not a solution to these same ills.

Bitcoin could ultimately fail as an experimental digital currency and payment system. An

unanticipated problem could arise and undermine the bitcoin economy. A superior cryptocurrency could outcompete and replace Bitcoin. It could simply fizzle out as a fad. The possibilities for failure are endless, but one reason for failure should not be that policymakers did not understand its workings and potential. We are ultimately advocating not for Bitcoin, but for innovation. It is important that policymakers allow this experimentation to continue. Policymakers should work to clarify how Bitcoin is regulated and to normalize its regulation so that we have the opportunity to learn just how innovative Bitcoin can be.

U.S. Immigration and Customs Enforcement

STATEMENT

OF

U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT

REGARDING A HEARING ON

"BEYOND SILK ROAD: POTENTIAL RISKS, THREATS, AND PROMISES OF VIRTUAL CURRENCIES"

BEFORE THE

UNITED STATES SENATE
COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS

Monday, November 18, 2013 -- 2:30 p.m.
106 Dirksen Senate Office Building

Introduction

Chairman Carper, Ranking Member Coburn, and distinguished members of the Committee, thank you for the opportunity to highlight the efforts of U.S. Immigration and Customs Enforcement (ICE) to combat the exploitation of virtual currency[1] platforms by transnational organized criminals (TOCs). Although virtual currencies may support important innovation and serve legitimate purposes, like traditional currencies or other methods of transferring value, virtual currencies may also be exploited for the purposes of money laundering, the facilitation and financing of terrorism, and to enable other crimes such as child pornography, drug trafficking, and cybercrimes.

ICE has expansive investigative authority and is the largest force of criminal investigators in the U.S. Department of Homeland Security (DHS). With more than 20,000 employees nationwide and in 48 countries, ICE promotes homeland security and public safety through the criminal and civil enforcement of federal laws governing border control, customs, trade, and immigration. ICE's primary priorities are to prevent terrorism and enhance security; protect the borders against illicit trade, travel and finance; and protect the borders through smart and effective immigration enforcement.

The ICE Homeland Security Investigations (HSI) Directorate, a critical asset in the ICE mission, is responsible for investigating a wide range of domestic and international activities arising from the illegal movement of people and goods into, within, and out of the United States.

[1] There is no single commonly accepted definition of virtual or digital currency. For purposes of this statement, **virtual currency** is a digital representation of value that can be traded on the Internet and functions as (1) a medium of exchange; (2) a unit of account; and/or (3) a store of value, but does not have legal tender status in any jurisdiction. 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. Virtual currency is also distinct from e-money, which is a digital representation of fiat currency used to electronically transfer value denominated in fiat currency. E-money is a digital transfer mechanism for fiat currency—i.e., it electronically transfers value that has legal tender status. **Digital currency** is a digital representation of either virtual currency or e-money.

HSI investigates immigration fraud, human rights violations, human smuggling and human trafficking, the smuggling of narcotics, weapons and all other types of contraband, intellectual property rights violations, and financial crimes—including those involving virtual currencies, cybercrimes, and export enforcement issues, among other offenses.

In addition, HSI oversees the agency's international affairs operations and intelligence functions. HSI consists of more than 10,000 employees, with over 6,700 special agents assigned to more than 200 cities throughout the United States and 48 countries around the world.

Illicit Finance

One of the most effective methods for dismantling TCOs is to attack the criminal proceeds that are the lifeblood of their operations. Through the work of HSI, ICE takes a holistic approach toward investigating money laundering, illicit finance, and other financial crimes by examining the ways that individuals and criminal organizations earn, move, store, and launder their illicit proceeds.

The combination of successful financial investigations, reporting requirements under the Bank Secrecy Act (BSA) of 1970, as amended, and anti-money laundering compliance efforts by financial institutions has no doubt strengthened payment systems and forced criminal organizations to continuously seek other means to diversify the movement of illicit funds.

Virtual Currency

In contrast to traditional currency, monetary instruments, or other methods of transferring value, virtual currencies serve as mediums of exchange, but are not accepted as legal tender in any recognized government jurisdiction. However, virtual currencies can be used to conduct

transactions entirely within a virtual economy, transferred between individuals, or used in lieu of a government-issued currency to purchase goods and services.

The appeal of virtual currencies, especially "open" or "convertible" currencies that can be exchanged for traditional currency, and vice versa, is that they may allow value to be transferred much more rapidly and cheaply (especially internationally) than through traditional banking payment systems, and often with greater anonymity and reduced oversight. Existing criminal statutes are available for law enforcement to target the illicit use of virtual currency systems by purchasers, administrators, and exchangers. Specifically, the transfer of virtual currency arguably does constitute a transfer of "funds" within the meaning of Sections 1956 and 1960 of Title 18 of the United States Code (U.S.C.). As a result, if criminals are using a virtual currency system to promote criminal activities, to disguise or conceal the source of their illicitly derived proceeds, or to evade federal or state reporting requirements, they may be prosecuted for money laundering.

Similarly, the failure of a virtual currency exchanger or administrator to register with the Treasury Department's Financial Crimes Enforcement Network (FinCEN) or the act of engaging in the transfer of criminally derived proceeds on behalf of the public, constitutes a violation of 18 U.S.C. §§ 1960 and 1956, respectively.

While electronic payment systems are certainly nothing new, ICE has recognized the potential for criminal exploitation and the money laundering threat posed by virtual currency. ICE has, therefore, strategically deployed a multi-prong investigative strategy designed to target illicit virtual currency platforms, currency exchangers, and underground black markets such as "carding," illegal drugs, illegal firearms, and child pornography forums.

Silk Road

On October 2, 2013, the collaborative efforts of ICE, the Federal Bureau of Investigation (FBI), Drug Enforcement Administration (DEA), the U.S. Postal Inspection Service (USPIS), and the Internal Revenue Service (IRS) resulted in the seizure of the website "Silk Road," which served as an online international marketplace for users to buy and sell controlled substances, false identifications and other contraband anonymously over the Internet. Silk Road utilized "bitcoins"[2] as the only accepted payment mechanism on the site.

The suspect was charged with a three-count indictment with conspiracy to distribute a controlled substance, attempted witness murder and using interstate commerce facilities in the commission of murder for hire. Between December 2012 and January 2013, the suspect is alleged to have knowingly conspired and agreed with others to distribute and possess with intent to distribute controlled substances including cocaine. The suspect is alleged to have profited from the operation of Silk Road by collecting a fee for each transaction.

During the course of the investigation, ICE special agents identified bitcoins used by buyers and sellers to complete their transactions on the Silk Road site. The bitcoins, worth an estimated $3.6 million, were located in Silk Road's operating account and ultimately seized by the FBI. Estimates indicate that Silk Road processed over $1.2 billion worth of business and earned commissions totaling 600,000 bitcoins, or about $80 million using bitcoin rates at the time of the seizure. ICE has subsequently provided additional leads to several international law enforcement partners resulting in the arrest of four additional co-conspirators.

---

[2] Bitcoin is a complex peer-to-peer virtual currency system that generates a virtual currency consisting of mathematical tokens (unique strings of numbers and letters) created entirely outside the world's regulated financial system by a network of computers' solving an algorithm. Because using bitcoins requires no personal identification and allows for transactions on networks in nearly complete isolation from the mainstream financial system, they have become an attractive option for money launderers and other illicit online activity.

Mt.Gox

In May 2013, through an interagency taskforce led by ICE in Baltimore, Maryland, three U.S. bank accounts associated with what was then the world's largest bitcoin exchanger, Japan-based Mt.Gox, which was moving approximately $60 million per month into a number of Internet-based hidden black markets operating on the Tor network, including Silk Road, were seized for violations of 18 U.S.C. § 1960, operating a money service business in the United States without a license. The bulk of the funds were associated with the illicit purchase of drugs, firearms, and child pornography. As a result of the forfeiture action, Mt.Gox, which allows users to trade bitcoins for U.S. dollars and several other currencies, has implemented varying degrees of user verification for its customers. These and many other ongoing criminal investigations have provided ICE with a better understanding of the risks and challenges posed by virtual currencies.

Illicit Pathways Attack Strategy (IPAS)

Transnational organized crime (TOC) poses a significant and growing threat to national and international security, with implications for public safety, public health, democratic institutions, and economic stability across the globe.

In July 2011, the Administration took an important step in fighting transnational crime when it issued its *Strategy to Combat Transnational Organized Crime* (TOC Strategy). This strategy complements the current *National Security Strategy* and other national initiatives related to human trafficking, money laundering, and transnational crime affecting the United States, by focusing on the growing threat of international criminal networks. The TOC Strategy's single unifying principle is to build, balance, and integrate the tools of American strength to combat

transnational organized crime, and related threats to national security—and to urge our international partners to do the same.

Consistent with the TOC Strategy, ICE developed the Financial Crimes Illicit Pathways Attack Strategy (IPAS) to enhance ICE's ability to disrupt the financial networks that support transnational criminal activity. By targeting the profits generated and used by criminal organizations, and not just targeting the contraband being smuggled, the IPAS will protect financial systems and strategic markets by addressing how criminal organizations earn, move and store illicit proceeds.

Partners and Cooperation

ICE recognizes that our approach to combating the illicit use of virtual currency systems must include collaboration and coordination with our domestic and international partners. ICE works closely with our federal, state, local, international law enforcement and other members of the interagency. Notably, ICE is an active participant in the Virtual Currency Emerging Threats Working Group, which was founded by the FBI in early 2012 to mitigate the cross-programmatic threats arising from illicit actors' use of virtual currency systems.

ICE also contributes to several other interagency groups dealing with digital currencies and emerging payment systems, including the New Payment Methods Ad Hoc Working Group, a subgroup of the Terrorist Finance Working Group led by the State Department; and the Financial Action Task Force, which is an inter-governmental body established in 1989 to set global standards and promote effective implementation of legal, regulatory, and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system.

ICE is also an active partner in the Secret Service-led Electronic Crimes Task Forces which leverage the private sector, academia, and state and local law enforcement to support cyber-crime investigations. Additionally, ICE is proudly supporting the Digital Economy Task Force spearheaded by the International Center for Missing and Exploited Children. The mission of the Digital Economy Task Force is to foster a balanced solution to the digital economy where people can enjoy the convenience of the digital currencies while there are controls in place to combat illegal activity, as the Federal Government does with any other form of money. The Digital Economy Task Force strives to achieve the goal of producing and releasing an official report in February 2014 to inform individuals and lawmakers globally about the current state of the digital economy. In addition, the task force intends to explore the inherent opportunities and risks associated with an increasingly digital economy and its impact on human rights, regulation, crime, and law enforcement.

Virtual currency systems have a global reach and clientele. Investigations into illicit virtual currency activities often require considerable cooperation from international partners.

ICE attachés work with international organizations and foreign law enforcement counterparts to build capacity, strengthen relationships, and conduct joint enforcement activities to ultimately disrupt and dismantle TOCs. As part of these efforts, ICE maintains nine vetted units worldwide that are composed of highly-trained host country counterparts that have the authority to investigate and enforce violations of law in their respective country. Since ICE officials who work overseas do not possess law enforcement or investigative authority in host countries, the use of vetted units enables ICE to dismantle, disrupt, and prosecute TOCs while respecting the sovereignty of the host country.

Challenges

The criminal use of virtual currencies challenges the effectiveness of U.S. laws and regulations intended to limit the ability of criminals to profit from their illicit activities and move their criminal proceeds. The key U.S. laws that typically pertain to investigations involving the illicit administration or exchange of virtual currencies include the Bank Secrecy Act of 1970, the Money Laundering Suppression Act of 1994, and Title III of the USA PATRIOT Act of 2001; which are further supported by various associated Federal regulations. The ability of agencies to enforce current laws and regulations to suppress the use of financial systems by criminal enterprises is complicated by the increasingly transnational nature of the criminal organizations and their continued efforts to circumvent these legal controls.

Virtual currencies often support crime that is transnational in nature, thus requiring close international partnership to conduct investigations, make arrests, and seize criminal assets. Fostering these partnerships and conducting these transnational investigations requires continual investment to maintain effective international law enforcement collaborations, and constant efforts to harmonize anti-money laundering laws and regulations. Investigating crimes involving virtual currencies and the transnational organized cyber criminals that use them also requires highly skilled criminal investigators. Hiring, developing, and retaining these special agents is a high priority for DHS, but is challenging in the present fiscal environment. Additionally, while virtual currencies may support the activities of transnational criminals who prey upon Americans, some administrators and exchangers of virtual currencies are based in other countries in an effort to minimize the exposure of individuals to potential arrest and prosecution by U.S. law enforcement officials.

Conclusion

Thank you again for the opportunity to highlight ICE's leading role in combating TOCs and their ability to launder illicit proceeds. ICE recognizes and fully supports the growth of the virtual currency payments as a legitimate financial platform via the Internet. However, as these and other new technologies continue to evolve, ICE will remain vigilant and adapt its investigative tools and techniques to effectively dismantle those criminal organizations that use virtual currencies to hide and launder their illicit proceeds.

Statement for the Record of

Sarah Meiklejohn
Ph.D. Candidate
University of California, San Diego

before the

Committee on Homeland Security and Governmental Affairs
United States Senate

November 18, 2013

Good afternoon, Chairman Carper, Ranking Member Coburn, and Members of the Committee. I appreciate the opportunity to provide a written statement for the record, as I believe the emergence of Bitcoin and other virtual currencies is an important issue. I would like to speak specifically to the perceived anonymity of Bitcoin, and discuss the extent to which Bitcoin participants can be de-anonymized.

Overview of Bitcoin

Bitcoin is, in a nutshell, the first widely-adopted form of electronic cash. As the name suggests, Bitcoin is — unlike other online payment systems such as Paypal — a currency, and as such its value is market-based (i.e., based on the price of a bitcoin relative to the price of an existing fiat currency such as the US dollar). At the time of writing this statement, Bitcoin is trading at over $350 per bitcoin: the highest it has traded since its introduction in January 2009.

To understand the potential promises and risks of Bitcoin, it is useful to first gain some understanding of how Bitcoin works. Bitcoin transactions are created and broadcast throughout a global peer-to-peer network, which acts as a decentralized accounting mechanism for all transactions. In almost all other current forms of electronic payment, money is debited from or credited to participants by some financial institution that maintains a central ledger. In Bitcoin, this ledger is decentralized, and it is thus this peer-to-peer network that is responsible for bearing witness to these transactions.

This decentralized architecture means that no central entity acts to validate Bitcoin transactions or enforce certain behavior. Instead, Bitcoin uses cryptography to ensure correct behavior in two crucial ways: to control the supply of bitcoins and to ensure the anonymity of its participants. For the former, Bitcoin requires that its users solve a computationally difficult problem in order to generate new bitcoins. While the supply of commodities like gold is thus limited by the size of known physical reserves, the supply of bitcoins is instead limited by the computational power required to solve the cryptographic problem. As the computational power of the network increases, the difficulty of the problem increases as well, so that new bitcoins are — by design — produced only every ten minutes. Counterfeiting bitcoins requires the same sizable effort, and stealing bitcoins — assuming the thief tries to do so cryptographically, rather than simply stealing the owner's secret information — requires exponentially more effort.

Another consequence of Bitcoin's decentralized nature is that no central entity knows the real-world identity of every Bitcoin participant. Instead, users are identified by pseudonyms that cryptographically reveal no information about their owner. Thus, while every Bitcoin transaction is globally visible (as each participant is responsible for bearing witness to the movement of bitcoins), these transactions inherently reveal no information about their real-world participants. Furthermore, Bitcoin users can operate arbitrarily many of these pseudonyms (with no additional cost), and their activities using different sets of pseudonyms are largely unlinked. The use of pseudonyms, coupled with the ability of each user to control many pseudonyms, is the main mechanism by which Bitcoin achieves anonymity.

Anonymity in Bitcoin

Despite the potential for anonymity that Bitcoin provides, the fact that every Bitcoin transaction is globally visible leaves Bitcoin open to two forms of de-anonymization that we have performed: algorithmic tools that link together pseudonyms according to evidence of shared ownership, and a "re-identification" attack that unmasks the real-world owner of pseudonyms.

This analysis is most effective when applied to Bitcoin services, rather than to individual users. Recently, Bitcoin has seen a large rise in the number of services that are supported, such as currency exchanges, "wallet services" (i.e., Bitcoin banks), vendors such as Wordpress accepting Bitcoin for payment, and infamous Tor-based drug marketplaces such as Silk Road. Many Bitcoin participants now use these services, as they provide two key advantages over maintaining an individual Bitcoin client: transaction speed and usability.

Combining re-identification attacks on these services with simple algorithms for linking together the many pseudonyms they operate, it is possible to identify the behavior of these large services throughout the Bitcoin network; i.e., in a given Bitcoin transaction, it is possible to identify whether the sender or recipient is one of these services. It is more difficult to perform this analysis on individuals, however, because the re-identification attack relies on the ability to engage in transactions with the entity. While Bitcoin services are by design open to interaction with any user, individuals may be significantly more cautious about whom they transact with.

Nevertheless, identifying the activity of Bitcoin services has an impact on the anonymity of any user who transacts with these services. In particular, Bitcoin exchanges know the real-world identity of every user that holds an account with them, as these exchanges are responsible for performing, e.g., wire transfers to and from the user's bank account. Using the ability to watch individuals deposit bitcoins into these exchanges, an agency could thus track illicitly-obtained bitcoins (obtained, for example, from the sale of drugs or theft) to their point of deposit into an exchange, and then — using subpoena power — learn the real-world owner of the account from the exchange.

Implications

We have had several opportunities to apply this analysis in practice.

First, we were able to identify the transactions made by a reporter at Forbes, who had made small purchases at each of three Bitcoin- and Tor-based drug sites (Silk Road, Atlantis, and Black Market Reloaded, all no longer active). Given the list of his addresses at the Bitcoin exchange Coinbase — the data we hypothesized could be obtained by an agency with subpoena power — we were able to identify his deposits into and withdrawals from all three of the sites. For Atlantis and Black Market Reloaded, this required additional manual inspection of the transaction ledger, but for Silk Road this required only the data our analysis had already provided, so no additional work was needed.

Second, we were able to identify over 300 Bitcoin addresses belonging to Cryptolocker, which is a popular form of ransomware that encrypts a victim's hard drive and provides him with the decryption key only after he has paid them $300 in either bitcoins or MoneyPak. By applying

our analysis to these addresses, we were able to identify several deposits into BTC-e, a Bitcoin exchange based in Russia. This indicates that the perpetrator likely cashed out into fiat currency.

Third, we were also able to see, on a broad scale, how many bitcoins each service was handling at any given time; i.e., in a given time frame, how many bitcoins were deposited into and withdrawn out of a Bitcoin service. For example, media outlets such as *The New York Times* reported that Silk Road transactions accounted for half of all transactions (or, similarly, that half of all bitcoins had passed through Silk Road). Our analysis indicates that this is simply not the case: in both June and July 2013, we observed that only 5% of all transactions involved Silk Road; i.e., were either deposits to or withdrawals from the service, and that the percentage of total bitcoins transacted was comparable.

Limitations

While our analysis provides a powerful tool for identifying certain types of Bitcoin activity (and thus potentially regulating aspects of it), this is of course a preliminary analysis and there are a range of transaction types that cannot be traced in the manner described.

First, our algorithms link together only a subset of the pseudonyms that a Bitcoin entity operates. This means that we underestimate — by an unknown amount — the traffic of a service; for example, we cannot identify every single deposit into and withdrawal from exchanges.

Second, our re-identification attack must be continually applied in order to identify new and evolving services. To identify the pseudonyms of any new service, it is thus necessary to engage in transactions with this service, and even for old services — that commonly switch between different sets of pseudonyms — intermittent transactions with such services are necessary as well.

While a highly motivated and sophisticated user could therefore hide their transactions in a way that would currently be impossible for us to trace, such obfuscation becomes ever more difficult for larger sums of bitcoins.

Conclusions

Our analysis provides a way to track suspicious activity in the Bitcoin network. If an agency with subpoena power can track this suspicious activity to an exchange — or any other entity that knows the real-world identity of its users — then it has the potential to learn the owner of the pseudonyms involved, and thus the real-world identity of the criminal.

Post-Hearing Questions for the Record
Submitted to Jennifer Shasky Calvery
From Senator Thomas R. Carper
"Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies"
November 18, 2013

1. As the Director of the Financial Crimes Enforcement Network, your job is to keep the U.S. financial system safe from illicit use. I'm told that there is little in the way of reliable estimates about the size of the virtual currency market.

    a. Do you see virtual currency being used in a large scale manner to conduct illegal activity? Can you compare illegal activity using virtual currency to illegal activity using traditional financial instruments?

The most significant example of illegal use of a virtual currency was identified in the U.S. government's indictment and proposed special measures against Liberty Reserve, which alleges it was involved in laundering more than $6 billion. The Department of Justice has also alleged that customers of Silk Road, the largest narcotic and contraband marketplace on the Internet to date, were required to pay in Bitcoins to enable both the operator of Silk Road and its sellers to evade detection and launder hundreds of millions of dollars. In terms of how this activity compares with traditional payment methods, in the case of Bitcoin, it has been publicly reported that its users processed transactions worth approximately $8 billion over the twelve-month period preceding October 2013; however, this measure may be artificially high due to the extensive use of automated layering in many Bitcoin transactions. By way of comparison, according to the United Nations Office on Drugs and Crime, the best estimate for the amount of all global criminal proceeds available for laundering through the financial system in 2009 was $1.6 trillion. Yet in 2012 alone, Bank of America processed $244.4 trillion in wire transfers; PayPal processed approximately $145 billion in online payments; Western Union made remittances totaling approximately $81 billion; and the Automated Clearing House Network processed more than 21 billion transactions with a total dollar value of $36.9 trillion. All of this illustrates that, while of growing concern, to date, virtual currencies have yet to overtake more traditional methods to move funds, whether for legitimate or criminal purposes.

    b. Are you seeing virtual currency being used in large scale to fund terrorism, launder money, or to further organized crime? Do you believe we will start to see that sort of thing?

While we recognize the possibility that virtual currencies could be used to fund acts of terrorism, do not believe that virtual currencies have replaced the channels that terrorist organizations have historically used. With respect to laundering money, as stated before, Liberty Reserve is alleged to have laundered more than $6 billion of illicit proceeds before the U.S. government took steps to shut down its operations. Looking ahead, we certainly appreciate the potential vulnerabilities created whenever any new payment method is introduced to the U.S. financial system. This is why FinCEN continues to work hard to identify the latest emerging trends and typologies in

order to stay one step ahead of criminal organizations that might see an opportunity to exploit virtual currencies for illegal purposes.

c. Are there other virtual currencies that regulators and policymakers should be paying attention to? How do they differ from bitcoin and to what extent do they address potential limitations with bitcoin?

As discussed in my written testimony, FinCEN has focused on two types of convertible virtual currencies: centralized and decentralized. Centralized virtual currencies, like Liberty Reserve, have a centralized repository and a single administrator. Decentralized virtual currencies, such as Bitcoin, have no central repository and no single administrator to maintain information on users and report suspicious activity to government authorities. Instead, value is electronically transmitted between parties without an intermediary. There are numerous types of both centralized and decentralized convertible virtual currencies, with more being introduced all the time. Decentralized convertible virtual currencies are typically cryptocurrencies, which rely on cryptographic software protocols to generate the currency and validate transactions. Bitcoin is the best known of these, and by some measures it is the most successful, in that it is widely accepted as a medium of exchange and a store of value. But FinCEN is monitoring the growth, acceptance and development potential of other convertible virtual currencies as well.

2. FinCEN issued guidance that says that users of virtual currencies are not money service businesses, but that administrators and exchangers of the currency are money transmitters and must register as money services businesses and become licensed.

a. What prompted FinCEN to issue this guidance this past March?

FinCEN always strives to ensure regulated industries under our purview are fully apprised of their obligations pursuant to anti-money laundering (AML) compliance, and that they apply those requirements appropriately. To that end, on March 18, 2013 FinCEN published guidance that further explains the application of FinCEN's money services business (MSB) regulations with respect to persons creating, obtaining, distributing, exchanging, accepting, or transmitting virtual currencies. The guidance clarifies definitions and expectations to ensure that businesses engaged in such activities are aware of their regulatory responsibilities. The guidance also explains that those persons who obtain convertible virtual currency and use it to purchase real or virtual goods or services is not an MSB and therefore not subject to regulatory requirements under the Bank Secrecy Act (BSA).

b. Did FinCEN engage with the Commodity Futures Trading Commission, the Securities and Exchange Commission, other relative regulatory agencies, and interested stakeholders when crafting its guidance?

FinCEN consulted with several regulatory and law enforcement agencies while preparing the guidance. In addition to the Securities and Exchange Commission and the Commodity Futures Trading Commission, these included the Federal Deposit Insurance Corporation (FDIC), the Office of the Comptroller of the Currency, the Internal Revenue Service, the Federal Reserve,

the National Credit Union Administration, the Consumer Financial Protection Bureau (CFPB), the Federal Bureau of Investigation (FBI), the United States Secret Service, the Drug Enforcement Administration, and U.S. Immigration and Customs Enforcement.

c. To date, how many virtual currency exchanges have registered with FinCEN? How many would you say are fully compliant now? Are there mechanisms in place to identify noncompliant exchanges and bring them into compliance?

As of December 2013, approximately 40 virtual currency exchangers obligated to register with FinCEN have done so. FinCEN is also in the process of conducting direct outreach to virtual currency exchangers that have a domestic presence. We have sent an initial series of letters to the entities outlining the appropriate BSA requirements and referencing the March 2013 interpretative guidance. The letter also instructs the entities on the process for registering with FinCEN, or for contacting FinCEN if they believe they are not required to register. FinCEN will continue to monitor the registration list to identify which entities have yet to register despite direct and specific instructions regarding their obligation to do so, and will take appropriate action with those who, despite our outreach, remain noncompliant.

3. The New York State Department of Financial Services recently issued a notice that they may begin issuing "BitLicenses" for certain Bitcoin related businesses. What do you know about these "BitLicenses" and to what extent is FinCEN working with New York or other states to inform and coordinate the state-level money service business licensing process?

While we require virtual currency exchangers to register with FinCEN as a class of money services businesses, it remains the prerogative of the individual states to establish a licensing regime for virtual currency businesses operating within their jurisdiction. Such is the case with the state of New York's recent announcement that its Department of Financial Services may soon require licenses for Bitcoin-specific enterprises. Although FinCEN does not opine on the efficacy of an individual state's decision to apply licensing standards on financial services entities, we do closely coordinate with our state regulatory counterparts to encourage appropriate application of FinCEN guidance as part of the states' separate AML compliance oversight of financial institutions. We communicate with our state counterparts directly, through the Conference of State Bank Supervisors, and through official, FinCEN-led initiatives such as the Bank Secrecy Act Advisory Group.

4. Many working groups, from the Terrorist Finance Working Group, to the Virtual Currency Emerging Threats Working Group, have been convened by or among government agencies that have authorities in the virtual currency space.

a. What inter-agency working groups is your agency participating in?

As mentioned in my written testimony, FinCEN participates in the Federal Financial Institutions Examination Council BSA Working Group to review and discuss FinCEN's regulations and guidance, and the most recent and relevant trends in virtual currencies. FinCEN also participates

in the FBI-led Virtual Currency Emerging Threats Working Group; the State Department-led Terrorist Finance Working Group and its subgroup on New Payment Methods; the FDIC-led Cyber Fraud Working Group; the Treasury-led Cyber Working Group; and, with a community of other financial intelligence units. Through all of these working groups we discuss current trends, and provide information on FinCEN resources and authorities as we work with our partners in an effort to foster an open line of communication across the government regarding bad actors involved in virtual currency and cyber-related crime.

b. If you are involved in more than one working group do you think these different working groups are all doing the same thing, or is each tackling a different problem? Is this the most effective way to handle this issue?

When it comes to a complex topic like virtual currency, there is no one-size-fits-all approach to examining the issue at the working group level. Rather, the most effective way to identify and correct vulnerabilities in our nation's regulatory and law enforcement framework is to ensure you have the most capable and adept agencies coming together and sharing their expertise with one another. The various working groups studying virtual currencies all approach the topic from different perspective, which brings together a diversity of mandates, skill sets, and perspectives on the subject matter. This approach positively challenges opinions and informs the outcome of each working group's findings and deliverables.

c. Keeping in mind that every agency tackling this issue has a different stake in it, do you think there should be a lead entity "steering the ship" and making sure all of the angles are covered?

The issue of virtual currency itself is an Administration priority, and through the Administration, stakeholders already receive the necessary guidance and direction to ensure all relevant Departments and Agencies are maximizing their abilities and resources to safeguard the U.S. financial system from real or perceived threats and vulnerabilities borne out by this emerging payment method.

5. Two recent cases of fraud using Bitcoins raise concerns related to consumer protection. In one case, the SEC alleges that Bitcoin Savings and Trust was engaged in a Ponzi scheme, promising investors 7 percent weekly, when it had no way of paying back the investors. In another recent case, hackers stole about $ 1 million worth of Bitcoins from an online payment processor, placing many consumers at risk of losing funds they had with this processor. What if anything, could law enforcement and regulatory agencies do to address consumer protection issues related to virtual currencies and their networks? Which agencies do you believe should play a role in consumer protection issues related to bitcoins?

This question goes to the heart of why it is so important for the various working groups studying the impact of virtual currency to continue to include a broad array of Federal Agencies with different equities in the topic. As mentioned earlier, part of the consultation process for our March 2013 guidance included soliciting the views and perspectives of the CFPB given the

extremely valuable role it plays in this space. Likewise, the federal banking regulators have consumer protection regulations in place to safeguard their customers from fraudulent activity. Including this specific element of expertise into the broader discussion means law enforcement, in turn, is able to learn from these agencies about what types of red flag indicators are emerging, which greatly informs their investigative processes.

U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

March 10, 2014

The Honorable Thomas R. Carper
Chairman
Committee on Homeland Security and Governmental Affairs
United States Senate
Washington, D.C. 20510

Dear Mr. Chairman:

Enclosed please find responses to questions for the record arising from the appearance of Mythili Raman, Acting Assistant Attorney General of the Criminal Division, before the Committee on November 18, 2013, at a hearing entitled "Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies." We hope that this information is of assistance to the Committee.

Please do not hesitate to contact this office if we may be of additional assistance regarding this or any other matter. The Office of Management and Budget has advised us that there is no objection to submission of this letter from the perspective of the Administration's program.

Sincerely,

Peter J. Kadzik
Principal Deputy Assistant Attorney General

Enclosure

cc: The Honorable Tom Coburn
Ranking Member

Questions for the Record
Mythili Raman
Acting Assistant Attorney General
Criminal Division
U.S. Department of Justice

Committee on Homeland Security and Governmental Affairs
United States Senate
"Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies"
November 18, 2013

Questions Posed by Senator Thomas R. Carper

1. From your perspective, which features of virtual currencies increase crime risks?

Certain features of any payment system, including virtual currency systems, may attract illicit users and make it more difficult for law enforcement authorities to investigate criminal activity. Most significantly, criminals are drawn to virtual currency services that they believe will afford them a greater level of anonymity than would otherwise be possible through the traditional banking or financial system. Virtual currency systems may offer such increased anonymity either through technical features of their design or, more simply, if they lack effective anti-money laundering programs. Ineffective anti-money laundering programs are, of course, not unique to virtual currency systems. As with certain financial institutions or payment systems that have weak anti-money laundering programs, criminals are able to exploit the lax anti-money laundering programs of certain virtual currency systems to further their crimes or launder criminal proceeds. In at least some virtual currency cases, such as the Department's Liberty Reserve prosecution, we have alleged that the principals of the systems intentionally allowed criminals to exploit these vulnerabilities.

Decentralized virtual currency systems in particular may be attractive to criminals because they lack an administering authority to collect customer information or receive legal process, and thus make it more difficult for law enforcement authorities to obtain customer records. The lack of a central repository for customer information, and the ability of individuals to conduct transactions using these systems without financial intermediaries, can pose obstacles to our traditional efforts to follow the money.

Additionally, the internationalization of virtual currency transactions can pose significant challenges to the ability of investigators to effectively track the flow of funds. Criminals often exploit differences in national regulatory regimes, and gravitate toward services operating out of countries that have poor regulatory oversight or that are known to be less cooperative with American law enforcement. When investigations involve virtual currency services that allow users to easily move funds across the globe, law enforcement authorities will typically need to rely on more extensive cooperation from their foreign partners. The investigation of Liberty Reserve, for example, involved coordinated steps in 17 different countries. Moreover, in general, the use of legal process to obtain foreign records is often slow, and thus can significantly delay the progress of a criminal investigation.

2. To what extent can the work done by researchers to map Bitcoin addresses to identify users, help law enforcement efforts?

The Department is familiar with efforts by researchers to exploit publicly available information captured in the Bitcoin "blockchain." Due to law enforcement sensitivities, however, we are unable to describe here our evaluation of those efforts and their utility to criminal investigations.

3. Aside from Bitcoin, are there other virtual currencies that have come to the Department's attention for their use to conduct illicit activities? How do they differ from Bitcoin, and to what extent do they address potential limitations with Bitcoin, such as the cost of mining Bitcoins?

A number of centralized virtual currencies, such as eGold and Liberty Reserve, existed long before Bitcoin, and have been used by criminals to fund criminal schemes and launder criminal proceeds. Investigations involving centralized systems present some of the same challenges as those involving decentralized systems, including greater customer anonymity, as described in the response to Question 1 above. Unlike decentralized systems, however, centralized systems have a single administrator that can collect customer information and receive legal process, which, assuming the system is legitimate and located in a cooperative jurisdiction, may mitigate some of the obstacles that law enforcement would otherwise encounter in tracking virtual currency transactions. But as seen in our prosecutions of eGold and Liberty Reserve, significant criminal activity can occur, and has occurred, through these centralized virtual currency systems as well.

Various virtual currencies have claimed to improve upon Bitcoin by offering such features as faster transaction times, the absence of a hard limit on the amount of available currency, predetermined inflation rates, and lower energy consumption from computer processing. Although the Department continually works to ensure that we have a complete understanding of the workings of virtual currency systems, we generally focus on features and vulnerabilities that malicious users may seek to exploit, rather than on the overall benefits of one system over another. That said, the Department continues to monitor all types of emerging virtual currencies insofar as those currencies are connected to illicit activity.

4. We know virtual currency has been used for the sale of child pornography, ammunition, weapons, and other illicit activity. We also know that law enforcement is obviously on the lookout for the use of virtual currencies in other illegal markets. Are you seeing virtual currency being used in large scale to fund terrorism, launder money, or to further organized crime? Do you think we will start to see that sort of thing?

The Department is seeing an increasingly broad range of criminals using virtual currency, and we expect this trend to continue. Moreover, generally speaking, terrorists are known to adopt money laundering techniques that have been successfully employed in other criminal schemes and we thus intend to remain vigilant about any use of virtual currency systems by terrorists. Additionally, though few decentralized virtual currency systems currently exist that

could easily accommodate large-scale money transfers, the systems' capacities are growing rapidly, which could lead to their use by larger-scale money laundering enterprises.

5. Many working groups, from the Terrorist Finance Working Group, to the Virtual Currency Emerging Threats Working Group, have been convened by or among government agencies that have authorities in the virtual currency space.

a. What inter-agency working groups is your agency participating in?

The Department is involved in two working groups that are specifically focused on emerging payment systems: the Virtual Currency Emerging Threats Working Group and the Terrorist Finance Working Group's (TFWG) Ad Hoc Working Group on New Payment Systems. Additional working groups in which the Department participates, notably the Bank Fraud Working Group and the Payments Fraud Working Group (which is a subset of the Bank Fraud Working Group), have received presentations and/or information regarding virtual currencies.

b. If you are involved in more than one working group do you think these different working groups are all doing the same thing, or is each tackling a different problem? Is this the most effective way to handle this issue?

Although there is some overlap in the agency representation in and missions of these groups, these working groups have different focuses, objectives, and memberships. For example, the Bank Fraud Working Group includes representatives from the federal banking authorities, as well as the Financial Crimes Enforcement Network (FinCEN), the Securities and Exchange Commission, the Commodity Futures Trading Commission, and various federal law enforcement agencies. The Bank Fraud Working Group deals with a wide array of issues and has sought to educate and inform its members about virtual currency within the context of its larger mission of combating the fraudulent exploitation of the formal financial sector in the United States. The Payments Fraud Working Group mirrors this approach, with virtual currency an ancillary, but relevant, topic of discussion.

Moreover, even the two groups that are more directly focused on virtual currency have different missions and focuses. While the Virtual Currency Emerging Threats Working Group specifically addresses virtual currency and furthers efforts to counter the illicit use of virtual currency, the TFWG Ad Hoc Working Group on New Payments Systems approaches the issue from the context of advancing the overall TFWG mission to coordinate assistance and capacity building support to the key partner states that are most at risk with respect to terrorist financing.

While there is substantial value in having a specific working group focusing almost exclusively on virtual currency issues, other working groups also add value by developing and contributing information about the use and misuse of virtual currencies within their areas of focus and by facilitating discussion among all relevant agencies. The Department has found this collaborative approach to be effective in promoting cooperation among agencies and in ensuring the formulation of consistent policies by relevant government entities.

c. **Keeping in mind that every agency tackling this issue has a different stake in it, do you think there should be a lead entity "steering the ship" and making sure all of the angles are covered?**

Virtual currency functions as a medium of exchange, a unit of account, and/or a store of value. No single department or agency has jurisdiction to regulate all aspects of the offering, sale, or exchange of virtual currencies or to direct agencies with regulatory authority to adopt particular rules or enforcement policies with regard to virtual currencies. We have found that the most effective approach has been to facilitate coordination among regulatory and enforcement agencies to ensure the most cohesive government response to the illicit use of virtual currencies.

6. **The Department of Justice has the responsibility of prosecuting cases in which individuals and companies violate the law with regard to registration. As we see virtual currencies used in Ponzi schemes, in money laundering cases, and in unlicensed money service businesses, the Department will be standing in court dealing with these issues. What is the Department of Justice doing to ensure policies are being consistently developed and applied in virtual currencies?**

Under the Bank Secrecy Act (BSA), exchangers and administrators of convertible virtual currency, whether centralized or decentralized, operate as money transmitters, which are part of a larger class of institutions called money services businesses. Pursuant to 31 U.S.C. § 5330, money transmitters are required to register with FinCEN. In addition, most states require money transmitters to obtain a state license in order to conduct business in that state. If a money transmitter fails to register with FinCEN or obtain the requisite state licensing, it may be subject to criminal prosecution under 18 U.S.C. § 1960. The Department has successfully used this authority against virtual currency businesses in the past and will continue to do so in appropriate cases. Moreover, the Department has conducted outreach to federal prosecutors and law enforcement on virtual currency issues to ensure that relevant policies and authorities are consistently applied nationwide.

In general, the Department believes that current money laundering and forfeiture authorities provide sufficient flexibility to enable federal law enforcement to investigate and prosecute cases involving virtual currencies. That said, in order to keep pace with evolving threats posed by virtual currencies and other new financial services, the Department will continue to assess whether existing authorities should be amended or new authorities are needed.

7. **Two recent cases of fraud using Bitcoins raise concerns related to consumer protection. In one case, the SEC alleges that Bitcoin Savings and Trust was engaged in a Ponzi scheme, promising investors 7 percent weekly, when it had no way of paying back the investors. In another recent case, hackers stole about $1 million worth of Bitcoins from an online payment processor, placing many consumers at risk of losing funds they had with this processor. What, if anything, could law enforcement do to address consumer protection issues related to virtual currencies and their networks?**

The two examples in the question reflect very different types of fraud risks for consumers. The Department of Justice works closely with other federal agencies that engage in substantial consumer education and fraud prevention messaging in relation to online fraud, such as the Federal Trade Commission, the Consumer Financial Protection Bureau, and the Internet Crime Complaint Center. In addition, through interagency working groups such as the Bank Fraud Working Group, the Identity Theft Working Group, and the International Mass-Marketing Fraud Working Group, the Department and other agencies can discuss appropriate coordinated responses to use of virtual currencies in committing fraud. With regard to hacking, the Department vigorously investigates and prosecutes hacking crimes involving fraud or theft of money and other valuable data.

8. The FBI recently arrested the owner of the website Silk Road, which used Tor software to allow users to purchase illicit drugs and other illegal goods in an anonymous fashion with virtual currency. Recently there have been reports that similar sites are being developed. What lessons can be learned about virtual currencies and the use of software that allows users to visit websites anonymously that could help identify pertinent information for law enforcement?

First, as the use of virtual currencies like Bitcoin and anonymization tools like Tor grow, we anticipate that criminal use of these technologies may also increase. Law enforcement is committed to responding by ensuring that we have the right personnel and tools to investigate crimes committed through the use of virtual currency systems, Tor, or other similar technologies.

Second, as the question implies, there are different kinds of virtual currencies and Internet anonymization technologies, each of which can pose its own set of challenges to investigators. Law enforcement agencies are committed to staying current on all players and developments in this dynamic and innovative area to support investigations. This means not only fully understanding the various virtual currencies and anonymization technologies that exist, but also tracking improvements and modifications that are periodically made to them.

Secret Service Response to the
Post-Hearing Questions for the Record
Submitted to Edward W. Lowery III
From Senator Thomas R. Carper

"Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies"
November 18, 2013

1.) From your perspective, which features of virtual currencies increase crime risks?

Digital currencies, as a specific subset of virtual currencies that operate online, provide a useful tool for cybercriminals to launder and move illicit funds transnationally and avoid controls which exist in the traditional financial system. Examples of key features of digital currencies that increase crime risks include: anonymity of both users and transactions; transnational reach; low transaction costs; limited record keeping; limited or no verification of account holder identity; ability to open multiple accounts using multiple bogus identities; ability to control accounts over the Internet through anonymous proxies; ability to use (sometimes collusive) exchangers scattered throughout the globe to obscure money flows in and out of digital currency accounts; widespread acceptance of digital currency as a means of conducting transactions in the criminal underground; and a record of not cooperating with law enforcement investigations. Currently available digital currencies provide these identified features in varying extents and accordingly attract differing level of use for criminal activities.

2.) To what extent can the work done by researchers to map Bitcoin addresses to identify users, help law enforcement efforts?

The public ledger feature of the Bitcoin block chain differentiates Bitcoin, and other decentralized digital currencies, from many of the centralized digital currencies, such as e-gold and Liberty Reserve. The block chain makes it harder for criminals to hide their illicit activity. The work of researchers to link known transactions to individual identities reduces the attractiveness of Bitcoin for criminal activities. This research also provides an additional tool for law enforcement to identify illicit transactions, assets, and the individuals associated with this activity in support of apprehension, asset forfeiture, and prosecution.

3.) Aside from Bitcoin, are there other virtual currencies that have come to the Department's attention for their use to conduct illicit activities? How do they differ from Bitcoin, and to what extent do they address potential limitations with Bitcoin, such as the cost of mining Bitcoins?

There are numerous digital currencies in existence, and like any financial transaction system they have likely been used, to some extent, by criminals to conduct illicit activities. Established in 1996, e-gold Inc. is generally considered the first digital currency to gain a large user base.

Unlike Bitcoin, e-gold provided a gold-backed, centralized, non-cryptographic, digital currency and a web-based application programming interface (API) to support e-commerce transactions. As it quickly grew in popularity, similar gold-backed digital currencies were created, such as Goldmoney.com, e-Bullion.com, CrowneGold.com, Pecunix.com, INTgold.com, all of which could also be exploited by criminals, in addition to Ponzi schemes like OSgold.com. Operating as an unlicensed money transmitter, e-gold grew to be a major facilitator of criminal activity and was eventually shut down as a result of a Secret Service led joint investigation.

In coordination with IRS-CI and ICE/HSI as a part of the Global Illicit Financial Team (GIFT), the Secret Service investigated, and ultimately shut down, Liberty Reserve – a centralized digital currency based in Costa Rica. The alleged principle founder of Liberty Reserve moved to Costa Rica to operate Liberty Reserve after being convicted in the United States in December 2006 for operating "Gold Age, Inc."[1] as an unlicensed money transmitting business and one of the first exchangers of e-gold. Liberty Reserve allegedly provided money laundering services to support transnational organized cyber crime. According to the Department of Justice, this is the largest money laundering case ever prosecuted in the United States. Liberty Reserve also allegedly operated as a centralized, non-cryptographic, digital currency that only required a name, e-mail address, and birth date to register and transfer funds. The indictment of Liberty Reserve alleges it did not follow basic know your customer standards in validating identity information, and that apparent criminal monikers such as "Russia Hackers" and "Hacker account" were used to establish accounts under false names.

There are numerous other centralized digital currencies in operation today, which also could be exploited by criminals, including WebMoney, Perfect Money, Paymer, cashU, and Ripple. Some also consider online payment systems such as PayPal and credit cards as a form of *"soft digital currency"* (in that they allow transactions to be reversed). Additionally, currencies used in online games or virtual environments, such as Linden Dollars in Second Life, Gold in World of Warcraft, and ISK in EVE Online, are used to conduct transactions outside of the virtual environment through either official or unofficial third party exchangers. All such systems can be used to conduct illicit activities, including money laundering, to varying extents. However, all of these systems differ from Bitcoin in that they operate as centralized digital currencies, and as such services based on these centralized digital currencies depend on the continued operation and cooperation of the digital currency provider or administrator.

Bitcoin, as described by its pseudonymous developer(s), "Satoshi Nakamoto" in their October 2008 paper "Bitcoin: A Peer-to-Peer Electronic Cash System," was designed to eliminate the requirement for a digital currency provider or administrator to act as a third party to financial transactions, by creating a decentralized cryptographic system to conduct transactions. To incentivize participation in this system and introduce currency, Bitcoin is designed to provide new bitcoins to the owners of computers that contribute to validating transactions—a process known as mining. Bitcoin began operation in January 2009 and is the first known decentralized cryptographic to enter widespread use. Since its creation, numerous other decentralized digital

[1] Secret Service investigated GoldAge in 2001 as part of a credit card fraud investigation. The founder of GoldAge sold it to new owners in 2002. GoldAge was ultimately shutdown following a New York State Indictment in 2006.

currencies have been created as variants of the Bitcoin design, including, among others, LiteCoin, Peercoin, and Namecoin. The Secret Service is not aware of a way to operate a decentralized cryptographic digital currency without the need for participants in the network to validate transactions, the process known as "mining."

4.) We know virtual currency has been used for the sale of child pornography, ammunition, weapons, and other illicit activity. We also know that law enforcement is obviously on the lookout for the use of virtual currencies in other illegal markets. Are you seeing virtual currency being used in large scale to fund terrorism, launder money, or to further organized crime? Do you think we will start to see that sort of thing?

Although digital currencies have the potential to support more efficient and transparent global commerce, they are particularly well-suited for supporting crime that is transnational in nature. They provide an efficient means of moving large sums of money globally for both legitimate and criminal purposes. Over the past decade, the Secret Service and its partners have observed extensive use of digital currencies to launder money and support the operations of transnational organized cyber crime. Digital currencies are also reportedly being used to solicit the assassination of political leaders and in other murder for hire schemes.

As the use of digital currencies continue to grow, so too will their use for large scale illicit activities. Consequently, it is essential for law enforcement to maintain close domestic and international partnerships in order to conduct investigations, make arrests, and seize criminal assets. Fostering these partnerships and conducting these transnational investigations requires continual investment to maintain effective international law enforcement collaborations, and constant efforts to harmonize anti-money laundering laws and regulations. The recent coordinated regulatory and criminal enforcement against Liberty Reserve, which has been described as the largest money laundering case ever prosecuted in the United States, is an excellent example of what can be accomplished through effective partnerships. The Secret Service will continue to use its investigative assets, in cooperation with FinCEN and other key partners, to suppress the illicit use of digital currencies.

5.) Many working groups, from the Terrorist Finance Working Group, to the Virtual Currency Emerging Threats Working Group, have been convened by or among government agencies that have authorities in the virtual currency space.

a. **What inter-agency working groups is your agency participating in?**

   The Secret Service participates in the Virtual Currency Threats Working Group in addition to other inter-agency efforts that addresses challenges posed by digital currencies. Most notable among these, is the work by the Department of Treasury through FinCEN and the Department of Justice through their Asset Forfeiture and Money Laundering section and Computer Crimes and Intellectual Property section.

b. **If you are involved in more than one working group do you think these different working groups are all doing the same thing, or is each tackling a different problem? Is this the most effective way to handle this issue?**

Digital currencies present challenges and opportunities that affect many federal agencies in the execution of their assigned responsibilities. The working groups on digital currencies the Secret Service participate in are addressing different issues presented by the illicit uses of digital currencies. In the Secret Service's experience, working groups narrowly focused on particular aspects or challenges posed by digital currencies are most effective, whereas large international multi-agency working groups tend to be less efficient.

c. **Keeping in mind that every agency tackling this issue has a different stake in it, do you think there should be a lead entity "steering the ship" and making sure all of the angles are covered?**

Digital currencies present a wide variety of challenges. These issues are likely best addressed by a variety of agencies working in collaboration with key partners as appropriate. For federal law enforcement issues concerning digital currencies, the U.S. Department of Justice's Criminal Division provides important guidance for investigations and prosecutions involving digital currencies. Similarly, the U.S. Department of Treasury's FinCEN provides an important role in leading regulatory and enforcement efforts in regards to the financial system. In conducting criminal investigations and assisting state and local law enforcement, the Secret Service operates Electronic Crimes Task Forces which provide common resources for investigating crimes involving computers, like digital currencies. Each of these entities, among others, plays an important role in addressing the challenges posed by digital currencies for criminal investigations. The breadth of potential issues regarding digital currencies is likely too broad to be efficiently managed and steered by a single lead federal agency.

6.) Two recent cases of fraud using Bitcoins raise concerns related to consumer protection. In one case, the SEC alleges that Bitcoin Savings and Trust was engaged in a Ponzi scheme, promising investors 7 percent weekly, when it had no way of paying back the investors. In another recent case, hackers stole about $ 1 million worth of Bitcoins from an online payment processor, placing many consumers at risk of losing funds they had with this processor. What if anything, could law enforcement do to address consumer protection issues related to virtual currencies and their networks?

Protecting consumers from criminal activity, including frauds involving digital currencies, is a primary purpose of federal law enforcement. Law enforcement accomplishes this objective by identifying, investigating, ending such ponzi schemes, seizing their illicit assets, and supporting prosecution to punish those criminally responsible to deter others from engaging in such fraudulent activity. Law enforcement also informs the public of current criminal activity, so they can make informed risk decisions.

In accordance with its statutory authorities,[2] the Secret Service prioritizes its criminal investigations to focus on high consequence illicit activity related to federally insured financial institutions. Through the Secret Service's network of 33 Electronic Crimes Task Forces (ECTFs), the Secret Service conducts its investigations involving information technology in close partnership with the private sector, academia, and state, local, and international law enforcement agencies. Through our partnerships we work to inform the public of the risks posed by criminal exploitation of new technologies, so they can make informed risk management decisions and protect themselves from cyber crime.

However, the primary means by which law enforcement protects consumers is investigating and arresting criminals that engage in fraudulent activities to prevent, deter, and suppress these sorts of illicit activities. Over the past four years, Secret Service cyber crime investigations have resulted in over 4,900 arrests, totaling over $1.3 billion in fraud losses and potential losses of over $13 billion.

[2] See *Powers, authorities, and duties of United States Secret Service* 18 U.S.C. 3056 (b)(3).

Post-Hearing Questions for the Record
Submitted to Ernie Allen, President & CEO
International Centre for Missing & Exploited Children
From Senator Thomas R. Carper

1. **Overall, how would you assess the federal government's activities thus far regarding virtual currencies and in what areas do you believe more work needs to be done?**

Overall, the response of the US federal government has been very good. US recognition of this problem and its response far exceeds the response internationally.

In March 2013 FinCEN acted to apply AML/CFT rules and regulations to virtual currencies at the exchange level. And there are many other examples of ways in which federal government agencies are working together to monitor and combat illegal uses of virtual currencies and payment systems. The Justice Department's National Cyber Investigative Joint Task Force, the Treasury Department's Money Laundering Threat Assessment (MLTA), and the Terrorist Finance Tracking Program (TFTP), are all excellent examples of existing mechanisms that coordinate policy, assess threats and make recommendations including violations associated with illicit activities in using virtual currencies.

However, the lack of definition of virtual currencies makes policy implementation somewhat ambiguous and uncoordinated because no one agency has ownership of the issue. For example, if it was designated as a "currency," then the Treasury Department would have ownership. If it were a "commodity," then the Commodity Futures Trading Commission would have ownership, etc.

Moreover, it creates gaps in coordinating and implementing a comprehensive policy. While it is obvious that the Treasury and Justice Departments play a positive role in enforcement, they are only as effective as existing laws allow which have not necessarily kept pace with technology. Likewise, the FCC, FTC, Department of Commerce (NTIA/ICANN) are not necessarily at the table to regulate use of the virtual currencies over the internet or through mobile devices, because they are also limited by existing laws.

Finally, due to the complexities of virtual currencies, the National Security Council should establish a body to coordinate policies across the US government, but also to ensure that all relevant agencies are included in the discussions.

At a minimum we believe that there is a need for a clear definition of virtual currencies to provide clarity to the Administration on their treatment in the interagency system; that a central body should be established at the National Security Council to coordinate a holistic policy on virtual currencies across the US government; and that the FCC, FTC and Department of Commerce (NTIA) should institute a type of "Know Your Customer Policy" much like the Treasury Department's Anti-Money Laundering standards to help minimize anonymity in virtual currency uses while still protecting privacy.

2. **The virtual currency working group you coordinated was one of the first, if not the first. That said, what sorts of lessons would you offer to your government counterparts who are similarly trying to coordinate policy around this issue?**

When addressing issues and challenges that do not fit traditional models, laws or systems, it is important that we talk to each other and share information. In my judgment the success of our process to date is a direct result of the fact that it is collaborative. Following your hearing, the General Counsel of the Bitcoin Foundation told me that some of his most fervent supporters are uncomfortable with the fact that he is working with me and ICMEC in a quest for solutions. I told him that some of ICMEC's supporters felt the same way regarding our work with him and the Bitcoin Foundation.

My conclusion is that we are where we need to be. Neither of us is using the other. What we are doing is working together to find answers that work. By talking to each other, we each have gained understanding of the larger issues and challenges facing the other. It was clear to him that the future of an innovative virtual currency like Bitcoin is threatened if it is allowed to become defined and identified as the currency of choice for illegal activities including child sexual exploitation. And it was clear to me that while our goal is the elimination of the use of virtual currencies for child exploitation and other criminal activity, at the same time we had to protect Bitcoin's enormous potential for social good, including its use in helping achieve financial inclusion for billions. Thus, we needed to understand each other and work together.

Thus, to our friends and allies in government who have been an integral part of our process from its inception, our message has been that there is a need to develop the broadest possible system for information sharing and collaboration. In addressing a new complex phenomenon like virtual currencies, we must overcome the traditional silos of information and decision-making. We need to approach these issues in a collaborative, consultative manner, and seek solutions that work.

That is why the conference we convened on this issue at the US Institute of Peace on June 13, 2013 in partnership with our friends at Thomson Reuters was titled, "The Virtual Economy: Potential, Perplexities and Promises."

3. Do you think virtual currencies, including Bitcoin, fit into our current legal and regulatory framework? Do you see any gaps in our statutes and regulations regarding virtual currencies? Which agencies do you believe need to be at the forefront of the federal government's work on virtual currencies?

Our Digital Economy Task Force is currently exploring these issues and is moving toward finalizing recommendations, which will be included in our report to be issued in February 2014. Thus, our specific ideas and recommendations are still evolving. Nonetheless, there are some fundamental premises on which we have agreement.

Our view is that regulation should be focused at the exchange level, the point at which virtual currencies are exchanged for fiat currencies, and that there are existing laws and mechanisms in place to effectively achieve such reasonable regulation. However, a consideration of appropriate regulation raises many other questions.

For example, are virtual currency businesses money services businesses (MSBs)? MSBs must comply with the provisions of the Bank Secrecy Act to combat money laundering, terrorist financing and other forms of financial crime.

The FinCEN guidance issued in March 2013 distinguished between three types of participants in virtual currency transactions: users, exchanges and administrators. Users are not deemed to be MSBs and therefore are not subject to the regulatory requirements placed upon MSBs. However, the IRS would deem users to be subject to income tax on any transactions used for real goods and services.

However, exchangers and administrators are deemed in the guidance to be MSBs and subject to its registration, reporting, and recordkeeping requirements. Exchanges are those engaged as a business in the exchange of virtual currency for real currency, funds or other virtual currencies; administrators are those who are engaged as a business in putting virtual currency into circulation and who have the authority to withdraw that currency from circulation. As decentralized currencies have no single administrator the guidance on this point appears to focus on the administrators of centralized currencies, rather than decentralized currencies like Bitcoin.

A second question relates to the treatment of Third Party Payment Processors (TPPPs). These entities process transactions between their clients (traditionally, merchants) and banks with whom the TTTP has a relationship. The nature of this relationship has raised concern due to the potential to obscure the identities of the ultimate customer.

A primary challenge is that the existing regulations were written for more conventional products and services, and are difficult to apply to transactions which are global in scope and technological in nature.

Another question is the applicability of income tax laws to transactions in the digital economy. The IRS has taken the view that transactions conducted in virtual currencies should be treated the same as those in normal currencies if they are used to purchase real goods and services or government issued currency. On that basis, they are subject to federal tax in the same way that mainstream transactions are.

Moreover, a GAO report indicates that mining virtual currencies constitutes taxable income, though the IRS has not made an explicit pronouncement to that effect. Thus, at the federal level the tax implications of mining and transacting business in the digital economy may already be covered.

There are other questions, including the security of accounts holding virtual currencies. There are no minimum security standards required by law. Absent regulatory requirements or self-regulatory standards there is no assurance that businesses will invest adequate resources to provide security for customer funds.

There are also concerns regarding the safety and soundness of businesses holding, transmitting or handling virtual currencies. These businesses are not covered by federal or state insurance and so the closing of one would subject the consumer to the potential loss of some or all of the funds.

Finally, we are examining the larger question of how best to approach regulation. The choices include simple disclosure of risks to consumers and potential consumers; the extension of existing regulatory regimes to cover the digital economy; and the creation of new rules and regulations specifically tailored to digital transactions.

Standard written risk warnings are already required in the securities and commodities industries. This approach is fairly straightforward, though it does create administrative and compliance costs.

Some regulatory issues are already being addressed by extending existing rules to the digital economy. However, the application of rules written for more conventional products and services will require interpretation and entail uncertainty.

The creation of new rules and regulations is costly, time-consuming and difficult. It is also compounded if state and federal regulators do not take a well-coordinated approach in determining new requirements.

This leaves the question of some level of self-regulation, as is utilized to some extent in industries such as securities, commodities, law and medicine. Among the roles that can be played by self-regulation are the drafting and enforcement of rules as well as a code of conduct, enforcement of rules, and standard setting (for instance minimum security standards). If membership is required in order to participate in an industry, self-regulatory organizations can also act as the watchdog to bar from the industry those who engage in egregious violations.

Lastly, the level of jurisdiction of a regulatory regime needs to be considered. Many of the key regulatory questions must be answered at the state level. We must also ask whether regulation of the virtual economy can be effective even at the federal level, given that the virtual economy is international and highly mobile (firms can close their doors and re-open in another country). In the end, solutions must involve international coordination both in terms of drafting comparable regulation and in terms of enforcement, but such an orchestration is likely to take many years to achieve and so addressing issues within the United States first is more prudent than attempting one large globally coordinated regime.

4. Most of the research and media coverage on virtual currencies has focused on Bitcoin.

a. Are there other virtual currencies that we should be paying attention to?

On June 14, 2013 we participated in a meeting on this issue at the World Bank, which included the International Monetary Fund, the European Central Bank, the US Federal Reserve and the US Treasury Department. The representative of the European Central Bank reported that the ECB classifies virtual currencies into three categories:

(a) closed virtual currency schemes with "almost no link to the real economy," and that cannot be traded outside the virtual community (tied to computer games, etc.);

(b) virtual currency schemes with unidirectional flow, purchased using real currency but which cannot be exchanged back (Facebook Credits, Amazon Coins, Nintendo Points, frequent-flyer points, etc.); and

(c) virtual currency schemes with bidirectional flow in which you can buy and sell virtual money and real goods and services. (Bitcoin falls into this third category.)

The ECB has drawn four conclusions based on current information: (1) that at this point virtual currencies do not yet pose a risk to price stability nor can they jeopardize financial stability; (2) that since they are not yet regulated and not closely supervised or overseen by any public authority, they pose a risk for users; (3) that they fall within the realm of central banks' authority as a result of characteristics shared with payment systems; and (4) that they represent "a challenge for authorities, as they might be used by criminals, fraudsters, and money launderers." The ECB committed to monitor developments, set payments security requirements, keep legal frameworks updated and "facilitate a social dialogue."

From the ECB analysis, it is clear that the primary area of interest and concern should be virtual currencies with bidirectional flow, like Bitcoin. Bitcoin is a cryptocurrency, a decentralized digital currency that relies on cryptography. It does not rely on a bank or other central issuing authority. Cryptocurrencies are utilized on peer-to-peer networks.

Currently, all cryptocurrencies are based on Bitcoin. However, Bitcoin is not the only such currency. Alternative digital currencies include Litecoin, Peercoin, Namecoin, Primecoin, Feathercoin, Novacoin, Megacoin, Anoncoin and others. Clearly, innovation will continue in this field and we should anticipate more such alternative currencies in the future. It will be essential that we continually monitor the developments and innovations.

In addition, we should be aware of and concerned about centralized digital currencies which act as payment processors. Costa Rica's Liberty Reserve is a well-known example, a centralized digital currency system which was shut down in 2013 by the US government for allegedly laundering more than $6 billion in illegal funds. Other centralized digital currency systems include Russia/Belize's WebMoney, Panama's PerfectMoney, and others.

Law enforcement reports suggest that digital currencies such as Perfect Money and Web Money are becoming more popular for criminal activities. Russian cybercriminals also accept currencies such as yandex money, liqpay and qiwi.

b. How do they differ from Bitcoin and to what extent are they perhaps more or less troublesome for regulators or law enforcement?

Digital currencies like Liberty Reserve, WebMoney or Perfect Money differ from Bitcoin in that they are centrally controlled and issued. However, they are not overseen by any government, they are controlled by single companies that manage the transfer of units between customers. Companies can choose to accept payment for goods or services in these kinds of digital currencies. However, what makes them particularly vulnerable to misuse and criminal activity is their anonymity. The challenge is to ensure that centralized digital currencies are closely monitored and exercise serious due diligence to minimize the risk of illegal money laundering activity.

Alternative cryptocurrencies like Litecoin differ from Bitcoin primarily in their size and scope. Litecoin is based on the Bitcoin model, but has a higher limit. According to various reports, the total number of coins that can be mined is capped at 21 million Bitcoins and 84 million Litecoins. However, Bitcoins are worth more and are currently accepted more widely.

For regulators and law enforcement, the challenge is to keep up with the pace of innovation. This is not likely to be a static problem. There will be new virtual currencies, new technologies and evolving systems. Our assumption is that it will continue to morph and change.

5. **The point has been made that the way to see Bitcoin and virtual currencies today is a bit like we saw email or the internet itself 20 years ago. At the time, we thought email might replace mail but it was sort of complicated and difficult to work unless you were more technically minded. Obviously as the technology matured it became easier to use and more widely adopted and its changed the way we communicate in fundamental ways. With that said, if you could hazard a guess, what do you see for Bitcoin 20 years from now?**

I believe that Bitcoin and/or its successors will become a central feature of a global effort to achieve genuine financial inclusion for the 2.5 billion adults with no access to banks, credit cards or the financial system. Further, I believe that it will provide an increasingly viable financial alternative for tech-centric young people, and will play a central role in the mobile-based payments system that is emerging worldwide.

In the June 14, 2014 meeting at the World Bank that I cited in my answer to question #4 above, the representative from the US Federal Reserve asked seven key questions:

(a) Is Bitcoin a more efficient currency for illegal activities than physical currency?
(b) How anonymous is it?

(c) How vulnerable is Bitcoin to theft and counterfeiting? Like cash, there is no recourse for a victim of theft. Is it easier to steal virtual currency or physical currency?

(d) How vulnerable are Bitcoin exchanges to cyber attacks? This introduces volatility to the value of the currency.

(e) Will other virtual currencies emerge to challenge Bitcoin?

(f) Will Bitcoin or another virtual currency become "widespread enough to have implications for central bank currency and monetary policy?"; and

(g) "Will bank-like institutions emerge to take deposits and make loans of virtual currencies?"

I believe that the answer to your question is dependent upon the answers to those seven questions. If we can address the criminal misuse of Bitcoin while providing a measure of safety and security for Bitcoin users, a reasonable framework of regulation on a global basis at the point at which Bitcoins are exchanged for fiat currencies, and while ensuring that Bitcoin does not threaten the viability of the global economy, I have no doubt that Bitcoin and/or its successors will become an effective instrument for global financial inclusion and much more.

6. What can we as policymakers and legislators be doing to encourage innovation by good actors interested in being involved in the virtual currency space?

You can ensure that Congress not overreact to the real and complex challenges we face. As I argued in my oral testimony, my fear is that if Congress imposes a harsh regimen of draconian regulations that the primary result will be the relocation of the innovators and the movement of venture capital to locations outside the United States. Such a development would create a safe haven for illegal activity with no regulation or oversight.

I applaud the action of FinCEN and fervently believe that we need to apply anti-money laundering rules and regulations and apply money transmitter laws at the exchange level, the point at which virtual currencies are being exchanged for conventional currencies. Congress can ensure that such a policy is implemented consistently and uniformly.

I also think it is essential that you encourage dialogue and action on these issues at the global level. The US should take the lead internationally and promote this kind of balanced, reasonable approach within the international bodies in which it is a member.

Within the United States, we should work to achieve consistency and uniformity of approach between the federal government and the state governments.

Finally, I believe that it is imperative that you initiate reasoned, constructive dialogue nationally and globally on the core challenge, internet anonymity. There is a difference between privacy and anonymity. I recognize the difficulty in defining this distinction today in this era of the internet, a medium that is global in scope. Nonetheless, if we are to protect the viability and extraordinary potential of these new technologies and innovations while simultaneously addressing their misuse for criminal purposes, there have to be limits.

Responses to Post-Hearing Questions for the Record Submitted to Patrick Murck From Senator Thomas R. Carper "Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies" November 18, 2013

1. **Overall, how would you assess the federal government's activities thus far regarding virtual currencies and in what areas do you believe more work needs to be done?**

The U.S. federal government's work on Bitcoin has been notably thoughtful and careful. As you have pointed out, the Treasury Department, the Internal Revenue Service, the Justice Department, the Department of Homeland Security, and the Consumer Financial Protection Bureau have looked into Bitcoin, educated themselves about it, and found little that is troubling. There will be areas where Bitcoin's unique characteristics challenge the application of existing law, but in most areas the laws already on the books are sufficient to protect the public. We will continue to assist federal, state, and international governments seeking to understand Bitcoin, apply existing law to its use, and resolve any issues that arise. We believe the jurisdictions that foster Bitcoin innovation and use will be rewarded with jobs and economic growth.

Though we believe that the U.S. federal government's agencies have acted with care, the U.S. Bitcoin business ecosystem is very sensitive to their activities. So far, most U.S. Bitcoin businesses have been founded by individuals with greater technical knowledge than familiarity with the laws and regulations that may apply to the new business models they are creating. Start-up businesses do not regard the cost of legal counsel as trivial; legal fees can be the difference between a successful new business and a business idea foregone. And all U.S. businesses know that being on the wrong side of a U.S. financial regulator or security agency can bring massive legal costs, fines, destruction of reputation, and even the threat of incarceration. Because Bitcoin is new and fascinating to the public, the media will whip even faint signals from regulators as though they are heavy-handed threats.

All this makes it very important that federal regulators act with circumspection toward Bitcoin users and businesses. Uses of Bitcoin that are clearly illegal deserve no dispensation, but a business that may be in a legal gray area should get light-touch treatment until the legal questions are resolved. We expect federal agencies to know that they can be a "bull in a china shop," and that their inadvertence can do a great deal of damage to the U.S. Bitcoin ecosystem, frustrating your goal for the country, which is to get the benefits of Bitcoin while mitigating the risks.

Bitcoin Foundation

2. **Do you think virtual currencies, including Bitcoin, fit into our current legal and regulatory framework? Do you see any gaps in our statutes and regulations regarding virtual currencies? Which agencies do you believe need to be at the forefront of the federal government's work on virtual currencies?**

Most of the functions that Bitcoin serves are already covered by existing law. There will, of course, be gaps that arise over time, as ways of using Bitcoin and the Bitcoin protocol evolve. The ingenious Bitcoin protocol may come to be used for many things beyond value storage and transfer over time.

Rather than thinking of any one agency being "at the forefront," each agency should examine how Bitcoin interacts with the laws that it is charged with implementing and the protections that it provides the public. If a use of Bitcoin falls within its purview, or if a use of Bitcoin threatens consumer welfare in a way Congress empowered the agency to address, then that agency should work with us toward a corrective.

At the present time, the Internal Revenue Service's treatment of Bitcoin transactions is a matter of speculation and educated guessing. The U.S. Bitcoin community would benefit from clarity about how the IRS believes the law applies to various kinds of transactions. This would create confidence among Bitcoin businesses and their customers by reducing uncertainty. The issues are complicated and changing, so the IRS should commence an open and transparent notice-and-comment rulemaking, allowing all dimensions of the issues to be well considered.

3. **As I understand things, currently there is still a relatively very small group of people that use Bitcoin. That being the case, the full scope of the ramifications of the use of Bitcoin remains to be seen.**

a. **What are some examples of uses that might have a positive impact for consumers or the broader economy? What are some of the promises of this new technology, as you see them?**

There are many obvious uses for Bitcoin that will benefit consumers and the broader economy. Bitcoin allows individuals to send money to one another nearly instantly at very low cost. Bitcoin allows small businesses to receive payments without paying the high fees charged by many payment processors. Bitcoin allows immigrants to send money to their families without paying the exorbitant fees currently charged for international remittances. These benefits can return billions of dollars per year to consumers, and the competition that these uses of Bitcoin present to financial services providers should force them to lower their prices and improve their services.

As important—if not more important—are the innovations that creative Bitcoiners may build onto this open platform. Their experimentation will not just shave some inefficiency off of financial services. It will produce inventions that benefit consumers in ways we cannot predict. If public policy does not get in the way, someone will build a service on the Bitcoin protocol that is the

Bitcoin Foundation

equivalent of what Google did with search or what Wikipedia did with information-gathering and dissemination.

b. What kinds of businesses and opportunities might emerge around Bitcoin if the currency continues to grow?

The obvious business opportunities are in payments. Bitcoin businesses are already positioned to deliver needed competition in online payments. Bitcoin may produce advances in mobile payments and micro-payments. Remittances, as noted earlier, is an area where a small number of providers charge huge fees for transferring funds to people who rather badly need all the money they can get.

But the Bitcoin protocol has many features, and advanced services can be built on top of the protocol. So, just as one example, there may be a business providing escrow services—cost-effective, credit-card-like assurance of transactions when needed. We cannot predict all the ways that Bitcoin might underlie new business models and businesses. There are many opportunities in the Bitcoin space.

4. Since its introduction in 2008, Bitcoin has experienced a number of significant price swings. For example, in 2013, the price per Bitcoin fell from $266 in early April to $50 in late April, but today is hovering around $1000.

a. What factors have contributed to this volatility?

Volatility is a challenge to perceptions that Bitcoin is suitable for payments and for storing value. People rendering their judgments based on the behavior of markets for Bitcoin during its present infancy take volatility to be damning, but it will fall over time and mechanisms already exist to insulate some users from its effects.

Bitcoin has existed for just five years, and it has garnered widespread attention in only the last year. It is very thinly traded compared to the depth Bitcoin markets will reach when Bitcoin and the Bitcoin protocol reach their potential.

At its highest price against the U.S. dollar so far, in December 2013,[1] the total stock of Bitcoin was valued at about US$14.5 billion. At this writing, the value of all Bitcoin in U.S. dollars is about US$11 billion.[2] Compare this to the quantity of U.S. dollars: $11 to 12 trillion (varying with different measures of money supply).[3] The market for Bitcoin is roughly 1/1000th the size of the market for U.S. dollars. Unsurprisingly, it acts like a thinly traded market. The quantity of "stable" U.S. dollars, its worth noting, has increased more than 25% over the last four years.

---

[1] The date on which these responses are being submitted is January 10, 2014.
[2] *See* Blockchain.info, "Market Capitalization" Web page, https://blockchain.info/charts/market-cap.
[3] *See* Federal Reserve Back of St. Louis, *Monetary Trends* (current to Dec. 4, 2013), p. 3 http://research.stlouisfed.org/publications/mt/page3.pdf

As some observers have noted, owning Bitcoin now is like owning shares of a startup company long before its initial public offering. Changes in valuation are substantial as different prospects for the success or failure of Bitcoin, and for its value against other currencies and goods, express themselves in its price. Unlike shares in an early-stage company, these changes are visible in constantly updated, online charts.

A substantial amount of Bitcoin trading and holding is by investors who see opportunity in Bitcoin, including the opportunity to anticipate other investors' recognition of Bitcoin's value. This is entirely normal price discovery. While entrepreneurs discover uses for Bitcoin and the Bitcoin protocol, investors will discover the value of Bitcoin against other currencies and goods. This process will continue indefinitely.

Government policies around the world have contributed to volatility. Part of the dramatic rise in the price of Bitcoin against the dollar late last year is probably attributable to the easing of uncertainty around how the U.S. Congress would view Bitcoin. A later fall in price is probably associated with Chinese government policy appearing to change. Aggressive anti-money laundering laws in many jurisdictions, including recent changes that may have dispensed with the *mens rea* (or "guilty mind") requirement so deeply ingrained in criminal law, amplify the perception of governments as a threat to Bitcoin. We anticipate government action and signaling to be one of the primary drivers of volatility in the near future, diminishing as governments grow more comfortable with Bitcoin and as investors and users grow more confident that governments are comfortable with Bitcoin.

Time will iron out volatility in the Bitcoin price. As there are more users and more investors in coming years and decades, price spikes will diminish. And because Bitcoin is a global protocol, it may ultimately reach a trading depth well beyond the dollar or any other currency.

b. For those companies trying to build businesses around this technology, does this volatility concern you? What can be done so the price is not so volatile?

Volatility is a concern because it inhibits acceptance and adoption of Bitcoin. As noted above, we believe that volatility will fall over time, but while it exists, it retards the growth of the Bitcoin ecosystem. Much of present volatility is, however, a natural and essential part of price discovery. There should be no formal effort to inhibit volatility as such. Rather, fostering growth in the Bitcoin ecosystem will naturally cause volatility to fall.

There are already mechanisms in place to limit the effects of volatility. In the area of payments, for example, a number of companies allow online retailers, web sites, and any other business or individual to accept payment in Bitcoin, immediately converting bitcoins received into dollars. These businesses absorb the risk of short-term fluctuations in Bitcoin's value against local currency, which is a welcome service. Volatility is no reason to avoid accepting Bitcoin payments.

At present, we believe there lacks a sufficient number of stable exchange platforms, both in the United States and abroad. If Bitcoin price discovery were to occur on multiple exchanges that had deposit/withdrawal capabilities similar to existing equities and futures exchanges, volatility would drop. More streamlined inter-exchange arbitrage would remove the "regional" price spikes and plunges that have occurred in certain time zones.

The ability to sell bitcoins short will also help stabilize the price of Bitcoin. There are platforms where this can be done already, but more of them, operating in deeper markets, will be good for the Bitcoin ecosystem because of the input they bring to price discovery. Any effort to limit short-selling of Bitcoin artificially—an idea that has surfaced in other investment areas—should be stoutly resisted.

Though we have yet to see them, it is possible that fraudulent schemes to manipulate the price of Bitcoin could emerge (entirely distinct from investment, speculation, arbitrage, and other sophisticated price-discovery behaviors). If truly fraudulent manipulations of Bitcoin prices were to occur, those should be punished under ordinary law. Likewise, any government's policies or programs that aim to manipulate Bitcoin prices or interfere with normal price discovery in Bitcoin markets should be rejected.

Volatility in Bitcoin prices will fall as Bitcoin arrives at scale, business models exist to insulate Bitcoin users from volatility, and more techniques, such as arbitrage and short-selling, are in the offing. Bitcoin's best weapons against volatility are time and freedom for entrepreneurs and investors to act as they will.

5. **Most of the research and media coverage on virtual currencies has focused on Bitcoin. Are there other virtual currencies that we should be paying attention to? How do they differ from Bitcoin?**

The most important distinction to make between different types of digital currencies—which are quite real, not "virtual"—is between decentralized and centralized currencies. Bitcoin is a decentralized currency and protocol because it allows transfers directly from one user to any other, effectuated by publishing transactions on the global public ledger known as the "blockchain." Centralized currencies require an intermediary organization of some kind to effect transactions, record them, and confirm them.

The Bitcoin software is open source. Anyone can use it to start their own payment system or to make any other use of the protocol. Different versions of the Bitcoin protocol and software may have properties that make them more useful than Bitcoin in certain respects. Any of them that come into common use are worth paying attention to and encouraging.

Bitcoin is the current leader among decentralized currencies because of the strong network effects that exist in protocols and payment systems. If many people are using a protocol, it is more valuable to everyone, and many people are using Bitcoin. But other decentralized

currencies based on the Bitcoin protocol are seeking and may find a welcome place in the digital currency arena.

Time and experience will tell how important and valuable alternative implementations of the Bitcoin protocol will be. There are and will be other decentralized currencies based on it, and perhaps in future on other protocols. There is plenty of room for innovation, and in the end multiple decentralized digital currencies may co-exist, each put to use for the purposes to which it is best suited.

6. **The point has been made to me that the way to see Bitcoin and virtual currencies today is a bit like we saw email or the internet itself 20 years ago. At the time, we thought email might replace mail but it was sort of complicated and difficult to work unless you were more technically minded. Obviously as the technology matured it became easier to use and more widely adopted and it's changed the way we communicate in fundamental ways. With that said, if you could hazard a guess, what do you see for Bitcoin 20 years from now?**

I respectfully decline to offer myself up for some future list of the "worst predictions about Bitcoin"!

The point of your question is a salient one, though. Email—also known as the "Simple Mail Transfer Protocol"—has dramatically reformed the way people communicate with one another. It has parallels with traditional postal mail in that text communications and pictures are its primary payload. And the "mail" metaphor was probably useful because it made the idea of sending a "letter" over the Internet understandable. SMTP has many flaws, but email is incredibly valuable, and most people could probably scarcely imagine what their lives would be like today without it.

The name "Bitcoin" similarly uses metaphor to convey what this protocol is about. The Bitcoin protocol can be used to transfer value more quickly and cheaply than conventional methods. It is relatively easy to understand as "online money." Like email, the Bitcoin protocol and software have flaws, but its potential is similarly huge.

Like email differs from postal mail, Bitcoin differs from conventional currencies. Bitcoin may be programmable money that allows a payment to be held in escrow, for example, until goods are delivered. Indeed, the protocol can be used for many more things than value transfer. It might be used, for example, to prove the existence and authorship of documents or texts, to identify people or things in a registry beyond the control of any central actor, and even for distributed democratic decision-making. We will learn more about the potential uses of the Bitcoin protocol over time.

An essential element of reaching the Bitcoin protocol's potential is the freedom of its designers and users to experiment. Because it is open source and worldwide, the Bitcoin protocol and software are naturally resistant to centralized control, but forbearance on the part of

governments will give the inventors and entrepreneurs within their jurisdictions the latitude to discover the highest and best uses of the Bitcoin protocol. Inventors, entrepreneurs, and investors will produce jobs and economic growth in the countries that give them room.

I cannot predict what the most valuable uses of it will be, but Bitcoin's potential extends well beyond payments and storage of value, which alone may dramatically increase economic growth and global financial inclusion. Future uses of the Bitcoin protocol may improve the social and economic circumstances of people around the globe even further still. As you've suggested, we should seek the benefits of Bitcoin while minimizing the risks.

7. **What can we as policymakers and legislators be doing to encourage innovation by good actors interested in being involved in the virtual currency space?**

The bulk of responsibility for Bitcoin's success lies with the inventors, entrepreneurs, and investors building the services and businesses that can make Bitcoin's prospects a reality. Our role at the Bitcoin Foundation is to standardize, protect, and promote the use of Bitcoin for the benefit of users worldwide. Much of what we seek from Bitcoin will materialize if conditions are right. That means many things, but chiefly, for these purposes, that means giving Bitcoin's innovative community wide latitude to experiment and innovate.

We are pleased with your approach to Bitcoin and the statements of many federal agency officials about seeking the benefits of Bitcoin while mitigating the risks. The formula for doing that is fairly simple: Policymakers should educate themselves about Bitcoin. There will be areas where Bitcoin's unique characteristics challenge the application of existing law, but in most areas the laws already on the books are sufficient to protect the public. Where the law is unclear, circumspection should be the first response. It is very easy for government action intended as modest to be magnified in the press, to impose large costs on small start-up businesses, and to dissuade potential investors and Bitcoin users.

I encourage you to treat the Bitcoin Foundation is a resource. Bitcoin's potential for improving global financial inclusion, advancing privacy and liberty, and providing sound money are incentive enough to bring innovators and investors to the digital currency space. While policing against truly wrongful and damaging uses of Bitcoin, our job is to provide them the latitude they need to find out how people worldwide will use Bitcoin to improve their lives.

Post-Hearing Questions for the Record
Submitted to Jeremy Allaire
From Senator Thomas R. Carper

"Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies"
November 18, 2013

1. Overall, how would you assess the federal government's activities thus far regarding virtual currencies and in what areas do you believe more work needs to be done?

   The government has taken a thoughtful, deliberate approach toward digital currency to date, including the recent hearings held by two separate Senate committees on these matters. Digital currency is an evolving technology that poses many benefits and risks, which must be reviewed carefully. Law enforcement has acted appropriately in bringing actions against bad actors when needed. Agencies like FinCEN have offered some useful guidance to start to define the regulatory expectations.

   As with any emerging technology, there is more work that needs to be done in what will hopefully be a cooperative effort between the industry and government. Unfortunately, the current regulatory environment has had a chilling effect for businesses attempting to enter digital currency in several aspects. Some of the digital currency firms have not been able to find banking partners, audit firms and bond companies to assist them with their business. In addition, state regulators have been reluctant to accept and review money transmitter applications for these firms to do business in those states.

   The most important thing the government can do at this point is to provide regulatory certainty and encourage this type of innovation that will lead to jobs and commerce in the United States (specific recommendations are covered below in Question #2). We believe there would be a positive domino effect upon the messaging that the regulatory framework has been identified and established for digital currency. As it currently stands, the largest players in the digital currency space, including the exchanges, are located in China and Europe. Once the regulatory framework in the United States is settled, we believe more digital businesses will gravitate toward the U.S. markets. With that said, the government should continue to vigorously enforce the laws to ensure that there is a level playing field and that the industry is operating in an appropriate manner.

2. Do you believe virtual currencies, including Bitcoin, fit into our current legal and regulatory framework? Do you see any gaps in our statutes and regulations regarding virtual currencies? Which agencies do you believe need to be at the forefront of the federal government's work on virtual currencies?

We believe that digital currency can indeed be regulated under the current statutory framework. Recent high profile enforcement actions suggest that law enforcement can, and will, bring actions, against bad actors in this area. For legitimate businesses, the current barriers to entry and related regulatory compliance challenges are appropriate for a financial services business, which is assisting with payment transactions and securing currency for consumers. As a regulated money service business, it is entirely appropriate to be required to register with FinCEN, establish Know Your Customer ("KYC") standards, monitor transactions and report suspicious activity.

The biggest area that needs to be addressed in the short term relates to the tax treatment of digital currency. Without certainty in this area, merchants and consumers that utilize digital currency will be discouraged from doing so. In addition to the tax issues, there is some inconsistency among the states about the various requirements for money transmitter applications. We are encouraged that groups, such as the Conference of State Bank Supervisors, are forming a working group to review this situation. Finally, there should be some additional guidance around protection for consumers utilizing these services.

In terms of which agencies should lead this effort, FinCEN should continue to provide guidance and work with law enforcement officials to ensure that the current statutes are being followed. State agencies will also play a critical role under the current laws for money transmitters. As previously stated, the IRS should consider providing guidance regarding digital currency and related revenue. And, agencies like the Consumer Financial Protection Bureau should also weigh in on relevant consumer protection issues to ensure the consumer is educated on the products and services. Finally, the Federal Reserve, as the central banker, should review digital currency and consider its impact on the U.S. banking system and the economy. The Federal Reserve should ensure the banking system is coordinating appropriately with digital currency firms and should also assist with the coordination of international regulators in this area (similar to its approach on other key area such as capital adequacy standards).

3. As I understand things, currently there is still a relatively very small group of people that use Bitcoin. That being the case, the full scope of the ramifications of the use of Bitcoin remains to be seen. What are some examples of uses that might have a positive impact for consumers or the broader economy? What are some of the promises of this new technology, as you see them?

Bitcoin offers tremendous potential economic benefits, including:
- Materially lowering the costs associated with electronic payments, from an average of 2-3% down to close to 0%
- Open up trade globally, specifically e-commerce and online services, by facilitating trade and transactions across borders with low overhead.
- Radically lower the costs of money transfers, including and especially international remittances, which often carry 7-10% transaction fees.

- Reducing fraud associated with current electronic payment methods, where customers must constantly share sensitive bank account information, compared to Bitcoin whose cryptography-based architecture enables payments to happen without providing counter-parties with sensitive financial account information.
- Because of Bitcoin's low-cost transaction model, it can support payments for products and services priced on a micro-payment basis, including innovative metered pricing models.
- By leverage software and online services as well as smart mobile devices, help to improve the consumer retail experience.

Long-term, as a core set of technology and protocols, Bitcoin offers significant opportunities in establishing and enforcing contracts, including financial contracts, as well as new methods of trust in commercial exchanges.

4. Since its introduction in 2008, Bitcoin has experienced a number of significant price swings. For example, in 2013, the price per Bitcoin fell from $266 in early April to $50 in late April, but today is hovering around $1000.

a. What factors have contributed to this volatility?

Primarily, the price swings reflect the fact that Bitcoin is a nascent market with limited float and trade volume. Similar to small cap stocks on public exchanges, lack of liquidity at scale and lower trade volume will tend to yield higher levels of volatility. Likewise, Bitcoin has been a news-driven phenomenon, which in the early stages can lead to more significant price swings.

b. For those companies trying to build businesses around this technology, does this volatility concern you? What can be done so the price is not so volatile?

While it is a short-term concern, it is not a long-term concern. As more legal exchanges begin to operate in key financial markets (US, UK, Germany, Japan, etc.), we expect to see trade volumes grow considerably, and exchange products to become more sophisticated in terms of features that would be attractive to institutional investors. This broader institutional participation will drive greater price stability and greater liquidity for consumers and businesses using the currency.

5. Most of the research and media coverage on virtual currencies has focused on Bitcoin. Are there other virtual currencies that we should be paying attention to?

Bitcoin is currently the predominant currency of choice and we believe will be the focus of digital currency in the short term. There are several other emerging alternative currencies, such as Litecoin and Ripple that are attempting to enter the marketplace. We believe that the short term focus should be on emphasizing Bitcoin for its intended use, which is an alternative payment and way to transfer value. There will be innovation in the future and may be an opportunity for other

currencies to emerge. It will be important for the government to monitor the development of all of these currencies similar to Bitcoin to ensure that the same safeguards and are in place as the technology evolves.

6. The point has been made that the way to see Bitcoin and virtual currencies today is a bit like we saw email or the internet itself 20 years ago. At the time, we thought email might replace mail but it was sort of complicated and difficult to work unless you were more technically minded. Obviously as the technology matured it became easier to use and more widely adopted and it's changed the way we communicate in fundamental ways. With that said, if you could hazard a guess, what do you see for Bitcoin 20 years from now?

   I think that in 20 years we will be operating in a even more globally integrated world and economy, and that global digital currency will become a critical component to how world trade and e-commerce takes place. Like much of the rest of the Internet, tremendous industry opportunities will exist to build infrastructure as well as consumer and business-focused financial services that support this global adoption.

   At that point in time, we expect to see global currency emerge that is independent of any given nation-state, but which interacts with national central banks and global supranational financial institutions in a regulated fashion.

   In short, in 20 years, conducting commerce and trade anywhere on the planet will be as easy, instant and cost effective as using email or browsing a website.

7. What can we as policymakers and legislators be doing to encourage innovation by good actors like yourself, who are interested in being involved in the virtual currency space?

   Ongoing education within federal and state agencies, and with policy makers generally is critical at this stage. Likewise, ensuring that legitimate actors have clear guidance on rules that apply to them.

   By nature, digital currency operators such as Circle are either national or global in scope, yet are regulated on a state-by-state basis, which creates challenges in terms of scale and efficiency. We would encourage the Federal government to work closely with States to provide clear frameworks for national adoption of online products and services in the digital currency space.

   It would also be helpful for policymakers and regulators to provide sufficient clarity to existing financial institutions and banks who have been reticent to provide 'financial connectivity' to digital currency firms, which is materially limiting the innovation potential for this technology.

Post-Hearing Questions for the Record
Submitted to Jerry Brito
From Senator Thomas R. Carper

"Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies"
November 18, 2013

1. **Overall, how would you assess the federal government's activities thus far regarding virtual currencies and in what areas do you believe more work needs to be done?**

The federal government's approach to virtual currencies thus far has been understandably cautious.

On the anti-money-laundering and terrorist-financing front, FinCEN has issued guidance that adequately addresses virtual currencies, and it is heartening to see recent reports that the agency is clarifying for entrepreneurs and consumers how they plan to apply that guidance.[1] Additionally, with the tools already at their disposal, law enforcement has also successfully taken down the Silk Road online black market, as well as Liberty Reserve, a centralized digital currency favored by online criminals and responsible for laundering billions of dollars.

On the consumer protection front, state financial regulators are currently developing guidelines for the licensing of money transmitters, which are meant to ensure that such businesses are well-run and adequately capitalized. As noted in a question below, however, virtual currencies like Bitcoin are still not in use by very many consumers, and those who do use them likely understand the risks involved, giving regulators the luxury of seeing how the market develops and whether any problems arise before intervening.

One area where more guidance may be necessary is tax compliance. The IRS has indicated that it is working on guidance related to virtual currencies. Clear and simple rules for the tax treatment of virtual currency capital gains and other tax questions would be welcome.

2. **Do you believe virtual currencies, including Bitcoin, fit into our current legal and regulatory framework? Do you see any gaps in our statutes and regulations regarding virtual currencies? Which agencies do you believe need to be at the forefront of the federal government's work on virtual currencies?**

To date we have seen that regulators have been able to apply existing law to virtual currencies. In the future, there may be situations in which existing law may not be able to fully account for virtual currencies. For example, to the extent we may someday see a Bitcoin futures market, the Commodities Future Trading Commission may want to exercise its authority over "foreign-exchange forwards" or "foreign-exchange swaps." However, it would be difficult to justify that virtual currencies are "foreign" currency, which Congress did not define in Commodity

---

[1] Jon Southurst, FinCEN: Bitcoin Miners Need Not Register as Money Transmitters, CoinDesk, Dec. 29, 2013, at http://www.coindesk.com/fincen-bitcoin-miners-need-not-register-money-transmitters.

Exchange Act presumably because the meaning was obvious at the time. That said, the CFTC would have no problem treating bitcoins as commodities, since "commodity" is defined very broadly by the Act. What this suggests is that rather than attempt to predict how current law may not become incompatible with virtual currency use, a better approach may be to wait for actual "cases and controversies" to arise and to intervene only if regulators cannot apply existing law. To do otherwise may invite unintended consequences or simply waste time and resources.

3. **As I understand things, currently there is still a relatively very small group of people that use Bitcoin. That being the case, the full scope of the ramifications of the use of Bitcoin remains to be seen.**

    a. **Can you share with us some examples of uses that might have a positive impact for consumers or the broader economy? What are some of the promises of this new technology, as you see them?**

    b. **What kinds of businesses and opportunities might emerge around Bitcoin if the currency continues to grow?**

I would refer you to pages 10 – 20 of *Bitcoin: A Primer for Policymakers* in which my colleague Andrea Castillo and I detail the ways Bitcoin may positively affect the economy, as well as the business opportunities it presents.[2] One clear opportunity lies in international remittances, which is a $500 billion industry. For example, sending money to Kenya using Western Union MoneyGram or some other traditional money transmitter costs around five to ten percent of the amount being sent, and can take days for the deposit to take place. A new startup, BitPesa, is looking to charge only three percent, and to carry out transfers virtually instantaneously. This would be a win for immigrants in developed countries, their families back home, the entrepreneurs providing the service, and global economic development as well.

More importantly, perhaps, are uses of Bitcoin that go beyond the simple payments application. We have to keep in mind that Bitcoin is more than simply a currency, it is a programmable platform. For example, built into Bitcoin is a facility for decentralized arbitration. Essentially, Bitcoin allows for transactions that require two out of three signatures to verify a transaction, thus allowing payer and payee to turn to an arbitrator if there is a dispute about whether the payment should go through. Paypal and credit card companies essentially provide this service today, but decentralized arbitration would likely be cheaper and would certainly enjoy much more competition. Additionally, there's no reason that the arbitrator must be a human; using Bitcoin's scripting language the arbitrator can be a trusted automated source of information that on a regular basis broadcasts facts such as the price of gold, or price of stocks, or sports scores. Making that data stream the arbitrator would allow for the development of a decentralized predictions market. Prof. Ed Felten at Princeton is working on executing the concept.[3]

---

[2] Jerry Brito & Andrea Castillo, Bitcoin: A Primer for Policymakers, Mercatus Center at George Mason University, 2013, available at http://mercatus.org/sites/default/files/Brito_BitcoinPrimer_v1.2_1.pdf.

[3] Ed Felten, Bitcoin Research in Princeton CS, Freedom to Tinker, November 29, 2013, available at https://freedom-to-tinker.com/blog/felten/bitcoin-research-in-princeton-cs.

Finally, Bitcoin allows for microtransactions in a way that has never before been possible. Because bitcoin transactions are relatively inexpensive, one can send incredibly small amounts (say five cents or half a cent), something that would be cost-prohibitive using traditional payments systems. A start-up called BitWall takes advantage of this feature and allows publishers to easily charge tiny amounts for their content. More interesting, perhaps, are tiny microtransactions. Bitcoin transactions are so inexpensive that one could conduct hundreds per second using the micropayments channels feature of the Bitcoin protocol. It's not yet been widely exploited, but it is in the specification waiting to be implemented. One potential use of the ability to make many tiny transactions is offering metered services, such as Wi-Fi.

4. **Since its introduction in 2008, Bitcoin has experienced a number of significant price swings. For example, in 2013, the price per Bitcoin fell from $266 in early April to $50 in late April, but today is hovering around $1000.**

    a. **What factors have contributed to this volatility?**

There are at least three reasons that the price of Bitcoin fluctuates so wildly. First, the total value of all outstanding bitcoins is still relatively low. This means that even a small absolute increase in interest in Bitcoin can send prices soaring.

Second, a large fraction of the existing stock of bitcoins seem, for now, to be held as a long-term investment. This means that the market is not very liquid.

Finally, when there is a change in the demand for Bitcoin, the supply of Bitcoin cannot adjust to accommodate it, so all of the adjustment has to happen in the price, rather than in the quantity. This effect may be somewhat offset for now by the fact that many bitcoins are held as investments, but it means that Bitcoin is likely to be relatively volatile even if people stop holding bitcoins as investments.

    b. **For those companies who are trying to build businesses around this technology, doesn't this volatility concern you? What can be done so the price is not so volatile?**

Merchants that accept payment in bitcoins and companies trying to build businesses around the protocol no doubt already take the volatility into consideration. For example, merchants that accept bitcoins often use payment services like BitPay, which deposit dollars into merchant accounts on a daily basis, and companies like BitPay hedge against currency volatility. That said, as more and more consumers begin to use Bitcoin, the market will become more liquid and volatility should subside. Additionally, there are many potential uses of Bitcoin that are immune to price fluctuation, for example using Bitcoin's blockchain as a property register. In that application, each registered item would essentially be a miniscule amount of a bitcoin unit.

Because Bitcoin is an international phenomenon, no one government's policy will be able to calm volatility. However, the development of a bitcoin futures market would help stabilize the currency, and regulators can help combat volatility by allowing such a market to develop.

5. **Most of the recent research and media coverage on virtual currencies has focused on Bitcoin. Are there other virtual currencies that we should be paying attention to?**

It is important to keep in mind the difference between centralized and decentralized digital currencies. Centralized currencies like the defunct Liberty Reserve are of greater concern to law enforcement, as Special Agent Edward Lowery explained at the hearing. As for decentralized digital currencies, it is not surprising that Bitcoin has earned the lion's share of attention since it is the first ever decentralized currency as well as the largest. Indeed, the economy of the next largest decentralized digital currency—Litecoin—is less than one-tenth that of Bitcoin. Despite their current low market caps, competing cryptocurrencies have proliferated at an impressive rate since Bitcoin was first conceived. Many of these alternative cryptocurrencies offer different features—including varying block rates, hashing functions, and coin supplies—that their creators believe make them more attractive than Bitcoin.[4] Indeed, it is possible that an alternative cryptocurrency could one day overtake Bitcoin as the most popular. Competing decentralized currencies are very important, especially as they develop technical innovations, but the regulatory and law enforcement issues they raise are essentially the same as Bitcoin. Additionally, Bitcoin, as a first mover, benefits from much larger network effects.

6. **The point has been made to me that the way to see Bitcoin and virtual currencies today is a bit like we saw email or the internet itself 20 years ago. At the time, we thought email might replace mail but it was sort of complicated and difficult to work unless you were more technically minded. Obviously as the technology matured it became easier to use and more widely adopted and it's changed the way we communicate in fundamental ways. With that said, if you could hazard a guess, what do you see for Bitcoin 20 years from now?**

Email is a good analogy, but a better one might be the World Wide Web. As Mike Hearn, an engineer at Google who serves as one of Bitcoin's core developers, says, "The Web started out as scientists simply showing documents to each other. You could link documents and embed images, but the true potential of the Web really came when these pages became interactive and started gaining more and more features allowing people to build things like Facebook or online shops. Those things are not documents, and now probably half the time people use the Web they aren't really interacting with documents; they are actually using applications."

Unlike email, the Web is a platform, which means that it can be programmed to be just about anything. Bitcoin is similarly a platform that can be programmed. As a result, it's difficult to predict what developers and entrepreneurs allowed to freely innovate may come up with. However, some innovations that Bitcoin may make possible include micropayments, smart property, decentralized assurance contracts, and competitive arbitration services. Some of these, including micropayments and arbitration services, are currently being offered in beta form.

It is very difficult to project what the Bitcoin space will look like in 20 years or even 5 years from now. Bitcoin is a powerful tool that allows for innovation in payments, finance,

---

[4] A list of known cryptocurrencies can be found at: https://en.bitcoin.it/wiki/List_of_alternative_cryptocurrencies

communications, and even law. In its short history, we have seen that some of these innovations have been tested and improved by early adopters before businesses develop user-friendly services to expand access to later adopters. It is a good guess that we will continue to see this process of early adopter trial and error followed by entrepreneurial problem-solving and market expansion for the most promising of these innovations.

It is also possible that improvements will be made on the Bitcoin protocol itself or an alternative cryptocurrency that could present innovations that do not seem obvious in the present. However, if this space were to be unduly prevented from free discovery by poorly designed regulations, we will never get a chance to know either way.

7. **What can we as policymakers and legislators be doing to encourage innovation by good actors interested in being involved in the virtual currency space?**

As I said in my testimony, policymakers' first imperative should be to do no harm. Bitcoin and other decentralized digital currencies are an experiment, just as the wider Internet once was. The Internet has become the amazing engine of innovation and economic prosperity because it has largely been left alone by regulators. This was a deliberate policy articulated by President Clinton's chief policy counsel Ira Magaziner, who was in charge of crafting the administration's Framework for Global Electronic Commerce in July 1997.[5] Its recommendations read in part:

> **1. The private sector should lead.** The Internet should develop as a market driven arena not a regulated industry. Even where collective action is necessary, governments should encourage industry self-regulation and private sector leadership where possible.
>
> **2. Governments should avoid undue restrictions on electronic commerce.** In general, parties should be able to enter into legitimate agreements to buy and sell products and services across the Internet with minimal government involvement or intervention. Governments should refrain from imposing new and unnecessary regulations, bureaucratic procedures or new taxes and tariffs on commercial activities that take place via the Internet.
>
> **3. Where governmental involvement is needed, its aim should be to support and enforce a predictable, minimalist, consistent and simple legal environment for commerce.** Where government intervention is necessary, its role should be to ensure competition, protect intellectual property and privacy, prevent fraud, foster transparency, and facilitate dispute resolution, not to regulate.
>
> **4. Governments should recognize the unique qualities of the Internet.** The genius and explosive success of the Internet can be attributed in part to its decentralized nature and to its tradition of bottom-up governance. Accordingly, the regulatory frameworks established over the past 60 years for telecommunication, radio and television may not fit

[5] President William J. Clinton & Vice President Albert Gore, Jr., A Framework for Global Electronic Commerce (July 1, 1997), available at http://clinton4.nara.gov/WH/New/Commerce/

the Internet. Existing laws and regulations that may hinder electronic commerce should be reviewed and revised or eliminated to reflect the needs of the new electronic age.

5. Electronic commerce on the Internet should be facilitated on a global basis. The Internet is a global marketplace. The legal framework supporting commercial transactions should be consistent and predictable regardless of the jurisdiction in which a particular buyer and seller reside.

The same principles should apply to Bitcoin today. If there is one thing policymakers could do today to encourage innovation by good actors in the Bitcoin space it is to signal to the traditional financial sector—especially in banking—that while Bitcoin presents some challenges, it is nothing to be feared, and they will not be penalized by regulators for servicing, working with, and even investing in Bitcoin-related businesses.

○