BLOCKCHAIN ASSOCIATION

TESTIMONY OF

Kristin Smith

Executive Director of the Blockchain Association

BEFORE THE

United States House of Representatives Committee on Homeland Security Subcommittee on Intelligence and Counterterrorism

"Terrorism and Cryptocurrency: Industry Perspectives"

June 9, 2022

I. Crypto Networks Are Essential to the Internet of the Future

Thank you for inviting me to testify today. My name is Kristin Smith and I am the Executive Director of the Blockchain Association, a nonprofit trade association dedicated to advancing good policy so that crypto networks can flourish in the United States. The Blockchain Association includes more than 90 leading companies who are committed to responsible innovation and strengthening the United States' strategic position in global finance and technology. Our diverse membership reflects this dynamic industry, and includes exchanges, developers, investors, and other participants in the crypto ecosystem.

I'm honored to be testifying today with professionals from Chainalysis and Coinbase who partner with law enforcement everyday to stop bad actors from using crypto networks. Today, I will explain what crypto networks are, what problems they solve, and why they will be the source of the next wave of American innovation.

Bitcoin is the world's first cryptocurrency – and the Bitcoin network is the world's first crypto network. Invented in 2009, Bitcoin allows anyone, anywhere in the world to send and receive value using nothing more than a computer with an internet connection. Before Bitcoin, if someone wanted to make a payment over the internet, they had to rely on an intermediary, like a bank, to add an entry to its private ledger debiting them and crediting the person they wanted to

pay. In other words, before Bitcoin, all online payments depended on gatekeepers and middlemen, who are slow and expensive under the best of circumstances. Under the worst of circumstances, they expose Americans' sensitive information to cyber attacks, discriminate against underserved communities, and exploit their own customers in the pursuit of profit.

Bitcoin solves these problems by replacing centralized intermediaries with a decentralized ledger that allows anyone, anywhere, to send payments across the world, almost instantly at almost no cost. Unlike the legacy banking system, which is dominated by large, private financial institutions, the Bitcoin network is a public payments infrastructure: digital cash for the digital era.

It's critical to note that crypto is more than currency. Digital cash was the first use case for crypto networks, but far from the last. American innovators, entrepreneurs, and developers are now using that same technology – crypto networks – to build the next iteration of the internet: sometimes called "Web 3." Web 1 refers to the early internet of the 1990s, when users could only do basic tasks like read websites or send emails. Web 2 refers to the internet we have today, with all its interactive applications and services. But just like the banking system, Web 2 is dominated by a few large companies – the tech giants – who wield outsized power and influence for their own benefit at the expense of the American public.

Web 3 – born from and built on crypto networks – is the solution to this imbalance of power. Web3 brings property rights to the web. It not only allows individuals to own their own data and content, but it also allows them to possess digital goods and property. Just like when the mainframe computer was replaced with personal computers, and proprietary operating systems were replaced with web-based software, the opening of internet platforms – and the ability to have digital ownership that comes along with it – will unleash immense innovation and change how we live, work, and play. For the United States to realize the full benefits of Web 3 – and ensure we remain the global leader in this space – we must ensure American entrepreneurs have the freedom to innovate.

Crypto networks present extraordinary opportunities, but also risks. The subject of today's hearing is an important one to address head-on, and thankfully, policymakers at the Treasury Department and across the government have been doing just that for many years. FinCEN was

the very first regulator to issue guidance related to crypto networks back in 2013. Since then, the US law enforcement and intelligence communities have proven highly effective in identifying and stopping bad actors from using crypto networks. The Blockchain Association and all of its members are strongly committed to protecting the integrity of the financial system, supporting US national security, and advancing US interests.

II. Crypto Networks Are Not Vulnerable to Use By Bad Actors

In the United States, custodial crypto companies like exchanges, payment processors, and other "fiat on-ramps and off-ramps" are regulated as money services businesses (MSBs) and are responsible for compliance with the Bank Secrecy Act (BSA). These companies have established highly effective anti-money laundering (AML) compliance programs and regularly coordinate with US law enforcement authorities to detect and prevent illicit activity. Peer-to-peer transactions, on the other hand, are not subject to the BSA pursuant to longstanding guidance from FinCEN. Yet, for several reasons, these transactions pose little risk of money laundering and terrorist financing.

First, before cryptocurrencies are exchanged for goods or services, they typically have to be converted to a national currency, which requires that they be exchanged through a regulated financial institution where they will be subject to the same level of due diligence as transactions in the traditional financial system. In these cases, cryptocurrency transactions pose no greater risk of money laundering or terrorist financing than ACH payments or wire transfers.

Second, the transparent and immutable nature of public blockchains allows law enforcement to "follow the money" and establish attribution in cases involving cryptocurrencies. According to The Department of Justice, "armed only with the knowledge of a target's cryptocurrency address and this single—but highly valuable—data set, [the blockchain], law enforcement can learn a myriad of vital pieces of information about a target." Indeed, many of the individuals charged in recent high-profile "busts" involving cryptocurrencies were identified after sending their assets to custodial accounts at regulated financial institutions that law enforcement was able to subpoena to establish attribution for the relevant criminal activity. It is largely due to law enforcement's ability to leverage blockchain technology and coordinate with industry participants that the amount of illicit activity on crypto networks is so low.

Third, the reality is that nearly fourteen years after the invention of Bitcoin, the vast majority of money laundering and terrorist financing continues to occur in the traditional financial system. According to the United Nations, "The best estimate for the amount available for laundering through the financial system, emerging from a meta-analysis of existing estimates, would be equivalent to 2.7% of global GDP (2.5%-4%) or US$1.6 trillion in 2009." From this statistic, it becomes clear that the value of illicit funds laundered each year through the traditional financial system is nearly greater than the value of all cryptocurrencies combined. For context, the largest cryptocurrency by market capitalization is bitcoin, which has a capitalization of about $568 billion, and the combined market capitalization of stablecoins that reference the US dollar is about $144 billion. Additionally, the level of illicit activity in cryptocurrency markets, which according to blockchain analytics firm Chainalysis represented just 0.15% of cryptocurrency transaction volume in 2021, further proves that cryptocurrencies have not been widely adopted by illicit actors.

Despite the minimal amount of illicit activity, some observers have suggested that the risk of illicit activity in peer-to-peer transactions is substantial enough to justify restricting the ability of crypto users to transact outside the confines of regulated financial institutions. It is not. Restricting the right of individuals to engage in peer-to-peer transactions on crypto networks would be akin to banning paper cash, a disproportionate response that would cause broad and long-lasting harm to the ideals of privacy and economic freedom at the core of our society.

III. Exhibits and Further Reading

For more information on the level and typology of illicit activity as well as a deeper dive into the importance of self-hosted wallets, I recommend the subcommittee read the following exhibits:

The Blockchain Association | Miller Whitehouse-Levine and Lindsey Kelleher | Self-Hosted Wallets and the Future of Free Societies | November 2020

This report is divided into two sections that seek to offer policymakers a broad introduction to self-hosted wallets. The first section describes what self-hosted wallets are, their role in the digital asset ecosystem, and the current regulatory framework for managing digital asset

transactions involving self-hosted wallets. The second section argues that imposing restrictions on individuals' ability to use self-hosted wallets would be misguided.

CoinCenter | Jerry Brito | The Case for Electronic Cash | February 2019

This paper shows that a cashless economy is a surveillance economy, arguing that removing the option to freely transact without intermediation greatly limits economic self-determination and places economic lives in the hands of financial institutions and governments. By presenting several case studies that demonstrate negative externalities associated with a completely intermediated payments system, the paper ultimately concludes that electronic cash, i.e. peer-to-peer transactions using self-hosted wallets, should be fostered and celebrated.

Consensys | James Beck | What is Web3? Here Are Some Ways To Explain It To A Friend | January 12, 2022

This article describes Web3 and how it is different from the internet that we know and use today. Critically, this article describes the motivation behind the creation of Web3 as "a reaction to social networks not keeping our data secure, and selling it for their own profit."

Chainalysis | The 2022 Crypto Crime Report | February 2022

This report gives an overview of illicit activity within the cryptocurrency ecosystem. The author of this report is Chainalysis, one of the world's preeminent blockchain analytics firms. According to the report, "with the growth of legitimate cryptocurrency usage far outpacing the growth of criminal usage, illicit activity's share of cryptocurrency transaction volume has never been lower…Transactions involving illicit addresses represented just 0.15% of cryptocurrency transaction volume in 2021."

Unchained | Laura Shin, Zia Faruqui, and Jessi Brooks | How This DOJ Strike Force Hunts Down Cryptocurrency Criminals | October 20, 2020

In this podcast, Laura Shin discusses how Zia Faruqui, Magistrate Judge, and Jessi Brooks, assistant U.S. attorney in the National Security Section at the United States Attorney's Office, prosecuted a number of federal criminal and civil forfeiture cases involving cryptocurrency, including the Welcome to Video case, which led to the takedown of one of the web's largest child pornography sites, a case involving the North Korea affiliated Lazarus group, and another case

involving Hamas and the Al Qassam Brigades. Interestingly, the success of each of these cases was contingent upon law enforcement's ability to leverage blockchain analytics to identify the perpetrators of these crimes.

Reuters | Brett Wolf | Recovery of Colonial Pipeline Ransom Funds Highlights Traceability of Cryptocurrency, Experts Say | June 23, 2021

This article describes the Colonial Pipeline attack and the efforts of law enforcement to identify and return the stolen funds. According to one blockchain analytics expert who was quoted in the article, “the seizure of approximately 85% of the ransom paid by Colonial Pipeline highlights how successful U.S. law enforcement has been in developing the capacity to execute this sort of complex operation using blockchain analysis in real time.”

LawFare | Andrew Mines and Devorah Margolin | Cryptocurrency and the Dismantling of Terrorism Financing Campaigns | August 26, 2020

This article describes how several U.S.-designated terrorist organizations attempted to receive funding using cryptocurrency. Ultimately, these terrorists were thwarted by law enforcement, who partnered with members of the cryptocurrency ecosystem to identify the terrorists and trace the flow of funds. Of particular note is the article’s assertion that “despite common assumptions that Bitcoin transactions are fully anonymous, U.S. officials used third-party blockchain analysis and personally identifying information from virtual exchanges to track 150 cryptocurrency accounts associated with al-Qassam, and to investigate U.S.-based individuals who donated to these campaigns.”

Bloomberg | Matt Levine | Business Rapper Was Bad at Bitcoin Laundering | February 9, 2022

This article describes the hack of the cryptocurrency exchange, Bitfinex, and law enformcent’s efforts to identify and prosecute the culprits as well as recover about 80% of the 119,754 Bitcoin worth $3.6 billion that was stolen. One critical aspect of this article is Mr.Levine’s comparison of money laundering with cash to money laundering with cryptocurrency: “If you come to a bank with a sack of cash and say, ‘I, uh, inherited this from my grandmother, she kept cash in sacks,’ that is somewhat hard for the authorities to check. If you come to a crypto exchange with a sack of Bitcoins and say ‘I got these cheap in 2014,’ that is easier to check. Permanent immutable public ledger on the blockchain!”