UNC SCHOOL OF LAW

NORTH CAROLINA LAW REVIEW

Volume 97 | Number 2 Article 4

1-1-2019

Cyber Pickpockets: Blockchain, Cryptocurrency, and the Law of Theft

Henry S. Zaytoun

Cyber Pickpockets: Blockchain, Cryptocurrency, and the Law of Theft*

INTRODUCTION

"Code is law."[1]

This bold proclamation, championed by the Bitcoin community, is meant to be a summation of the "new world order"[2] ushered in by

1. LAWRENCE LESSIG, CODE VERSION 2.0, at 5 (2d ed. 2006) (rewording the phrasing of other cyberspace advocates).

2. *See, e.g.*, Nikola Grozdanovic, *Cryptocurrencies: A New Financial World Order*, WORLD FIN. (Aug. 11, 2017), https://www.worldfinance.com/markets/cryptocurrencies-a-new-financial-world-order [https://perma.cc/93DL-7MRU]; Brian Worley, *Into the Ether*,

innovations in peer-to-peer software protocols[3] commonly known as blockchain technology. These protocols make it possible for individuals to safely and securely complete transactions in digital information of some value, also known as "cryptocurrency,"[4] without the need for either a central authority[5] to act as a third party or government-enforced rule of law.[6] But what happens when code fails to protect the basic rights that our existing laws have always sought to protect?

Bitcoin—a cryptocurrency that is one form of blockchain information—continues to dominate the daily headlines, primarily due to its wild fluctuations in market price.[7] The all-time-high market price reached in 2017 correlates, unsurprisingly, with the record number of transactions[8] and wallet users[9] achieved. But the meteoric rise in price occurred without much public discussion of blockchain's technological innovation outside of a relatively small group of

COINREPORT (July 27, 2016), https://coinreport.net/into-the-ether-ethereum/ [https://perma.cc/GB9X-K53K].

3. Protocols, in this sense, are the rules written into the code that govern how the software may be used. *See* PEDRO FRANCO, UNDERSTANDING BITCOIN: CRYPTOGRAPHY, ENGINEERING, AND ECONOMICS 18 (2015).

4. The use of this term merely reflects common usage and the common understanding of the items of value exchanged in basic blockchain transactions. It is not to suggest that these items of value are currency. While some maintain and advocate this position, whether or not the items are currency is inconsequential to the inquiry here. In addition, while the creator of blockchain protocols, Satoshi Nakamoto, and others argued that these items must have value, I do not argue that point here. Rather, this Comment merely assumes a basic premise that if a market exists for some item, it therefore has some value.

5. *See* SATOSHI NAKAMOTO, BITCOIN, BITCOIN: A PEER-TO-PEER ELECTRONIC CASH SYSTEM 4, https://bitcoin.org/bitcoin.pdf [https://perma.cc/Y4LH-SC68].

6. *See* John V. Orth, *The Rule of Law*, 19 GREEN BAG 2D 175, 179 (noting the "generic" definition of the term to mean "a legal system that prevents arbitrariness, guarantees equal treatment, and – in many usages – enforces contracts and protects property"). One of the earliest advocates of Bitcoin, Erik Voorhees, now runs a website devoted to promoting Bitcoin and explaining the underlying blockchain technology. The website's tagline is a quotation that embodies the above described sentiment: "Give me control of a nation's money, and I care not who makes its laws." MONEY & ST., http://moneyandstate.com [https://perma.cc/8YPZ-FY6Q].

7. *E.g.*, Samuel Gibbs, *Bitcoin Drops $2,000 in Value as South Korea Announces Planned Trading Ban*, GUARDIAN (Jan. 11, 2018, 5:42 AM), https://www.theguardian.com/technology/2018/jan/11/bitcoin-drops-value-south-korea-trading-ban-cryptocurrencies-tax-gambling [https://perma.cc/C2DE-X8SL (staff-uploaded archive)].

8. *Confirmed Transactions Per Day*, BLOCKCHAIN (Aug. 27, 2018), https://blockchain.info/charts/n-transactions?timespan=1year [https://perma.cc/RME5-L6GW].

9. *Blockchain Wallet Users*, BLOCKCHAIN (Aug. 27, 2018), https://blockchain.info/charts/my-wallet-n-users?timespan=all [https://perma.cc/Z82M-XHQU].

advocates and academics.[10] This may be partly by design—in the early efforts to brand Bitcoin in a palatable, easy-to-understand way, advocates referred to Bitcoin as "digital gold,"[11] a cryptocurrency,[12] and, most simply, as a new form of money.[13] Yet it is the blockchain code, rather than Bitcoin in particular, that is garnering the largest investments for further development from companies like Google, Citibank, and Goldman Sachs.[14] In addition, companies like IBM are actively developing blockchain technology for use by a variety of business.[15]

These investments and developments appear to be the result of varied potential uses of the blockchain protocol beyond mere "storage and transfer" of Bitcoin as currency.[16] The list of alternate applications is long—digital asset, smart property, micropayments, crowdfunding, smart contracts, and storage of metadata—but, as of this writing, each remains in the relatively early stages of development.[17] Some argue that these applications are operable using

10. *See* Trevor I. Kiviat, Note, *Beyond Bitcoin: Issues in Regulating Blockchain Transactions*, 65 DUKE L.J. 569, 571–72 (2015).

11. *See* Jeff Cox, *Novogratz: Bitcoin is 'Digital Gold' and Will End the Year at $10,000*, CNBC (Nov. 21, 2017, 11:27 AM), https://www.cnbc.com/2017/11/21/novogratz-Bitcoin-is-digital-gold-and-will-end-the-year-at-10000.html [https://perma.cc/EGD6-GKYA].

12. NAKAMOTO, *supra* note 5.

13. Erik Voorhees, *The Role of Bitcoin as Money*, MONEY & ST. (May 23, 2013), http://moneyandstate.com/role-Bitcoin-money/ [https://perma.cc/JN2E-D9U4] ("Forget the tech. Forget the mining. Forget the cryptography and the peer to peer networks and the open source code. . . . The core of the Bitcoin experiment is not about tech at all, it's about money."). This might explain, in part, why the main focus of Bitcoin reporting centers on the daily fluctuations in its price.

14. *Blockchain Investment Trends in Review*, CBINSIGHTS, https://www.cbinsights.com/research/report/blockchain-trends-opportunities/ [https://perma.cc/CY6R-XBG6]. "Since 2012, corporates have participated in 140+ equity investments totaling nearly $1.2 [billion]," with most of that total coming in the last three years. *Id.* At the same time, however, some banks, like Goldman Sachs, are investing in Bitcoin futures. Dakin Campbell & Laura J. Keller, *Goldman Sachs Plans to Clear Bitcoin Futures When They Go Live*, BLOOMBERG (Dec. 7, 2017, 4:05 PM), https://www.bloomberg.com/news/articles/2017-12-07/goldman-sachs-is-said-to-clear-bitcoin-futures-when-they-go-live [https://perma.cc/7G7Q-MZTV (dark archive)].

15. *Unpack Research into Leading Blockchain Use Cases Here*, IBM, https://www.ibm.com/blockchain/use-cases/?cm_mmc=Search_Google-_-Blockchain+and+Watson+Financial+Services_Blockchain-_-WW_NA-_-+Public++Private++Blockchain_Broad_CoG&cm_mmca2=10007330&cm_mmca7=9009670&cm_mmca8=kwd-413097755984&cm_mmca9=4046a6b3-9f59-4422-849e-a062164cc286&cm_mmca10=250822637185&cm_mmca11=b&mkwid=4046a6b3-9f59-4422-849e-a062164cc286&cvosrc=ppc.google.&cvo_campaign=000026VG&cvo_crid=250822637185&Matchtype=b&gclid=CjwKCAjw39reBRBJEiwAO1m0OfT2a39dcUR2xK8QWzZl7mY8opmFr0V1ElWA5J7TQVmFYQuUq7zAahoCsbMQAvD_BwE [https://perma.cc/GF2A-EHQK] (identifying thirty-three use cases to date).

16. FRANCO, *supra* note 3, at 183.

17. *See generally id.* at 183–207 (detailing the various types of digital assets).

current blockchain protocol with few, if any, changes required.[18] But because of the undeveloped nature of these use cases, most scholarly articles are devoted to Bitcoin's use and regulatory efforts directed at treating Bitcoin as money.[19] Still others explore the idea of Bitcoin as a security[20] or a commodity.[21] At the same time, however, both scholarly and development-focused efforts tend to sidestep one of the major issues plaguing blockchain to date: theft.

While the impact of cryptocurrency theft is presently limited to niche markets and a select group of investors, it will become a more widespread problem as the underlying blockchain technology is implemented across industries. This threat forecasts the potential for huge economic loss. Perhaps more importantly, it also undermines a universal principle of any organized society, one that most intuitively accept as true[22]: "[i]t is a crime to steal what belongs to someone else."[23] And rule of law values are implicit in this principle—that "rule *by* law" is an important aspect of effective government and a bulwark against tyranny.[24]

These principles, however, are merely a starting point—both raise important questions concerning what *actions* a society considers theft and the *things* that may be objects of theft.[25] The concepts are interrelated; each tends to track closely both societal and economic developments.[26] As Bitcoin continues to dominate public conversation and remains the most widely used cryptocurrency[27] to date, it provides the best conduit to explore the application of these concepts to blockchain and blockchain-based assets.

It is estimated that, since its inception, over 980,000 Bitcoins have been lost through unauthorized takings, mostly individual

18. *Id.* at 183.

19. *E.g.*, Ed Howden, Comment, *The Crypto-Currency Conundrum: Regulating an Uncertain Future*, 29 EMORY INT'L L. REV. 741, 761–63 (2015).

20. *E.g.*, Christopher Burks, Recent Development, *Bitcoin: Breaking Bad or Breaking Barriers*, 18 N.C. J.L. & TECH. ONLINE 244, 246 (2017).

21. *E.g.*, Sarah Jane Hughes & Stephen T. Middlebrook, *Advancing a Framework for Regulating Cryptocurrency Payment Intermediaries*, 32 YALE J. ON REG. 495, 507–11 (2015).

22. *See* STUART P. GREEN, THIRTEEN WAYS TO STEAL A BICYCLE 1 (2012) ("[I]t is hard to imagine any organized society without [prohibitions on theft].").

23. LAURENCE M. FRIEDMAN, CRIME AND PUNISHMENT IN AMERICAN HISTORY 108 (1993).

24. Orth, *supra* note 6, at 181.

25. Michael E. Tigar, *The Right of Property and the Law of Theft*, 62 TEX. L. REV. 1443, 1443–44 (1984).

26. *Id.* at 1444.

27. For discussion of cryptocurrency, see *infra* Part II.

accounts located on major Bitcoin exchanges.[28] This loss represents an amount over $3.5 billion,[29] and most of these losses have occurred within the last four years.[30] When such losses occur, the media often reports them in terms of theft.[31] This reaction implies a general understanding, without analysis, that such a taking is legally theft—that is, the taking of a *thing* (Bitcoin) belonging to someone else that society recognizes as an *action* deserving punishment. This framing generally mirrors the response by victims of Bitcoin theft.

While some individuals simply accept this risk of loss as an inevitable result of participating in the Bitcoin market,[32] a growing number are complaining to regulatory agencies about the problem.[33] This uptick in complaints is due in part to the rapid increase in losses attributed to Bitcoin theft, and the fact that once a Bitcoin is stolen, it

28. Jim Finkle & Jeremy Wagstaff, *Hackers Steal $64 Million from Cryptocurrency Firm NiceHash*, REUTERS (Dec. 6, 2017, 10:20 PM), https://www.reuters.com/article/us-cyber-nicehash/hackers-steal-64-million-from-cryptocurrency-firm-nicehash-idUSKBN1E10AQ [https://perma.cc/7P2X-J5TK].

29. Calculated using the coinbaseUSD exchange rate on November 26, 2018 at 9:10 p.m. For this rate, as well as other rates of exchange, see BITCOINCHARTS, https://Bitcoincharts.com [https://perma.cc/4EFV-9J93].

30. *See* Timothy W. Martin, Eun-Young Jeong & Steven Russolillo, *North Korea Is Suspected in Bitcoin Heist*, WALL ST. J. (Dec. 20, 2017, 6:59 PM), https://www.wsj.com/articles/north-korea-is-suspected-in-Bitcoin-robbery-1513790899 [https://perma.cc/9YEW-QVKT (dark archive)]; Rishi Iyengar, *More than $70 Million Stolen in Bitcoin Hack*, CNN (Dec. 8, 2017), http://money.cnn.com/2017/12/07/technology/nicehash-Bitcoin-theft-hacking/index.html [https://perma.cc/EBV2-92S3]; Justina Lee, *Even a $31 Million Hack Couldn't Keep Bitcoin Down*, BLOOMBERG (Nov. 21, 2017, 1:22 AM), https://www.bloomberg.com/news/articles/2017-11-21/bitcoin-falls-after-31-million-theft-of-cryptocurrency-tether [https://perma.cc/23EE-9BUQ (dark archive)]; Robert McMillan, *The Inside Story of Mt. Gox, Bitcoin's $460 Million Disaster*, WIRED (Mar. 3, 2014, 6:30 AM), https://www.wired.com/2014/03/Bitcoin-exchange/ [https://perma.cc/6WW6-CQ4L (dark archive)].

31. Finkle & Wagstaff, *supra* note 28.

32. *See* Matt Levine, *Bitcoin Bankruptcy Wasn't Really a Bust*, BLOOMBERG (Nov. 14, 2017, 2:00 AM), https://www.bloomberg.com/view/articles/2017-11-14/bitcoin-bankruptcy-wasn-t-really-a-bust [https://perma.cc/SE2E-FD52 (dark archive)].

33. *See* Lily Katz & Julie Verhage, *Bitcoin Exchange Sees Complaints Soar*, BLOOMBERG (Aug. 30, 2017, 8:15 AM), https://www.bloomberg.com/news/articles/2017-08-30/bitcoin-exchange-sees-complaints-soar-as-users-demand-money [https://perma.cc/7ZUY-GLYU (dark archive)] (comparing the 6 complaints about Coinbase in 2016 to at least 293 complaints in 2017 filed with the U.S. Consumer Financial Protection Bureau—mostly due to "money not available when promised" but with a significant number of complaints related to "fraud or scam"); Jen Wieczner, *Hacking Coinbase: The Great Bitcoin Bank Robbery*, FORTUNE (Aug. 22, 2017), http://fortune.com/2017/08/22/Bitcoin-coinbase-hack/ [https://perma.cc/8LPZ-LC9T] (noting that complaints to the FBI's Internet Crime Complaint Center concerning "losses from crimes involving virtual currency were . . . more than triple[d]" in 2016 when compared to 2015).

is unlikely that the lost Bitcoin will ever be recovered.[34] In a normative sense, however, this reaction demonstrates the general proposition that victims of unauthorized takings expect protection and redress from the traditional source: the government.[35] Public perception, as alluded to above,[36] further supports this normative view. Yet, as a prominent member of the Bitcoin community candidly admits, "no one . . . has gone to jail for . . . electronically pilfering cryptocurrencies."[37]

This growing tension surrounding unauthorized takings of Bitcoin—and the slow pace of actionable steps taken by both prosecutors and the government in general—stands in stark contrast to prior government responses to innovations in theft. In the not-so-distant past, both state and federal legislative bodies and law enforcement agencies implemented a rigorous approach to theft and cybercrime. The National Stolen Property Act ("NSPA") was an initial response to perceived gaps in state larceny laws to counter fraudulent transfers of stolen property.[38] When the advent of computers complicated this scheme, Congress introduced the Computer Fraud and Abuse Act ("CFAA") to enlarge prosecutors' toolkits.[39] The CFAA was subsequently amended numerous times over the following thirty-plus years.[40] Prior to its passage, prosecutors relied on the mail and wire fraud statutes as a stop-gap measure to combat fraud perpetrated in the new computer forum.[41] None of the

34. Finkle & Wagstaff, *supra* note 28; *see also* Alexandra Harney & Steve Stecklow, *Twice Burned – How Mt. Gox's Bitcoin Customers Could Lose Again*, REUTERS (Nov. 16, 2017, 1:15 PM), https://www.reuters.com/investigates/special-report/bitcoin-gox/ [https://perma.cc/TY8Y-KHS3].

35. *See* NATHANIEL POPPER, DIGITAL GOLD 114 (2015) ("[I]n each case of big theft, Bitcoin users eventually went to government authorities to seek redress . . . .").

36. *See, e.g.*, Mike Huynh, *Latest Bitcoin Theft Bankrupts South Korean Cryptocurrency Exchange*, D'MARGE (Dec. 20, 2017), https://www.dmarge.com/2017/12/Bitcoin-theft.html [https://perma.cc/NS8Z-HNJP]. Additionally, the article's subheading, "Another day, another stolen Bitcoin" succinctly sums up this perception. *Id.*

37. Wieczner, *supra* note 33. Coinbase is one of the largest Bitcoin exchanges currently in existence, offering both storage services and a platform to facilitate transactions in Bitcoin and other digital currencies. *About Coinbase*, COINBASE, https://www.coinbase.com/about [https://perma.cc/3N38-EACX].

38. Geraldine Szott Moohr, *Federal Criminal Fraud and the Development of Intangible Property Rights in Information*, 2000 U. ILL. L. REV. 683, 697 (2000) [hereinafter Moohr, *Federal Criminal Fraud*].

39. *See* COMPUT. CRIME & INTELLECTUAL PROP. SECTION, U.S. DEP'T OF JUSTICE, PROSECUTING COMPUTER CRIMES 1 (Scott Eltringham et al. eds., 2010) (explaining that Congress created the CFAA, in part, to help address emerging computer crimes that current statutes lacked the "tools . . . to combat").

40. *Id.* at 1–3.

41. *Id.* at 1.

above provisions, however, has yet been applied to the "electronic[] pilfering [of] cryptocurrencies."[42]

With blockchain's increasing prevalence and the promising potential of its widespread application, now is the time for prosecutors to act. Not only would prosecution of cryptotheft reinforce rule-of-law values, but it would also address societal expectations that unauthorized takings of blockchain-based assets are what they appear to be—theft. Such prosecutions would achieve the critical objectives of regulatory schemes—fostering trust in blockchain-based assets and a safe playing field for innovation—in a way that would be less onerous to developing blockchain's uses across industries. By targeting the bad actors, as opposed to regulating technology's operation, blockchain developers will retain the freedom to continue developing the technology without sacrificing other important societal goals and values.

This Comment argues that prosecutors already have the tools necessary to confront this rise in theft.[43] To lay the foundation of the law of theft, Part I highlights the technical aspects of blockchain protocol and Bitcoin that are relevant to this discussion. Tracing blockchain's development explains in part the early—often contradictory—efforts to define Bitcoin. It is also crucial to understanding why Bitcoin is best understood as property, which in turn clarifies the operation of the most common instances of theft from online exchanges. Part II then defines Bitcoin. Part III addresses the shortcomings of the most applicable federal theft statutes, the NSPA and CFAA, when applied to theft of Bitcoin. It then proposes that the Wire Fraud provision is a critical stop-gap measure for deterring such theft that serves both to protect individuals' interest in Bitcoin and the future development of blockchain protocol. Lastly, Part IV argues that prosecutors should move to enforce these provisions, while noting the social and economic realities of enforcement. It raises questions that Congress, government regulators, and the Bitcoin community should consider when searching for an equitable solution to this pervasive risk.

42. Weiczner, *supra* note 33.

43. Bitcoin is implicated in a number of other criminal schemes, all of which fall outside the scope of this Comment. For a discussion of other criminal issues involving cryptocurrency, see Rainer Böhme et al., *Bitcoin: Economics, Technology, and Governance*, 29 J. ECON. PERSP. 213, 230 (2015).

I. BLOCKCHAIN PROTOCOL: THE BASICS

While blockchain increasingly receives scholarly attention, most people's familiarity with the technology does not extend far past news headlines. This is certainly understandable considering that blockchain is a product of the relatively niche field of cryptography, which is replete with complicated math and deals exclusively in source code.[44] Furthermore, it seems that most primers on the technology are geared toward individual investors with the hope of securing that investor's business.[45] As blockchain continues to be developed and utilized across business cases, one would expect an increase in resources on the subject. This is not to say that in-depth analyses of blockchain are nonexistent. On the contrary, a number of scholars have already taken up the task of explaining the technical and legal implications of certain aspects of the technology. It is from these early efforts that an understanding of the application of the law of theft may be developed.

As a preliminary matter, the blockchain protocol allows two people to transact without the need for a "trusted third party" intermediary.[46] What is transacted between them is a specific line of code that is mathematically impossible to replicate.[47] Every transaction is recorded on a publicly accessible ledger—the "blockchain."[48] These aspects of blockchain most excite companies, investors, and the public at large because the protocol provides a safe, transparent, and direct system of exchanging valuable information. But a more developed understanding of these basic principles is an essential prerequisite to applying criminal provisions.[49]

44. Lauri Hartikka, *A Blockchain in 200 Lines of Code*, MEDIUM (Mar. 4, 2017), https://medium.com/@lhartikk/a-blockchain-in-200-lines-of-code-963cc1cc0e54 [https://perma.cc/5CLX-5CU4].

45. *See, e.g.*, *Bitcoin Primer*, FIDELITY (Jan. 19, 2018), https://www.fidelity.com/viewpoints/active-investor/beyond-Bitcoin [https://perma.cc/JH27-988G].

46. NAKAMOTO, *supra* note 5, at 1. For a popular historical account of Bitcoin's development, see generally POPPER, *supra* note 35.

47. Nakamoto uses the phrasing "electronic cash" to describe Bitcoin. NAKAMOTO, *supra* note 5, at 1.

48. *Id.* This Comment addresses only public blockchains. Recently, private blockchains operating within a "permissioned network" have become an option for those wishing to employ the technology. Praveen Jayachandran, *The Difference Between Public and Private Blockchain*, IBM (May 31, 2017), https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/ [https://perma.cc/UH5A-7BKX]. While the permissioned network might add another layer of security and privacy, the underlying blockchain technology remains the same and thus does not alter the discussion here. *Id.*

49. This discussion assumes some familiarity with Bitcoin protocol and focuses on the most critical aspects of the technology for current purposes. For a more detailed

A. How to Create, Transact, and Store Bitcoin

Public key cryptography—a way of using source code to securely transfer information—is far from new. The idea first appeared in a white paper in the mid-1970s,[50] but it was not until the advent of Bitcoin that it received broad public attention. To help communicate a complicated topic to the uninitiated, the early Bitcoin advocates personified math's use of "A" and "B" in proofs by creating Alice and Bob.[51] In the spirit of that convention, this Comment will assume the following transaction: Alice sends Bob five Bitcoin.

Before explaining how the transaction occurs, it is instructive to examine *where* the transaction takes place. Bitcoin transactions occur within the Bitcoin network. The network is "peer-to-peer," meaning that the computer servers, commonly called "nodes," that actively run the Bitcoin's open-source software are linked together.[52] Since the blockchain protocol is open-source, anyone with an internet connection can download and run it on their server.[53] So long as a node is actively running the software program, it is connected to the other nodes on the network. Skipping ahead in the process, peer-to-peer connection allows Alice and Bob to broadcast their completed transaction to all other active nodes.[54] It is within this network that transactions are eventually confirmed and recorded on the

introduction to the technology, see generally ARVIND NARAYANAN ET AL., BITCOIN AND CRYPTOCURRENCY TECHNOLOGIES: A COMPREHENSIVE INTRODUCTION (2016). For a popular account of the technology's history and some of its key players, see generally POPPER, *supra* note 35.

50. *See generally* Whitfield Diffie & Martin E. Hellman, *New Directions in Cryptography*, 22 IEEE TRANSACTIONS ON INFO. THEORY 644 (1976).

51. *See* POPPER, *supra* note 35, at 9, 11. For an example demonstrating that the convention of using "Alice" and "Bob" as hypothetical transactors continues in the Bitcoin community, see generally Brian Hayes, *Alice and Bob in Cipherspace*, AM. SCIENTIST, Sept.–Oct. 2012, at 362, https://www.americanscientist.org/article/alice-and-bob-in-cipherspace [https://perma.cc/K9J4-BPK5].

52. *See* NARAYANAN ET AL., *supra* note 49, at 66–67. For a brief explanation of the different kinds of nodes within the Bitcoin network, a topic outside the scope of this Comment, see GHASSAN KARAME & ELLI ANDROULAKI, BITCOIN AND BLOCKCHAIN SECURITY 48–49 (2016).

53. FRANCO, *supra* note 3, at 6.

54. KARAME & ANDROULAKI, *supra* note 52, at 49–51. Recently, given strong incentives to operate quickly, some developers have created alternative networks that interface with the Bitcoin network solely for speedier transmission of transaction information. *See id.* at 52.

blockchain.[55] The nodes effectively act as managers of the blockchain by running the Bitcoin protocol software.[56]

Transactions involving blockchain protocol involve a sender and a recipient who both rely on cryptography for security and privacy.[57] The first step in completing a transaction can occur offline; that is, without access or use of the Bitcoin protocol or the internet.[58] To begin, Alice first generates a public key using the Elliptic Curve Digital Signature Algorithm.[59] The public key will be, unsurprisingly, publicly available but void of direct links to Alice's identity. The public key is then "hashed" to create Alice's public address, which serves as her identifier to others on the Bitcoin network.[60] This public address itself, however, does not reveal any personally identifiable information about Alice.[61] Thus, Alice has anonymity to a point, though there are a number of ways that a public address may tip off others about the identity of the sender.[62]

Alice also generates a private key known only to her.[63] While still offline,[64] Alice creates her message—"send Bob five Bitcoin"—and signs it with her private key. The algorithmic combination of Alice's message and private key creates her digital signature.[65] The message consists of outputs (the five Bitcoin) that she previously received in

55. NARAYANAN ET AL., *supra* note 49, at 66–67.

56. *See* Shawn Bayern, *Of Bitcoins, Independently Wealthy Software, and the Zero Member LLC*, NW. U. L. REV. ONLINE 257, 258, 261 (2014) [hereinafter Bayern, *Of Bitcoins*].

57. For a broader discussion of cryptography used in Bitcoin transactions, see FRANCO, *supra* note 3, at 51–75. *See also* Bayern, *Of Bitcoins*, *supra* note 56, at 1–27.

58. *See* POPPER, *supra* note 35, at 358.

59. *Id.* at 17–18. The algorithm, initially created by the U.S. government, makes it statistically improbable for an "attacker"—defined as someone interested in discovering and using your private key—to discover the private key through randomized guesses. *See id.* at 15–18. For a more detailed explanation of the algorithm, see FRANCO, *supra* note 3, at 62–71.

60. NARAYANAN ET AL., *supra* note 49, at 18–19. While the public key is, in some sense, an identifier in that the sender's public key is required for the recipient of the transaction to verify it as valid, the recipient cannot determine the sender by the public key alone. *See* FRANCO, *supra* note 3, at 57.

61. NARAYANAN ET AL., *supra* note 49, at 19–20. As a practical matter, any user may have as many addresses as he desires—new pairs of public and private keys may be created at any time—and many use this as one way of protecting their identity on the blockchain. *Id.*

62. *See id.* at 143–51.

63. *Id.* at 18–20.

64. *See* POPPER, *supra* note 35, at 358.

65. NARAYANAN ET AL., *supra* note 49, at 15–19.

another transaction.[66] Alice then directs the outputs to Bob's public address[67] and broadcasts the transaction to all nodes in the Bitcoin network, requiring her to be online.[68] The nodes can then verify that the transaction is valid (i.e., the message was sent from a valid address and contains Bitcoin not previously spent by the sender).[69] If valid, the transaction is then added to a block of recent transactions by miners. Miners make up the group of nodes who actively pool all transactions to broadcast to the network.[70]

This block of transactions is then added to a string of other blocks previously created by miners—hence the name "blockchain."[71] Miners are the nodes that run the blockchain protocol.[72] They decide which transactions are included and verify the transactions as valid.[73] Then, they receive an incentive to create new blocks for the blockchain.[74] The incentive comes in the form of a "block reward" to the miner of a certain amount of Bitcoin.[75] Since all nodes running the protocol are gathering all transactions broadcast to the network, the node that successfully solves a complicated math equation by "hashing" all collected transactions earns the "block award."[76]

The first block is referred to as the "genesis block," and the protocol dictates that the longest chain of blocks is the valid blockchain[77]—that is, all transactions on the longest chain are deemed

66. This is true even if the sender is herself a miner—in that case, the outputs are received in the form of a block reward, as opposed to receiving the outputs from a prior transaction. *See id.* at 38–41.

67. FRANCO, *supra* note 3, at 57. This assumes, of course, that the recipient has also generated a public and private key. As of this writing, the operation of generating keys is the same for both sender and recipient.

68. *Id.* at 112; NARAYANAN ET AL., *supra* note 49, at 29.

69. FRANCO, *supra* note 3, at 78–79.

70. NARAYANAN ET AL., *supra* note 49, at 105.

71. FRANCO, *supra* note 3, at 105.

72. *Id.* at 105–06.

73. *Id.*

74. *Id.*

75. NARAYANAN ET AL., *supra* note 49, at 39. The block reward started at fifty Bitcoin and is set to decrease, per Bitcoin protocol, by half for every 210,000 blocks created. *Id.* For the current number of blocks, which is 555,955 as of December 28, 2018, at 3:00 p.m., requiring a current block reward of 12.5 Bitcoin, as well as the current block reward, see BITCOINCHARTS, *supra* note 29. Transaction fees are the other incentive for mining, and one that will become more important when the 21 million Bitcoin limit is reached. *See* NARAYANAN ET AL., *supra* note 49, at 39–40.

76. FRANCO, *supra* note 3, at 105–07.

77. *Id.* at 109.

valid, and once recorded, are essentially irreversible.[78] The blockchain, then, contains the definitive record of transactions and unspent outputs in the Bitcoin network. For ease of use, the record of all unspent outputs within the Bitcoin protocol is kept in the unspent transaction outputs cache ("UTXO").[79]

These unspent outputs recorded on the UTXO are merely bits of code existing within blocks on the blockchain.[80] As mentioned previously, Bitcoin is tied to a specific public address[81] and can only be accessed using the private key tied to the public address. That is, if Alice wants to send Bob five Bitcoin, then (1) Alice must have five Bitcoin from a previous transaction; (2) the Bitcoin are accessible to Alice through use of Alice's private key; and (3) the nodes must verify that Alice has five Bitcoin by searching the UTXO.[82] If it is confirmed that Alice does indeed have five Bitcoin, then the transaction is approved, and Bob's public address is now associated with the five Bitcoin.[83] Thus, this illustrates the importance of the private key.

Since the private key accesses all available Bitcoin associated with the corresponding public address, users must protect their private key, and most choose to store keys in online exchanges.[84] The exchange acts as a place where users can keep Bitcoin, exchange Bitcoin for fiat currency, and easily make Bitcoin transactions.[85] Others may store them in some form of digital wallet software.[86] This

78. *Id.* at 107–08; *see also* Böhme et al., *supra* note 43, at 219. For a discussion showing that this irreversible nature was Satoshi Nakamoto's original intent, see NAKAMOTO, *supra* note 5, at 1.

79. FRANCO, *supra* note 3, at 79–80.

80. This point is crucially important to properly define Bitcoin. *See infra* Part II.

81. *See supra* notes 59–62 and accompanying text.

82. *See* FRANCO, *supra* note 3, at 78–79. This example oversimplifies the process, retaining—without diluting—the points that are essential to our discussion here. For a full discussion of the transaction process, see *id.* at 77–93.

83. *See id.* at 78–79. This example oversimplifies the process, retaining, without diluting, the points that are essential to our discussion here. For a full discussion of the transaction process, see *id.* at 77–93.

84. *See* Mark, *12 Ways to Store Your Bitcoins*, NULLTX (Mar. 1, 2017), https://nulltx.com/12-ways-to-store-your-Bitcoins/ [http://perma.cc/NZ2P-CL3U].

85. *See* KARAME & ANDROULAKI, *supra* note 52, at 146.

86. NARAYANAN ET AL., *supra* note 49, at 88. There are a number of other ways that private keys may be stored locally, *see id.* at 76–87, but most of the reported thefts have occurred either from online exchanges or online wallet software. *See* Jeff John Roberts, *How Bitcoin Is Stolen: 5 Common Threats*, FORTUNE (Dec. 8, 2017), http://fortune.com/2017/12/08/Bitcoin-theft/ [https://perma.cc/3UD2-8EEC].

allows users to store their keys in the cloud, where the keys can be accessed by most devices with an internet connection.[87]

B. How to Take Bitcoin

Before it is possible to confirm the recent headlines of Bitcoin theft as true legal theft, it is important to examine the type of *interference* concerning individual users' private keys.[88] One of the more commonly reported thefts involves compromising an online exchange. Exchanges continue to be the most common way for individuals to transact in Bitcoin.[89] Generally, the exchanges operate "off-blockchain," meaning that they operate on software unrelated to the Bitcoin protocol.[90] Individuals create accounts on the exchange, much like bank accounts, where both cash and private keys can be stored.[91] The individual can then direct the exchange to use the cash to make purchases of Bitcoin.[92] In addition, many exchanges also offer digital wallet services, permitting cloud-based storage for a user's private keys.[93] The exchanges, then, tend to operate as a one-stop shop, providing a forum for both purchasing and storing Bitcoin.[94]

The most common form of theft from exchanges involves some compromise of the exchange to gain access to exchange users' private keys stored in digital wallets on the exchange.[95] Once the thief accesses the private keys, he may transfer the Bitcoin associated with

87. NARAYANAN ET AL., *supra* note 49, at 88.

88. The scope of this Comment is restricted to this interference. There are, of course, many other potential violations that might occur surrounding the interference at issue. *See, e.g.*, *Former Secret Service Agent Pleads Guilty to Money Laundering*, U.S. DEP'T JUST. (Aug. 15, 2017), https://www.justice.gov/opa/pr/former-secret-service-agent-pleads-guilty-money-laundering [https://perma.cc/D46P-UAT9].

89. Reuters, *Cryptocurrency Exchanges Are Increasingly Roiled by Hackings and Chaos*, FORTUNE (Sept. 29, 2017), http://fortune.com/2017/09/29/cryptocurrency-exchanges-hackings-chaos/ [https://perma.cc/QEA6-NJ52].

90. FRANCO, *supra* note 3, at 42.

91. *Id.*

92. *See* KARAME & ANDROULAKI, *supra* note 52, at 146.

93. *Id.* at 146–49.

94. BITSTAMP, https://www.bitstamp.net [http://perma.cc/Z8M7-PUZM]; COINBASE, https://www.coinbase.com/home [https://perma.cc/7FT9-JJJR]; *Security*, BITFINEX, https://www.bitfinex.com/legal/security_policy [https://perma.cc/L3FT-CN5G].

95. *See, e.g.*, McMillan, *supra* note 30. While outside the scope of this Comment, this initial interference, commonly termed "hacking," may be addressed by various state statutes. *Computer Crime Statutes*, NAT'L CONF. ST. LEGISLATURES, http://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx#Hacking [https://perma.cc/S6W5-CBMC]. In addition, while it may be difficult to prosecute theft under current federal provisions, this initial interference may be addressed by the CFAA, discussed in Section III.B.2.

each private key to his personal addresses.[96] Nothing in the transaction process, as demonstrated above, initially indicates to the network that the transaction is not being made by the legitimate owner of the compromised keys—to other nodes on the network, it simply appears as if the user herself is completing a transaction. Since the transactions initiated by the thief appear valid,[97] they are also likely to be verified on the network and incorporated into a valid block. And, given that reversing these transactions is incredibly difficult,[98] the rightful owner of the private key is likely forever deprived of the lost Bitcoin.

II. DEFINING BITCOIN

The well-worn notion of technology outpacing law[99] is especially apparent in early efforts to define Bitcoin. As one judge candidly admits in a recent opinion, "[n]othing in our frame of references allows us to accurately define or describe Bitcoin."[100] This reaction may explain, in part, the early efforts by government agencies in this regard. Many agencies seeking to define Bitcoin within existing regulatory frameworks rely almost exclusively on the way the cryptocurrency is *used* and fail to take on a more searching inquiry into what Bitcoin *is*. This analysis does not align with the traditional framework of the law of theft—for something to be an object of theft, it must be a *thing* capable of being stolen. This part details early efforts at defining Bitcoin by its use and proceeds to build on the argument for the existence of individual property interests in Bitcoin.

A. Early Use Cases and Definitional Difficulties

Originally, Bitcoin was simply another effort to create a workable system for digital cash. Satoshi Nakamoto, the original

96. *See* Mark, *supra* note 84. Technically, it is likely that the thefts will only compromise the private keys in "hot storage," that is, those that are stored on a system that has internet access, by virtue of the fact that a thief with internet access can theoretically gain access to the private keys; those in "cold storage," on the other hand, are offline. NARAYANAN ET AL., *supra* note 49, at 79. Many of the most popular exchanges claim to store the vast majority of private key in cold storage. FRANCO, *supra* note 3, at 41. This, however, can fluctuate—if demand for buying and selling increases, presumably fewer private keys will remain in "cold storage."

97. The transactions will involve the valid keys of the victim and valid keys of the thief. *See* Mark, *supra* note 84.

98. KARAME & ANDROULAKI, *supra* note 52, at 146.

99. Vivek Wadhwa, *Laws and Ethics Can't Keep Pace with Technology*, MIT TECH. REV. (Apr. 15, 2014), https://www.technologyreview.com/s/526401/laws-and-ethics-cant-keep-pace-with-technology/ [http://perma.cc/E48M-Y26U].

100. State v. Espinoza, No. F14-2923, slip op. at 5 (Fla. Cir. Ct. July 22, 2016).

developer of blockchain protocol, largely built on the shoulders of the so-called cypherphunks, the libertarian advocates for electronic cash and other privacy-driven transactional methods who made the first efforts in this regard.[101] Early advocates strongly pushed for Bitcoin as a "new global monetary system,"[102] or a new form of cash, both as a continuation of libertarian goals and as a way to attractively market Bitcoin to the public. On a more practical level, many early developers thought that Bitcoin must be valuable in order to effectively incentivize miners to continue verifying transactions.[103] Further, many of the early adopters of Bitcoin began to use it as currency, albeit in most situations for the purchase of illegal goods.[104] Over time, traditional sources of financial news also adopted the language of Bitcoin as money or cryptocurrency.[105] While some early advocates are backing away from the idea of Bitcoin as money,[106] this perception continues to exist—a number of judges faced with early cases involving Bitcoin unequivocally adopted the monetary definition.[107]

Others in the Bitcoin, financial, and government communities recently have shied away from defining Bitcoin as money and instead have argued that it is better defined as a security. Recent guidance distributed by the Securities and Exchange Commission ("SEC")

101. *See infra* text accompanying notes 235–36.

102. Erik Voorhees, *Bitcoin-The Libertarian Introduction*, MONEY & ST. (Apr. 13, 2012), http://moneyandstate.com/Bitcoin-libertarian-introduction-used-care/ [http://perma.cc/MSQ6-5T2B].

103. *See* NARAYANAN ET AL., *supra* note 49, at 47. In fact, Bitcoin's first proponents believed that the profit motive was the only way for the project to operate effectively. *See id.* As mentioned above, however, this motivation is far less important today as blockchain's use cases continue to expand.

104. *See, e.g.*, Joshua Bearman, *The Rise & Fall of the Silk Road: Part I*, WIRED (May 2015), https://www.wired.com/2015/04/silk-road-1/ [https://perma.cc/Q8SY-JU39 (dark archive)].

105. Rob Copeland, *Peter Thiel's Founders Fund Makes Monster Bet on Bitcoin*, WALL ST. J. (Jan. 2, 2018), https://www.wsj.com/articles/peter-thiels-founders-fund-makes-big-bet-on-Bitcoin-1514917433/ [http://perma.cc/4BVG-UNEP].

106. *See* Erik Voorhees, *The Importance of Bitcoin Not Being Money*, MONEY & ST. (Aug. 8, 2016), http://moneyandstate.com/the-importance-of-Bitcoin-not-being-money/ [https://perma.cc/E3RW-ARHC] (clarifying his early position of Bitcoin as "the best money mankind had ever seen" by proposing, instead, that "Bitcoin isn't money after all").

107. *See* State v. Espinoza, No. F14-2923, slip op. at 5–6 (Fla. Cir. Ct. July 22, 2016) ("Nothing in our frame of references allows us to accurately define or describe Bitcoin."). *But see* United States v. Faiella, 39 F. Supp. 3d 544, 545 (2014) (holding that "Bitcoin clearly qualifies as 'money'" under 18 U.S.C. § 1960); SEC v. Shavers, No. 4:13-CV-416, 2013 WL 4028182, at *2 (E.D. Tex. Aug. 6, 2013) (finding, in dicta, that "Bitcoin is a currency or form of money").

states that "virtual coins or tokens . . . disseminated using distributed ledger or blockchain technology . . . may be securities . . . subject to the federal securities laws."[108] In addition, some foreign governments are taking similar steps to recognize Bitcoin as a security.[109] Both the SEC guidance and foreign government action seem to be mere extensions of the legal debate along the same lines.[110] Some in the tech community are taking up the argument as well.[111]

Many Bitcoin advocates and financial observers, however, believe that, despite its security-like use by some individuals, inaction by the SEC likely dooms this definition.[112] This may not be the case for blockchain-based cryptocurrencies other than Bitcoin—the SEC, for instance, specifically targets initial coin offerings.[113] But the conclusion that Bitcoin is, in all circumstances, a security appears far from settled in the courts. While courts may in theory have the authority to broaden the definition of security through statutory interpretation,[114] many seem hesitant to do so.[115] The SEC guidance,

108. *Investor Bulletin: Initial Coin Offerings*, U.S. SEC. & EXCHANGE COMMISSION (July 25, 2017), https://www.sec.gov/oiea/investor-alerts-and-bulletins/ib_coinofferings/ [http://perma.cc/WA42-F483].

109. Angelica Ballesteros, *Regulators Eye Wider Virtual Currency Use*, MANILA TIMES (Nov. 22, 2017), http://www.manilatimes.net/regulators-eye-wider-virtual-currency-use/364344/ [http://perma.cc/42BN-RUJ5].

110. *See, e.g.*, Burks, *supra* note 20, at 246; Dan Stroh, Article, *Secure Currency or Security? The SEC and Bitcoin Regulation*, U. CIN. L. REV. (Nov. 18, 2014), https://uclawreview.org/2014/11/18/secure-currency-or-security-the-sec-and-Bitcoin-regulation/ [http://perma.cc/KF6B-LSG8].

111. *See, e.g.*, Mario Lattuga, *Yes, Bitcoin Will Be Regulated by the SEC. Here's Why:*, MEDIUM (Dec. 3, 2017), https://medium.com/@mlattuga1/yes-Bitcoin-is-probably-a-security-heres-why-4f6410d9787c/ [http://perma.cc/L99C-GK9S].

112. *See* PETER VAN VALKENBURG, COIN CTR., FRAMEWORK FOR SECURITIES REGULATION OF CRYPTOCURRENCIES 50–54 (2016), https://coincenter.org/wpcontent/uploads/2016/01/SECFramework2.5.pdf/ [http://perma.cc/5349-5DE8]. Another knowledgeable author on the subject rightly notes that "if [the SEC] thought Bitcoin was a security, [it] would probably have done something about it by now." *See* Matt Levine, *SEC Halts a Real Initial Coin Offering*, BLOOMBERG VIEW (Dec. 12, 2017, 3:20 PM), https://www.bloomberg.com/view/articles/2017-12-12/sec-halts-a-real-initial-coin-offering#footnote-1513099636855/ [https://perma.cc/HC42-PR5A (dark archive)].

113. *Id.* For a brief primer on the concept of Initial Coin Offerings, see Gregory J. Nowak & Joseph C. Guagliardo, *Blockchain and Initial Coin Offerings: SEC Provides First U.S. Securities Law Guidance*, HARV. L. SCH. F. ON CORP. GOVERNANCE FIN. REG. (Aug. 9, 2017), https://corpgov.law.harvard.edu/2017/08/09/blockchain-and-initial-coin-offerings-sec-provides-first-u-s-securities-law-guidance/ [http://perma.cc/YX8Q-DMLN].

114. Steven J. Cleveland, *Resurrecting Court Deference to the Securities and Exchange Commission: Definition of "Security,"* 62 CATH. U. L. REV. 273, 300–01 (2013).

115. *See, e.g.*, SEC v. Shavers, No. 4:13-cv-416, 2013 WL 4028182, at *1–2 (E.D. Tex. Aug. 6, 2013). While the court did not specifically hold that Bitcoin itself is a security under the Securities Acts, it did hold that investments in a company that bought and sold Bitcoin are considered securities. *Id.* at *2. Specifically in the criminal context, courts

often a reliable source of interpretive help for the courts,[116] does not offer much clarity since its language—that Bitcoin and other virtual currencies may be securities—leaves ample room for disagreement.

Still other government actions focus on Bitcoin's myriad of other uses to situate it neatly within their respective regulatory frameworks. The Financial Crimes Enforcement Network ("FINCEN") considers those dealing in Bitcoin to be "money transmitters" and recently brought actions against certain exchanges for alleged money laundering.[117] This action implicitly acknowledges monetary properties in Bitcoin. Other agency actions mirror this trend. The Internal Revenue Service ("IRS"), without defining the term explicitly, equates Bitcoin to "real currency" and thus subjects income in Bitcoin to taxation.[118] The Commodity Futures Trading Commission ("CFTC"), on the other hand, considers Bitcoin to be a commodity, and its regulatory action similarly reflects this disposition.[119] While the list is long and varied, a unifying strand runs through each effort at definition—the focus is constrained to Bitcoin's use, and no further. That is not to say that this definition is without value. At the same time, however, it side-steps the important inquiry into what Bitcoin *is*.

B. The Case for Property Interests in Bitcoin

The technical description of Bitcoin leads to an intuitive assumption that individuals have intangible property interests in it—

consistently rely on the rule of lenity to avoid broadening criminal statutes beyond the boundaries delineated by Congress. *See, e.g.*, United States v. Aleynikov, 676 F.3d 71, 82 (2d Cir. 2012) (finding that, under 18 U.S.C. § 1832(a), a high frequency trading system of a global bank, relatively new technology first implemented around the time of the decision, was not "'produced for' nor 'placed in' interstate or foreign commerce" within the meaning of the statute).

116. *See* Cleveland, *supra* note 114, at 301.

117. *FinCEN Fines BTC-e Virtual Currency Exchange $110 Million for Facilitating Ransomware, Dark Net Drug Sales*, FIN. CRIMES ENFORCEMENT NETWORK (July 27, 2017), https://www.fincen.gov/news/news-releases/fincen-fines-btc-e-virtual-currency-exchange-110-million-facilitating-ransomware/ [http://perma.cc/6QZ9-2YPL]; *see also* FIN. CRIMES ENF'T NETWORK, U.S. DEP'T OF THE TREASURY, FIN-2014-R011, REQUEST FOR ADMINISTRATIVE RULING ON THE APPLICATION OF FINCEN'S REGULATIONS TO A VIRTUAL CURRENCY TRADING PLATFORM 1 (2014), http://www.fincen.gov/news_room/rp/rulings/pdf/FIN-2014-R011.pdf [http://perma.cc/HL78-LDHQ].

118. I.R.S. Notice 2014-21, 2014-16 I.R.B. 938.

119. *CFTC Orders Bitcoin Options Trading Platform Operator and Its CEO to Cease Illegally Offering Bitcoin Options and to Cease Operating a Facility for Trading or Processing of Swaps Without Registering*, U.S. COMMODITY FUTURES TRADING COMMISSION (Sept. 17, 2015), http://www.cftc.gov/PressRoom/PressReleases/pr7231-15 [http://perma.cc/R5GT-V5WU].

that it is something capable of being owned to the exclusion of the whole world. As discussed above, Bitcoin is, by its nature, intangible. It is nothing other than electronic data, a string of "bits" hosted on software without any physical existence. And the holder of the private key is the only individual who may access, transact, or transfer the associated Bitcoin. Concluding that Bitcoin is legally the object of theft requires, however, more than a bare assumption. This is critical for purposes of the theft analysis—for something to be impermissibly taken, it must first be owned exclusively.

"The act of stealing—of unlawfully treating *tuum* as *meum*" is necessarily predicated on the idea that what is yours, which I treat as mine, is *actually* yours.[120] Naturally, this seems to imply principles of ownership and thus property interests.[121] To address theft of Bitcoin, then, someone who claims rights of ownership in Bitcoin must, in fact, have those rights in the first place.[122]

The Supreme Court has not found property interests to stem from the Constitution;[123] rather, the Court looks to "existing rules or understandings that stem from an independent source such as state law" to define when a person has an interest in property.[124] States are varied in their approach to intangible interests in property. North Carolina property law, for example, is unclear as to whether intangible property rights exist, at least insofar as it pertains to conversion claims.[125] To bring a conversion action in North Carolina, a plaintiff must show "ownership [of goods or personal chattels] . . . and a wrongful conversion by defendant."[126] Intangible interests "such

120. *See* GREEN, *supra* note 22, at 1.

121. *See* Moohr, *Federal Criminal Fraud*, *supra* note 38, at 684. The Supreme Court has noted that "property is a creation of the law" and "the law limits rights of property according to the public interest and when public policy demands it." *Id.* at 695.

122. *See id.* In fact, whether the intangible item is property continues to be a central issue in cases concerning theft of the item. *See id.* at 696.

123. Town of Castle Rock v. Gonzales, 545 U.S. 748, 756 (2005).

124. *Id.* Some argue that this approach "leads to the confusing possibility of fifty different versions" of property interests under federal provisions, and, thus, the federal courts should be hesitant to use state law in defining property under federal statutes. *See* Moohr, *Federal Criminal Fraud*, *supra* note 38, at 715–16. The plain language of the Court, however, does not seem to constrain the use of state law, despite this cautionary note. *Id.*

125. *See* Spinks v. Taylor, 303 N.C. 256, 264, 278 S.E.2d 501, 506 (1981) (defining conversion as "an authorized assumption and exercise of the right of ownership over goods or personal chattels belonging to another, to the alteration of their condition *or the exclusion of an owner's rights*" (quoting Peed v. Burleson, Inc., 244 N.C. 437, 439, 94 S.E.2d 351, 353 (1956))).

126. *See* Gallimore v. Sink, 27 N.C. App. 65, 67, 218 S.E.2d 181, 183 (1975) (citing Wall v. Colvard, Inc., 268 N.C. 43, 49, 149 S.E.2d 559, 564 (1966); and then citing Vinson v. Knight, 137 N.C. 408, 408, 49 S.E. 891, 892 (1905)).

as business opportunities and expectancy interests" are not goods or personal chattels and thus are not "owned" for purposes of conversion.[127] This finding seems to hinge on whether or not the property interest is "reduced to tangible form."[128] This makes sense—courts appear to be worried about overextending property protections to items too ethereal to adequately define. But it may also be attributed to the historical lack of intangible goods that one could reasonably claim ownership over.

At the same time, however, when reading the Court's language closely, state law is but one of many sources that may be persuasive in determining property rights. North Carolina law, and other states for that matter, may not have the definitive last word. To this end, federal court decisions have not constrained the analysis of intangible rights to state law choices. Continuing with North Carolina as an example in this regard, one federal district court has held that, "as a matter of law, electronic data and computer software is intangible property."[129] *Kremen v. Cohen*,[130] a recent decision in the Ninth Circuit, further broadens, if only incrementally, the test for determining intangible property rights. There, the Court held that an intangible good is a property interest if it meets three requirements: (1) the interest must be "capable of precise definition," (2) "it must be capable of exclusive possession and control," and (3) some individual must be able to make a "legitimate claim" of ownership.[131] Both examples, at the very least, unmoor the concept of individual property rights from tangibility and thus open the door for recognition of property interests in Bitcoin.

Other sources of law and government agency actions further indicate a shift in recognizing intangible property interests. *Black's Law Dictionary*, for instance, seems amenable to defining Bitcoin as property.[132] Bitcoin, anecdotally, is pledged as collateral in

127. Norman v. Nash Johnson & Sons' Farms, Inc., 140 N.C. App. 390, 414, 537 S.E.2d 248, 264 (2000).

128. HCW Ret. & Fin. Servs. LLC v. HCW Emp. Benefit Servs. LLC, No. 10 CVS 1447, 2015 WL 4238193, at *21 (N.C. Bus. Ct. July 14, 2015).

129. *See* Capitol Comm'n Inc. v. Capitol Ministries, 2013 WL 5493013, at *12 (E.D.N.C. 2013) (citing Am. Online Inc., v. St. Paul Mercury Ins. Co., 347 F.3d 89, 96 (4th Cir. 2003)).

130. 337 F.3d 1024 (9th Cir. 2003).

131. *Id.* at 1030 (quoting G.S. Rasmussen & Assocs., Inc. v Kalitta Flying Serv., Inc., 958 F.2d 896, 903 (9th Cir. 1992).

132. *Property*, BLACK'S LAW DICTIONARY (10th ed. 2014); *see also Intangible Property*, BLACK'S LAW DICTIONARY (10th ed. 2014) ("Property that lacks a physical existence."); *see, e.g.*, James D. Lamm et al., *The Digital Death Conundrum: How Federal*

compliance with Uniform Commercial Code Article 9, and the Uniform Fiduciary Access to Digital Assets Act from the Uniform Law Commission folds Bitcoin into trust and estates law.[133] Furthermore, actions and statements of other government agencies seem to support this definition. The actions of the SEC, FINCEN, and the CFTC indicate recognition of individual interests in Bitcoin—whether a security, money, or a commodity (if it happens to be any), ownership must be attributable to an individual.[134] The IRS, although limiting the definition to "federal tax purposes," explicitly labels Bitcoin and other virtual currency as property.[135] Additionally, Bitcoin is subject to both civil and criminal forfeiture, as evidenced by the U.S. Marshals Service's recent auctions.[136]

The multiplicity of sources above suggests that many areas of the law are amenable to Bitcoin's definition as intangible personal property. As a result, Bitcoin easily satisfies the Ninth Circuit's three-part test. Returning to the example above, Bob's interest definitively lies in the outputs associated with his public address. And the outputs (Bitcoin) are capable of precise definition—each output is a specific, unique line of code. Further, Bitcoin is, by nature, exclusively held and controlled because Bob controls his own private key. Bob's interest in Bitcoin would be diminished, if not extinguished, if it were not capable of exclusive control. And the blockchain ledger announces to "all the world" that the Bitcoin belongs to Bob, and he, as exclusive holder of the private key, is the only person who can make a legitimate claim to the Bitcoin.[137] As indicated above, other

and State Laws Prevent Fiduciaries from Managing Digital Property, 68 U. MIAMI L. REV. 385, 388 (2014).

133. J. Dax Hansen & Joshua L. Boehm, *Treatment of Bitcoin Under U.S. Property Law*, PERKINS COIE 11–14 (Mar. 2017), https://www.virtualcurrencyreport.com/wp-content/uploads/sites/13/2017/03/2016_ALL_Property-Law-Bitcoin_onesheet.pdf [http://perma.cc/N6RF-RLV9]; Nate Lanxon, *Bitcoin Industry Grapples with Age-Old Problem of Inheritance*, BLOOMBERG (Feb. 13, 2018, 5:09 AM), https://www.bloomberg.com/news/articles/2018-02-13/bitcoin-industry-grapples-with-age-old-problem-of-inheritance [http://perma.cc/YQ3W-MX8G (dark archive)].

134. *See supra* text accompanying notes 118–20.

135. *See* I.R.S. Notice 2014-21, 2014-16 I.R.B. 938.

136. *FOR SALE 2,719.32669068 Bitcoins*, U.S. MARSHALS SERV., https://www.usmarshals.gov/assets/2016/Bitcoinauction/ [http://perma.cc/3GXF-6DY8].

137. It is important to mention here the problem of double-spending. It is sufficient for the purpose of this Comment to note that Bitcoin protocol generally prevents (again, relying on the earlier example) Alice from sending five Bitcoin to Bob, then proceeding to send the same five Bitcoin to Carl. For a more detailed explanation of the double-spend problem, see FRANCO, *supra* note 3, at 113–17. In addition, while this analysis serves the purposes here, others have analyzed this Ninth Circuit test in more detail. *See* Hansen & Boehm, *supra* note 133, at 7–8.

legal entities are prepared, or have already taken a definitive step, to recognize this interest. The weight of evidence to date, then, strongly indicates the existence of intangible property interests in Bitcoin.

If an ownership interest does exist in Bitcoin, as the above analysis suggests,[138] the question remains as to when the holder of the interest can claim that interest "against the world." To this end, it is important to briefly consider *when* the interest in ownership of Bitcoin might vest; that is, when the right is "completed . . . for present enjoyment."[139] Once the interest vests, a deprivation of that interest—here, a total loss of possession and use—is the point at which theft occurs.[140] Again applying these concepts to the hypothetical transaction in this Comment, once Alice's transaction to Bob is confirmed and included in a valid block, Bob's interest in the five Bitcoin vests. At that point, the right is "completed" in that the five Bitcoin are attributable to Bob, and only Bob's private key can facilitate use of the Bitcoin transferred to him.[141] Therefore, theft occurs when someone other than Bob takes control of Bob's private key and completes a transfer to another public address.

III. APPLYING THE LAW OF THEFT

Proceeding on the assumption that individuals possess intangible property interests in Bitcoin, its owner then must be afforded the "right against interference with possession from the world at large."[142] And this right necessarily implicates the law of theft—punishment for violating that right is critical to both deterrence and public confidence in its protection. To this end, the Model Penal Code has defined the proper object of theft as "anything of value," including "intangible personal property,"[143] seemingly in an effort to broaden the

138. *See* Shawn Bayern, *Dynamic Common Law and Technological Change: The Classification of Bitcoin*, 71 WASH. & LEE L. REV. ONLINE 22, 33–34 (2014) [hereinafter Bayern, *Dynamic Common Law*] (arguing for a functional approach to recognize rights of property in Bitcoin to match what individual holders already assume they own).

139. *Vested*, BLACK'S LAW DICTIONARY (10th ed. 2014).

140. *See* Tigar, *supra* note 25, at 1448.

141. *See* Hansen & Boehm, *supra* note 133, at 9.

142. Bayern, *Dynamic Common Law*, *supra* note 138, at 31. *Black's Law Dictionary* includes as rights of an owner of property the "right to possess and use, the right to exclude, and the right to transfer." *Property*, BLACK'S LAW DICTIONARY (10th ed. 2014).

143. *See* MODEL PENAL CODE § 223.0 (AM. LAW INST. 1985) (defining "property" for purposes of the provisions concerning theft as "anything of value" that includes items of "intangible personal property"). It is also interesting to note that this definition appears to stem from the Model Penal Code's choice to favor elimination of the common law distinctions between types of theft, consolidating the offense to a single crime that covers a broad array of interests. *See* Moohr, *Federal Criminal Fraud*, *supra* note 38, at 687–88.

protections of the criminal law. The critical question, however, is not whether intangible property rights are objects of theft in the abstract; it is rather "whether the victim's loss constituted property for purposes of the statute being considered."[144]

Two statutes, the NSPA and the CFAA, appear at first glance to provide potential solutions. Both statutes were enacted in response to pervasive issues of theft that created difficulties for state law enforcement. The NSPA sought to confront the problem of thieves escaping over state lines,[145] while the CFAA focused on theft by hacking that arose with the escalating use of computers.[146] By analyzing their application, courts may find adequate justification to extend the statutes to encompass Bitcoin theft. At the very least, this discussion should provide lawmakers with the necessary bases to amend the statutes to accommodate this new form of taking.

The strongest argument, and the statute most apt to deal with Bitcoin theft, is 18 U.S.C. § 1343, the Federal Wire Fraud statute. Long a favorite of federal prosecutors, the statute appears to be the perfect tool, from both a policy and legal perspective, to combat Bitcoin theft. The following discussion lays out the argument that must be made in this regard and will provide a roadmap for prosecution of theft of any blockchain-based crypto-asset.

A. The National Stolen Property Act

Enacted in 1934, the NSPA bars the "transport[], transmi[ssion], or transfer[] in interstate or foreign commerce [of] any goods, wares, merchandise, securities, or money, of the value of $5000 or more, knowing the same to have been stolen, converted, or taken by fraud."[147] When interpreting this statute, courts will find a violation of the statute if an individual "(1) transports or causes to be transported; (2) in interstate commerce; (3) [goods, wares, merchandise, securities, or money] valued at $5,000 or more; (4) with knowledge that the property has been stolen, converted, or fraudulently taken from its rightful owner."[148] The NSPA, however, treats only the symptom and not the disease—only transporting stolen goods, not the theft of those goods, is prohibited. At the same time, it is an effective tool for

144. *Id.* at 686.

145. *Id.* at 697.

146. Note, *The Vagaries of Vagueness: Rethinking the CFAA as a Problem of Private Nondelegation*, 127 HARV. L. REV. 751, 751 (2013).

147. 18 U.S.C. § 2314 (2012).

148. Moohr, *Federal Criminal Fraud*, *supra* note 38, at 697–98.

deterrence of theft.[149] But a key issue in applying the NSPA to Bitcoin theft lies in the courts' uncertain treatment of intangible property. This problem, however, can be overcome.

Courts often conflate the first two elements and simply ask whether the item was transferred through interstate commerce. Generally speaking, the Supreme Court has historically construed "interstate commerce" broadly.[150] Lower courts, however, appear divided as to whether, for the purpose of criminal statutes, the term encompasses internet transmissions of intangible items of property. Some require a showing that the internet transmission itself did in fact cross state lines—that is, an intangible item was transmitted from a server in one state to a server in another.[151] Other courts merely require a showing that the transmission used the internet.[152] In other criminal statutes, Congress specifically defines use of the internet as within "interstate commerce," but it has not amended the NSPA to that effect.[153]

Unfortunately, Congress left "goods, wares merchandise, securities or money" undefined without explanation.[154] In response, courts often rely on various common law methods to interpret these terms.[155] Generally, courts have found that some "physical identity between the property stolen and property transported" must be present.[156] This holding appears to hinge on depriving the owner of use—physical takings, by necessity, accomplish this. To this end, the Supreme Court found the NSPA inapplicable to theft of copyright, basing this holding primarily on the fact that copyright infringement

149. *See id.* at 697.

150. *See* McElroy v. United States, 455 U.S. 642, 652–54 (1982).

151. *See generally* Valeria G. Luster, Note, *Let's Reinvent the Wheel: The Internet as a Means of Interstate Commerce in* United States v. Kieffer, 67 OKLA. L. REV. 589 (2015) (discussing at length the split between federal courts). The Supreme Court has not stepped in to resolve this divide and the many other issues presented with use of the internet in criminal statutes. *Id.* at 590.

152. *Id.*

153. *See id.* at 596–97.

154. United States v. Aleynikov, 676 F.3d 71, 76 (2d Cir. 2012); U.S. DEP'T OF JUSTICE, JUSTICE, CRIMINAL RESOURCE MANUAL § 1312 (2018), https://www.justice.gov/usam/criminal-resource-manual-1312-national-stolen-property-act-goods-wares-merchandise [https://perma.cc/5JLK-XGWN].

155. *See* Tamara J. Wayland, Note, *Computer Technology—The National Stolen Property Act and its Applicability to Property Rights in Computer Source Code—Do Rights Exist?*—United States v. Brown*, 925 F.2d 1301 (10th Cir. 1991)*, 11 TEMP. ENVTL. L. & TECH. J. 155, 161 (1992).

156. Moohr, *Federal Criminal Fraud*, *supra* note 38, at 698; *see also Aleynikov*, 676 F.3d at 77.

does not totally deprive the holder of use.[157] In addition, other lower courts have held that the NSPA does not cover "purely intangible property" that lacks any physical element.[158] Courts premise the "physical taking" holding on the fact that such a physical taking clearly deprives the rightful owner of use, often completely.[159] In each of the above cited cases, however, theft of intangible property did not lead to complete deprivation of use.[160]

Therefore, this statute will not apply to the act of taking an individual's private key.[161] It, however, likely covers the unlawful transfer of Bitcoin from the rightful owner to the thief's public address.[162] Bitcoin transactions occur on the Bitcoin network; an internet connection plus the proper software are required.[163] The transmission of Bitcoin over the Bitcoin network remains substantially unaddressed by Congress and courts—Congress's silence in this regard remains unhelpful. It may be argued, then, that Supreme Court precedent dictates a broad reading of the interstate commerce element in the NSPA—this transfer, if accomplished via the internet, occurs in interstate commerce. In addition, technological properties of the Bitcoin network allow for an easy inference that, since the transaction is broadcast to all nodes on the network, and it is verifiable that operating nodes exist in more than one state, the transmission crossed state lines.[164]

The central difficulty in prosecuting Bitcoin theft under the NSPA largely resides in classifying Bitcoin as a "good, ware, or merchandise." Courts recognize that the statute, crafted in the 1930s,

157. Dowling v. United States, 473 U.S. 207, 215–16 (1985); Moohr, *Federal Criminal Fraud*, *supra* note 38, at 699.

158. *Aleynikov*, 676 F.3d at 77.

159. *Id.* at 78–79. In *Aleynikov*, the defendant was accused of stealing his employer's source code, uploading it to a server in one place, and downloading it in another. Crucially, the employer did not lose access to the source code; rather, the defendant merely gained access to a proprietary code that would be valuable to competitors. *Id.* at 73–75.

160. *See* United States v. Agrawal, 726 F.3d 235, 237–39 (2d Cir. 2013); United States v. Martin, 228 F.3d 1, 6–10, 13–15 (1st Cir. 2000); United States v. Stafford, 136 F.3d 1109, 1111–12, 1114–15 (7th Cir. 1998); United States v. Brown, 925 F.2d 1301, 1305–08 (10th Cir. 1991).

161. *See* Moohr, *Federal Criminal Fraud*, *supra* note 38, at 697 n.88 (noting that "refinements of larceny are not related to the primary congressional purpose of the Act").

162. As mentioned above, this transfer requires the use of the rightful owner's private key—other nodes will not verify the transaction unless the hash of the user's private key and the message containing Bitcoin are confirmed. *See supra* Section I.A.

163. *See id.*

164. *See* United States v. Kieffer, 681 F.3d 1143, 1154–55 (10th Cir. 2012).

does not comport with modern realities and creates ambiguities.[165] Courts, however, seem reluctant to stray from the "physical taking" requirement until Congress says otherwise.[166]

At the same time, in spite of the lack of a physical element, the theft of Bitcoin differs from other takings of intangible property in one critical aspect—once a user's private key is stolen, this completely deprives the user of its use, and any subsequent transaction involving Bitcoin tied to the user's private key is irreversible.[167] Thus, Bitcoin theft more closely mirrors the taking of a physical item—both owners are completely deprived of use of the thing—as opposed to business information or other forms of intangible property that courts have thus far been reluctant to recognize.

B. The Computer Fraud and Abuse Act

Another statute that may provide a basis for criminal prosecution for theft of Bitcoin is the CFAA.[168] Originally enacted in the 1980s, the CFAA initially targeted improper access of government computers.[169] Congress subsequently amended the CFAA five times to meet the growing number of criminal actions related to the increased use of computers by the general public.[170] To this end, the statute is typically applied in cases of "computer intrusion or hacking."[171] The CFAA now provides for forfeiture of "any property, real or personal," gained by violation of the Act, providing compensatory relief to victims of the fraud proscribed.[172]

165. *See* United States v. Zhang, 995 F. Supp. 2d 340, 348–49 (E.D. Pa. 2014).

166. *See* United States v. Aleynikov, 676 F.3d 71, 78–79 (2d Cir. 2012).

167. *See supra* Section I.B. Additionally, one district court noted in dicta that "courts have liberally construed" the terms to cover "personal property and chattels that are ordinarily the subject of commerce," and courts may "unduly restrict" the operation of the NSPA by requiring a physical taking. United States v. Riggs, 739 F. Supp. 414, 421 (N.D. Ill. 1990). This interpretation, coupled with the complete deprivation of use involved in Bitcoin theft, may be enough to overcome the tangibility requirement in arguing NSPA's application to theft of Bitcoin.

168. 18 U.S.C. § 1030 (2012).

169. H.R. REP. NO. 99-612, at 4 (1986).

170. *See* Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1561 (2010) [hereinafter Kerr, *Vagueness Challenges*].

171. Tiffany Curtiss, Comment, *Computer Fraud and Abuse Enforcement: Cruel, Unusual, and Due for Reform*, 81 WASH. L. REV. 1813, 1822 (2016).

172. 18 U.S.C. § 1030(i) (2012).

1. 18 U.S.C. § 1030(a)(2): Accessing a Computer and Obtaining Information

In relevant part, the provision defines as criminal any actor who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer."[173] The Act fails to define the statute's first term, "intentional access of a computer."[174] Currently, however, courts do not constrain the statute through this element.[175] Rather, "any internet-related transmission . . . that results in the user's computer 'accessing a series of networked computers'" will suffice.[176] Similar to "intentional access," Congress gives no definition of "without authorization or exceeds authorized access," and courts have largely not offered an interpretation.[177] In light of this uncertainty, the courts rely on the dictionary to define the term as "access . . . without permission or approval."[178] Ostensibly, the one who controls access to the information is the one who may grant, or deny, permission.[179] Lastly, the statute fails to define "information."[180] But the report on the 1996 amendments to § 1030(a)(2) offers guidance, specifically designating "information stored in intangible form" as falling within the statutory language.[181] Further, *obtaining* such intangible information is interpreted broadly and may be accomplished by "merely reading it."[182]

In contrast, Congress does define a "protected computer" as one "which is used in or affecting interstate or foreign commerce."[183] Congress intended the use of "affect" in the definition to demonstrate an intent for the provision to "reach as far as the Commerce Clause of

173. *Id.* § 1030(a)(2).

174. Patricia L. Bellia, *A Code-Based Approach to Unauthorized Access Under the Computer Fraud and Abuse Act*, 84 GEO. WASH. L. REV. 1442, 1464 (2016).

175. *Id.* at 1468.

176. *Id.* at 1465.

177. *See* Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1616–17 (2003) (noting that existing interpretations of the term, when given, are often in conflict) [hereinafter Kerr, *Cybercrime's Scope*]; Kerr, *Vagueness Challenges*, *supra* note 170, at 1572 (noting "[e]xactly what . . . makes an 'access' unauthorized[] is presently unclear").

178. Bellia, *supra* note 174, at 1468–69.

179. *See* WEC Carolina Energy Sols. LLC v. Miller, 687 F.3d 199, 203 (4th Cir. 2012). The analysis gets more complicated, however, when an employee accesses the computer systems of her employer. *See* Bellia, *supra* note 174, at 1469–71.

180. Czech v. Wall St. on Demand, Inc., 674 F. Supp. 2d 1102, 1108 (D. Minn. 2009).

181. S. REP. NO. 104-357, at 7 (1996).

182. *Id.*

183. 18 U.S.C. § 1030(e)(2) (2012).

the Constitution permits."[184] To this end, many courts have held that a computer's connection to the internet is sufficient to qualify it as a "protected computer."[185] Some commenters, in support of this point, make the inference that since all "internet-connected computer[s] [are] used in interstate communication," the computers are, by nature, in interstate commerce for purposes of this section.[186] Other courts have relied on the connection between the computer that is accessed and those who are interacting with its software, inferring "interstate commerce" from such an interaction that crosses state lines.[187]

Applied to theft of private keys, a forceful argument may be made for prosecution under § 1030(a)(2). The thief necessarily must intentionally use the internet to access the exchange's stored private keys; what remains is a showing that the exchange's computers are "networked." Given the technical description of the Bitcoin network above, this element is met with little difficulty—each node running blockchain software is part of a network that is constantly receiving transactions broadcast to it. And active nodes are spread out both among multiple states and internationally.[188] Showing "without authorization" presents little difficulty as well: hackers, by common definition,[189] do not have permission to access the exchange's network,[190] at least assuming that the online exchange has not given the thief this permission.[191] And Bitcoin outputs, as lines of code, are most simply defined as "information."[192] Intangibility is of no

184. *See* Bellia, *supra* note 174, at 1643.

185. *See, e.g.*, United States v. Drew, 259 F.R.D. 449, 457 (C.D. Cal. 2009).

186. *See* Bellia, *supra* note 174, at 1462.

187. *See, e.g.*, Quantlab Techs. Ltd. v. Godlevsky, 719 F. Supp. 2d 766, 775–76 (S.D. Tex. 2010).

188. *Global Bitcoin Nodes Distribution*, BITNODES, https://bitnodes.earn.com [https://perma.cc/5VT4-DQ5P].

189. *Hacker*, MERRIAM-WEBSTER DICTIONARY (11th ed. 2005) ("[A] person who illegally gains access to and sometimes tampers with information in a computer system."). The *Black's Law Dictionary* definition, while using language that appears somewhat outdated, is still applicable: "[s]omeone who surreptitiously uses or changes the information in another's computer system." *Hacker*, BLACK'S LAW DICTIONARY (10th ed. 2014).

190. It appears unlikely that the access would have to "circumvent[] a technological access barrier" in order to be unauthorized. United States v. Nosal, 844 F.3d 1024, 1024 (9th Cir. 2016).

191. The outcome may be different if the private keys were accessed by someone with authorization to access the host's exchange information, such as an employee of the particular exchange. *See* Kerr, *Cybercrime's Scope*, *supra* note 177, at 1632–37.

192. One common definition of "information" is "the attribute inherent in and communicated by one of two or more alternative sequences or arrangements of something

consequence—the amendment reports mentioned above support this reading, and others forcefully put forward this argument.[193] Lastly, much like the NSPA, the "protected computer" element will depend on the jurisdiction—one must show that the exchange was connected to the internet or that the exchange's users, those "interacting" with the computer's software, were located across state lines.

The difficulty with prosecution under this statute is its breadth, attributable to both statutory amendments and court interpretation, leaving prosecutions under the CFAA susceptible to vagueness attacks. Orin Kerr has argued that this breadth requires courts to engage in narrow statutory interpretation, which would appear to cast doubt on the above analysis.[194] As the doctrine stands, however, § 1030(a)(2) appears to provide a viable path for prosecution. At the very least, such a prosecution may draw Congress's attention to the changing application of the statute and the need for more precise definition of terms outpaced by technology.

2. 18 U.S.C. § 1030(a)(4): Accessing to Defraud and Obtain Value

In relevant part, § 1030(a)(4) bars

> knowingly and with intent to defraud, access[ing] a protected computer without authorization . . . and by means of such conduct further[ing] the intended fraud and obtain[ing] anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any one year period.[195]

"Knowingly and with intent to defraud" is not defined by statute, but Senate and House reports discussing the CFAA refer to the phrase in the context of its use in 18 U.S.C. § 1029.[196] Under § 1029, prosecutors must show "the property wrongfully obtained via computer furthers the intended fraud" and knowledge by the defrauder of this fact.[197] Fraud is "furthered" when the property obtained later is used to

(as . . . binary digits in a computer program) that produce specific effects." *Information*, MERRIAM-WEBSTER DICTIONARY (11th ed. 2005).

193. *See* Joshua A.T. Fairfield, *Bitproperty*, 88 S. CAL. L. REV. 805, 807–12 (2015).

194. *See* Kerr, *Vagueness Challenges*, *supra* note 170, at 1561.

195. 18 U.S.C. § 1030(a)(4) (2012).

196. CHARLES DOYLE, CONG. RESEARCH SERV., CRS 97-1025, CYBERCRIME: AN OVERVIEW OF THE FEDERAL COMPUTER FRAUD AND ABUSE STATUTE AND RELATED FEDERAL CRIMINAL LAWS 52 (2014).

197. S. REP. NO. 99-432, at 10 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 2479, 2487–88. The report notes that this distinction is crucial to treat the action under § 1030(a)(4) as a felony and not merely as a misdemeanor. *Id.*

commit the fraud intended.[198] The meaning of "fraud," however, remains undefined, and the common-law development of the term is unsettled.[199] Some courts, in an apparent desire for uniformity of meaning, equate fraud under § 1030(a)(4) to its use in the wire fraud statute.[200] This meaning, described below, is extraordinarily broad. Other courts, addressing the same section in a civil context, interpret the language more broadly to cover any "wrongdoing"[201] that deprives someone of a thing of value.[202] Lastly, the "access of a protected computer" and "authorization" elements track § 1030(a)(2).[203]

Returning to the prototypical theft described above, this statute might apply with similar force as § 1030(a)(2). The mens rea elements—knowledge and intent to commit fraud—are easily met. Hackers, again by definition, are likely knowing participants who aim to commit fraud. If fraud is given its civil meaning of "wrongdoing," depriving exchange users of private keys by hacking, a harm explicitly targeted by the CFAA, almost certainly fits within the statutory definition.[204] Finally, the fraud is "furthered" under this definition when the thief uses the private keys to transfer Bitcoin from the rightful owner to a public address controlled by the thief.[205]

The likely challenge to prosecution under this statute is whether Bitcoin meets the definition of "anything of value." Whether Bitcoin is "valuable," in the sense of possessing intrinsic monetary value, is a point of disagreement.[206] But any item is "valuable" in that individuals are willing to buy and sell it at a market price. This is arguably the

198. *See* COMPUT. CRIME & INTELLECTUAL PROP. SECTION, *supra* note 39, at 29.

199. *Id.* at 27–29.

200. *See* United States v. Czubinski, 106 F.3d 1069, 1079 (1st Cir. 1997) ("For the same reasons we deemed the trial evidence could not support a finding that [the Defendant] deprived the IRS of its property, . . . we find that [the Defendant] has not obtained valuable information in furtherance of a fraudulent scheme for the purposes of section 1030(a)(4).").

201. *See* COMPUT. CRIME & INTELLECTUAL PROP. SECTION, *supra* note 39, at 29.

202. DOYLE, *supra* note 196, at 52.

203. *See supra* Section III.B.1.

204. For the discussion of fraud under the wire fraud provision, see *infra* Section III.C.

205. For a recent example of this form of theft in action, see Nikhilesh De, *$400K: Hacker Makes Off with Stellar Lumens in BlackWallet Theft*, COINDESK (Jan. 16, 2018, 1:39 PM), https://www.coindesk.com/400k-hacker-makes-off-with-stellar-lumens-in-blackwallet-theft/ [http://perma.cc/9QEY-7MA4].

206. A prominent investor argues that the value of Bitcoin is "speculation" and not based on "underlying value or the appropriateness of . . . price." *See* Memorandum from Howard Marks to Clients of Oaktree Capital Mgmt., L.P. 17 (July 26, 2017), https://www.oaktreecapital.com/docs/default-source/memos/there-they-go-again-again.pdf [https://perma.cc/ZUK3-YTUU].

most natural reading of the term "value" as used in the statute. "Value" is not modified by either "intrinsic" or "monetary"; rather, "anything" seems to imply a broad definitional standard of "value." It is clear, through news headlines and otherwise, that Bitcoin is bought and sold daily for significant sums.[207]

Again, however, as with § 1030(a)(2) above, this broad language may leave prosecutions under the statute susceptible to vagueness challenges. But a similar proscriptive solution is apt here as well—until Congress makes the choice to amend the statute, and so long as courts interpret its language in the way described above, the path to prosecution of Bitcoin theft is viable.

C. 18 U.S.C. § 1343: Wire Fraud

The mail fraud provision, § 1341, and its "sister provision"[208] covering wire fraud, § 1343,[209] have long been a favorite of federal prosecutors.[210] Section 1343 implicates those

> having devised or intending 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, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice . . . .[211]

Because of courts' historically broad interpretation of the statute, it remains prosecutors' "first line of defense against virtually every new area of fraud to develop in the United States."[212] The statutes are aimed at frauds concerning property, and both have their "origin in

207. *See Markets*, BITCOINCHARTS, https://Bitcoincharts.com/markets/ [http://perma.cc/BB6J-7KFM].

208. *See* C.J. Williams, *What Is the Gist of the Mail Fraud Statute?*, 66 OKLA. L. REV. 287, 304, 320 (2014) (referring to the federal mail and wire fraud statutes as "sisters").

209. 18 U.S.C. § 1343 (2012).

210. *See* Jed S. Rakoff, *The Federal Mail Fraud Statute (Part I)*, 18 DUQ. L. REV. 771, 772 (1980). Judge Rakoff, writing at a time when he was Chief of Business Frauds Prosecutions as a U.S. Attorney, opined that "[t]o federal prosecutors of white collar crime, the mail fraud statute is our Stradivarius, our Colt 45, our Louisville Slugger, our Cuisinart—and our true love." *Id.* at 771.

211. § 1343.

212. Rakoff, *supra* note 210, at 772 (quoting United States v. Maze, 414 U.S. 395, 405 (1974) (Burger, C.J., dissenting)). Prosecutors may be even more likely to utilize the statutes following the 2002 amendments to both provisions that increased the maximum sentencing for convicted defendants "from 5 to 20 years." Jack E. Robinson, *The Federal Mail and Wire Fraud Statutes: Correct Standards for Determining Jurisdiction and Venue*, 44 WILLAMETTE L. REV. 479, 479–80 (2008).

the desire to protect individual property rights."[213] Partly in recognition of this underlying principle, and considering Congress's choice to use almost identical language in § 1343 as in § 1341, the Court interprets this identical language "in pari materia."[214] Predictably, the elements of § 1343 mirror those of § 1341,[215] reflecting an intent by Congress to simply extend § 1341's principles to frauds committed using a new medium.[216] The elements that must be met are uncomplicated—the government must establish that the defendant intended to carry out a scheme to defraud and used wires to further that scheme.[217] And if the government meets its burden, it establishes a predicate offense to other potential criminal sanctions.[218]

The "schemes to defraud" included under § 1343 are, in the words of some commentators, "too numerous to catalog."[219] Some suggest that its theoretical limits stretch to encompass not only

213. Carpenter v. United States, 484 U.S. 19, 25 (1987). This point is critical not only in the context of Bitcoin but also in the wider discussion of property interests in other forms information supported by blockchain protocols.

214. Pasquantino v. United States, 544 U.S. 349, 355 n.2 (2005). Lower courts have noted that "interpreting one [provision] govern[s] the other as well." United States v. Morelli, 169 F.3d 798, 806 n.9 (3d Cir. 1999). In other words, case law applying one statute equally applies to the other.

215. United States v. Frey, 42 F.3d 795, 797 (3d Cir. 1994). Most other circuit courts have held similarly. *See* U.S. DEP'T OF JUSTICE, CRIMINAL RESOURCE MANUAL, TITLE 9 § 941 (2018) (citing United States v. Briscoe, 65 F.3d 576, 583 (7th Cir. 1995); and then citing *Frey*, 42 F.3d at 797), https://www.justice.gov/usam/criminal-resource-manual-941-18-usc-1343-elements-wire-fraud [https://perma.cc/KEG8-T43J]. In addition, the Supreme Court, since its decision in *Carpenter*, conducts the analysis of fraud under both statutes similarly. *See* Debora Carfora, Note, United States v. Newark*: Semantics and Misrepresentation in Mail and Wire Fraud, Does it Really Matter Who Was Deceived?*, 60 CATH. U. L. REV. 779, 780–81 (2011).

216. *See* H.R. REP. NO. 82-1750, at 22 (1952), *as reprinted in* 1952 U.S.C.C.A.N. 2234, 2256 (expanding to include "Fraud by Radio").

217. *E.g.*, United States v. Wynn, 684 F.3d 473, 478 (4th Cir. 2012) ("To be convicted of mail fraud or wire fraud, a defendant must specifically intend to lie or cheat or misrepresent with the design of depriving the victim of something of value."). Turning to the text of § 1343, it applies to those

> having devised . . . 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.

18 U.S.C. § 1343 (2012). In addition, the Supreme Court has indicated that federal jurisdiction is established simply by interstate use of wires. *See* Neder v. United States, 527 U.S. 1, 20 (1999).

218. *See Pasquantino*, 544 U.S. at 383 (Ginsburg, J., dissenting). While beyond the scope of this Comment, it bears reinforcing that prosecutors may pursue both RICO and money laundering charges after establishing wire fraud. *See id.*

219. *See* Rakoff, *supra* note 210, at 772.

common law conceptions of fraud[220] but *any* scheme that involves "intent to take property by deception," far exceeding the common law principles deeply rooted in the law of theft.[221] In a few instances where the Court sought to narrow the scope of objects subject to fraud, Congress immediately responded with amendments to encompass the objects recently excluded.[222] At the very least, the Supreme Court recognizes property interests—both tangible and intangible[223]—as objects of fraudulent schemes.[224] In addition, the scheme may not, in fact, cause loss by the victim or benefit to the fraudster, nor is this required; rather, the scheme to defraud simply "must be material to the contemplated transaction."[225]

The use of wires must also be interstate. Some courts require a showing that the transmission by wire, in fact, crossed state lines.[226] However, the same division that exists in application of the term in the CFAA exists here—other courts merely require demonstrated use of the internet to be interstate.[227] In addition, the wire use must be in furtherance of the scheme to defraud.[228] The Court chooses to interpret this element broadly and generally incorporates the analysis

220. It appears, at the very least, that the statute does incorporate the frauds recognized at common law—since the term is not defined by statute, the Court will impute the "established meaning of th[is] term[]." *See Neder*, 527 U.S. at 21–22 (quoting Nationwide Mut. Ins. Co. v. Darden, 503 U.S. 318, 322 (1992)).

221. David Mills & Robert Weisburg, *Corrupting the Harm Requirement in White Collar Crime*, 60 STAN. L. REV. 1371, 1394 (2008). The Court, elsewhere, seems to state as much, noting that "to defraud" commonly means "wronging one in his property rights by dishonest methods or schemes," and that the words "usually signify the deprivation of something of value by trick, deceit, chicane, or overreaching." Hammerschmidt v. United States, 265 U.S. 182, 188 (1924).

222. Carfora, *supra* note 215, at 781.

223. Carpenter v. United States, 484 U.S. 19, 25 (1987) (quoting McNally v. United States, 483 U.S. 350, 359 n.8 (1987)).

224. McNally v. United States, 483 U.S. 350, 360 (1987), *superseded by statute*, Act of Nov. 19, 1998, Pub. L. No. 100-690, § 7603(a), 102 Stat. 4181, 4508 (1988), *as recognized in* Skilling v. United States, 561 U.S. 358, 402 (2010).

225. Mills & Weisburg, *supra* note 221, at 1395 (citing *Neder*, 527 U.S. at 25). Further, the federal wire fraud statutes appear to divorce from the civil law in another respect, not requiring "justifiable reliance" by the one defrauded for criminal culpability. *Id.* at 1394–95. Nor does it encounter the value problem posed by the CFAA contemplated above. *Id.*

226. United States v. Kieffer, 681 F.3d 1143, 1155 (10th Cir. 2012); United States v. Wright, 625 F.3d 583, 595 (9th Cir. 2010).

227. *Kieffer*, 681 F.3d at 1153–55 ("This case, then, is the 'typical case' where 'the evidence of the interstate element can be gleaned from the record' evidence . . . ." (quoting United States v. Swenson, 335 F. App'x 751, 753–54 (10th Cir. 2009))); *Wright*, 625 F.3d at 595.

228. 18 U.S.C. § 1343 (2012).

into the mens rea requirement.[229] To that end, any use of wires not required by law and intended to perpetrate fraud is enough to establish furtherance of the fraud.[230]

Applied to Bitcoin theft, § 1343 requires the least "extension" of statutory language and principles and, therefore, is the best path for prosecution. It appears clear that the property interest at stake, ownership of Bitcoin, is gained by deception in the prototypical theft. This is most true when the exchange software is hacked, the user's private keys are compromised, and the thief completes an unauthorized transaction. It is likely equally true when hackers exploit a flaw in an exchange's security mechanisms—the deception, in this instance, lies in the surreptitious search for the flaw only for purposes of wrongdoing. In many cases intent will not be difficult to prove—the hacker, through the act of hacking or deception, intends to defraud users of the host exchange. Further, private keys may be analogized to other forms of *intangible* property the Court recognizes.[231] The wires in this case, the internet connection used to facilitate the hack, are used in furtherance of the scheme. Lastly, the wire use is likely interstate: in most jurisdictions, prosecutors need to show that the origination of use of the wire occurred across state lines from the servers hosting the exchange. Given the reality of the modern internet, and the Bitcoin network described above, the showing required by many courts will be perfunctory.[232]

Section 1343, then, is the best vehicle for prosecution of Bitcoin theft. It aligns the congressional purposes behind the statute—a stop-gap for new forms of wrongdoing—with language amenable to encompassing the intricacies that blockchain presents. This stop-gap function, moreover, will become increasingly important if, or perhaps more likely *when*, blockchain-based assets become commonplace as a way to move and store valuable information.

229. *See* Schmuck v. United States, 489 U.S. 705, 710–11 (1989) (citations omitted) ("[T]he use of the mails need not be an essential element of the scheme. It is sufficient for the mailing to be 'incident to an essential part of the scheme . . . .'").

230. *See* United States v. Lake, 472 F.3d 1247, 1256 (10th Cir. 2007).

231. *See* Carpenter v. United States, 484 U.S. 19, 26 (1987) (discussing confidential business information); Int'l News Serv. v. Associated Press, 248 U.S. 215, 236 (1918) (discussing news information); United States v. Shyres, 898 F.2d 647, 652 (8th Cir. 1990) (discussing spending control).

232. *See Kieffer*, 681 F.3d at 1155; *Wright*, 625 F.3d at 595; *see also Global Bitcoin Nodes Distribution*, BITNODES, https://bitnodes.earn.com [https://perma.cc/5VT4-DQ5P].

IV. EXTRA-LEGAL OBSTACLES TO ENFORCEMENT OF CRYPTO-ASSET THEFT

While a solid path to prosecution appears to exist, the application of criminal provisions to theft of Bitcoin does not come without substantial challenges. As noted above, no one has been convicted of theft of crypto-assets. Prosecutors seem to prefer to charge the effects of theft—money laundering of proceeds derived from selling stolen Bitcoin—by waiting until the thief converts Bitcoin to cash.[233] There are a number of reasons for this approach, and this discussion will focus on two in particular: resistance from the Bitcoin community to regulation in any form and the many difficulties Bitcoin poses for law enforcement. But as the use cases for blockchain grow and are implemented, addressing these challenges and overcoming the legal hurdles to prosecution are essential.

A. The Bitcoin Community

The predecessors of Bitcoin trace their roots to libertarian politics of the early 1980s, which valued absolute privacy and freedom from any government intervention.[234] The earliest advocates of digital cash[235] envisioned complex source code and cryptography as the avenue to achieve both of those key values.[236] This led many of the same advocates to begin the search for and development of code written to provide individuals with complete anonymity and control over transactions.[237] While most early efforts failed to gain popular appeal,[238] the digital cash community persevered, as did their general

233. *See, e.g.*, Press Release, U.S. Attorney's Office N. Dist. of Cal., 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/NQZ3-Z2PX] (abstaining from charging the defendant with theft and instead charging him with money laundering).

234. *See* Steve Levy, *E-Money (That's What I Want)*, WIRED (Dec. 1, 1994, 12:00 PM), https://www.wired.com/1994/12/emoney/ [http://perma.cc/U2PN-BP89 (dark archive)] (discussing the 1980's Digicash inventor's political ideals).

235. *See* Eric Hughes, *A Cypherpunk's Manifesto*, ACTIVISM: CYPHERPUNK (Mar. 9, 1993), https://www.activism.net/cypherpunk/manifesto.html [https://perma.cc/5S4S-7EHD].

236. *Id.*

237. *See* David Chaum, *Achieving Electronic Privacy*, 267 SCI. AM. 96, 96–97 (Aug. 1992). Chaum is regarded as the first inventor of cryptocurrencies when he debuted the idea for "Digicash" in the 1980s, which would later become a reality in the 1990s. Levy, *supra* note 234.

238. *See* Jeremy Clark, Foreward to NARAYANAN ET AL., *supra* note 49, at IX. The only exception, PayPal, moved away from the idea of "cryptographic payments," instead opting for the payment mechanism to be handled by established banks. *See* Karlin

distaste for government regulation.[239] Fast forward to 2008, when this libertarian spirit meets a global financial crisis and subsequent government bailout—the formerly niche interest suddenly has a wider audience when the global banking system, trusted by many, failed spectacularly.[240] This general distrust of government intervention has not subsided and continues to permeate the Bitcoin community.[241]

Other early Bitcoin advocates, however, recognized the need for limited government intervention, and that limited prosecution of the most egregious thefts may be welcomed.[242] From a normative perspective, the rule of law must outweigh libertarian ambitions of anonymity and privacy, and practically speaking, prosecution of Bitcoin theft may help, not hinder, the development of the technology. The balance between encouraging innovation and maintaining order is tenuous, but both Congress and the courts indicate that the criminal law is an appropriate vehicle for enforcing that order.[243] Criminal prosecutions deter bad actors—and potential disrupters of the project—while leaving technological development largely uninterrupted. And prosecution of bad actors will bolster the general trust and confidence in blockchain, further incentivizing its development and application.

B. Law Enforcement

The most difficult challenge may be left to law enforcement—the relative anonymity of the crypto-asset thief will require enforcement agencies to expend tremendous resources, both time and money, to track down the bad actor. The Federal Bureau of Investigation

Lillington, *PayPal Puts Dough in Your Palm*, WIRED (July 27, 1999, 12:00 PM), https://www.wired.com/1999/07/paypal-puts-dough-in-your-palm/ [http://perma.cc/936M-FR9Z (dark archive)].

239. *See* Hughes, *supra* note 235. In the most relevant passage, Hughes notes:

> Cypherpunks deplore regulations on cryptography, for encryption is fundamentally a private act. The act of encryption, in fact, removes information from the public realm. Even laws against cryptography reach only so far as a nation's border and the arm of its violence. Cryptography will ineluctably spread over the whole globe, and with it the anonymous transactions systems that it makes possible.

240. POPPER, *supra* note 35, at 32–33.

241. *See, e.g.*, Hughes, *supra* note 235 (advocating for the resistance of regulation).

242. Wences Cesares, *Bitcoin Needs Both Unregulated and Regulated Network Nodes*, XAPO BLOG (May 11, 2017), https://blog.xapo.com/about-Bitcoins-censorship-resistance-regulation/ [https://perma.cc/65DE-3UZH].

243. *See* Geraldine Szott Moohr, *The Problematic Role of Criminal Law in Regulating the Use of Information: The Case of the Economic Espionage Act*, 80 N.C. L. REV. 853, 858–59 (2002) [hereinafter Moohr, *The Problematic Role*].

("FBI") was aware of the problem of anonymity and its implications for theft and other malicious uses of blockchain technology as far back as 2011.[244] To complicate matters further, the blockchain industry continues to create features to increase the relative anonymity of users like "mixing services" and multi-signature transactions.[245] And bad actors are paying attention to these innovations in anonymity, using them as a shield while they search for new weaknesses in the technology.[246] Considering these challenges, the FBI and other agencies will have to continue to be creative in forging solutions to these complex new crimes.[247]

Losses from cybercrime continue to rise, however, and if the market price of Bitcoin increases drastically or blockchain-based assets become critical parts of the transfer of business information, theft will increasingly play a role in that statistic.[248] While this may seem, in the larger scheme of federal criminal enforcement, to be a minor issue at present, Bitcoin theft fits neatly into other trends of increasing internet-based crimes already present.[249] Data breach—a crime with obvious similarities to Bitcoin theft—already accounts for the second-most number of victims in the last year of reported statistics.[250]

And, to their credit, enforcement agencies seem to be taking first steps in meeting the challenge of rapidly advancing technology.[251] Private-sector groups are similarly devising ways to use public

244. *See* FED. BUREAU OF INVESTIGATION, BITCOIN VIRTUAL CURRENCY: UNIQUE FEATURES PRESENT DISTINCT CHALLENGES FOR DETERRING ILLICIT ACTIVITY 1 (2012), https://www.wired.com/images_blogs/threatlevel/2012/05/Bitcoin-FBI.pdf [https://perma.cc/AXR9-AK8B].

245. KARAME & ANDROULAKI, *supra* note 52, at 97–120.

246. *See* Moohr, *The Problematic Role*, *supra* note 243, at 857–58; Andy Greenberg, *Mind the Gap: This Researcher Steals Data with Noise, Light, and Magnets*, WIRED (Feb. 7, 2018, 8:06 AM), https://www.wired.com/story/air-gap-researcher-mordechai-guri/ [http://perma.cc/LS32-B7NL (dark archive)] (discussing a new electronic theft technique called MAGNETO).

247. *See Major Financial Crime: Using Intelligence and Partnerships to Fight Fraud Smarter*, *News*, FBI (Apr. 4, 2012), https://www.fbi.gov/news/stories/major-financial-crime [http://perma.cc/Z3FU-SX5Y].

248. *See* FED. BUREAU OF INVESTIGATION, 2016 INTERNET CRIME REPORT 10, 13 (2016), https://pdf.ic3.gov/2016_IC3Report.pdf [https://perma.cc/JR8Z-RQLA] (explaining that virtual currencies, such as Bitcoin, are used in theft tactics like extortion and ransomware).

249. *See id.*

250. *Id.* at 17.

251. *Cyber Crime*, *What We Investigate*, FBI, https://www.fbi.gov/investigate/cyber [http://perma.cc/AL8H-CFAT].

addresses and information to identify bad actors.[252] Chainalysis, for example, has already established partnerships with the FBI, SEC, and other agencies.[253] It seems likely that social forces around Bitcoin theft, and possibly a correlated increasing economic effect, will be crucial in convincing enforcement agencies to dedicate the resources to overcome these challenges.

CONCLUSION

Bitcoin continues to grab headlines and will continue to play a part in the national conversation as the use cases for the technology expand. One can expect that the cases of theft will likely increase as well. Prosecution of this theft will merely recognize an interest in Bitcoin that society already acknowledges—Bitcoin is a *thing* that can be owned and taking it is an *action* that the law must punish.

This is not simply important as possible recourse to compensate victims, or even to deter future thieves, although this will play a part in the conversation. Rather, action will further fundamental concepts of the American rule of law—intolerance of unjust takings that violate another's rightful ownership interest. And from a practical perspective, enforcement will provide a necessary stop-gap while other government actors and agencies grapple with the proper approach to blockchain-based technologies and the law. A path exists and should be pursued.

HENRY S. ZAYTOUN**

252. *See* Mike Orcutt, *Criminals Thought Bitcoin Was the Perfect Hiding Place, but They Thought Wrong*, MIT TECH. REV. (Sept. 11, 2017), https://www.technologyreview.com/s/608763/criminals-thought-Bitcoin-was-the-perfect-hiding-place-they-thought-wrong/ [https://perma.cc/45QY-FXHF].

253. *Id.*

** I would like to first thank Professor Richard Myers for his thoughtful advice and direction that helped shape the idea for this Comment. And many thanks to Professors Lissa Broome and John Orth, as well as my friend Alfredo Watkins, for their invaluable comments and feedback. Lastly, a special thank you to Daniel Sanders and the Volume 97 Board of Editors for tremendous editorial work.