Robert Novy

Deputy Assistant Director
Office of Investigations
United States Secret Service

Prepared Testimony

Before the
United States House of Representatives
Committee on Financial Services
Subcommittee on Terrorism and Illicit Finance
June 20, 2018

Chairman Pearce, Ranking Member Perlmutter, and members of this Subcommittee: Thank you for inviting me to testify before you about the U.S. Secret Service's actions in response to the increasing illicit activities involving digital currencies.[1] The Secret Service's primary concern regarding this topic is digital currencies' use in criminal schemes that undermine the integrity of financial and payment systems, their use in cases of fraud, and their general use as a means of money laundering. The Secret Service possesses a unique record of success in countering criminal uses of digital currencies, and we are committed to continuing to keep pace with technology innovation, as well as evolving strategies and tactics, of cyber criminals. My testimony describes our observations on trends and patterns related to digital currency, as well as some of the challenges that may warrant Congressional attention.

As one of the nation's original investigative agencies charged with safeguarding the nation's financial and payment systems, the Secret Service has conducted criminal investigations to protect the American public, companies, financial institutions, and critical infrastructure from criminal exploitation since 1865. As early as 1982, the Secretary of the Treasury directed the U.S. Secret Service to investigate crimes related to electronic funds transfers, in order to keep pace with the growing role of computers in the U.S. financial system. Two years later, in 1984, Congress passed legislation to expand the Secret Service's responsibilities to include investigating a range of computer hacking and access device fraud violations. Today, we have extensive authorities to safeguard financial and payment systems from criminal exploitation, even as those illicit activities are increasingly transnational in nature and enabled by cyberspace and digital currencies.[2]

In executing our law enforcement mission, the Secret Service closely partners with Federal, state, local, and international law enforcement agencies, as well as with a range of other international and domestic partners. We do this in part through our network of Electronic Crimes Task Forces (ECTFs)[3] and Financial Crimes Task Forces. Specifically, as it relates to criminal investigations involving digital currency, we partner particularly closely with U.S. Immigration and Customs Enforcement's Homeland Security Investigations (ICE/HSI), the Financial Crimes Enforcement Network (FinCEN), the Federal Bureau of Investigations (FBI), and other Federal agencies with related responsibilities.

[1] The term "digital currency" is used to refer to a representation of value that is stored on and transferred through computer systems that is used similar to money (used as a medium of exchange, unit of account, store of value, or standard of deferred payment) and is used as a substitute for or converted to legal tender of the United States or another country. The term "digital currency" is closely related to "virtual currency" (as defined by the FinCEN Guidance issued 18 March 2013), but may also include digital currencies that are recognized as legal tender.

[2] Criminal activity related to digital currencies investigated by the U.S. Secret Service often involve violations relating to 18 U.S.C. §§ 1028, 1028A, 1029, 1030, 1343, 1956, 1957, 1960, and 3056(b).

[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 40 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 crimes.

Since the commercialization of the Internet in the early 1990s, there have been various efforts to develop payment systems that can function effectively within the digital economy. The market has predominately adopted payment cards as this solution, but there have also been numerous attempts to establish digital currencies that operate with greater independence from the established financial system. While some digital currencies have operated lawfully, others have been used extensively for illicit activity.

The Secret Service has been at the forefront of investigating the illicit use digital currencies. Working with our interagency partners, we have investigated and shutdown two major centralized digital currencies that supported extensive criminal activity: e-Gold Ltd. (in 2007)[4] and Liberty Reserve (in 2013).[5] Since then, the Secret Service has worked with our partners to investigate and shutdown a number of illicit digital currency exchangers,[6] including Western Express, which was prosecuted by the Manhattan District Attorney's Office, and, in 2017, the cryptocurrency exchange BTC-e,[7] working in partnership with the Internal Revenue Service's Criminal Investigations (IRS-CI) and other law enforcement agencies. These, and numerous other criminal investigations, have provided the Secret Service with insight on the risks and challenges posed by digital currencies, and the effectiveness of various potential law enforcement responses.

Criminal Use of Digital Currencies

In recent years, criminals have increasingly used digital currencies to facilitate illicit activities on the Internet. Digital currencies provide an efficient means of transferring large values globally, for both legitimate and criminal purposes. Some providers, exchangers and users of digital currencies attempt to avoid the international legal and regulatory systems established to counter illicit finance. Based on Secret Service investigations into criminal use of digital currencies, criminals prefer digital currencies they assess to have the following characteristics:

1) Widespread adoption as a medium of exchange for intended criminal activities;
2) The greatest degree of anonymity.
3) Protection against theft, fraud, and lawful seizure.
4) Can be readily exchanged to and from their preferred currency.[8]

[4] *See* https://www.justice.gov/usao-md/pr/over-566-million-forfeited-e-gold-accounts-involved-criminal-offenses.
[5] *See* https://www.justice.gov/opa/pr/founder-liberty-reserve-pleads-guilty-laundering-more-250-million-through-his-digital.
[6] Exchangers are businesses that allow for the trade of digital currencies for other assets, such as conventional fiat money, such as US dollars, or other digital currencies.
[7] *See* https://www.justice.gov/usao-ndca/pr/russian-national-and-bitcoin-exchange-charged-21-count-indictment-operating-alleged.
[8] The term "currency" is defined pursuant to 31 CFR 1010.100(m) as "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 U.S. silver certificates, U.S. notes

5) The ability to quickly and confidently transfer value transnationally.

There is a large number of digital currencies available today, but only a few have been substantially adopted for engaging in certain illicit activities. 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—particularly transnational transfers. The greatest risks are posed by digital currencies that have widespread use for both of these purposes. e-Gold and Liberty Reserve were prime examples of these risks. Both platforms effectively conducted no customer verification, and were extensively used for a range of illicit activities, from child exploitation to identity theft, before the Secret Service shut them down.

Use of a Blockchain as Digital Currency

In 2008, Bitcoin was proposed as a digital currency that could provide a decentralized payment system through use of cryptography to form a trusted chain of digital signatures, known as a blockchain.[9] Following the example of Bitcoin, beginning in 2011, various individuals and groups launched their own blockchain implementations that provide various other forms of cryptocurrencies.[10] As of 12 June 2018, there are over 600 blockchains in operation on the Internet and, based on current exchange prices, the total market capitalization of cryptocurrencies is approximately $290 billion. Currently, the four largest cryptocurrencies, by market capitalization, are: Bitcoin ($116 billion), Ethereum ($52 billion), Ripple ($22 billion), and Bitcoin Cash ($16 billion).[11] The Secret Service has adapted to this trend; for example, from FY 2015 to present, the Secret Service has seized over $28 million in cryptocurrencies in the course of our criminal investigations,[12] primarily in the form of Bitcoin.

In addition to the use of blockchains to provide a digital currency, various organizations are considering using blockchains for other purposes. These include a decentralized public ledger for tracking ownership of property, digital identity management, and supply chain management. For example, Ethereum, which provides a decentralized Turing-complete virtual machine (the Ethereum Virtual Machine, or EVM),[13]serves as platform for numerous decentralized applications and smart contracts. Ethereum has become one of the most popular platforms for

---

and 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."

[9] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," (31 October 2008). Available at: https://bitcoin.org/en/bitcoin-paper.

[10] The term "cryptocurrency" is used to refer to a decentralized system that uses cryptographic techniques to regulate the generation and transfer of a digital currency.

[11] *See* Coin Market Cap, "Top 100 Coins by Market Capitalization." Last accessed on 12 June 2018. Available at: https://coinmarketcap.com/coins/.

[12] Value at the time the seizure was executed.

[13] As a Turing-complete system, the EVM is able to compute every function general purpose computers are capable of—an important property in computer science.

conducting Initial Coin Offerings (ICOs). In 2017, approximately $3.88 billion was raised through Initial Coin Offerings.[14] The Secret Service partners with the Security and Exchange Commission (SEC) in addressing criminal risks related to ICOs, as the SEC has taken an active role in addressing risks to investors and businesses related to use of ICOs to raise capital and participate in investment opportunities.[15]

The growing popularity of blockchains has also resulted in the growth of criminal activities closely related to its proprieties. These include: crypto-jacking, thefts of private keys, ransomware, and attacks on blockchain networks themselves. Crypto-jacking is the use of malware or compromised websites to use, without authorization, computing power of others for cryptocurrency mining.[16] Control of assets on a blockchain is maintained through exclusive control and access to the associated private cryptographic key; however, there have been numerous instances of cryptocurrency heists, involving major exchanges, wallets and individual users resulting from the theft and illicit use of private cryptographic keys. While ransomware, which impairs the operation of a computer as part of an extortion demand, has been around since the late 1980s, its growth over the last four years has substantially been driven by use of cryptocurrencies as the means of paying extortion demands. Finally, we have observed a few instances of attacks on blockchain systems themselves, either to impair their operation, as part of a broader scheme, or as part of a "51% attack"[17] to defraud other users of the cryptocurrency. All such activities typically involve violations of the Computer Fraud and Abuse Act (18 U.S.C. § 1030) and potentially other criminal statutes.

Exchangers of cryptocurrency have been a particularly effective control point for law enforcement to focus its effort. For example, BTC-e was Internet-based, foreign-operated money transmitter that exchanged fiat currency as well as convertible cryptocurrency such as Bitcoin. Before it was shut down as part of a multi-national law enforcement operation, it was one of the largest digital currency exchanges by volume, receiving $4 billion worth of digital currency over the course of its operation from 2011 to 2017. BTC-e processed transactions involving the criminal proceeds of numerous computer intrusions and hacking incidents, ransomware scams, identity theft schemes, corrupt public officials and narcotics distribution rings. BTC-e also allegedly facilitated the exchange of roughly 95 percent of ransomware payments, according to a non-government report.

Challenges related to Digital Currencies and Potential Congressional Actions

[14] Coinschedule, "Cryptocurrency ICO Stats 2017." Last accessed on 12 June 2018. Available at: https://www.coinschedule.com/stats.html?year=2017.
[15] *See* https://www.sec.gov/ICO.
[16] Mining is the computational process that verifies and maintains a blockchain, and is typically incentivized by a blockchain protocol rewarding cryptocurrency to miners.
[17] A "51% attack" is scheme whereby over 50% of the computational power participating in a blockchain is used in a concerted manner that undermines the integrity of that blockchain.

The growing illicit use of digital currencies risks undermining the effectiveness of existing U.S. laws and regulations, especially those intended to limit the ability of criminals to profit from their illicit activities. The key U.S. laws relevant to Secret Service investigations involving the illicit uses of digital currencies include the Bank Secrecy Act of 1970, the Annunzio-Wylie Anti-Money Laundering Act, the Money Laundering Suppression Act of 1994, and Title III of the USA PATRIOT Act of 2001, in addition to other associated laws and Federal regulations. Congressional attention to the positive effects of these laws is especially needed today, as we are in a period of significant technology innovation within the financial sector.

Given the global nature of the Internet and modern communications, digital currencies are particularly well-suited for supporting crimes that are transnational in nature. Accordingly, effectively countering criminal activity involving digital currencies requires close international partnerships. Foreign partners play key roles in assisting U.S. law enforcement with conducting investigations, making arrests, and seizing criminal assets. Fostering these partnerships and conducting these transnational investigations requires continual investment in international law enforcement collaboration, and a persistent effort to harmonize anti-money laundering laws and related criminal statutes. It is critical that the United States continues to work internationally to improve controls related to digital currency through organizations like the Financial Action Task Force.[18] We should also consider additional legislative or regulatory actions to address potential challenges related to anonymity-enhanced cryptocurrencies, services intended to obscure transactions on blockchains (i.e. cryptocurrency tumblers or mixers) and cryptocurrency mining pools.

Some businesses, including providers of information and communications systems, are taking actions that impede timely access to digital evidence. As such, continued Congressional attention is warranted to ensure law enforcement agencies maintain lawful access to critical sources of evidence, regardless of where, or in what form, that information is stored. The recently enacted CLOUD Act was an important step in this regard, but further legislative or regulatory action may be needed, as case law and business practices continue to develop. Such legislative or regulatory actions could take the form of new reporting requirements or data collection, retention, and accessibility requirements for certain businesses or business activities.

Further, investigating crimes involving digital currencies, and the transnational organized cyber criminals that extensively use them, requires highly skilled criminal investigators. Hiring, developing, and retaining our investigative workforce, as well as partnering with and training our law enforcement and private sector partners to develop robust investigative capabilities, are all critical priorities for ensuring we are well prepared to address emerging risks resulting from technology innovation, both today and into the future.

[18] *See* http://www.fatf-gafi.org/.

Conclusion

Despite these challenges, we are committed to continuing to effectively execute our mission. Digital currencies have the potential to support more efficient and transparent global commerce, and to enhance U.S. economic competitiveness. However, because digital currencies continue to be used to facilitate illicit activity, law enforcement must adapt our investigative tools and techniques to dismantle criminal groups that use these instruments for fraudulent activity or money laundering.

Those that seek to further their illicit activities through use of digital currencies should have no illusions that they are beyond the reach of the law. As the investigative work of the Secret Service and our law enforcement partners continues to demonstrate, we are relentless in enforcing the law and will not be stopped by the perceived anonymity of the Internet or digital currencies.