COMMENT

PROSECUTING CRYPTOCURRENCY THEFT WITH THE DEFEND TRADE SECRETS ACT OF 2016

GREGORY BISCHOPING[†]

[†] Online Managing Editor, Volume 166, *University of Pennsylvania Law Review*. J.D., 2018, University of Pennsylvania Law School; B.S., 2015, Boston College. Thanks are due to the editors of the Volume 167 Law Review for their diligent and perceptive work on this Comment, especially Anna D'Ginto and the other Executive Editors, and Comments Editor Patrick Reischl.

INTRODUCTION

This Comment intends to advance a novel law for prosecuting the theft of cryptocurrency—the Defend Trade Secrets Act of 2016 (the DTSA or the Act). The DTSA is a powerful legal tool for combatting this difficult-to-define crime. Beyond the conceptual applicability of trade secret law, the confidentiality, extraterritoriality, and other uniquely tailored features of the Act make it practically useful. This Comment suggests this nonexclusive tool for prosecuting cryptocurrency theft and will not explore the many other ways that cryptocurrency may be regulated.

After explaining the technology of cryptocurrency, I will describe the growing threat posed by cryptotheft. I will briefly survey the legal tools currently used to deal with the theft of cryptocurrency. I will next propose that the DTSA should be used to prosecute, both civilly and criminally, the theft of blockchain-based currency. The DTSA includes a host of valuable features that make it particularly attractive and effective for both the government and individuals prosecuting cryptotheft. I will briefly compare the Act to other possible schemes for prosecuting cryptotheft. Finally, I will conclude by noting the challenge of applying American law to foreign actors and the technical difficulty associated with tracking and retrieving digital coins.

A. *Technological Background*

Cryptocurrencies are taking the financial world, and with it the regulatory world, by storm.[1] These relatively new technologies, many of which are described as "decentralized ledger technology" (DLT), revolutionize the way both information and money are stored.[2] Blockchain technology has formed the basis of a new wave of purely digital currency, beginning with the now ubiquitous Bitcoin. Like similar blockchain technology, Bitcoin provides "a way of recording and reconciling every transaction that has ever occurred, between every single participant, going back to the beginning."[3] This technology, while

[1] *See* Kevin Roose, *Is There a Cryptocurrency Bubble? Just ask Doge.*, N.Y. TIMES (Sept. 15, 2017), https://www.nytimes.com/2017/09/15/business/cryptocurrency-bubble-doge.html [http://perma.cc/D5PH-FQYW] (highlighting the "mania" among investors for cryptocurrency and describing regulatory responses).

[2] *See* Rob Marvin, *Blockchain: The Invisible Technology That's Changing the World*, PCMAG (Aug. 29, 2017), https://www.pcmag.com/article/351486/blockchain-the-invisible-technology-thats-changing-the-wor [https://perma.cc/59QL-QDLJ] (providing an introduction to the structure and usage of blockchain technology). This technology has the potential to radically change how businesses contract and interact with each other. *See generally* Jeremy M. Sklaroff, Comment, *Smart Contracts and the Cost of Inflexibility*, 166 U. PA. L. REV. 263 (2017) (summarizing and criticizing smart contracts, a key application of DLT). Not all cryptocurrencies are DLT, and for a description of the distinction, see *infra* note 110 and accompanying text.

[3] Sklaroff, *supra* note 2, at 269.

providing an exciting opportunity for investment, speculation, and innovation, also creates many new opportunities for exploitation.[4]

Bitcoin has existed since the mysterious Nakamoto paper was published in 2009,[5] though it is predated by a few lesser-known online currencies with similar ledger systems.[6] In 2009, the public began "mining" Bitcoins, a process by which new coins are created.[7] Mining takes progressively more computing power with each new Bitcoin created, with only a finite number of possible coins.[8] In 2010, 10,000 Bitcoins were exchanged for two pizzas—the first known sale.[9] In 2011, the first rival cryptocurrencies appeared, each attempting to offer a subtle but unique advantage, and these rivals have since multiplied into the thousands.[10]

Bitcoin, as an embodiment of blockchain technology, consists of a "shared database populated with entries that must be confirmed and encrypted," much like a shared document with each entry logically connected to every entry before.[11] This creates a secure log that, in the case of Bitcoin, is stored collectively.[12] Owners of cryptocurrency do not actually possess their coins,

[4] This author is not well suited to describe the technological processes of Bitcoin, but there are a plethora of publicly accessible resources that do so quite well. *See e.g.*, SATOSHI NAKAMOTO, BITCOIN: A PEER-TO-PEER ELECTRONIC CASH SYSTEM (2009) (providing a seminal description of Bitcoin and the potential of blockchain technology); Nathaniel Popper, *What Is Bitcoin, and How Does It Work?*, N.Y. TIMES (Oct. 1, 2017), https://www.nytimes.com/2017/10/01/technology/what-is-bitcoin-price.html [http://perma.cc/582W-HJA2] (answering commonly asked questions regarding Bitcoin); *How Does Bitcoin Work?*, BITCOIN, https://Bitcoin.org/en/how-it-works [https://perma.cc./9Y2V-HCCK] (last visited Aug. 20, 2018) (describing the basic concepts associated with Bitcoin technology). There are certain technological differences between major cryptocurrencies, but these differences do not undermine the legal analysis. *See* Arjun Kharpal, *All You Need to Know About the Top 5 Cryptocurrencies*, CNBC (Dec. 14, 2017, 5:28 AM), https://www.cnbc.com/2017/12/14/Bitcoin-ether-litecoin-ripple-differences-between-cryptocurrencies.html [https://perma.cc/88MW-P9UV] (describing the differences between the top five cryptocurrencies by market capitalization).

[5] *See* NAKAMOTO, *supra* note 4.

[6] *See* Bernard Marr, *A Short History Of Bitcoin and Crypto Currency Everyone Should Read*, FORBES (Dec. 6, 2017, 12:28 AM), https://www.forbes.com/sites/bernardmarr/2017/12/06/a-short-history-of-bitcoin-and-crypto-currency-everyone-should-read/#7e49051d3f27 [https://perma.cc/ZZC7-8F73] (reviewing history of online currencies prior to and following the introduction of Bitcoin).

[7] *Id.*

[8] For more information on Bitcoin mining, see *Bitcoin Mining*, BITCOIN.COM, https://www.Bitcoin.com/Bitcoin-mining [https://perma.cc/4CMS-AV9S] (last visited Apr. 17, 2018).

[9] *See* Marr, *supra* note 6. The value as of September 21, 2018 of this much Bitcoin is $67,290,300. *See Bitcoin*, COINMARKETCAP, https://coinmarketcap.com/currencies/bitcoin/ (last visited Sept. 21, 2018) (listing Bitcoin price at $6,729.03).

[10] *See* Marr, *supra* note 6 (describing emergence of Namecoin and Litecoin).

[11] Andrew Meola, *Understanding Blockchain Technology, Bitcoins and the Rise of Cryptocurrency*, BUS. INSIDER (Aug. 25, 2017, 4:36 PM), http://www.businessinsider.com/blockchain-technology-cryptocurrency-explained-2017-8 [https://perma.cc/DU5U-HYCY].

[12] For information on the security of blockchain, see Allison Berke, *How Safe Are Blockchains? It Depends.*, HARV. BUS. REV. (Mar. 7, 2017), https://hbr.org/2017/03/how-safe-are-blockchains-it-depends [https://perma.cc/4FR8-Z6VD].

which are stored in the blockchain—the agnostic public registry of all transactions. To designate ownership, Bitcoin owners rely on public and private keys: the public key is used to receive Bitcoin and can be safely published anywhere, while the private key is used to send Bitcoin and must be secured and protected.[13] Both keys allow users to access their portion of the blockchain, and are stored in one's digital wallet.[14] This information can be stored using a web-based (hot) wallet, or when large cryptocurrency values are at stake, in a more secure offline (cold) wallet such as a USB drive.[15]

B. *The Growing Problem of Cryptotheft*

Hackers targeting cryptocurrency have stolen massive sums of money, and these heists are only growing larger. In January of 2018, 500 million XEM (a blockchain-based currency)—worth $533 million—were lifted from a Japanese cryptocurrency exchange.[16] This was just one of "[a]t least three dozen heists on cryptocurrency exchanges since 2011" with over 980,000 Bitcoins stolen and few recovered.[17] The largest prior cryptoheist caused the bankruptcy of Mt. Gox, a Tokyo-based exchange, and led to an international collapse of cryptocurrency prices.[18] The 2018 XEM theft hardly impacted the cryptocurrency market—a statement of the world's increasing dependence on cryptocurrency. Given that cryptocurrencies are here to stay, it is concerning that "[h]ackers have compromised more than 14% of the Bitcoin and ether supply," and that "crypto hacking is a $200-million annual revenue industry."[19] This form of crime has cost companies and governments $11.3 billion in illegitimate transactions and lost tax revenue.[20]

Hackers not only target individuals and exchanges that hold Bitcoin, but they go after cryptocurrencies before the coins even reach the public, stealing

[13] *See* Fred M., *Bitcoin Wallets Explained: How to Choose the Best Wallet for You*, ASIC NEWS (Nov. 14, 2017), https://asicnews.com/guides/Bitcoin-wallets-explained-choose-best-wallet/ [https://perma.cc/G9W3-TLJ4].

[14] *Id.*

[15] *Id.*

[16] Henry Kenyon, *More Than $500 Million Stolen in Japanese Cryptocurrency Heist*, CONG. Q. ROLL CALL (Jan. 29, 2018), 2018 WL 578949.

[17] Jemima Kelly & Tommy Wilkes, *Exclusive: Coincheck Hackers Trying to Move Stolen Cryptocurrency – Executive*, REUTERS (Jan. 30, 2018, 8:08 AM), https://www.reuters.com/article/us-japan-cryptocurrency-cybercrime/exclusive-coincheck-hackers-trying-to-move-stolen-cryptocurrency-executive-idUSKBN1FJ28Y [https://perma.cc/ZG2L-GSD5].

[18] *Id.*

[19] Olga Kharif, *Hackers Have Stolen About 14% of Big Digital Currencies*, L.A. TIMES (Jan. 18, 2018, 11:30 AM), http://www.latimes.com/business/la-fi-bitcoin-stolen-hackers-20180118-story.html [https://perma.cc/A43N-7XDC].

[20] *Id.*

directly from Initial Coin Offerings (ICOs).[21] This can be done via "denial of service attacks, hacking web applications and exchanges, and breaching the accounts of people linked to companies running the ICOs."[22] And while American policing authorities have responded lethargically to this growing body of cryptothreats, private institutions are beginning to fill the void. For instance, "[m]ajor global insurers are starting to offer protection against cryptocurrency theft."[23] This is no light task for insurance companies: "the challenge is how to cover those risks for customers they know little about, who use technology few understand and represent a young industry that lacks troves of data insurers usually rely on in designing and pricing coverage."[24]

C. *Forays into Criminal and Civil Prosecution*

Because cryptocurrency theft involves the unauthorized discovery of an owner's private key, it is difficult to legally characterize as theft. The private key itself has no value, beyond unlocking access to however many Bitcoins the owner may possess under that key. Law enforcement has been demonstrably skeptical of pursuing investigations of cryptotheft, likely in part because Bitcoin is not by definition currency[25] and its theft does not fit into a neat legal box.[26] In one report from 2011, the FBI referred to a hacked and pilfered cryptocurrency platform as an alleged "computer intrusion," rather than theft.[27] There have been multiple instances of FBI investigations, but it is unclear if the investigators take this form of crime seriously.[28] The

[21] *See* Henry Kenyon, *Report: Hackers Target Cryptocurrency Funding Efforts*, CONG. Q. ROLL CALL (Jan. 23, 2018), 2018 WL 506079 (describing the rise of cybercriminal efforts targeting ICOs).

[22] *Id.*

[23] Suzanne Barlyn, *Insurers Gingerly Test Bitcoin Business with Heist Policies*, REUTERS (Feb. 1, 2018, 1:13 AM), https://www.reuters.com/article/us-markets-Bitcoin-insurance-insight/insurers-gingerly-test-Bitcoin-business-with-heist-policies-idUSKBN1FL406 [https://perma.cc/F2R4-XQWN] (explaining that insurers spend more time reviewing potential clients involved in the cryptomarket).

[24] *Id.* This is an extensive process that involves scrutinizing the client's storage, security, scale, and even employees. *Id.*

[25] *See* John Kelleher, *Why Do Bitcoins Have Value?*, INVESTOPEDIA (Mar. 7, 2018, 1:50 PM), https://www.investopedia.com/ask/answers/100314/why-do-Bitcoins-have-value.asp [https://perma.cc/8F5M-FNS9] (offering a model that values bitcoin both as currency and as a store of value).

[26] *See* Jason Leopold, *If Your Bitcoins Are Stolen in a Major Hack, Will the FBI Help?*, VICE (Feb. 9, 2017, 8:00 AM), https://www.vice.com/en_us/article/ypnn3g/if-your-Bitcoins-are-stolen-in-a-major-hack-will-the-fbi-help-v24n1 [https://perma.cc/3D9W-LTTM] (detailing the lack of an effective FBI response to an incident of cryptocurrency theft via hacking).

[27] *Id.*

[28] *See, e.g.*, Stan Higgins, *The FBI is Investigating a $1.3 Million Bitcoin Theft*, COINDESK (Oct. 6, 2016, 9:05 PM), https://www.coindesk.com/the-fbi-is-investigating-a-1-3-million-Bitcoin-theft/ [https://perma.cc/B24B-JHG5] (describing pending investigation into computer intrusion, but noting that the "status of the investigation and the extent to which the FBI has pursued the lead remains unknown").

FBI has shown more willingness to pursue action against those who redistribute Bitcoin without a license to do so,[29] or against those who employ ransomware to remotely lock computers.[30] The FBI and other relevant authorities should and likely will pay increasing attention to cryptotheft. In support of increased prioritization, a report from President Obama's Commission on Enhancing National Cybersecurity found that "we must move the responsibility for (or burden of) cybersecurity away from individual enterprises and citizens, and handle it at higher levels for everyone's benefit."[31]

Criminal actions have only tangentially circled the field of cryptotheft. For example, in January of 2018, a federal prosecutor brought criminal charges of wire fraud against a Chicago trader who allegedly stole $2 million worth of his firm's cryptocurrency holdings for personal use.[32] He then lied to the firm's management about the location of the company's cryptocurrency and his own trading.[33] Although this was one of the first known instances of direct federal prosecution of cryptocurrency theft, it seems more closely aligned with prosecutions of corporate misappropriation. In a similar 2018 case, the Commodities Futures Trading Commission pressed charges against a defendant corporation for "misappropriating over $6 million from at least twenty-eight customers by transferring customer funds into personal bank accounts, and using those funds for personal expenses and the purchase of luxury goods."[34] The case was about misrepresentation, consumer abuse, and unfair practices, not theft. These examples fit a trend among known prosecutions: none embody the paradigmatic case of cryptotheft characterized by offsite hacking by a third party with the goal of obtaining access to an entity's wallet to steal its private key and designate new ownership of its cryptocurrency. There is an ever-growing need to prosecute the direct theft of cryptocurrency, as thieves have gone so far as to engage in home invasions in pursuit of cryptoassets. For example, in Britain, armed

[29] *See, e.g.*, *Virtual Ticket to Prison: Investigation of Fraud Scheme Unravels Man's Illegal Bitcoin Exchange*, FED. BUREAU OF INVESTIGATION (May 3, 2017), https://www.fbi.gov/news/stories/fraud-scheme-leads-to-illegal-bitcoin-exchange [https://perma.cc/68Y3-R5RN] (detailing the FBI's arrest of Daniel Mercede for redistribution of bitcoin without a license).

[30] *See* Michael del Castillo, *To Catch a Ransomer: How the FBI Chases Crime on the Blockchain*, COINDESK (Feb. 1, 2017, 2:00 PM), https://www.coindesk.com/catch-Bitcoin-ransomer-inside-fbis-cyber-investigation-process/ [https://perma.cc/3N8V-4WGL] (providing an overview of an FBI agent's approach to identifying and pursuing criminals using cryptocurrency ransomware).

[31] David N. Lawrence et al., Special Comment, *It's the Cyber Crime and Its Sponsors (Not My Cyber-Security), Stupid*, 5 J.L. & CYBER WARFARE 1, 15 (2017).

[32] Press Release, U.S. Attorney's Office for the Northern District of Illinois, Chicago Trader Facing Federal Fraud Charge for Allegedly Misappropriating $2 Million in Cryptocurrencies (Feb. 15, 2018), https://www.justice.gov/usao-ndil/pr/chicago-trader-facing-federal-fraud-charge-allegedly-misappropriating-2-million [https://perma.cc/P3RK-R6EJ].

[33] *Id.*

[34] COMMODITY FUTURES L. REP. 1057 (Feb. 13, 2018), 2018 WL 817353.

men broke into the home of a cryptotrader and forced him at gunpoint to transfer his assets.[35]

Federal prosecutors recently brought charges of "operation of an unlicensed money service business," "conspiracy to commit money laundering," "money laundering," and "engaging in unlawful monetary transactions" against a Russian national, Alexander Vinnik.[36] Vinnik operated a Bitcoin currency exchange, known for illicit dealings, which helped launder Bitcoin stolen from Mt. Gox.[37] Despite a competing extradition request from Russia, Vinnik will face trial in the United States.[38] As evidenced by the charges, Vinnik's prosecution turns on his conversion of illicit Bitcoin into official currency—not the actual theft of the Bitcoin—demonstrating the limits of current legal theories.

Victims of cryptotheft have limited civil recourse. In a rare example of a civil suit, a Sprint customer sued the phone company after his phone was hacked and $360 million worth of cryptocurrency was stolen as a result.[39] The plaintiff asserted that Sprint made representations of cybersecurity, did not live up to its promises, and did not respond to his requests to freeze his account.[40] The complaint asserted negligence, breach of contract, breach of confidentiality, and violations of California's unfair competition and customer records laws.[41] While these assertions are certainly civil tools that victims of cryptocurrency theft may use to obtain compensation, they involve indirect and uphill battles that fail to hold the direct perpetrators accountable, facilitate increased damages, or impose criminal penalties.

An indicative incident of cryptotheft is seen in *Bittrex, Inc. v. Muller*, an arbitration over domain name trademark infringement. The defendant

[35] *See* Maev Kennedy, *Cryptocurrency Trader 'Forced at Gunpoint to Make Bitcoin Transfer'*, THE GUARDIAN (Jan. 28, 2018, 12:47 PM), https://www.theguardian.com/uk-news/2018/jan/28/cryptocurrency-trader-forced-at-gunpoint-to-make-bitcoin-transfer [https://perma.cc/X46Z-YU8J].

[36] Press Release, U.S. Attorney's Office for the Northern District of California, Russian National And Bitcoin Exchange Charged In 21-Count Indictment for Operating Alleged International Money Laundering Scheme and Allegedly Laundering Funds from Hack of Mt. Gox (July 26, 2017), https://www.justice.gov/usao-ndca/pr/russian-national-and-bitcoin-exchange-charged-21-count-indictment-operating-alleged [https://perma.cc/5PPE-MRWH].

[37] *Id.*

[38] *See Greek Top Court Clears Way for U.S. Extradition of Russian Cybercrime Suspect*, REUTERS (Dec. 13, 2017, 7:34 AM), https://www.reuters.com/article/us-greece-russia-extradition/greek-top-court-clears-way-for-u-s-extradition-of-russian-cybercrime-suspect-idUSKBN1E71K7 [https://perma.cc/63NG-HJV7] (detailing Vinnik's extradition to the United States, rather than to Russia).

[39] Dave Embree, *Sprint Negligently Failed to Protect Phone from Hackers, Suit Says*, WESTLAW DATA PRIVACY DAILY BRIEFING (Dec. 27, 2017), 2017 WL 6601899.

[40] Complaint at ¶¶ 4-5, McCarthy v. Sprint Corp., No. 2:17-09116, 2017 WL 6520978 (C.D. Cal. Dec. 20, 2017).

[41] *Id.* at ¶¶ 35, 51, 63, 72, 80, 86.

used domain names "to impersonate [the] Complainant in order to fraudulently obtain [the] Complainant customers' user identification and password credentials and steal from their cryptocurrency accounts."[42] The victims' only recourse, the seizure of the stolen domain name, did little to remedy the cryptotheft they suffered.

While the first civil and criminal prosecutions have tangentially dealt with cryptotheft, the core threat remains unaddressed. One of the primary reasons authorities have not prosecuted offsite cryptotheft is the mistaken belief that federal laws do not adequately cover this form of crime.[43] Significantly, "law enforcement agencies remain undecided as to whether or not stealing digital currency constitutes a crime."[44]

I. APPLYING THE DTSA

The DTSA was signed into law by President Obama on May 11, 2016, after moving through Congress remarkably quickly and with bipartisan support.[45] In his remarks, Obama noted that "one of the biggest advantages that we've got in this global economy is that we innovate, we come up with new services, new goods, new products, new technologies" and that the Act would protect against the theft of these assets.[46] At the time it was passed, the DTSA was called the "most significant expansion of federal law in intellectual property since the Lanham Act in 1946," but its practical impact has been limited.[47] This Act is the perfect tool for prosecuting cryptotheft both civilly and criminally.

[42] Bittrex, Inc. v. Muller, FA1801001768933, 2018 WL 1284549 at *2 (UDRP-ARB Feb. 26, 2018).

[43] Certain states have redefined currency to include cryptocurrency, or are considering doing so, which may provide prosecutors a legal vehicle to pursue individuals engaged in cryptotheft. *See* Leyla Amur, *CSI Crypto: Can Victims Recover Stolen Coin?*, BRAVE NEW COIN (Oct. 13, 2017), https://bravenewcoin.com/news/csi-crypto-can-victims-recover-stolen-coin/ [https://perma.cc/SQ3D-8UXL] (listing states that have broadened their definitions of currency to include cryptocurrency).

[44] *Id.*

[45] *See* Press Release, The White House Office of the Press Secretary, Remarks by the President at Signing of S. 1890—Defend Trade Secrets Act of 2016 (May 11, 2016), https://obamawhitehouse.archives.gov/the-press-office/2016/05/11/remarks-president-signing-s-1890-defend-trade-secrets-act-2016 [https://perma.cc/7ESC-5GZ6] ("What these members of Congress have done is to, on a bipartisan basis, pass a strong enforcement bill that allows us not only to go after folks who are stealing trade secrets through criminal actions, but also through civil actions, and hurt them where it counts in their pocketbook.").

[46] *Id.*

[47] Bradford K. Newman et al., *The Defend Trade Secrets Act: One Year Later*, BUS. L. TODAY (Apr. 2017), https://www.americanbar.org/publications/blt/2017/04/02_newman.html [https://perma.cc/X39L-926C].

A. *Is Cryptocurrency Really a Trade Secret?*

According to the DTSA, located within the Economic Espionage Act (EEA):

> [T]he term "trade secret" means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if—
>
> > (A) the owner thereof has taken reasonable measures to keep such information secret; and
> >
> > (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information . . . .[48]

The answer to this question—whether cryptocurrency is really a trade secret—is, quite simply, yes. The owner's use of a private key to send currency meets multiple paths to eligibility under this expansive definition. The technical information (the key), in combination with a publicly stored ledger that is intangible and stored electronically, is kept secret by one's digital wallet or by a public exchange, and derives very significant economic value from its not being known nor being readily ascertainable by proper means.

Perhaps the strongest counterargument to this description of cryptocurrency is the complete publicity of the blockchain ledger. However, it is the secrecy of the key necessary to designate ownership of the coin that creates the value, in combination with the public information. The Ninth Circuit, when construing the EEA, wrote:

> [A] trade secret may consist of a compilation of data, public sources or a combination of proprietary and public sources. It is well recognized that "it is the secrecy of the claimed trade secret as a whole that is determinative. The fact that some or all of the components of the trade secret are well-known does not preclude protection for a secret combination, compilation, or integration of the individual elements.[49]

Thus, the trade secret is not the coin itself, but the ability to send the coin via a private key. The trade secret definition is flexible enough to escape the

[48] 18 U.S.C. § 1839 (3) (2016).

[49] United States v. Nosal, 844 F.3d 1024, 1042 (9th Cir. 2016) (quoting RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 cmt. f (1995)), *cert. denied*, 138 S. Ct. 314 (2017).

pitfalls of laws designed to target standard theft. The similarly expansive definition of "misappropriation" under the DTSA encapsulates the many ways in which crypto-owners' assets could be hacked or taken.[50] In fact, the statute expressly defines "improper means" as including "espionage through electronic or other means."[51]

B. *Benefits of the DTSA Structure*

The DTSA creates a comprehensive scheme, authorizing both civil and criminal penalties for the misappropriation of trade secrets. Beyond the penalty structures, the Act includes provisions that uniquely address many of the problems inherent in prosecuting theft of cryptocurrency. These provisions allow for speedy and private ex parte seizure of stolen assets, protect the confidentiality of the trade secret and ancillary information, and incent strong cybersecurity practices by cryptocurrency owners. This structure is both practically and conceptually preferable to other legal schemes.

1. Criminal and Civil Liability

Criminally, the DTSA provides a neat, effective, and on-point tool for federal prosecutors to use when tracking hackers. Civilly, entities are given the opportunity to directly pursue the perpetrator, and to seek enhanced relief. This is not necessarily the case under any other scheme because of the unique technical configuration of cryptocurrency.

It is a crime to steal, misappropriate, or without authorization obtain a trade secret, with intent or knowledge that doing so will injure the owner.[52] The Act also covers attempt or conspiracy to commit such theft. The culprit shall be imprisoned for up to ten years or "fined not more than the greater of $5,000,000 or three times the value of the stolen trade secret to the organization, including expenses for research and design and other costs of reproducing the trade secret that the organization has thereby avoided."[53] As a result of these forceful punishments, the DTSA could be used to deter cryptotheft. Importantly, it includes the cost of reproducing the trade secret, allowing the government to account for the substantial expenses a victim has taken to mine and protect the cryptocurrency.

Similarly, an "owner of a trade secret that is misappropriated may bring a *civil action* under this subsection if the trade secret is related to a product or

[50] *See* 18 U.S.C. § 1839 (5) (2016) (expanding the scope of "misappropriation" to cover a wide array of possible intentional or knowing trade secret disclosures and uses).

[51] *Id.* § 1839 (6).

[52] *Id.* § 1832 (a)(1).

[53] *Id.* § 1832 (a)–(b).

service used in, or intended for use in, *interstate or foreign commerce*."[54] Cryptocurrencies are thus subject to regulation because coin ownership is exchanged both between states and between countries. Once a trade secret is part of interstate trade, the statute provides for civil seizure, injunctive relief, damages for the actual loss, unjust enrichment, or the creation of liability to third parties.[55] Furthermore, "if the trade secret is willfully and maliciously misappropriated," which would almost always be the case in cryptotheft, the court may "award exemplary damages in an amount not more than 2 times the amount of the damages . . . ."[56]

2. Ex Parte Seizures

One of the most pressing problems plaguing cryptotheft is the rapid dispersal of assets once stolen. This is evident from the XEM heist,[57] where authorities have only been able to identify these coins after layers of selloffs. The DTSA addresses the possibility of a redistribution of stolen coin by incorporating an ex parte seizure provision, when such a procedure is "necessary to prevent the propagation or dissemination of the trade secret that is the subject of the action."[58] This provision allows for the immediate and completely confidential court-ordered seizure of assets.

To apply for the order, the moving party must first show that an order under Rule 65 of the Federal Rules of Civil Procedure would be inadequate.[59] Rule 65 describes the power to grant preliminary injunctions and temporary restraining orders.[60] This is almost always true in cases of cryptotheft, because the thief would be found likely to "evade, avoid, or otherwise not comply with such an order."[61] Second, the movant must show that "an immediate and irreparable injury will occur" without seizure.[62] This is also probable given the ability to rapidly sell, hide, or disseminate cryptocurrency. Third, the weighing of harms must favor the movant over the legitimate interests of the person from whom it is seized and must "substantially outweigh" the harm to third parties.[63] This balancing of equities may become a problem after the coin has been sold without knowledge by the buyer, but if done early enough the balancing will clearly favor the movant. Fourth, the movant must be likely

[54] *Id.* § 1836 (b)(1) (emphasis added).

[55] *Id.* § 1836 (b)(3)(B).

[56] *Id.* § 1836 (b)(3)(C).

[57] *See supra* text accompanying notes 16–17.

[58] 18 U.S.C. § 1836 (b)(2)(A)(i) (2016).

[59] *Id.* § 1836 (b)(2)(A)(ii)(I).

[60] *See* Fed. R. Civ. P. 65(a)–(b) (defining standards for issuance of injunctions and restraining orders).

[61] 18 U.S.C. § 1836 (b)(2)(A)(ii)(I) (2016).

[62] *Id.* § 1836 (b)(2)(A)(ii)(II).

[63] *Id.* § 1836 (b)(2)(A)(ii)(III).

to succeed on the merits, showing that the person against whom seizure is ordered misappropriated an actual trade secret by improper means.[64] In a quintessential case of hacking, this will not be hard to demonstrate. Fifth, the person must have actual possession of the trade secret.[65] This is likely to be the case if the order is granted immediately after the theft but may prove technically difficult. Sixth, the movant must describe "with reasonable particularity the matter to be seized and, to the extent reasonable under the circumstances, identif[y] the location where the matter is to be seized . . . ."[66] This requirement will present the largest obstacle, given the practical difficulties in identifying the cyber location of the cryptothief. Still, it is likely that the circumstantial difficulty of providing a precise location will allow the court to still issue the order. Seventh, notice must make it likely that the stolen property would be destroyed, moved, hidden, or made inaccessible.[67] This is highly probable given the capacity to redistribute cryptocurrency. Lastly, the applicant cannot publicize the requested seizure.[68]

This ex parte seizure procedure provides cryptocurrency owners with an incredibly powerful and unique tool to recover their stolen coins. While practical difficulties remain, this provision puts the owner in the best legal position to recover the stolen coins, rather than forcing him or her to sue for replacement cost. A damages suit is likely to be particularly problematic due to the possibility of judgment-proof defendants.

3. Confidentiality

The Act provides for the protection of confidentiality in two important regards. First, in ex parte seizure proceedings the thief is shielded from any knowledge of the proceedings. Second, the contents of and information peripheral to the trade secret are protected throughout and beyond the litigation.[69] This protects the secrecy of the private key as well as other confidential information, potentially including the number of assets lost or the identity of the owner, so that the owner does not become a target of future heists.

The ex parte seizure procedure includes inherent confidentiality protections against any form of publicity, especially to the perpetrator. This confidentiality prevents the moving, hiding, or transferring of stolen cryptoassets. It also protects the victim from harms related to publicity.[70]

[64] *Id.* § 1836 (b)(2)(A)(ii)(IV).

[65] *Id.* § 1836 (b)(2)(A)(ii)(V).

[66] *Id.* § 1836 (b)(2)(A)(ii)(VI).

[67] *Id.* § 1836 (b)(2)(A)(ii)(VII).

[68] *Id.* § 1836 (b)(2)(A)(ii)(VIII).

[69] *See infra* text accompanying notes 72–75.

[70] *See, e.g.*, *At the End of Your Tether: Addressing, Responding to and Insuring Cryptocurrency Theft*, REEDSMITH (Dec. 5, 2017), https://www.reedsmith.com/en/perspectives/2017/12/addressing-

There is risk to alerting the public of possession of significant cryptoassets. Cryptothieves have been known to go so far as home invasion to steal coins, and a public statement of ownership invites targeting by bad actors.[71] Publicity would also cause public relations and reputational harm to individuals and groups responsible for protecting the cryptoassets of others. This legal tool is therefore an attractive option for an entity who may waver on pursuing legal action without the guarantee of confidentiality. While this complete confidentiality may not always extend to the later stages of litigation, ideally the assets can be returned via an ex parte seizure before the public is aware that anything occurred.

Second, the trade secret and related information are protected by "[o]rders to preserve confidentiality."[72] Under this provision, "the court shall enter such orders and take such other action as may be necessary and appropriate to preserve the confidentiality of trade secrets."[73] This protection is likely expansive enough to cover more than just the private key; it may also protect the number of assets, the type of asset, where and how the assets are stored, and any other information the owner feels worthy of protection. The Act holds that "[t]he court may not authorize or direct the disclosure of any information the owner asserts to be a trade secret unless the court allows the owner the opportunity to file a submission under seal that describes the interest of the owner in keeping the information confidential."[74] This means that even as the suit progresses, a party will be able to maintain expansive public-facing confidentiality. Further, the Act mandates specific technical procedures be followed regarding the protection of confidentiality, including the appointment of a special master bound by a nondisclosure agreement and the possibility of encrypting stored materials.[75] This generous confidentiality protection is an incredibly valuable tool for parties afraid of inviting attacks or staining a public image of cybersecurity.

responding-to-and-insuring-cryptocurrency-theft [https://perma.cc/FW72-5M86] ("The Tether hack illuminates the privacy, reputational, financial and recovery risks associated with issuing, owning and storing digital currencies.").

[71] *See Cryptocurrency Theft Presents New Challenge for Law Enforcement*, ORGANIZED CRIME AND CORRUPTION REPORTING PROJECT (Feb. 21, 2018, 4:07 PM), https://www.occrp.org/en/daily/7679-cryptocurrency-theft-presents-new-challenge-for-law-enforcement [https://perma.cc/7PNG-GHBS] ("Crypto celebrities are becoming red hot targets as criminals begin to realize that they're more likely to score a huge payday by extorting someone with crypto assets than they are someone with more traditional assets that are illiquid . . . .").

[72] 18 U.S.C. § 1835(a) (2016).

[73] *Id.*

[74] *Id.* § 1835(b).

[75] *Id.* § 1836 (b)(2)(D), (H).

4. Cybersecurity as a Prerequisite to Civil Protection

If the United States government is to expend resources in the civil protection of cryptoassets, it should encourage robust private cybersecurity. Inherent in the private enforcement of trade secret misappropriation is the requirement that the plaintiff had reasonable security measures in place to protect the confidentiality of the secret.[76] In this case, that would include protecting, at the very least, the private key. The DTSA furthers this priority by incorporating longstanding trade secret law, which requires reasonable security measures.[77] This standard of reasonableness should and likely would vary based on the value of the assets stored. Owners would be expected to protect their assets to a degree commensurate with the assets held.

No court has ruled on what would constitute statutorily sufficient cryptocurrency protection, and the answer would likely be situation specific.[78] However, many commentators have described best practices for protecting one's cryptoassets, and these can easily be extrapolated to legal requirements for trade secret protection. For instance, a firm trading in cryptocurrency should (1) "[n]ever transmit keys electronically;" (2) "[l]imit trading authorization" to only necessary employees; and (3) "[m]anage keys with a secure electronic wallet."[79] These suggestions may go beyond or fall short of what would be statutorily required, but they still constitute good advice for companies seeking to be certain of legal protection.

An important cybersecurity decision for courts is whether to require plaintiffs to store assets in a hot or cold wallet. The simplest definition of a hot wallet is one connected to the internet, while a cold wallet is one that is disconnected from the internet.[80] Cold wallets are much less convenient, but much more secure. Standard advice calls for storing the majority of

[76] *See* Michelle L. Evans, *Proof of Facts to Establish Information as Trade Secret Under Restatement of Torts*, 134 AM. JUR. PROOF OF FACTS 3d 321, § 8 (2018) ("The greater number of measures used by the trade secret owner to guard the secrecy of company information, the greater likelihood the information will be treated as a trade secret. If the company does not provide sufficient security measures for its information, the information will not be given trade secret status.").

[77] 18 U.S.C. § 1839(3)(A) (2016).

[78] One could expect a different degree of protection reasonable for a cryptocurrency exchange with cryptoassets worth billions of dollars, compared to an individual holding a few thousand dollars' worth of Bitcoin.

[79] Edmund Mokhtarian & Alexander Lindgren, *Rise of the Crypto Hedge Fund: Operational Issues and Best Practices for an Emergent Investment Industry*, 23 STAN. J.L. BUS. & FIN. 112, 155-56 (2018). These authors suggest a wallet capable of "sweeping." This means that the wallet, when "importing . . . private keys 'sweeps,' or generates a new transaction on the applicable blockchains and, in turn, creates new private keys that are then available only inside of that wallet." *Id.* at 156.

[80] Leah Stella Stephens, *Cold Wallet vs. Hot Wallet: What's the Difference?*, MEDIUM (Apr. 9, 2017), https://medium.com/dash-for-newbies/cold-wallet-vs-hot-wallet-whats-the-difference-a00d872aa6b1 [https://perma.cc/4GD8-LCFR].

one's funds in a cold wallet and a few funds that are actively traded in a hot wallet.[81] This puts as little coinage at risk as possible. This practical advice would likely inform trade secret protection, though it would vary based on the owner's circumstances. Most hot wallets have robust cybersecurity protection, so a small-scale cryptotrader would likely be protected even if all of his assets were stored hot. However, a large-scale trader, trading firm, or public exchange may be deemed unreasonable for storing all or most of their assets in a hot wallet, when it would be relatively economical to implement a majority cold-storage system. Regardless of where the court draws the line, parties would be incentivized to implement a safe but economically reasonable cybersecurity mechanism.

C. *Superiority of the DTSA over Other Legal Schemes*

While this Comment does not argue that the DTSA is the only legal scheme that could plausibly be used to prosecute the theft of cryptocurrency, it does contend that it is both practically and theoretically preferable to other options. Practically, no other scheme includes the built-in confidentiality, seizure, and cybersecurity elements of the DTSA. Furthermore, the DTSA is one of very few avenues for private federal civil suit. Theoretically, while a competing "property" conceptualization of the private key has a degree of persuasiveness, this characterization does not account for what is actually stolen, which is not the physical possession of a key or even the Bitcoin, but the ability to label a portion of a public ledger. For these reasons, the theft of cryptocurrency is best described as intellectual property misappropriation.[82]

Civilly, plaintiffs may have the option of bringing a state claim, and some states have even begun statutorily labeling cryptocurrency as currency for certain purposes.[83] In the prototypical case of cryptotheft, because the

[81] *Id.*

[82] The Commodities Futures Trading Commission has classified Bitcoin as a commodity, while the Securities Exchange Commission has taken steps to treat it as a security. *See* Jacob J, *US Regulators Debate Whether Bitcoin is Commodity or Security*, COINTELEGRAPH (Oct. 19, 2017), https://cointelegraph.com/news/us-regulators-debate-whether-Bitcoin-is-commodity-or-security [https://perma.cc/6ATR-HZ4Z] (detailing the debate over proper classification of digital currencies); *see also* Public Statement, Jay Clayton, Chairman, U.S. Sec. & Exch. Comm'n, Statement on Cryptocurrencies and Initial Coin Offerings (Dec. 12, 2017), https://www.sec.gov/news/public-statement/statement-clayton-2017-12-11 [https://perma.cc/7YXZ-WSWK] ("It has been asserted that cryptocurrencies are not securities and that the offer and sale of cryptocurrencies are beyond the SEC's jurisdiction. Whether that assertion proves correct with respect to any digital asset that is labeled as a cryptocurrency will depend on the characteristics and use of that particular asset."). This Comment does not weigh in on the debate, nor does it believe that its advocacy for criminal and civil DTSA prosecution affects either proposed regulatory classification.

[83] *See, e.g.*, W. VA. CODE § 61-15-1(3) (2017) (defining cryptocurrency, in the context of money laundering, as "digital currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, and which operate independently of a central bank").

defendant is foreign, diversity jurisdiction in federal court may be proper over such a state claim. However, it is improbable that any state has a scheme covering a comparable scope of cryptotheft as the DTSA, and even less probable that these schemes would include the private seizure, confidentiality, and requisite cybersecurity of the DTSA.

In the federal context, as courts have described, cryptocurrency cannot be easily defined as official currency. For instance, in *United States v. Petix*[84] the "Government's theory of prosecution require[d] treating Bitcoin as money in the ordinary understanding of that term. Because Bitcoin does not fit an ordinary understanding of the term 'money,' Petix cannot have violated Section 1960[85] in its current form."[86] This district court described Bitcoin as analogous to "marbles, Beanie Babies™, or Pokémon™ trading cards [in that] bitcoins have value exclusively to the extent that people at any given time choose privately to assign them value."[87] While this is an incomplete comparison, it demonstrates well the lack of inherent value to cryptocurrency.

Wire Fraud offers one of the best alternatives for federal criminal prosecution.[88] Under this statute, it is a crime

> to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire . . . in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice . . . .[89]

This definition would likely cover most instances of cryptotheft, but only if cryptocurrency can be defined as property.[90] Defining Bitcoin as property is a contentious issue that makes this statute difficult to apply.[91]

[84] No. 15-227A, 2016 WL 7017919 (W.D.N.Y. Dec. 1, 2016).

[85] *See* 18 U.S.C. § 1960 (2016) (describing the "[p]rohibition of unlicensed money transmitting businesses").

[86] *Petrix*, 2016 WL 7017919, at *6. *But see* Memorandum Opinion Regarding the Court's Subject Matter Jurisdiction at 3, SEC v. Shavers, No. 4:13-416 (E.D. Tex. Aug. 6, 2013) ("[Bitcoin] can also be exchanged for conventional currencies, such as the U.S. dollar, Euro, Yen, and Yuan. Therefore, Bitcoin is a currency or form of money, and investors wishing to invest in [Bitcoin Savings and Trust] provided an investment of money.").

[87] *Petix*, 2016 WL 7017919, at *5-6.

[88] 18 U.S.C. § 1343 (2012).

[89] *Id.*

[90] It should be noted that the stolen coin could be labeled an "honest service" under the Wire Fraud statute. *See* 18 U.S.C. § 1346 (2012) ("For the purposes of this chapter, the term 'scheme or artifice to defraud' includes a scheme or artifice to deprive another of the intangible right of honest services."). This interpretation would likely stretch the intent of this statutory expansion.

[91] *See generally* Kelvin FK Low & Ernie GS Teo, *Bitcoins & Other Cryptocurrencies as Property?*, 9 LAW INNOV. & TECH. 235, 245-54 (2017) (discussing how attempts at defining Bitcoin as property are challenged by the intangible nature of Bitcoin and the presumption of the law against conceptualizing confidential information, such as cryptographic keys, as property).

Alternatively, the private key itself could be described as the property being defrauded. This conception, while more plausible, suffers at a theoretical level in two primary ways. First, the private key on its own has no value. Second, the key is not an entity unto itself, but the embodiment of the capability to perform a specific action. It therefore takes the form its owner desires. The key could even consist of an ever-changing output of a random sequence generator. The private key is therefore only a representation of the ability to designate new ownership of a publicly viewable cryptocoin, and such a power is wholly intangible. While stealing a complex physical or even digital key and using it to break into a safe to take the assets inside would undoubtedly be a crime, this situation is far less clear.

To understand this conceptualization, let's imagine a one-coin cryptocurrency blockchain as a sheet of paper posted in the center of a town. This paper can only be written on by a special and secret type of ink (the private key) known only by the highest name appearing on the paper. If I, improperly and without permission, learn what the special ink is, write my name above the previous name, and thereby designate my own secret ink, what have I stolen? I haven't really stolen anything, but I've improperly commandeered the secret ability to write on the ledger. This ability to write on the ledger, conferred by knowledge of the secret ink (private key), has no inherent value other than the speculative value society places on it, and thus escapes typical definitions of property. It is best described as a trade secret.

II. Obstacles to Prosecuting Cryptotheft

There are two primary obstacles to effectively enforcing the DTSA against cryptocurrency thieves. First, there are statutory and constitutional barriers to establishing and enforcing jurisdiction over foreign defendants who have never set foot in the United States. This concern is largely alleviated by the expansiveness of the DTSA wording and case law establishing broad personal jurisdiction under the EEA. Second, there are practical challenges to enforcing a judgment over hidden digital assets. This technical barrier is reduced by the immediacy of the ex parte procedure and can be overcome with sufficient investment in tracking down these bad actors.

A. *Extraterritoriality of the DTSA*

The DTSA incorporates the same scope of jurisdiction as the EEA, meaning trade secret theft is covered if

> (1) the offender is a natural person who is a citizen or permanent resident alien of the United States, or an organization organized under the laws

> of the United States or a State or political subdivision thereof; or (2) an act in furtherance of the offense was committed in the United States.[92]

The challenge in enforcing this Act will arise under clause two, in demonstrating that a foreign actor's computer hacking constitutes an action in the United States.

While few prosecutions test the range of this statute, *United States v. Sinovel Wind Group Co.*[93] provides important instruction on the scope of the DTSA. In *Sinovel*, the defendant was charged with pilfering computer source code from a competitor and filed a motion to dismiss for improper service and a lack of jurisdiction.[94] The Seventh Circuit approved of jurisdiction (by declining appellate review) when the jurisdictional contacts of the defendant were only via a subsidiary located in the United States.[95] While the facts are not exactly parallel to those of cryptothieves, the idea of exercising international jurisdiction to protect the necessary scope of the law is relevant in both contexts.

To find jurisdiction, the second prong must be interpreted to include a foreign entity engaged in offsite hacking.[96] Further, there must be constitutionally sufficient personal jurisdiction over this statutory jurisdiction.[97] Statutory subject matter jurisdiction is met when a private key is misappropriated from a server in the United States. This is a novel question of statutory interpretation, but the situation fits with the wording and the intention of Congress, which was to protect domestic secrets from unfair foreign behaviors. However, if the hacker targets a server belonging to a United States citizen but located overseas, statutory jurisdiction is unlikely. There are lesser degrees of interaction with United States servers that may make for a difficult decision, but it is sufficient for this Comment to note that the statutory standard would likely be met by a foreign attack on an American server.

Would personal jurisdiction lie over such a foreign attack on an American server, and if so, where would that jurisdiction lie? An obvious path around this constitutional dilemma is consent: It is unlikely a defendant in a civil suit for cryptocurrency trade secret misappropriation would appear before the court, even to assert lack of jurisdiction, for fear of apprehension for criminal

[92] 18 U.S.C. § 1837 (2016).

[93] 794 F.3d 787 (7th Cir. 2015).

[94] *Id.* at 789.

[95] *Id.*

[96] *See, e.g.*, Lulu Yilun Chen & Yuji Nakamura, *Cryptocurrency Cyber Crime Has Cost Victims Millions This Year*, BLOOMBERG (Aug. 23, 2017, 10:32 PM), https://www.bloomberg.com/news/articles/2017-08-24/cyber-criminals-extracting-a-heavy-toll-from-ethereum-advocates [https://perma.cc/Z366-GV5E] (describing the various forms of hacking attacks and their relative percentage usages).

[97] There are interesting interactions between this extraterritoriality jurisdiction analysis and the ex parte seizure proceeding, as there is a realistic possibility of a court-ordered property seizure before the party has had an opportunity to challenge jurisdiction.

misconduct. If a defendant did appear to defend himself, "it is worth investigating whether jurisdictional roadblocks would prevent meaningful use of this statutory tool."[98] Professor Robin Effron describes how modern developments in personal jurisdiction have limited the available forums for DTSA enforcement. However, Professor Effron points to *MacDermid, Inc. v. Deiter*,[99] where the Second Circuit exercised jurisdiction over an Ontario woman because she accessed a computer in Connecticut, despite being out of state.[100] The Second Circuit found that such jurisdiction affords due process under *World-Wide Volkswagen Corp. v. Woodson*[101] and *Int'l Shoe Co. v. Washington*[102] because the defendant intentionally directed her actions toward the residents of Connecticut.[103] She was aware that the servers were located in Connecticut and still chose to access them improperly.[104] Under this framework, which appears to be uncontradicted, jurisdiction over cryptotheft targeted at a known location within the United States meets due process requirements.

A final question arises: would the hacking of a server of unknown location, or of a mobile device, meet constitutional requirements? It may be straightforward to impute knowledge of location at the time of hacking, given the technical sophistication of the wrongdoers. Even if the court is unwilling to impute knowledge, jurisdiction exists when "the defendant is not subject to jurisdiction in any state's courts of general jurisdiction; and exercising jurisdiction is consistent with the United States Constitution and laws."[105] The DTSA and the Constitution thus authorize jurisdiction over a truly foreign defendant who knew he was hacking a U.S. server but did not know where in the U.S. that server was located.

The extraterritorial reach of the DTSA makes it a powerful legal tool for pursuing cryptocurrency thieves. This expansive power fits with the purpose of the Act—to protect the assets of Americans from foreign bad actors.

B. *The Technical Challenges of Finding and Returning Stolen Cryptocurrency*

Practically, it is difficult to track stolen coins, and even more difficult to return coins to their rightful owners. Hackers hide behind sophisticated layers of deception, and the architecture of cryptocurrency prevents the

[98] Robin J. Effron, *Trade Secrets, Extraterritoriality, and Jurisdiction*, 51 WAKE FOREST L. REV. 765, 773 (2016).

[99] 702 F.3d 725 (2d Cir. 2012).

[100] *Id.* at 776-77. Jurisdiction was proper in part because the Connecticut long arm statute "reaches persons outside the state who remotely access computers within the state." *Id.* at 729.

[101] 444 U.S. 286, 291 (1980).

[102] 326 U.S. 310, 316 (1945).

[103] *Macdermid*, 702 F.3d at 730.

[104] *Id.*

[105] Fed. R. Civ. P. 4(k)(2)(A)–(B).

application of administrative oversight. However, recent developments demonstrate that both public and private enforcement services are capable of overcoming these technical obstacles.

First, the immediacy of the ex parte seizure procedure may reduce any need to combat the redistribution of coins. "[T]he accounts holding the pilfered funds can be immediately identified because the virtual coins are traceable" and if the "case were a regular bank robbery, identifying the bank accounts holding the stolen money would let law enforcement easily return the funds to victims."[106] However, unlike bank accounts, suspicious cryptowallets are not connected to an identified owner, and are often hidden behind multiple IP addresses or proxies. The government has taken steps to overcome these hiding techniques. For example, in 2017 "several agencies including the FBI invested hundreds of thousands of dollars to team up with digital currency analysis company Chainalysis to help track wallet addresses of suspicious transactions made on the blockchain."[107] Companies like Chainalysis specialize in cracking the algorithms used by criminals to cover their tracks. Given adequate technical resources, the government "has the capacity to pinpoint and arrest cyber criminals."[108] One way to pinpoint criminals is to connect a digital wallet suspected of bad activity to an IP address and cross check the address with social media.[109] Private individuals working through a company like Chainanalysis may be able to do the same, but without FBI support this would likely require significant personal resources.

Alternatively, courts could attempt to force certain non-DLT cryptocurrency administrators to rewrite their virtual ledgers to immediately return stolen coin. While this is not possible for Bitcoin (a DLT),[110] the NEM

[106] Tyler Durden, *How Do You Hide Stolen Cryptocurrency?*, ZEROHEDGE (Feb. 3, 2018), https://www.zerohedge.com/news/2018-02-03/how-do-you-hide-stolen-cryptocurrency [https://perma.cc/VPP9-LNUD].

[107] *See* Amur, *supra* note 43.

[108] *Id.* The European Union, through Europol, has established an efficient and resourceful approach that should be mirrored in the United States. *See* Kieran Corcoran, *Here's How Police in Europe Work Together Against Cryptocurrency Crime*, BUS. INSIDER (Mar. 3, 2018, 3:35 AM), https://www.businessinsider.com/how-european-police-fight-cryptocurrency-crime-2018-2 [https://perma.cc/966X-BNTE] (noting how Europol "helps connect the many hundreds of law enforcement organizations across the continent" [with] a centralised system by which officers can access information and pool tactics.").

[109] The power of this technique is evidenced by the arrest of drug trafficker Gal Vallerius. *See* Curt Anderson, *Frenchman in US Beard Contest, aka OxyMonster, Pleads Guilty in Drug Case*, CHI. SUN-TIMES (June 12, 2018, 2:32 PM), https://chicago.suntimes.com/news/oxymonster-gal-vallerius-beard-contest-guilty-drug-sales/ [https://perma.cc/3N74-MZBL] ("DEA also discovered that Vallerius had Instagram and Twitter accounts. They compared the writing style of 'OxyMonster' on the Dream Market forum to the writing style of Vallerius on his social media accounts.").

[110] *See* Oliver Belin, *The Difference Between Blockchain & Distributed Ledger Technology*, TRADEIX, *https://tradeix.com/distributed-ledger-technology/* [https://perma.cc/MUA6-E3EC] (last visited Apr. 17, 2018) (explaining how distributed ledger technology is one type of blockchain, and discussing how it cannot be rewritten).

foundation, for example, has the ability to rewrite its XEM ledger—though it has promised its customers it will never do so.[111] An order from a federal court may force the hand of a blockchain governing foundation. The possibility thereof may move the market toward cryptocurrencies willing to respond to court orders redressing theft. This market move, however, may prove unlikely due to the mass appeal of the untouchability of blockchain, especially the Bitcoin-style distributed ledger.[112]

Another avenue for returning stolen Bitcoin is by court seizure orders against the exchanges or individual wallets where the stolen coins eventually appear. However, "[m]any people would have coins—that they innocently bought—seized."[113] This may run into problems under the DTSA ex parte seizure procedure, which weighs the interests of third parties. On the other hand, a universal policy of seizing stolen coins, wherever they lie, may encourage cryptocurrency exchanges and investors to be more careful about the coins they accept in the first place, thereby decreasing the liquidity of stolen cryptoassets and disincentivizing such theft in the first place.

CONCLUSION

Cryptotheft has crippling effects on individuals, institutions, and the economy. In the last few years, this type of crime has only become more pervasive, culminating in the half-billion-dollar heist of the Japanese NEM exchange. It has not been a priority of United States law enforcement to pursue this brand of crime, likely due to the newness of the technology, the technical and extraterritorial difficulty inherent in prosecution, and the lack of an on-point legal theory. This Comment addresses these obstacles, proposing the DTSA as a novel and ideal tool to prosecute cryptothieves. Not only does the Act thoroughly, precisely, and uniquely encompass this difficult-to-define crime, but it does so in a manner that minimizes the theoretical and practical obstacles of civil and criminal suit.

[111] *See* Durden, *supra* note 106.

[112] *See* Jacques Legault, *The Psychological Appeal of Blockchain Technology*, FOUND. FOR ECON. EDUC. (Aug. 10, 2017), https://fee.org/articles/the-psychological-appeal-of-blockchain-technology/ [https://perma.cc/N5PX-Z4LK] (describing the appeal of "decentralized control, an immutable ledger, trustless smart-contracts, distributed autonomous organizations, [and] consensus decision making processes").

[113] Kipp Rogers, *Do Bitcoin Markets have a Conversion Tort Problem?*, MECHANICAL MKTS. (Nov. 5, 2017), https://mechanicalmarkets.wordpress.com/2017/11/05/Bitcoin-nemo-dat/ [https://perma.cc/P2E7-A66L].

*   *   *   *   *