**TESTIMONY OF**

**Jerry Brito**

**Executive Director of Coin Center**

**BEFORE THE**

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

**"Financial Innovation and National Security Implications"**

**June 8, 2017**

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

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

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

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

---

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

---

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

[7] *Id.*

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

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

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

1. Bitcoin, the most widely used digital currency, is not anonymous as you sometimes read in the press, and it can be traced by law enforcement.[10]

2. This is a technology like the internet, or indeed like fire, that can be used for good or bad. Its inherent nature is neutral.

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

4. While there is substantial criminal use, terrorist use is nascent and experimental, so there is time to develop a considered response.

Thank you.

---

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

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