WRITTEN TESTIMONY

SHANE T. STANSBURY
Duke University School of Law

United States Senate Committee on Banking, Housing, and Urban Affairs

Hearing on "Understanding the Role of Digital Assets in Illicit Finance"

March 17, 2022

———

Chairman Brown, Ranking Member Toomey, and distinguished members of the Committee, thank you for the opportunity to testify today.

I am a Senior Lecturing Fellow in Law and the Robinson Everett Distinguished Fellow in the Center on Law, Ethics, and National Security at Duke University School of Law. At Duke, I teach primarily in the areas of cybercrime and national security law.

I previously spent more than eight years as a federal prosecutor in the U.S. Attorney's Office for the Southern District of New York (SDNY). At SDNY, I spent much of my time investigating and prosecuting transnational crimes, including terrorism, cybercrime, international narcotics trafficking, money laundering, international public corruption, and global weapons trafficking. I also served as a representative in the Department of Justice's (DOJ) National Security Cyber Specialists Network.

Although my testimony is based on my experience as a prosecutor and my current academic work, I am testifying today on my own behalf. No organization has paid for or approved this testimony.

Introduction

Criminals have always sought to take advantage of new forms of technology to facilitate their illegal activity. Over the last two decades, the pace at which they have done so has increased dramatically as the internet, social media, smartphones, and other innovations have changed the way we communicate and do business. I witnessed these rapid changes firsthand as a federal prosecutor focused on terrorism, international narcotics trafficking, and other transnational crimes.

For example, my colleagues and I saw new digital communication methods revolutionize the way terrorist organizations recruit members, spread propaganda, and carry out operations. An early example was the launching in 2010 by Al Qaeda in the Arabian Peninsula (AQAP) of a digital English-language magazine that could be easily distributed around the world through social media channels. Not long after that, we saw the Islamic State of Iraq and al-Sham (ISIS) take that strategy to another level. The group expanded its reach by exploiting a variety of platforms, including social media networks such as Twitter and Facebook and encrypted messaging apps like Telegram. These

technologies allowed the group to reach individuals around the world at a speed and scale previously unthinkable—sometimes to devastating effect. Of course, these new technologies did not just benefit terrorists. Drug traffickers and criminals of all types were quick to adopt social media, encrypted messaging apps, and other tools to better communicate with one another and carry out their illicit operations.

In the same way these technologies revolutionized the way terrorists and criminals communicate, cryptocurrency has provided new avenues for how they finance illegal activities. I will describe some of those avenues in a moment. But it is worth noting at the outset that in its current form cryptocurrency presents challenges that are in some ways distinct from technologies previously adopted by bad actors. Because of their principal features, cryptocurrencies can often act as magnets for criminal activity. They are decentralized, borderless, and most provide a high degree of anonymity. Add to these features other advantages—such as convenient access, storage, and transfer—and it is not hard to see why many criminals are attracted to cryptocurrency.

How Criminals Use Cryptocurrency To Facilitate Criminal Activity

As DOJ has explained, criminals can exploit cryptocurrency in several different ways, including (1) using cryptocurrency to facilitate the commission of crimes, or to support terrorist activity; (2) using cryptocurrency to illegally hide financial activity, such as through money laundering or sanctions evasion; and (3) committing crimes within the cryptocurrency market itself.[1] I will highlight a few examples of each of these types of activities.

The most obvious way cryptocurrency has changed the criminal landscape is simply by making some crimes easier to commit and harder to detect. By avoiding or minimizing cash transactions or bank transfers, criminals can seek to accomplish more easily one of their chief objectives—not getting caught.

My colleagues at SDNY saw this phenomenon firsthand in the early days of Bitcoin's adoption, when they were investigating the now infamous Silk Road website, which allowed users to buy and sell illegal drugs and other unlawful goods and services anonymously and beyond the reach of law enforcement. Bitcoin was the established currency on Silk Road, and it served as the perfect vehicle for anonymous, illegal transfers. With criminals free to buy, sell, and trade without ever having to exchange cash or deposit money in a mainstream account, the website flourished. At the time of its seizure in 2013, Silk Road was considered the most sophisticated criminal marketplace on the internet, having been used by several thousand drug dealers to distribute hundreds of kilograms of illegal drugs.[2]

Since that time, cryptocurrency has grown even more popular—and unfortunately so has its use in criminal conduct. Cryptocurrency is now used in connection with a broad array of illicit activity,

[1] U.S. Dep't of Justice, *Report of the Attorney General's Cyber Digital Task Force: Cryptocurrency Enforcement Framework* (Oct. 2020), at 5-6, available at: https://www.justice.gov/archives/ag/page/file/1326061/download.

[2] "Manhattan U.S. Attorney Announces The Indictment of Ross Ulbricht, The Creator And Owner Of The 'Silk Road' Website," U.S. Dep't of Justice (Feb. 4, 2014), available at: https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-indictment-ross-ulbricht-creator-and-owner-silk-road.

ranging from child exploitation and human trafficking to extortion and fraud.[3] According to one estimate, illegal cryptocurrency transactions reached a record total of more than $14 billion in 2021.[4] There are also signs that terrorists may be turning to cryptocurrency to finance their operations. In August 2020, DOJ seized millions of dollars as part of a wide-scale seizure of cryptocurrency tied to the al-Qassam Brigades (Hamas's military wing), al-Qaeda, and ISIS.[5]

Perhaps nowhere is cryptocurrency's role in criminal activity more vivid than in ransomware attacks.[6] As many are aware, ransomware is not just a growing problem for U.S. businesses,[7] but also a serious threat to public safety and national security. The hack of Colonial Pipeline in 2021 was perhaps the most visible reminder of this fact, but it did not stand alone. In 2021, U.S. agencies observed incidents involving ransomware against 14 of the 16 U.S. critical infrastructure sectors.[8] Thousands of hospitals, school districts, city governments, and other institutions in the U.S. have been impacted in recent years by this modern-day hostage scheme.

Cryptocurrency's primary appeal for ransomware criminals is the same as for other cybercriminals: obscurity. Indeed, cryptocurrency's central features make it particularly well-suited to the model of ransomware that has emerged in recent years. Under the so-called "Ransomware-as-a-Service" (RaaS) model, a developer typically licenses ransomware tools to affiliates, sometimes in exchange for a share of ransomware payments.[9] As is the case with other types of illicit monetary transfers, payments in ransomware attacks often do not travel directly from the victim to the perpetrators, but rather through multiple layers involving different entities, each of which may or may not be part of a regulated financial market.

The cryptocurrency market offers multiple opportunities for obfuscation along the path from payor to payee. One well-known technique is the use of "mixing" or "tumbling" services, which allow for the commingling of legitimate cryptocurrency transmissions with those involving illicit payments, thereby making the criminal activity harder to trace.[10]

---

[3] DOJ Cryptocurrency Enforcement Framework, *supra* n. 1, at 6-7. *See also* U.S. Gov't Accountability Off., GAO-22-105462, *Virtual Currencies: Additional Information Could Improve Federal Agency Efforts to Counter Human and Drug Trafficking* (Dec. 2021), available at: https://www.gao.gov/assets/gao-22-105462.pdf.

[4] Chainalysis, *The 2022 Crypto Crime Report* (Feb. 2022), at 3, available for download at: https://go.chainalysis.com/2022-Crypto-Crime-Report.html.

[5] "Global Disruption of Three Terror Finance Cyber-Enabled Campaigns," U.S. Dept. of Justice (Aug. 13, 2020), available at: https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns.

[6] *See, e.g.,* Erik Schatzker, "FBI Calls Crypto 'Only Game in Town' as Ransomware Flourishes," Bloomberg.com (Feb. 16, 2022), available at: https://www.bloomberg.com/news/articles/2022-02-16/fbi-calls-crypto-only-game-in-town-as-ramsonware-flourishes.

[7] U.S. Dep't of the Treasury, Fin. Crimes Enf't Network, *Financial Trend Analysis: Ransomware Trends in Bank Secrecy Act Data Between January 2021-June 2021* (Oct. 15, 2021), at 1 (describing ransomware as "an increasing threat to the U.S. financial sector, businesses, and the public"), available at: https://www.fincen.gov/sites/default/files/2021-10/Financial%20Trend%20Analysis_Ransomware%20508%20FINAL.pdf.

[8] Cybersecurity & Infrastructure Security Agency, *Alert (AA22-040A): 2021 Trends Show Increased Globalized Threat of Ransomware* (Feb. 9, 2022), available at: https://www.cisa.gov/uscert/ncas/alerts/aa22-040a.

[9] Institute for Security and Technology, *Combatting Ransomware* (Apr. 2021), at 16-17, available at: https://securityandtechnology.org/wp-content/uploads/2021/09/IST-Ransomware-Task-Force-Report.pdf.

[10] *See, e.g.,* DOJ Cryptocurrency Enforcement Framework, *supra* n. 1, at 41-44.

Another established method is "chain hopping," whereby criminals move illicit transmissions from one cryptocurrency to another using some form of cryptocurrency exchange. By using this method, criminals shift their digital trail from one cryptocurrency's blockchain to another cryptocurrency's blockchain, again making the illicit assets much harder to trace.[11]

A final example is the use of a so-called "privacy coin," such as Monero, to obfuscate illicit transactions. Unlike a cryptocurrency like Bitcoin, which relies on a public blockchain and reveals some information about the transaction itself (albeit not specific identifying information about the participants), a privacy coin generally adds another layer of anonymity by obscuring virtually all details of the transaction.[12]

These and other obfuscation methods make cryptocurrency attractive not only for the actual execution of crimes like ransomware, but also for money laundering and other efforts to conceal and promote criminal conduct. That criminals would adopt this new tool is not surprising. As a prosecutor, I regularly witnessed drug traffickers and corrupt officials look for innovative methods to avoid the scrutiny of U.S. financial authorities, particularly when they were trying to move money across borders.

But some of cryptocurrency's features—such as decentralized operation and control, and opportunities for anonymity—make it particularly enticing as a money laundering instrument. Criminals seeking to move illicit funds across borders can avoid risky intermediaries; they may have a network of options available at the click of a button. Their work is made easier by actors who expressly build technologies to reduce or avoid regulatory compliance. Indeed, as cryptocurrencies become more common and accepted, criminals could choose to keep their profits in cryptocurrency for use in other illicit activities.

Finally, cryptocurrency itself can create entirely new avenues for criminal activity. As DOJ has noted, because of cryptocurrency's features and the fact that much of its market is characterized by opaqueness, wallets and exchanges can become attractive targets for theft and fraud.[13] By one estimate, last year criminals stole approximately $3.2 billion worth of cryptocurrency and earned more than $7.8 billion from cryptocurrency-related scams.[14] As cryptocurrency grows in popularity, these crimes could increasingly harm the general public and less sophisticated investors. And the threat is not just from ordinary criminals. Rogue nation states have turned to cryptocurrency theft and other crimes to finance their regimes, as witnessed by North Korea's reported theft of hundreds of millions of dollars in cryptocurrency.[15]

---

[11] *See, e.g., id.*

[12] *See, e.g., id.* at 4, 41.

[13] *See id*. at 15-16.

[14] Chainalysis 2022 Crypto Crime Report, *supra* n. 4, at 5-6.

[15] Kevin Collier, "North Korea Stole a Record $400 Million in Cryptocurrency Last Year, Researchers Say," NBC News (Jan. 13, 2022), available at: https://www.nbcnews.com/tech/security/north-korea-stole-record-400-million-cryptocurrency-last-year-research-rcna12080. *See also* DOJ Cryptocurrency Enforcement Framework, *supra* n. 1, at 1, 16 (describing the threats posed by North Korea, including through illicit mining of cryptocurrency).

The Challenges Cryptocurrency Presents for Law Enforcement

The same factors that make cryptocurrency attractive to criminals can present challenges for prosecutors and law enforcement agents seeking to stop illicit activity.

As I mentioned previously, criminal actors are always looking for new ways to commit crimes or hide their illicit proceeds. Some find particularly clever methods for covering their tracks, and it is the job of investigators and prosecutors to use the tools at their disposal to find and assemble the pieces of the evidentiary puzzle.

When my colleagues and I investigated international money laundering cases, dedicated investigators spent countless hours analyzing records requested from financial entities to establish the use of shell companies, phony accounts, and other means to conceal the transfer and ownership of illicit funds. We were often successful because of the cooperation of international partners and because of the financial information made available by regulated institutions that followed their compliance and disclosure obligations. But much of the cryptocurrency ecosystem operates outside of the universe of resources that prosecutors and investigators routinely rely upon to gather the information they need to establish criminal malfeasance.

To be sure, law enforcement is getting much better at tracing digital assets used to commit and cover up criminal activity. With forensic blockchain analysis and access to other helpful information, like know-your-customer (KYC) information provided by regulated entities, law enforcement can penetrate the otherwise opaque world of illicit cryptocurrency transfers. Last year, we witnessed DOJ recover a substantial portion of the $4.4 million in ransomware payments made in connection with the Colonial Pipeline attack discussed previously.[16] And just last month, DOJ recorded its largest financial seizure ever when it recovered $3.6 billion in cryptocurrency allegedly related to the 2016 hack of the virtual currency exchange Bitfinex.[17] These are indeed promising and welcome developments.

It would be somewhat naïve, however, to conclude from these developments that tracing and recovering cryptocurrency assets is always easy—or even always possible. Even with the latest blockchain analytics, investigations can take years to complete. Frequently, the hardest part of a cyber-related prosecution is demonstrating what investigators sometimes refer to as "hands on the keyboard." Digital breadcrumbs left by criminals can prove invaluable to investigators. But ultimately prosecutors must demonstrate that an identifiable person is behind the criminal activity. And in a criminal case, that identity must be established beyond a reasonable doubt. That is, of course, as it should be, but in cryptocurrency-related cases prosecutors will often have the distinctive challenge of relying on a very complex series of digital patterns and transactions to meet their burden.

---

[16] "Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside," U.S. Dep't of Justice (Jun. 7, 2021), available at: https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside.

[17] "Two Arrested for Alleged Conspiracy to Launder $4.5 Billion in Stolen Cryptocurrency," U.S. Dep't of Justice (Feb. 8, 2022), available at: https://www.justice.gov/opa/pr/two-arrested-alleged-conspiracy-launder-45-billion-stolen-cryptocurrency. It should be noted that this case is pending and the criminal charges remain allegations.

That crucial connection of a criminal's identity to their criminal conduct is one of the main challenges posed by cryptocurrency. A public blockchain can be helpful, but often it can get one only so far. Prosecutors can spend years trying to penetrate the layers of obfuscation by savvy criminals. Even if they succeed, they may still face obstacles due to the current state of the cryptocurrency market.

Criminal investigations are only as successful as the information available. Sometimes prosecutors and investigators will get the information they need. For example, if a cryptocurrency exchange used by a criminal is complying with KYC and other regulatory requirements, that may provide the information needed for learning the criminal's identity or developing other leads. But too often this is not the case. Not all cryptocurrency platforms comply with existing regulations, and many operate in jurisdictions with less stringent requirements or beyond the reach of relevant treaties. This information gap could grow wider if more cryptocurrency platforms move to a decentralized model or if more anonymous instruments such as privacy coins gain wider adoption.

This is a remarkable period for technological innovation. Blockchain technology offers fascinating possibilities for the future, and I look forward to seeing how it might be applied to enrich our society. But we should also recognize the serious role that cryptocurrency is playing in criminal activity. Only then can we take the steps necessary to protect our health, our safety, and our national security.