TESTIMONY OF

Kathryn Haun Rodriguez

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

BEFORE THE

U.S. House of Representatives Committee on Financial

Services and Subcommittee on Terrorism and Illicit Finance

"Financial Innovation and National Security Implications"

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Moreover, cryptocurrency technology actually helps us solve bad acts. I witnessed this firsthand in prosecutions I brought. One was a case involving the Silk Road darknet marketplace and the agents investigating it. In 2014, we got a tip that there was a rogue agent on the DEA payroll. This agent happened to be on the Silk Road Task Force and was the government's lead undercover agent in communication with Ross Ulbricht, the Silk Road mastermind. Our investigation ultimately revealed that he was using his status as a federal agent to seize the cryptocurrency balances of ordinary citizens at exchanges across the world, and liquidating hundreds of thousands of dollars of bitcoin monthly. He was also selling Mr. Ulbricht information about the government's investigation in exchange for bitcoin, and, through a series of online personas, he was simultaneously defrauding and extorting Mr. Ulbricht for hundreds of thousands of dollars of bitcoin. There is much more to the story, but what enabled us to solve the crime was this rogue agent’s use of cryptocurrency. Because he had used bitcoin, we were able to trace all transactions directly back to him using the blockchain -- a permanent, immutable and public ledger, which can be an invaluable source of evidence. Attached to this written testimony is what was Exhibit 1 in our federal indictment. This shows you the tracing that we were able to do given the subject’s use of cryptocurrency. Unlike a series of money orders, a bulk cash transfer, or an anonymous prepaid card, here the criminals left immutable, digital footprints that our team followed.

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

This was just one early example. We have since uncovered (and solved) many hacking and major ransomware schemes by looking at the movement of bitcoin. Many of those cases are not yet public, but I can tell you with confidence that we would not have solved them had cryptocurrencies not been used. Since then, law enforcement around the globe and my former colleagues across the country – from New York to Colorado to Florida to Illinois – have successfully used the fact that criminals used cryptocurrency not only to solve crimes but to prove cases. Investigators like digital footprints and that is exactly what digital currencies provide.

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

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

The question naturally arises, "Why not go after those exchanges?" In 2013, the Digital Currency Task Force I founded, together with the IRS and U.S. Treasury Department's Financial Crimes Enforcement Network (FinCEN), conducted a criminal investigation into virtual currency company Ripple Labs for failure to follow AML laws and KYC regulations. In 2015, we reached a settlement -- it was the first enforcement ever against a virtual company under the Bank Secrecy Act -- under which Ripple agreed to collect customer data and identity before activating accounts, to enhance their compliance program, and to follow all money laundering laws. Today Ripple has emerged as a major player in this industry.

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

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

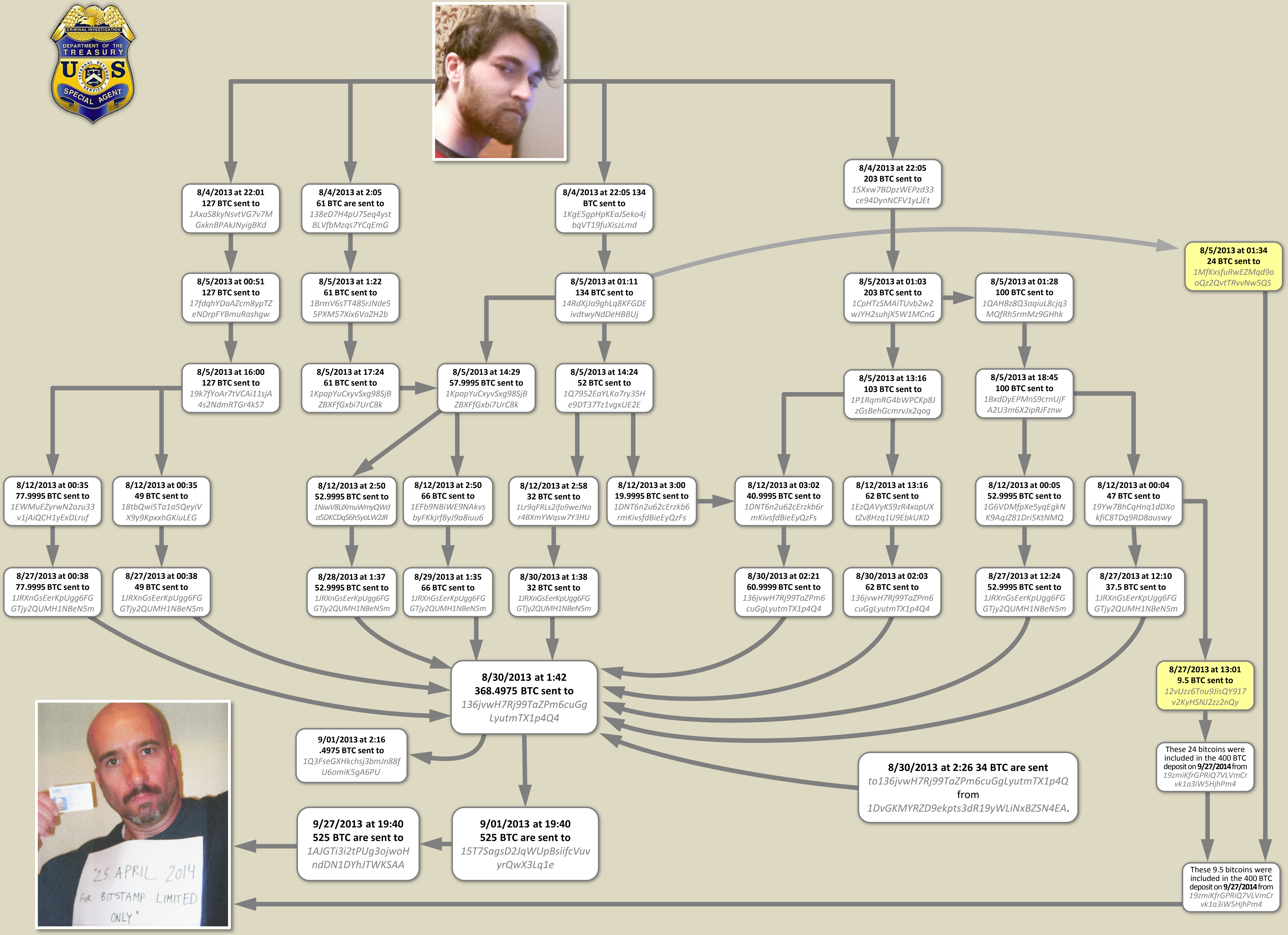
However, with broader adoption of cryptocurrencies, these companies are being stretched from a compliance perspective. They are also subject to having their correspondent banking relationships terminated as banks engage in blanket "de-risking" exercises that can cut these companies off from the rest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

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

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

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

All times are UTC (Coordinated Universal Time)



8/4/2013 at 22:01
127 BTC sent to
1AxaS8kyNsvtVG7v7M
GxknBPAkJNyigBKd

8/4/2013 at 2:05
61 BTC are sent to
138eD7H4pU7Seq4yst
BLVfbMzqs7YCqEmG

8/4/2013 at 22:05 134
BTC sent to
1KgE5gpHpKEaJSeko4j
bqVT19fuXiszLmd

8/4/2013 at 22:05
203 BTC sent to
15Xxw7BDpzWEPzd33
ce94DynNCFV1yLJEt

8/5/2013 at 00:51
127 BTC sent to
17fdqhYDaAZcm8ypTZ
eNDrpFYBmuRashgw

8/5/2013 at 1:22
61 BTC sent to
1BrmV6sTT485rJNde5
5PXM57Xix6VaZH2b

8/5/2013 at 01:11
134 BTC sent to
14RdXjJa9ghLq8KFGDE
ivdtwyNdDeHBBUj

8/5/2013 at 01:34
24 BTC sent to
1MfKxsfuRwEZMqd9o
oQz2QvtTRvvNw5QS

8/5/2013 at 01:03
203 BTC sent to
1CpHTzSMAiTUvb2w2
wJYH2suhjX5W1MCnG

8/5/2013 at 01:28
100 BTC sent to
1QAHBz8Q3aqiuL8cjq3
MQfRh5rmMz9GHhk

8/5/2013 at 16:00
127 BTC sent to
19k7fYoAr7tVCAi11sjA
4s2NdmRTGr4kS7

8/5/2013 at 17:24
61 BTC sent to
1KpapYuCxyvSxg98SjB
ZBXFfGxbi7UrC8k

8/5/2013 at 14:29
57.9995 BTC sent to
1KpapYuCxyvSxg98SjB
ZBXFfGxbi7UrC8k

8/5/2013 at 14:24
52 BTC sent to
1Q7952EaYLKa7ry35H
e9DT37Tz1vgxUE2E

8/5/2013 at 13:16
103 BTC sent to
1P1RqmRG4bWPCKp8J
zGsBehGcmrvJx2qog

8/5/2013 at 18:45
100 BTC sent to
1BxdDyEPMnS9crnUjF
A2U3m6X2ipRJFznw

8/12/2013 at 00:35
77.9995 BTC sent to
1EWMuEZyrwN2azu33
v1jAiQCH1yExDLruf

8/12/2013 at 00:35
49 BTC sent to
18tbQwi5Ta1a5QeyiV
X9y9KpxxhGKiuLEG

8/12/2013 at 2:50
52.9995 BTC sent to
1NiwV8UXmuWmyQWd
a5DKCDqS6h5yoLW2JR

8/12/2013 at 2:50
66 BTC sent to
1EFb9NBiWE9NAkvs
byFKkjrf8yJ9a8iuu6

8/12/2013 at 2:58
32 BTC sent to
1Lr9qFRLs2ifo9weJNa
r4BXmYWqsw7Y3HU

8/12/2013 at 3:00
19.9995 BTC sent to
1DNT6n2u62cErzkb6
rmKivsfdBieEyQzFs

8/12/2013 at 03:02
40.9995 BTC sent to
1DNT6n2u62cErzkb6r
mKivsfdBieEyQzFs

8/12/2013 at 13:16
62 BTC sent to
1EzQAVyKS9zR4xapUX
tZv8Hzq1U9EbkUKD

8/12/2013 at 00:05
52.9995 BTC sent to
1G6VDMfpXe5yqEgkN
K9AqJZ81Dri5KtNMQ

8/12/2013 at 00:04
47 BTC sent to
19Yw7BhCqHnq1dDXo
kfiC8TDq9RD8auswy

8/27/2013 at 00:38
77.9995 BTC sent to
1JRXnGsEerKpUgg6FG
GTjy2QUMH1NBeN5m

8/27/2013 at 00:38
49 BTC sent to
1JRXnGsEerKpUgg6FG
GTjy2QUMH1NBeN5m

8/28/2013 at 1:37
52.9995 BTC sent to
1JRXnGsEerKpUgg6FG
GTjy2QUMH1NBeN5m

8/29/2013 at 1:35
66 BTC sent to
1JRXnGsEerKpUgg6FG
GTjy2QUMH1NBeN5m

8/30/2013 at 1:38
32 BTC sent to
1JRXnGsEerKpUgg6FG
GTjy2QUMH1NBeN5m

8/30/2013 at 02:21
60.9999 BTC sent to
136jvwH7Rj99TaZPm6
cuGgLyutmTX1p4Q4

8/30/2013 at 02:03
62 BTC sent to
136jvwH7Rj99TaZPm6
cuGgLyutmTX1p4Q4

8/27/2013 at 12:24
52.9995 BTC sent to
1JRXnGsEerKpUgg6FG
GTjy2QUMH1NBeN5m

8/27/2013 at 12:10
37.5 BTC sent to
1JRXnGsEerKpUgg6FG
GTjy2QUMH1NBeN5m

8/27/2013 at 13:01
9.5 BTC sent to
12vUzz6Tnu9JisQY917
v2KyHSNJ2zz2nQy

8/30/2013 at 1:42
368.4975 BTC sent to
136jvwH7Rj99TaZPm6cuGg
LyutmTX1p4Q4

9/01/2013 at 2:16
.4975 BTC sent to
1Q3FseGXHkchsj3bmJn88f
U6omiK5gA6PU

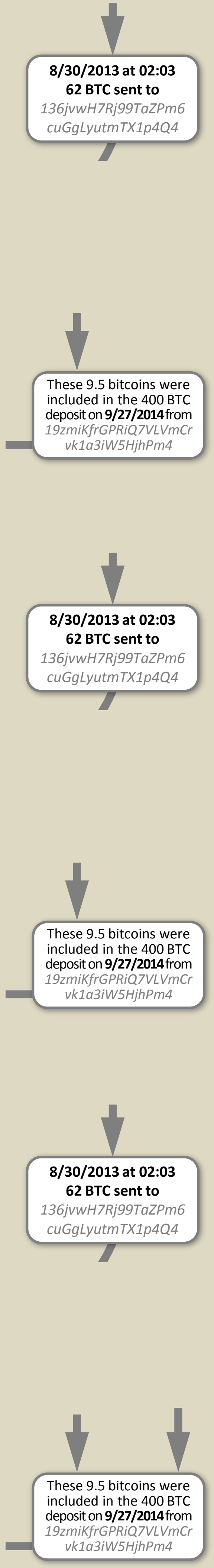
8/30/2013 at 2:26 34 BTC are sent
to136jvwH7Rj99TaZPm6cuGgLyutmTX1p4Q
from
1DvGKMYRZD9ekpts3dR19yWLiNxBZSN4EA.

These 24 bitcoins were
included in the 400 BTC
deposit on **9/27/2014** from
19zmiKfrGPRiQ7VLVmCr
vk1a3iW5HjhPm4

9/27/2013 at 19:40
525 BTC are sent to
1AJGTi3i2tPUg3ojwoH
ndDN1DYhJTWKSAA

9/01/2013 at 19:40
525 BTC are sent to
15T7SagsD2JqWUpBsiifcVuv
yrQwX3Lq1e

These 9.5 bitcoins were
included in the 400 BTC
deposit on **9/27/2014** from
19zmiKfrGPRiQ7VLVmCr
vk1a3iW5HjhPm4



8/30/2013 at 02:03
62 BTC sent to
136jvwH7Rj99TaZPm6
cuGgLyutmTX1p4Q4

These 9.5 bitcoins were
included in the 400 BTC
deposit on **9/27/2014** from
19zmiKfrGPRiQ7VLVmCr
vk1a3iW5HjhPm4

8/30/2013 at 02:03
62 BTC sent to
136jvwH7Rj99TaZPm6
cuGgLyutmTX1p4Q4

These 9.5 bitcoins were
included in the 400 BTC
deposit on **9/27/2014** from
19zmiKfrGPRiQ7VLVmCr
vk1a3iW5HjhPm4

8/30/2013 at 02:03
62 BTC sent to
136jvwH7Rj99TaZPm6
cuGgLyutmTX1p4Q4

These 9.5 bitcoins were
included in the 400 BTC
deposit on **9/27/2014** from
19zmiKfrGPRiQ7VLVmCr
vk1a3iW5HjhPm4

TRACE OF FRENCHMAID PAYOFF

770 BTC (worth approximately **$97,000** on 9/15/2013)
Per records obtained from the Silk Road marketplace and Ross Ulbricht's laptop, the 770 bitcoins transaction into bitcoins address *14rE7Jqy4a6P27qWCCsngkUfBxtevZhPHB* appears to the **payment to "Frenchmaid".** This transaction was a withdrawal made **by Ross Ulbricht from Silk Road**.

The sum of these **9/15/2013, 2:10 UTC**, payments to *14rE7Jqy4a6P27qWCCsngkUfBxtevZhPHB* is 520 BTC. Total BTC deposited into *14rE7Jqy4a6P27qWCCsngkUfBxtevZhPHB* = **770 BTC**

9/17/2013 20:08
14rE7Jqy4a6P27qWCCs
ngkUfBxtevZhPHB
sends 154 BTC to
15gCsMtTDZ2zt1ydW66
52jSTQXpCAHAtZL

9/22/2013 00:52
15gCsMtTDZ2zt1ydW6
652jSTQXpCAHAtZL
sends 154 BTC to
17p1DgXbvbDm5DQ3z
u9vc2q9TzJe9vn5ct
This address received other deposits, for a **total of 388.9995 BTC**

9/29/2013 18:10
17p1DgXbvbDm5DQ3zu9
vc2q9TzJe9vn5ct
sends 189 BTC to
1HEuVmWKybo1ZXAVTT
BYFiXSvQNEat46B
This is Carl Mark Force's CampBX address

9/17/2013 20:09
14rE7Jqy4a6P27qWCCs
ngkUfBxtevZhPHB
sends 154.0005 BTC to
13QGtr5jCut3uwzjW8ZP
zRs9Sku9bBxWt3

9/22/2013 00:56
13QGtr5jCut3uwzjW8ZP
zRs9Sku9bBxWt3
sends 154 BTC to
1JFKEvq3593ksDuEVQjS
uAaLX167rhuP1f

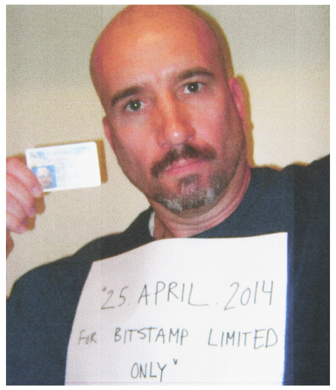
9/29/2013 23:17
17p1DgXbvbDm5DQ3zu9
vc2q9TzJe9vn5ct
sends 154 BTC to
1HDvYvhcFJJV3HxnRYZN
mh5ZNHZwik13qL
This is Carl Mark Force's CampBX address

9/20/2013, 23:29
48 BTC deposited into
156RBPqUCw6dxsXHCsJ
SKsuAC6JUmSRy2C.
These BTC were also traced to Silk Road wallets.

9/17/2013 20:11
14rE7Jqy4a6P27qWCCs
ngkUfBxtevZhPHB
sends 147 BTC to
1Mmna8iB9JyuTcMxsJk
UyDEeiszy7ctP6p

9/22/2013 1:08
1Mmna8iB9JyuTcMxsJk
UyDEeiszy7ctP6p
sends 146.9995 BTC to
156RBPqUCw6dxsXHCsJ
SKsuAC6JUmSRy2C

9/23/2013, 18:13
156RBPqUCw6dxsXHCsJS
KsuAC6JUmSRy2
sends 194.9995 BTC to
12ey8T8V9erbDjNGz6jsAj
S3TXafPc8S9p
This is Carl Mark Force's CampBX address



9/17/2013 20:12
14rE7Jqy4a6P27qWCCs
ngkUfBxtevZhPHB
sends 154.0005 BTC to
1N4NAD2ZnwB74gVRed
WjH1NPFkjtyy5tx9

9/22/2013 1:17
1N4NAD2ZnwB74gVRed
WjH1NPFkjtyy5tx9
sends 154 BTC to
1L9HxpQdakGzQT4o1mT
XZ8AqUVEkz9m6xS

9/29/2013, 23:14
1L9HxpQdakGzQT4o1mT
XZ8AqUVEkz9m6xS
sends 154 BTC to
1HDvYvhcFJJV3HxnRYZN
mh5ZNHZwik13qL
This is Carl Mark Force's CampBX address

9/17/2013 20:13
14rE7Jqy4a6P27qWCCs
ngkUfBxtevZhPHB
sends 160.999 BTC to
17Uu5TUSgCYgQqiMzVo
iFR6u3BDph4rV2J

9/22/2013 1:17
17Uu5TUSgCYgQqiMzVo
iFR6u3BDph4rV2J
sends 160.9985 BTC to
1CJx8u5VCZfCekkzQfMi
5NCq5fL6GwrN4n

9/29/2013, 23:13
1CJx8u5VCZfCekkzQfMi5
NCq5fL6GwrN4n
sends 160.9985 BTC to
1HDvYvhcFJJV3HxnRYZN
mh5ZNHZwik13qL
This is Carl Mark Force's CampBX address

All times are UTC (Coordinated Universal Time)