NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY

Volume 20
Issue 5 *Online Issue*

Article 4

12-1-2018

La Crypto Nostra: How Organized Crime Thrives in the Era of Cryptocurrency

Chelsea Pieroni

NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY
VOLUME 20, ONLINE: DECEMBER 2018

LA CRYPTO NOSTRA: HOW ORGANIZED CRIME THRIVES IN THE ERA OF CRYPTOCURRENCY

Chelsea Pieroni*

The advent of Bitcoin and other forms of cryptocurrency has left a permanent mark on the world as we know it, regardless of what percentage of the populace will ever touch or comprehend cryptocurrency in its lifetime. Thanks to the advent of blockchain technology, cryptocurrency has given rise to expedited international exchanges, increased protection of consumer identity, and secured methods for logging transactions. But cryptocurrency's nebulous nature makes it inherently vulnerable to a slew of hacks, cyberattacks, and run-of-the-mill theft. Moreover, its indeterminate qualities make cryptocurrency incredibly difficult for federal law to wrangle. But, perhaps most chillingly, the rise of cryptocurrency has given organized crime a new look, swapping society's Kuklinskis[1] and Capones[2] for pseudonymous sleuths and computer-clad criminals, and underground operations for "dark web" schemes that transcend international borders at the click of a button. This Recent Development will examine how organized crime leverages cryptocurrency, and how U.S. federal law can adapt to stop it.

---

* J.D. Candidate, University of North Carolina School of Law, 2020. Thank you, NC JOLT editors and Professor Richard Myers for your feedback and wisdom. I would also like to thank Duke University's Department of Philosophy, where I received my B.A., for laying the foundation of my academic writing. Finally, I would like to express my appreciation for Kelsey Van Dyke, former supervisor and current friend. Your no-holds-barred approach to copy-editing imparted to me the importance of efficient, effective, and time-sensitive writing.

[1] Richard Kuklinski, also known as "The Iceman," was an American serial killer, hired by various Mafia families to work as a hitman, who terrorized New York City for decades throughout the 20th Century. Patricia Bauer, *Richard Kuklinski*, ENCYCLOPÆDIA BRITANNICA (May 23, 2018), https://www.britannica.com/biography/Richard-Kuklinksi.

[2] Al Capone, "the most famous American gangster, who dominated organized crime in Chicago from 1925 to 1931." *Al Capone*, ENCYCLOPÆDIA BRITANNICA, https://www.britannica.com/biography/Al-Capone (updated Aug. 9, 2018).

I. INTRODUCTION

The birth of cryptocurrency (or "virtual currency") kickstarted a new era for technology, banking, and finance. The United States Government Accountability Office defines virtual currency as "a digital unit of exchange that is not backed by a government-issued legal tender. Virtual currencies can be used entirely within a virtual economy, or can be used in lieu of a government-issued currency to purchase goods and services in the real economy."[3] When Bitcoin arrived nearly ten years ago,[4] it boasted being the first peer-to-peer online payment provider that eliminated financial institutions.[5] It also purported to make international transactions simpler and more accessible, eliminating the barriers that credit cards impose, as not

[3] Lawrence Trautman, *Virtual Currencies; Bitcoin & What Now After Liberty Reserve, Silk Road, & Mt. Gox?*, 20 RICH. J.L. & TECH., 2014, at 1 (citation omitted).

[4] *See* Rosemary Bigmore, *A Decade of Cryptocurrency: From Bitcoin to Mining Chips*, TELEGRAPH (May 25, 2018), https://www.telegraph.co.uk/technology/digital-money/the-history-of-cryptocurrency/.

[5] *See* SATOSHI NAKAMOTO, BITCOIN: A PEER-TO-PEER ELECTRONIC CASH SYSTEM 1 (2008), https://bitcoin.org/bitcoin.pdf (last visited Sept. 26, 2018) ("What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party."). The author of this white paper was anonymous, using "Satoshi Nakamoto" as a pseudonym, and has since remained silent, adding to the cloud of mystery that Bitcoin created for itself. *Frequently Asked Questions*, BITCOIN, https://bitcoin.org/en/faq#general (last visited Dec. 17, 2018).

all countries allow credit card payments.[6] For those who dislike relying on banks, Bitcoin and other virtual currency offer an appealing way to store finances by way of digital wallets containing coins[7] that do not need to be registered with any government or financial institution.[8] Though it has not been adopted into mainstream commerce since its inception,[9] Bitcoin's impact has nonetheless affected global commerce. This impact is evidenced by the growing number of retail and service providers accepting cryptocurrency[10] and the creation of many new cryptocurrencies to

---

[6] *See* Timothy Carmody, *Money 3.0: How Bitcoins May Change the Global Economy*, NAT'L GEOGRAPHIC (Oct. 15, 2013), https://news.nationalgeographic.com/news/2013/10/131014-bitcoins-silk-road-virtual-currencies-internet-money/ ("For many of these countries, if this payment system works, if the U.S. and Congress can support and tolerate a reputable, well-paid industry, this will be a big connector to the world economy.").

[7] *Bitcoin Wallet*, INVESTOPEDIA, https://www.investopedia.com/terms/b/bitcoin-wallet.asp#ixzz5V9nsjaZ3 (last visited Oct. 27, 2018) ("A Bitcoin wallet [, or digital wallet,] is a software program where Bitcoins are stored. To be technically accurate, Bitcoins are not stored anywhere; there is a private key (secret number) for every Bitcoin address that is saved in the Bitcoin wallet of the person who owns the balance. Bitcoin wallets facilitate sending and receiving Bitcoins and gives ownership of the Bitcoin balance to the user . . . . Just as Bitcoins are the digital equivalent of cash, a Bitcoin wallet is analogous to a physical wallet. But instead of storing Bitcoins literally, what is stored is a lot of relevant information like the secure private key used to access Bitcoin addresses and carry out transactions. The four main types of wallet are desktop, mobile, web and hardware.").

[8] Nathaniel Popper, *For Ransom, Bitcoin Replaces the Bag of Bills*, N.Y. TIMES (July 25, 2015), https://www.nytimes.com/2015/07/26/business/dealbook/for-ransom-bitcoin-replaces-the-bag-of-bills.html.

[9] *See* Michael Henman, *7 Benefits of Accepting Cryptocurrency Payment*, BUSINESS.COM (July 10, 2018), https://www.business.com/articles/7-benefits-of-accepting-cryptocurrency/. However, Coinbase, a digital-assets exchange, is currently doing its best to make cryptocurrency common. The company is developing a platform that enables mainstream merchants to accept a variety of cryptocurrencies, including Bitcoin, Bitcoin Cash, Ethereum, and Litecoin. *See* Jesse Damiani, *Coinbase Launches 'Coinbase Commerce' To Let Mainstream Merchants Accept Crypto Payments*, FORBES (Feb. 15, 2018), https://www.forbes.com/sites/jessedamiani/2018/02/15/coinbase-launches-coinbase-commerce-to-let-mainstream-merchants-accept-crypto-payments/#42dd80ae3e8b.

[10] *See* Sarah Gruber, Note, *Trust, Identity, & Disclosure: Are Bitcoin Exchanges the Next Virtual Havens for Money Laundering and Tax Evasion?*, 32

compete with Bitcoin.[11] But Bitcoin's quick and mysterious ascent has led to many roadblocks, because the world simply was not ready. Confusion and vulnerability appear to continue to reign supreme over the general public's understanding of how this digital domain operates.[12] To many, the distinction between cryptocurrency and blockchain technology (or just "blockchain"), the system upon which cryptocurrency is made possible, still remains unclear.[13] Additionally, since 2008, there have been hacking incidents,[14] security breaches,[15] and forks in the Bitcoin blockchain[16]— incidents that have been addressed behind the scenes and outside the legal sphere. But the nature of all these issues is, at least in theory,

---

QUINNIPIAC L. REV. 135, 151–52 (2013) (listing precious metals, flowers, gun parts, language learning services, lottery tickets, books, cupcakes, Australian beef, and prescription drugs as a sample of the cornucopia of things one can purchase via Bitcoin today).

[11] *See* Bigmore, *supra* note 4.

[12] Saeed Elnaj, *The Problems with Bitcoin and the Future of Blockchain*, FORBES **(**Mar. 29, 2018), https://www.forbes.com/sites/forbestechcouncil/2018/03/29/the-problems-with-bitcoin-and-the-future-of-blockchain/#31dd974968dc.

[13] *Id.* ("There are key differences between Bitcoin and blockchain. Blockchain is a digitized, distributed and secure ledger that guarantees immutable transactions and solves the trust problem when two parties exchange value. Cryptocurrencies like Bitcoin rely on blockchain to conduct transactions. Yet blockchain transcends cryptocurrencies and offers many solutions that are likely to disrupt numerous industries with some profound implications."). However, the simplest, most straight-forward description of the Bitcoin-Blockchain relationship can be credited to reporter Sally Davies, quoted by Bernard Marr: "Blockchain is to Bitcoin, what the internet is to email. A big electronic system, on top of which you can build applications. Currency is just one." Bernard Marr, *A Very Brief History of Blockchain Technology Everyone Should Read*, FORBES (Feb. 16, 2018), https://www.forbes.com/sites/bernardmarr/2018/02/16/a-very-brief-history-of-blockchain-technology-everyone-should-read/#2c6c6d927bc4.

[14] Andrea Tan & Yuji Nakamura, *Timeline: Growing List of Major Cryptocurrency Heists*, INS. J. (Feb. 1, 2018), https://www.insurancejournal.com/news/international/2018/02/01/479206.htm.

[15] *See id.*

[16] *See* Bigmore, *supra* note 4; *see also* Amy Castor, *A Short Guide to Bitcoin Forks*, COINDESK (Mar. 24, 2017), https://www.coindesk.com/short-guide-bitcoin-forks-explained/ ("[A] fork is what happens when a blockchain diverges into two potential paths forward—either with regard to a network's transaction history or a new rule in deciding what makes a transaction valid. As a result, those who use the blockchain have to show support for one choice over the other.").

resolvable with additional literature and education on cryptocurrency. If and when Bitcoin reaches the general population,[17] we can only hope the passage of time and an ensuing greater access to information would allow consumers and non-consumers alike to possess more clarity on the matter. And with more clarity come less roadblocks.

Cryptocurrency's impact on the law, however, has been more difficult to determine, without a clear solution in sight. Virtual currency constantly shifts in monetary value,[18] exceeds national

---

[17] Bitcoin's future remains unclear. University of Cambridge Research Fellow Garrick Hileman says:

> [T]here are two key factors that would limit Bitcoin's ability to become used for everyday purchases. One of those factors is high-transaction fees for every Bitcoin exchange. Another factor is the high volatility of cryptocurrencies which means that [its] value fluctuates much quicker than other traditional, more stable currencies.

Jasper Pickering & Fraser Moore, *These Are the Major Roadblocks Stopping Bitcoin from Becoming a Mainstream Currency*, BUS. INSIDER (Dec. 15, 2017), https://www.businessinsider.com/what-is-stopping-bitcoin-from-becoming-mainstream-currency-finance-tech-2017-12. On the latter issue Hileman addresses, Forbes writer Jesse Damiani has some words of advice: "Investing in cryptocoins or tokens is highly speculative and the market is largely unregulated. Anyone considering it should be prepared to lose their entire investment." Damiani, *supra* note 9. To Nouriel Roubini, an economist at New York University's Stern School of Business quoted by journalist Tom Zanki, one of Bitcoin's biggest problems is scalability: "[B]itcoin is limited to five transactions per second, whereas Visa performs 25,000 transactions per second." Tom Zanki, *Crypto is 'Father of All Scams,' Economist Tells Senate*, LAW360 (Oct. 11, 2018), https://www.law360.com/articles/1091055/crypto-is-father-of-all-scams-economist-tells-senate. Additionally:

> [Roubini] also took issue with the lack of security involving cryptocurrencies, noting that such assets don't come with deposit insurance that traditional banks provide. He added that if someone steals a credit card, the victim can block further usage of that card. 'If someone is hacking your crypto wealth, it is gone forever . . . .'

Id.

[18] Zachary Sonenblum, *Some Background on Legal Issues Surrounding Bitcoin and Other Cryptocurrencies*, HEITNER LEGAL (July 18, 2017), https://heitnerlegal.com/2017/07/18/some-background-on-legal-issues-surrounding-Bitcoin-and-other-cryptocurrencies/.

borders,[19] and shrouds its users in (relative) anonymity.[20] As a result of its inherently amorphous nature, cryptocurrency has spurred transactions for illegal substances on the "dark web," and brought into question the efficacy of criminal law.[21] Although the federal government has addressed legal and regulatory concerns with varying degrees of success,[22] there appears to be a sizable, ever-growing loophole: organized crime may have found a new fuel in virtual currency.[23]

This Recent Development will consider how organized crime thrives in the world of cryptocurrency in five parts. Part II will offer a timeline of Bitcoin and other cryptocurrencies, including major criminal events and losses. Part III will address the legal and regulatory concerns regarding cryptocurrency and the measures that have been taken to address them to date. Part IV will address specifically the element of organized crime, its history, and its presence today in relation to the world of cryptocurrency; it will also feature an analysis of the Racketeer Influenced and Corrupt Organizations Act ("RICO"). In conclusion, Part V will propose solutions to tackling the problem of organized crime as it relates to

---

[19] *See* Carmody, *supra* note 6.

[20] Trautman, *supra* note 3, at 1. The article also quotes the Financial Crimes Enforcement Network definition of virtual or cryptocurrency, which is particularly indicative of its inherent incompatibility with the law: "those currencies that operate like a currency in some environments, but does not have legal tender status in any jurisdiction." *Id.* at 2.

[21] Sonenblum, *supra* note 18.

[22] *See, e.g.*, *id.*; EDWARD V. MURPHY ET AL., CONG. RESEARCH SURV., R43339, BITCOIN: QUESTIONS, ANSWERS, AND ANALYSIS OF LEGAL ISSUES (2015), https://fas.org/sgp/crs/misc/R43339.pdf.

[23] *See, e.g.*, C. Edward Kelso, *Highly Organized Crime Blamed for $2mil Bitcoin Mining Burglaries*, BITCOIN.COM (Mar. 4, 2018), https://news.bitcoin.com/highly-organized-crime-blamed-for-2mil-bitcoin-mining-burglaries/; Ted Knutson, *Cryptocurrency Tax Evasion, Other Illicit Activity Frequent, Says CFTC Chair Giancarlo*, FORBES (Feb. 15, 2018), https://www.forbes.com/sites/tedknutson/2018/02/15/cryptocurrency-tax-evasion-other-illicit-activity-frequent-says-cftc-chair-giancarlo/#4959440b2035 ("'There is a lot of cryptocurrency illicit use. I don't have hard data,' [Commodity Futures Trading Commission Chair Christopher] Giancarlo told a Senate Agriculture Committee.").

cryptocurrency and address the inherent legal and regulatory problems therein.

II. CRYPTOCURRENCY: A CRIMINAL HISTORY

Before Bitcoin, there had been a few, unceremonious attempts at creating virtual currency; none were successful.[24] In 2008, Bitcoin's manifesto was mysteriously posted to a cryptography-focused mailing list.[25] This whitepaper also introduced the concept of blockchain technology,[26] the foundation of Bitcoin[27] that is best described as "a constantly updated list of transactions."[28] In 2009, Bitcoin software became available to the public, and a new process called "mining"[29] facilitated the creation and transfer of new Bitcoins.[30] In 2010, the first Bitcoin purchase was made: 10,000 coins for two pizzas.[31] The following year, rival virtual currencies began to pop up. Approximately 1,000 virtual currencies exist today.[32] Thus far, all seemed well in the virtual currency realm as it steadily grew and gained traction.

---

[24] Marr, *supra* note 13.

[25] *Id.*

[26] Nakamoto, *supra* note 5.

[27] Robert Hackett, *Wait, What is Blockchain?*, FORTUNE (May 23, 2016), http://fortune.com/2016/05/23/blockchain-definition/.

[28] Dana Love, *My Blockchain 101: A Timeline*, MEDIUM (Nov. 15, 2017), https://medium.com/@DanaFLove/as-i-talk-about-blockchain-i-find-colleagues-making-use-of-blockchain-101-articles-which-seem-to-d6e6ddfd404b; *see also* Marr, *supra* note 13.

[29] Sean Williams, *The Basics of Cryptocurrency Mining, Explained in Plain English*, MOTLEY FOOL (Mar. 14, 2018), https://www.fool.com/investing/2018/03/14/the-basics-of-cryptocurrency-mining-explained-in-p.aspx ("Cryptocurrency mining is one of the most commonly used methods of validating transactions that have been executed over a blockchain network. Not only does blockchain work to protect transaction data through encryption, as well as store this data in a decentralized manner (i.e., on hard drives and servers all over the world) so as to keep a single entity from gaining control of a network, but also the primary goal is to ensure that the same crypto token isn't spent twice. In effect, 'mining' is one means of making sure that cryptocurrency transactions are accurate and true, such that they can never be compromised in the future.").

[30] Marr, *supra* note 13.

[31] *Id.*

[32] *Id.*

But after 2010, virtual currency's development took a dark turn, showing just how problematic cryptocurrency's indeterminate nature and unregulated market can be. The year 2012 marked one of the first instances of trouble in virtual currency paradise: BitFloor, a New York exchange, was hacked and subsequently lost approximately $250,000 in Bitcoin before shuttering its doors in 2013.[33] Then, Bitcoin's value crashed just after reaching the price of $1,000 for the first time.[34] In 2014, Bitcoin endured its worst financial loss ever:[35] Mt. Gox,[36] a Japanese exchange, reported losing about $480,000,000 worth in Bitcoin, likely due to theft.[37] In 2016, $2,000,000 in Bitcoin and Ether, a competing virtual currency, were stolen from Gatecoin in Hong Kong during a cyber attack.[38] But the following year appeared more optimistic, when Bitcoin was valued at $10,000.[39]

To understand the pitfalls of Bitcoin and other virtual currency, it is imperative to understand the notion of the "Dark Web." The Dark Web received widespread public attention in October of 2013, when the FBI arrested Ross Ulbricht, the founder of Silk Road.[40] Silk Road was an online marketplace that relied on the Dark Web and allowed the sale of illegal drugs, weapons, and even murder for hire.[41] All purchases made on Silk Road were made using Bitcoin.[42] But before Silk Road's rise and fall (and rise and fall again) clouded it with criminality,[43] the Dark Web was simply "a collection of

---

[33] *Id.*

[34] *Id.*

[35] *Id.*

[36] MT.GOX, https://www.mtgox.com/ (last visited Sept. 26, 2018).

[37] Tan & Nakamura, *supra* note 14.

[38] *Id.*

[39] *Id.*

[40] Andrew Norry, *The History of Silk Road: A Tale of Drugs, Extortion & Bitcoin*, BLOCKONOMI (Nov. 20, 2018), https://blockonomi.com/history-of-silk-road/.

[41] Joshuah Bearman, *The Untold Story of Silk Road, Part 2: The Fall*, WIRED (June 2015), https://www.wired.com/2015/05/silk-road-2/.

[42] Norry, *supra* note 40.

[43] Andy Greenberg, *Global Web Crackdown Arrests 17, Seizes Hundreds of Dark Net Domains*, WIRED (Nov. 7, 2014, 6:00 A.M.), https://www.wired.com/2014/11/operation-onymous-dark-web-arrests/. In 2013:

websites that are publicly visible, yet hide the IP addresses of the servers that run them, [meaning] anyone can visit a Dark Web site, but it can be very difficult to figure out where they're [sic] hosted—or by whom."[44] To ensure anonymity, Dark Web websites use

> The FBI had finally caught up with Ulbricht having infiltrated Silk Road by 'flipping' many of Ulbricht's closest associates and using their identities to gradually unravel the Silk Road network. The final connection was made between Silk Road and Ulbricht when a simple Google search connected the Dread Pirate Roberts [Ulbricht's alias] with another alias called 'altoid' that was an early promoter of Silk Road on another drug forum. That alias was traced through the internet to a bitcoin forum where Ulbricht had posted his personal email address.

Norry, *supra* note 40. After Ulbricht's initial arrest, 26-year old coder Blake Benthall managed Silk Road 2.0. *Id.* He was arrested in November of 2014. *Id.* While the FBI did not clearly express how it was able to crack down on Silk Road 2.0, "FBI agent Vincent D'Agostini [stated] merely that in May of 2014 the FBI 'identified a server located in a foreign country believed to be hosting the Silk Road 2.0 website at the time,' without explaining how it bypassed Tor's protections." Greenberg, *supra*. In June 2016, Benthall was sentenced to eight years in prison after pleading guilty to the charge of conspiracy to distribute heroin, cocaine, and methamphetamine. Nate Raymond, *An Alleged Staff Member of Silk Road 2.0 Was Sentenced to 8 Years in Prison*, BUS. INSIDER (June 4, 2016), https://www.businessinsider.com/r-key-player-in-silk-road-successor-site-gets-eight-years-in-us-prison-2016-6.

[44] Andy Greenberg, *Hacker Lexicon: What Is the Dark Web?*, WIRED (Nov. 19, 2014, 7:15 AM), https://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/. The media and general public often confuse the Dark Web and the "Deep Web," and while there is some overlap, the two are very much not the same:

> When news sites mistakenly describe the Dark Web as accounting for 90% of the Internet, they're confusing it with the so-called Deep Web, the collection of all sites on the web that aren't reachable by a search engine. Those unindexed sites do include the Dark Web, but they also include much more mundane content like registration-required web forums and dynamically-created pages like your Gmail account . . . . The actual Dark Web, by contrast, likely accounts for less than .01 [percent] of the web: Security researcher Nik Cubrilovic counted less than 10,000 Tor hidden services in a recent crawl of the Dark Web, compared with hundreds of millions of regular websites.

Id.

encrypting software, like Tor[45] or I2P,[46] which make it nearly impossible for the websites to view the IP addresses of the users visiting them.[47] Although the Dark Web is not, in spite of its name, inherently nefarious, it was only a matter of time before criminals

---

[45] In its own words, Tor is:

> A network [composed of] a group of volunteer-operated servers that allows people to improve their privacy and security on the Internet. Tor's users employ this network by connecting through a series of virtual tunnels rather than making a direct connection, thus allowing both organizations and individuals to share information over public networks without compromising their privacy. Along the same line, Tor is an effective censorship circumvention tool, allowing its users to reach otherwise blocked destinations or content. Tor can also be used as a building block for software developers to create new communication tools with built-in privacy features. Individuals use Tor to keep websites from tracking them and their family members, or to connect to news sites, instant messaging services, or the like when these are blocked by their local Internet providers. Tor's onion services let users publish web sites and other services without needing to reveal the location of the site. Individuals also use Tor for socially sensitive communication: chat rooms and web forums for rape and abuse survivors, or people with illnesses.

Tor: Overview, TOR, https://www.torproject.org/about/overview.html.en (last visited Oct. 15, 2018). "Onion services[—in other words, hidden services—]are anonymous network services that are exposed over the Tor network. In contrast to conventional Internet services, onion services are private, generally not indexed by search engines, and use self-certifying domain names that are long and difficult for humans to read." PHILP WINTER ET AL., HOW DO TOR USERS INTERACT WITH ONION SERVICES?, SEC'18 PROC. OF THE 27TH USENIX CONF. ON SECURITY SYMP. (Aug. 15, 2018), https://nymity.ch/onion-services/pdf/sec18-onion-services.pdf.

[46] In its own words:

> I2P is an anonymous overlay network[—]a network within a network. It is intended to protect communication from dragnet surveillance and monitoring by third parties such as [Internet Service Providers]. I2P is used by many people who care about their privacy: activists, oppressed people, journalists and whistleblowers, as well as the average person. No network can be 'perfectly anonymous'. [sic] The continued goal of I2P is to make attacks more and more difficult to mount. Its anonymity will get stronger as the size of the network increases and with ongoing academic review.

What is I2P?, I2P, https://geti2p.net/en/ (last visited Oct. 15, 2018).

[47] Greenberg, *supra* note 44.

took advantage of its anonymity.[48] In fact, though Silk Road was the FBI's main target, by 2014, the FBI had also ended numerous online contraband markets and money laundering sites, seized over 400 Tor domains, and made numerous arrests around the world.[49] But the Silk Road saga did not end with its founder's conviction: in 2015, two former U.S. federal agents credited with helping shut down Silk Road were charged with wrongfully retaining hundreds of thousands of dollars in Bitcoin.[50] As for Ulbricht, he is currently serving two life sentences plus forty years in prison.[51]

III. CRYPTOCURRENCY & THE LAW

For the past decade, the state of the law generally has attempted to take on the unique and unenviable task of giving the mysterious territory of cryptocurrency a legal compass.[52] Given the tumultuous timeline Bitcoin and other cryptocurrencies have experienced to date, it comes as no surprise that this endeavor has been complex.

One of the first government rulings to impact the treatment of cryptocurrency occurred in 2014.[53] The Federal Election Commission ("FEC") unanimously voted to allow Make Your Laws, Inc., a nonpartisan political action committee ("PAC") registered with the FEC, to collect Bitcoin contributions and make investments via Bitcoin.[54] To comply, Bitcoin contributions to a PAC must be regarded as "anything of value" contributions.[55] Thus,

---

[48] *Id.*

[49] *Id.*

[50] *Id.*

[51] Jasper Hamill, *Silk Road Founder Ross 'Dread Pirate Roberts' Ulbricht is Sneaking Tweets Out of Prison*, METRO (Aug. 14, 2018), https://metro.co.uk/2018/08/14/silk-road-founder-ross-dread-pirate-roberts-ulbricht-sneaking-tweets-prison-7838166/.

[52] *See* MURPHY ET AL., *supra* note 22, at 9 ("In providing this information, we have identified some federal statutes and regulatory regimes that may have some applicability to digital currency, although none contains explicit language to that effect or explicitly mentions currency not issued by a government authority. Some federal statutes, because of their broad coverage, are likely to be held by courts to apply in connection with digital currency.").

[53] *Id.*

[54] *See id.*

[55] 52 U.S.C. § 30101(8)(A)(i) (2017).

the Federal Election Campaign Act[56] can extend the scope of its power to include Bitcoin and other cryptocurrencies.[57] The purpose of this action was to ensure that Make Your Laws would abide by the Federal Election Campaign Act with regard to examining contributions and determining the eligibility of its contributors.[58] It remains unclear, however, whether this action treats Bitcoin as proper currency.[59] This move by the FEC was particularly interesting at the time. It seemed to clash with the general attitude the FEC harbored toward Bitcoin just a few months prior, when some commissioners expressed the concern that cryptocurrency would allow donors to conceal their identity.[60]

The Internal Revenue Service ("IRS"), which currently views virtual currency as "an immediate concern"[61] with regard to tax evasion, issued Notice 2014-21 in 2014.[62] This action treated virtual currency that can be converted into cash[63] as "property" for tax

---

[56] 52 U.S.C. § 30101 et seq.

[57] *See* MURPHY ET AL., *supra* note 22.

[58] *Id.*

[59] *Id.* While the FEC allowed Make Your Laws to buy Bitcoins and hold them for sale, the PAC was not allowed to use Bitcoin for the purpose of making payment transactions. *Id.*

[60] Matea Gold, *Federal Election Commission Approves Bitcoin Donations to Political Committees*, WASH. POST (May 8, 2014), http://www.washingtonpost.com/blogs/post-politics/wp/2014/05/08/federal-election-commission-approves-bitcoin-donations-to-political-committees/.

[61] *IRS Acknowledges that Cryptocurrency is a Threat*, WINSTON & STRAWN LLP (May 10, 2018), https://www.winston.com/en/thought-leadership/irs-acknowledges-that-cryptocurrency-is-a-threat.html ("[There are] three areas of tax enforcement focus involving the use of virtual currency: [(1) t]he absence of taxpayers to report gains on the disposition of virtual currency; [(2) u]se of cryptocurrency in business transactions that are unreported, including payment of wages and goods and services; . . . [and (3) u]se of cryptocurrency in business transactions that are unreported, including payment of wages and goods and services.").

[62] *See, e.g.*, IRS Notice 2014–21, http://www.irs.gov/pub/irs-drop/n-14-21.pdf (discussing how existing tax principles apply to transactions using virtual currency); Sonenblum, *supra* note 18.

[63] To be "convertible virtual currency" means to have "an equivalent value in real currency or act[] as a substitute for real currency. [However, n]ot all cryptocurrencies act this way[;] but most of the major ones, like [B]itcoin, do." Anna Bahney, *4 Things to Know About Your Cryptocurrency at Tax Time*, CNN

purposes. Thus, by treating Bitcoin as property rather than currency, the IRS made it so that the sale, exchange, or use of virtual currencies has tax consequences.[64] In other words, any individual or business who engages in any of the above transactions without properly reporting them could face tax liability.[65]

For those who handle large quantities of cryptocurrency, improper reporting could even lead to criminal liability.[66] This possible consequence was further emphasized in 2017, when Congress passed a tax reform that honed in on the peculiarities of crypto-meets-tax, putting an end to the swapping of one virtual currency for another without incurring tax obligations.[67] However, with the onus remaining on individual consumers to properly report exchanges, transactions, or investments in virtual currency,[68] the "tax headaches" for the general law-abiding, Bitcoin-wielding population are unlikely to end soon."[69]

In an additional effort to safeguard cryptocurrency use and to prevent tax evasion, the New York State Office of the Attorney General launched the Virtual Markets Integrity Initiative in April of

---

MONEY (Mar. 26, 2018), https://money.cnn.com/2018/03/26/pf/how-to-pay-taxes-on-cryptocurrency/index.html.

[64] Sonenblum, *supra* note 18. "Cryptocurrenices [sic] apply the same general property transaction tax principles. Cryptocurrency wages are taxable to the employee, must be reported by the employer on a W-2 Form, and are subject to federal income tax withholding and payroll taxes." *Id.*

[65] *IRS Acknowledges that Cryptocurrency is a Threat*, *supra* note 61.

[66] *Id.*

[67] Jeff John Roberts, *New Tax Law Closes Bitcoin Loophole*, FORTUNE (Dec. 21, 2017), http://fortune.com/2017/12/21/Bitcoin-tax/ (explaining that this shift was made possible by "a tweak to [the] definition of property eligible for exemption: 'The tax act in Sec. 13303 *amends IRC Section 1031 (a)(1) to delete property and replace it with real property* . . . So, you can see that now I can no longer take the position that my Bitcoin to Litecoin exchange was a like kind one under Sec. 1031, and I have to recognize the gain when I do it.'") (alteration in original) (emphasis in original) (internal quotations omitted).

[68] Bahney, *supra* note 63.

[69] Roberts, *supra* note 67 ("[D]igital currency investors [will have to] figure out how to account for spin-off currencies like Bitcoin Cash, and [deal with] the IRS deploy[ing] special software to identify Bitcoin tax cheats.").

2018.[70] This project looks into the policies, practices, and internal operations of virtual currency trading platforms.[71] This initiative will hopefully increase transparency, accountability, and an overall understanding of tax implications triggered by cryptocurrency among crypto investors and consumers.[72]

In 2014, the Federal Trade Commission ("FTC"), which has the authority to enforce the prohibition of "unfair or deceptive acts or practices in or affecting commerce,"[73] brought suit against Butterfly Labs, a Missouri-based Bitcoin mining operation.[74] Although the district court initially granted the FTC's *ex parte* temporary restraining order against Butterfly Labs,[75] ultimately the FTC's suit ended (somewhat anticlimactically) in a settlement.[76] Thus, the outcome was binding only on the two parties involved. Doubtless, a settlement was likely less than what the FTC desired—nonetheless, the benefit the FTC derived from it was pivotal in cryptocurrency law-making.[77] It confirmed that the federal government was taking action toward ensuring that FTC prohibitions apply to matters involving Bitcoin and other forms of cryptocurrency as well as traditional forms of currency, thereby normalizing the regulation of virtual currency.[78] In its original suit, the FTC alleged Butterfly Labs deliberately misled consumers to spend thousands of dollars purchasing Bitcoin mining operations that were either never

---

[70] BARBARA D. UNDERWOOD, N.Y. STATE ATT'Y GEN., VIRTUAL MARKETS INTEGRITY INITIATIVE, https://virtualmarkets.ag.ny.gov/ (last visited Nov. 13, 2018).

[71] *Id.*

[72] *Id.*

[73] 15 U.S.C. § 45 (2012).

[74] Press Release, FTC, *At FTC's Request, Court Halts Bogus Bitcoin Mining Operation* (Sept. 23, 2014), https://www.ftc.gov/news-events/press-releases/2014/09/ftcs-request-court-halts-bogus-bitcoin-mining-operation.

[75] Fed. Trade Comm'n v. BF Labs, Inc., 4:14-CV-00815-BCW, 2014 WL 12600149, at *2 (W.D. Mo. Sept. 18, 2014).

[76] Press Release, FTC, *Operators of Bitcoin Mining Operation Butterfly Labs Agree to Settle FTC Charges They Deceived Consumers* (Feb. 18, 2016), https://www.ftc.gov/news-events/press-releases/2016/02/operators-bitcoin-mining-operation-butterfly-labs-agree-settle.

[77] *See* MURPHY ET AL., *supra* note 22.

[78] *See, e.g., id.*; *BF Labs*, 2014 WL 7238080.

delivered after purchase or were delivered with significant defects,[79] in violation of Section 5(a) of the FTC Act.[80] The United States District Court for the Western District of Missouri granted the FTC's request for a temporary restraining order on Butterfly Labs, which required defendants to immediately stop making misrepresentations about their operations to customers, and froze all of their assets.[81] The court initially granted this request on the fact that not only had Butterfly Labs likely violated the FTC Act, but also there was enough evidence showing the defendant was likely to continue to act in violation of the FTC, bringing "immediate and continuing" harm to consumers unless the court intervened.[82] After multiple amended complaints, Butterfly Labs agreed to settle.[83] The details of this settlement prohibited Butterfly Labs from making misrepresentations of its products to consumers and imposed monetary judgments.[84] Despite not winning the suit, this settlement

---

[79] *BF Labs*, 2014 WL 7238080, at *1. At trial, in regards to Butterfly's lab's deliverability, the FTC gave evidence that:

> (1) the delivery dates were repeatedly extended[;] (2) the initial shipments of BitForce and Monarch machines were several months after the originally-stated delivery dates[;] (3) cloud mining services did not start when originally stated[;] (4) the Monarch was offered for purchase despite an extensive backlog of BitForce orders[;] (5) hundreds of consumers complained about BFL to Plaintiff[;] (6) thousands of consumers complained about BFL to PayPal and[;] (7) a pre-order model is problematic.

Id. at *4. The court, however, while finding these facts "concerning and possibly create inferences of falsity," ultimately concluded Plaintiff did not meet its burden for calling for a preliminary injunction. *Id.*

[80] *See* 15 U.S.C. § 45(a) (2012).

[81] *At FTC's Request, Court Halts Bogus Bitcoin Mining Operation*, *supra* note 74.

[82] *BF Labs, Inc.*, 2014 WL 12600149, at *2.

[83] *Operators of Bitcoin Mining Operation Butterfly Labs Agree to Settle FTC Charges They Deceived Consumers*, *supra* note 76.

[84] *Id.* Specifically, those misrepresentations entailed "whether a product or service can be used to generate Bitcoins or any other virtual currency, on what date a consumer will receive the product or service, and whether the product is new or used[,]" in addition to "be[ing] prohibited from taking up-front payments for Bitcoin machines and other products used to mine for any virtual currency unless those products are available and will be delivered within 30 days. If the product is not actually delivered within 30 days, the defendants must provide a refund." *Id.* As for the monetary damages—totaling $38,615,161 against Butterfly

was a significant for the FTC because it signals the FTC's intention to prevent future operations where defendants would mislead crypto consumers.[85] The Butterfly Labs settlement is an indication of openness to change on behalf of the federal government, which is essential in keeping up with cryptocurrency.

More efforts have been made to compare cryptocurrency regulation to regular cash regulation. Recently, Massachusetts federal court found in favor of the United States Commodity Futures Trading Commission ("CFTC"), whose stance on cryptocurrency is that all virtual currency should fall within its control, not just Bitcoin.[86] The case, *CFTC v. My Big Coin Pay Inc.*,[87] now allows the CFTC to pursue fraud investigations in all virtual currency markets.[88] This ruling is optimistic: it is representative of the steps that courts and agencies alike are taking toward regulating the crypto-sphere from a broad standpoint, rather than on a case-by-case (or, rather, crypto-by-crypto) basis.[89]

Outside of the realm of Congress, the United States Government Accountability Office has released the *Virtual Currencies: Emerging Regulatory, Law Enforcement, and Consumer Protection Challenges* report.[90] This report lists the efforts taken by a variety of

---

itself and its vice president and co-owner Sonny Vleisides, and $135,878 against general manager Darla Drake—those were currently partially suspended because Butterfly Labs is unable to pay. *Id.*

[85] *See id.*

[86] Aaron Leibowitz, *CFTC Official Lauds Ruling Putting Crypto Under Its Purview*, LAW360 (Oct. 3, 2018), https://www.law360.com/articles/1089054/cftc-official-lauds-ruling-putting-crypto-under-its-purview. The logic behind this position is that "Congress intended for the CFTC to regulate a swath of products that should be considered generally, not by individual good. [Thus, if t]he well-known cryptocurrency [B]itcoin meets the legal standard of a commodity . . . smaller virtual currencies should, too." *Id.*

[87] Comm. Fut. Trading Comm'n v. My Big Coin Pay, Inc., No. 18-10077-RWZ, 2018 U.S. Dist. LEXIS 164932 (D. Mass. Sep. 26, 2018).

[88] The Commodity Futures Trading Commission ("CFTC") claimed the defendant, founder and salesman of My Big Coin Pay, "l[ied] about the value and financial backing of the virtual currency in order to steal $6 million from 28 people." Leibowitz, *supra* note 86.

[89] *Id.* ("'We will continue to police these markets in close coordination with our sister agencies,' [James] McDonald [CFTC Director of Enforcement] said.").

[90] MURPHY ET AL., *supra* note 22.

federal financial services regulators and law enforcement agencies to address the regulation of virtual currency.[91] The report also calls for an increased attention toward consumer protection.[92] This is just another manifestation of a growing consensus at the federal level that the United States government needs to take action quickly to keep up with the modernization of currency as we know it.

Other laws and federal efforts, however, have not been successful and still remain unclear as to whether they apply to cryptocurrency.[93] For example, Sections 470–477 and Sections 485–489 of Title 18 of the United States Code impose criminal punishment on counterfeiting and forging American coins and currency.[94] Like many of the above laws, these do not expressly apply to currency that only exists in the digital sphere.[95] Currently,

---

[91] The lists includes:

> [T]he Board of Governors of the Federal Reserve System, the [Consumer Financial Protection Bureau (CFPB)], the Commodity Futures Trading Commission, the Department of Homeland Security (including the U.S. Immigration and Customs Enforcement and the U.S. Secret Service), the Department of Justice (including the Federal Bureau of Investigation), the Department of the Treasury (including the Financial Crimes Enforcement Network and the Office of the Comptroller of the Currency), the Federal Deposit Insurance Corporation, the National Credit Union Administration, and the Securities and Exchange Commission.

Id. The CFPB issued consumer advisory warnings in 2014, stating that:

> Virtual currencies may have potential benefits, but consumers need to be cautious and they need to be asking the right questions . . . . Virtual currencies are not backed by any government or central bank, and at this point consumers are stepping into the Wild West when they engage in the market.

CFPB Warns Consumers about Bitcoin, CFPB (Aug. 11, 2014), https://www.consumerfinance.gov/about-us/newsroom/cfpb-warns-consumers-about-bitcoin/. Additionally, the CFPB also warns against "hackers and scammers pos[ing] serious threats," and alerts readers that not all virtual currency companies may offer help or refunds for lost or stolen goods. *Id.*

[92] MURPHY ET AL., *supra* note 22.

[93] *See id.*

[94] *See, e.g.*, *id.*; 18 U.S.C. §§ 470–77, 485–89 (2012).

[95] *See, e.g.*, MURPHY ET AL., *supra* note 22; 18 U.S.C. §§ 470–77, 485–89.

there is no legal precedent specifically indicating whether these Sections would apply to cryptocurrency or virtual currency.[96]

Another gray area can be found in the realm of money laundering and how best to define cryptocurrency.[97] Specifically, there is a lack of a agreement between state and federal courts as to whether cryptocurrency is to be regarded as "money" or "property."[98] This indecisiveness directly impacts whether cryptocurrency is subject to state and federal anti-money laundering statutes, and, thus, whether individuals engaged in money laundering activity via virtual currency will be prosecuted.[99] If virtual currency is "money," then it is subject to money laundering statutes, which means that persons accused of money laundering may be prosecuted under the appropriate state or federal anti-money laundering statutes.[100] If, instead, virtual currency is treated as "property," this creates a legal loophole: individuals utilizing cryptocurrency to launder money will not have violated state or

---

[96] MURPHY ET AL., *supra* note 22. These sections were, however, successfully utilized in convicting a man in 2011 who coined his own, physical currency ("Liberty Dollars," among others) and had disseminated it across the United States and Puerto Rico since 1998. Press Release, Fed. Bureau of Investigation: Charlotte Division, Defendant Convicted of Minting His Own Currency (Mar. 18, 2011), https://archives.fbi.gov/archives/charlotte/press-releases/2011/defendant-convicted-of-minting-his-own-currency.

[97] Brandon M. Peck, *The Value of Cryptocurrencies: How Bitcoin Fares in the Pockets of Federal and State Courts*, 26 U. MIAMI BUS. L. REV. 191, 193 (Dec. 13, 2017). This discord between state and federal courts is due to a 2016 decision in *State v. Espinoza* from the Eleventh Judicial Circuit Court of Florida. *Id.* at 191; *see* Order Granting Defendant's Motion to Dismiss the Information, State v. Espinoza, No. F14-2923, at *7 (July 22, 2016), https://www.scribd.com/document/319504645/State-of-FL-v-Michell-Abner-Espinoza. In this case, Judge Pooler opined that Bitcoin did not meet the definition of "money" per Florida money laundering statutes, and dismissed the complaint brought against defendant Espinoza. *Espinoza*, *supra* at *7. By doing so, Judge Pooler disagreed with contrasting opinions held previously by a number of federal court judges, all of whom treated Bitcoin as "money" or "funds" with regard to federal anti-money laundering statutes. It's important to note that the court based its decision on the IRS's Notice 2014-21. *Id.* at *5; *see* IRS Notice 2014-21, *supra* note 62.

[98] Peck, *supra* note 97, at 193.

[99] *Id.*

[100] *Id.* at 193–94, 202.

federal anti-money laundering statutes.[101] This issue is particularly problematic because it directly undermines Congress's efforts in adapting money laundering laws to changing currency currents—pointedly, this directly impacts Congress's ability in combatting organized crime.[102] If state courts disagree with federal courts as to the proper interpretation of Bitcoin and other cryptocurrency, this in turn undermines the federal government's attempts to uniformly regulate money laundering in the crypto-sphere, which in turns gives much more leeway for organized crime to blossom via the use of virtual currency.

The indefinite state of virtual currency, along with its inconsistent ebbing and flowing in mainstream use and market value, has led to laws regulating virtual currency in a piece-meal fashion, often leaving many questions about the scope of applicability still unanswered. However, the efforts appear optimistic, as they showcase a willingness by lawmakers to maintain flexibility and stretch monetary rules to stay current with the changing times. In essence, these efforts are demonstrating that, sometimes, you can teach proverbial old dogs new tricks. Regulation, however, becomes even more difficult when the crypto-crimes involve highly organized enterprises spread across the globe, concealed by online anonymity and cross-continental elusiveness.

IV. ORGANIZED CRIME IN THE MODERN WORLD

Racketeering and organized crime are alive and well, despite popular belief to the contrary.[103] The city of Providence, Rhode

---

[101] *Id.* at 193.

[102] *See id.* at 194. In 1970, Congress passed both Racketeer Influenced and Corrupt Organizations ("RICO") Act, targeting mafia syndicates and the Bank Secrecy Act. This became "one of the most important tools in combatting money laundering [by] [e]stablish[ing] requirements for recordkeeping and reporting by [both] . . . individuals . . . and financial institutions in order to aid in the identification of the source, volume, and movement of currency." *Id.* at 194–95 (citations omitted) (internal quotations omitted). Congress then expanded RICO in 1984 to broaden its scope and address money laundering more broadly outside of the realm of Mafia syndicates. *Id.* at 195.

[103] Although passed in the Nixon era, RICO has been pivotal in shutting down large parts of criminal organizations across North America in recent years, such as the Gambino and Lucchese families, as well as the Latin Kings gang members.

Grand Jury Indicts in RICO Case, SOUTH FLA. BUS. J., (Dec. 5, 2003), https://www.bizjournals.com/southflorida/stories/2003/12/01/daily42.html; Paula McMahon, *Latin Kings Gang Members Plead Guilty to Racketeering*, SUN SENTINEL (Nov. 5, 2015), http://www.sun-sentinel.com/news/fl-latin-kings-hearing-broward-20151105-story.html; Selwyn Raab, *Suspected New York Mob Leaders Are Indicted in Contract Rigging*, N.Y. TIMES, May 31, 1990, at A1. Rudy Giuliani, in his role as then-United States Attorney for the Southern District of New York, indicted and brought down a substantial number of mob bosses and mafia members in New York City, ranging from the Genovese to the Colombo to the Bonanno families, via RICO. *Rudolph Giuliani*, MOB MUSEUM, https://themobmuseum.org/notable_names/rudolph-giuliani (last visited Sept. 26, 2018). The Bonanno, Colombo, Gambino, Genovese, and Lucchese families constituted the notorious "Five Families" of New York City, established in 1931 by The Commission, a group including bosses from each of the five families plus the heads up the Buffalo and Chicago mobs, formed the same year to oversee the mob families and end turf wars in New York. *Id.*; Robert Anglen, *The Five Families of New York: How the Mafia Divides the City*, AZCENTRAL (Oct. 31, 2017), https://www.azcentral.com/story/news/local/arizona-investigations/2017/10/31/five-families-new-york-how-mafia-divides-city/777899001/. The Bonanno family, which is part of the international syndicate known as the Mafia or La Cosa Nostra, originated around 1880 in Sicily. *Bonanno Family History*, AM. MAFIA HIST. (Apr. 17, 2014), https://americanmafiahistory.com/bonanno-family/. In the 1920s, a few members relocated to New York, mainly populating Brooklyn. *Id.* The family is still active, though not as strong today: there remain about 150 members of the Bonanno Family. *Id.* However, in July 2018, a son of a supposed Bonanno associate was shot in the Bronx in an attempted daytime murder. *Shocking Video Shows Attempted Hit on Son of Bonanno Crime Family Associate*, FOX NEWS (July 13, 2018), https://www.foxnews.com/us/shocking-video-shows-attempted-hit-on-son-of-bonanno-crime-family-associate. The Colombo family is the "youngest" of the Five, officially forming in New York in 1928. *See Colombo Family History—The Youngest of the "Five Families"*, AM. MAFIA HIST. (Oct. 19, 2015), https://americanmafiahistory.com/colombo-family/. It is also the last group to be formed under La Cosa Nostra. Brad Hamilton, *The Brutal Rise and Bloody Fall of the Colombos*, N.Y. POST (Jan. 30, 2011), https://nypost.com/2011/01/30/the-brutal-rise-and-bloody-fall-of-the-colombos/. Though the Colombo family is regarded as the weakest of the Five, it is also one of the most "blood thirsty." *Id.* As of 2011, it appears that the Colombo family dwindled significantly, with the only active member being Carmine Persico, a longtime boss, "who continues to call the shots" from his prison cell, where he is still serving a 139-year sentence today. *Id.*; *see also* Seth Ferranti, *This "Snake" of a Mafia Boss Was First Accused of Murder at 17*, VICE (Aug. 22, 2018), https://www.vice.com/en_us/article/ev8kpj/this-snake-of-a-mafia-boss-was-first-accused-of-murder-at-17. However, five supposed members of the Colombos and Gambinos were indicted in Brooklyn in 2018. Rob Abruzzese, *Five from South*

Island is still reeling from its late Mayor Vincent "Buddy" Cianci's extensive entanglements with the state's organized crime families,[104] including the third-largest faction of La Cosa Nostra.[105] In October

Brooklyn Indicted on Loan Sharking and Illegal Gambling Charges, BROOK. DAILY EAGLE (July 11, 2018), http://www.brooklyneagle.com/articles/2018/7/11/five-south-brooklyn-indicted-loan-sharking-and-illegal-gambling-charges. The Gambino crime family was formed in the early 1900s, *Gambino Crime Family*, CRIME MUSEUM, https://www.crimemuseum.org/crime-library/organized-crime/gambino-crime-family/ (last visited Oct. 10, 2018), and rose to prominence under John Gotti, also known as "The Teflon Don" because he successfully avoided prosecution for decades, until 1990. *See* Elena Nicolaou, *The True Stories Behind 2018's Biggest Mafia Biopic*, REFINERY29 (June 14, 2018), https://www.refinery29.com/2018/06/201880/gotti-movie-cast-mafia-gambino-family-2018. The Genovese family, originally "Morello," was formed after its founder Giuseppe Morello arrived in New York from Sicily in 1892; it was renamed in 1957 after Vito Genovese took over. *Genovese Family—One of the "Five Families"*, AM. MAFIA HIST. (Aug. 31, 2015), https://americanmafiahistory.com/genovese-family/; *Giuseppe "The Clutch Hand" Morello—The First "Capo di Tutti Capi" of New York*, AM. MAFIA HIST. (May 25, 2014), https://americanmafiahistory.com/giuseppe-morello/. Though regarded as one of the most successful families in evading criminal justice, the Genoveses ultimately met their demise under Vincent "The Chin" Gigante, who was known for feigning a mental handicap by wandering the streets dressed in a robe in order to defy the FBI. *Id.* The Lucchese family, which also exerted power over areas of New Jersey and Florida, and who inspired the movie *Goodfellas*, appears to be very active today. Anglen, *supra*. "In May 2017, federal authorities arrested 19 members of the Lucchese crime family, including two top bosses, captains and its consigliere, on charges of racketeering and murder." *Id.*

[104] *Crimetown Chapter One: Divine Providence*, GIMLET MEDIA, https://www.crimetownshow.com/episodes-1/2016/11/2/episode-one-divine-providence (last visited Nov. 18, 2018) (explaining how, at Mayor Buddy Cianci's funeral in 2016, cops, politicians, and judges sat shoulder-to-shoulder with "crooks and ex-cons"). Mayor Cianci's involvement in Rhode Island's mob scene also gave way to a vital federal court opinion. In *United States v. Cianci*, where Cianci, along with Providence's Director of Administration and a member of the Providence City Towing Association, was charged "with forty-six violations of federal statutes prohibiting public corruption," the First Circuit held that even "[m]unicipal entities" may be treated as enterprises for the purpose of RICO charges, as long as all parties involved in the enterprise shared the same purpose. United States v. Cianci, 378 F.3d 71, 77, 83 (1st Cir. 2004).

[105] La Cosa Nostra, whose name derives from the Italian for "Our Thing,":

> evolved from the [early 1990s] Sicilian Mafia and is one of the foremost organized criminal threats to American society . . . . It is a nationwide

2018, notorious Boston-based gangster James "Whitey" Bulger was murdered in his prison cell, with the prime suspect being a mob hitman who is already serving time for murdering a Genovese family mob boss in 2003.[106] In 2006, journalist Roberto Saviano's now-infamous investigative novel *Gomorrah* exposed the chilling reality of organized crime in southern Italy, led by Camorra and 'Ndrangheta[107] groups, among others, whose grip on the country has not loosened in the twenty-first century.[108] In fact, to this day, the mafia has reduced areas of southern Italy to a trash-ridden hellscape through control of the waste industry since the 1980s, dumping

> alliance of criminals . . . dedicated to pursuing crime and protecting its members. It also is called the Mafia, a term used to describe other organized crime groups. . . . [It] consists of different 'families' or groups that are generally arranged geographically and engaged in significant and organized racketeering activity. [Such activity includes]: murder, extortion, drug trafficking, corruption of public officials, gambling, infiltration of legitimate businesses, labor racketeering, loan sharking, prostitution, pornography, tax-fraud schemes, and stock manipulation schemes.

Transnational Organized Crime, FED. BUREAU OF INVESTIGATION, https://www.fbi.gov/investigate/organized-crime/ (last visited Oct. 10, 2018).

[106] Lia Eustachewich, *Meet the Mob Hitman Suspected of Killing Whitey Bulger*, N.Y. POST (Oct. 31, 2018), https://nypost.com/2018/10/31/meet-the-mob-hitman-suspected-of-killing-whitey-bulger/amp/.

[107] The word "ndrangheta" is derived from the Greek word ἀνδραγαθία, or "andrangathia," meaning "courage" or "loyalty." *See 'ndràngheta*, TRECCANI, http://www.treccani.it/vocabolario/ricerca/ndrangheta/ (last visited Oct. 10, 2018); *see also Transnational Organized Crime*, *supra* note 105. The 'Ndrangheta,' also known as the Calabrian Mafia, was formed in the 1860s in the southern Italian region of Calabria and currently counts approximately 6,000 active members. *Transnational Organized Crime*, *supra* note 105.

[108] *See generally* ROBERTO SAVIANO, GOMORRAH: A PERSONAL JOURNEY INTO THE VIOLENT INTERNATIONAL EMPIRE OF NAPLES' ORGANIZED CRIME SYSTEM (Virginia Jewiss trans., Farrar, Straus and Giroux, 1st American ed. 2007) (2006) (primarily reporting on the Camorra, the Campanian Mafia primarily prevalent in Naples and the surrounding region of Campania, and its ongoing, bloody impact on modern day southern Italy). Since publishing the novel in 2006, Saviano, now regarded as one of Italy's most famous writers, has received threats from various mafia groups in Italy, requiring police protection for the last decade. *See* Stephanie Kirchgaessner, *Matteo Salvini Threatens to Remove Gomorrah Author's Police Protection*, GUARDIAN (June 21, 2018), https://www.theguardian.com/world/2018/jun/21/matteo-salvini-threatens-to-remove-gomorrah-roberto-saviano-police-protection.

hazardous cargo into the sea and mounds of garbage onto public property.[109] Even the United Nations is convinced that "[o]rganized crime has globalized and turned into one of the world's foremost economic and armed powers[.]"[110]

For the past decade, syndicates across the world have seen Bitcoin and other virtual currency as an opportunity, and national governments have become increasingly concerned.[111] The Australian government believes that the rise of organized crime in its nation can be sourced back to Bitcoin and other cryptocurrencies,

---

[109] Kelsey Campbell-Dollaghan, *The Mob is Secretly Dumping Nuclear Waste Across Italy and Africa*, GIZMODO (Jan. 31, 2014), https://gizmodo.com/the-mob-is-secretly-dumping-nuclear-waste-across-italy-1513190243; *see also* SAVIANO, *supra* note 108, at 295 ("The clans find space everywhere for waste, but the regional administration of Campania, run for ten years by an external commission because of Camorra infiltrations, was unable to dispose of its own trash. While waste from every part of Italy was finding its way illegally into Campania, Campania trash was being shipped to Germany at fifty times the removal price the clans offered their clients. Investigations indicate that in the Naples area alone, of eighteen waste management firms, fifteen are directly tied to the Camorra clans. The south is flooded with trash and it seems impossible to find a solution.").

[110] *See* Press Release, Office of Drugs and Crime, Organized Crime Has Globalized and Turned into a Security Threat (June 17, 2010) (quoting Antonio Maria Costa, Executive Director of the United Nations Office on Drugs and Crime) (describing a report that finds global organized crime to blame for extensive human trafficking, migrant smuggling, fire-arm smuggling, illegal exploitation of natural resources, counterfeiting goods, cyber attacks, and identity theft).

[111] *See Beyond the Silk Road: Potential Risks, Threats and Promises of Virtual Currencies: Hearing Before the S. Comm. on Homeland Sec. and Governmental Affairs*, 113th Cong. 64–70 (2013) (Statement of Mythili Raman, Acting Assistant Attorney General, Criminal Division, United States Department of Justice). Assistant United States Attorney General Mythili Raman stated:

> Criminals are nearly always early adopters of new technologies and financial systems, and virtual currency is no exception. As virtual currency has grown, it has attracted illicit users along with legitimate ones. Our experience has shown that some criminals have exploited virtual currency systems because of the ability of those systems to conduct transfers quickly, securely, and often with a perceived higher level of anonymity than that afforded by traditional financial services. The irreversibility of many virtual currency transactions additionally appeals to a variety of individuals seeking to engage in illicit activity, as does their ability to send funds cross-border.

Id. at 65.

causing organized crime to "run rampant."[112] Europol warns that criminals currently hide "billions" of stolen cash in cryptocurrency.[113] In 2013, Nicolae Popescu, a Romanian fugitive who lead an international crime syndicate, was charged along with six other collaborators in a multi-million dollar cyber fraud scheme that entailed choreographing the transfer of illicitly obtained American cash into U.S. banks and then to Popescu himself or his collaborators in Europe.[114] In March 2018, Iceland lost the equivalent of $2 million United States dollars ("USD") through a Bitcoin mining burglary, the "largest theft of its kind," involving the theft of hundreds of Bitcoin mining rigs, power sources, motherboards, memory discs, and CPUs from four data centers located in Reykjavik;[115] though not involving the direct theft of Bitcoin or other virtual currency, this incident is indicative of the escalation of cryptocurrency's power, and mobs around the world have taken note.[116] Similarly, in January 2017, the Organized Crime

---

[112] Sterlin Lujan, *Australian Government: Bitcoin is Causing Organized Crime to Proliferate*, BITCOIN.COM (Aug. 30, 2017), https://news.bitcoin.com/australia-believes-bitcoin-is-causing-organized-crime-to-proliferate/ ("Virtual currencies, such as Bitcoin, are increasingly being used by serious and organised [sic] crime groups as they are a form of currency that can be sold anonymously online, without reliance on a central bank or financial institution to facilitate transactions.").

[113] Mathew J. Schwartz**,** *Criminals Hide 'Billions' in Cryptocurrency, Europol Warns*, BANK INFO SECURITY (Feb. 15, 2018), https://www.bankinfosecurity.com/criminals-hide-billions-in-cryptocurrency-europol-warns-a-10653 ("Europol, the EU's law enforcement intelligence agency, estimates that criminals in Europe generate $140 billion in illicit proceeds annually, of which about 3 or 4 percent - $4 billion to $6 billion - is being laundered via cryptocurrencies.").

[114] Press Release, U.S. Dep't of Just., Indictment Unsealed and "Wanted" Posters Issued for Fugitives Charged with Multimillion Dollar International Cyber Fraud Scheme (updated Sept. 15, 2014), https://www.justice.gov/opa/pr/indictment-unsealed-and-wanted-posters-issued-fugitives-charged-multimillion-dollar.

[115] Kelso, *supra* note 23 ("Everything points to this being a highly organized crime.").

[116] *Id.* Although, in this specific instance, the loss of the 600 mining rigs could quickly shift to an illegal acquisition of Bitcoin for whomever is in possession of them. According to Icelandic authorities, "those in possession could begin earning

Bureau of the Bolivarian National Police busted a large Bitcoin mining farm operation in Venezuela, linked to an international organized crime syndicate in Poland, for stealing electricity.[117] The 2013 case of Liberty Reserve, a virtual currency founded in Costa Rica, is indicative of just how many people may be affected by digital organized crime: the Secret Service estimated Liberty Reserve, accused of money laundering and of "illegally operating as an unlicensed money transmitter," counted over one million users worldwide.[118]

Criminals across the globe are also using Bitcoin for digital ransoms, the number of which has been steadily increasing.[119] One group in particular, spread across Russia and Ukraine, has collected over $16,500,000 USD in Bitcoin, primarily by targeting American victims.[120] These operations are made possible because criminals can securely store their stolen coins in digital wallets that are not tethered to any government entity.[121] It is also easy to convert the

---

Bitcoin. And considering the number of rigs stolen, the profit could be substantial." *Id.*

[117] Steve Torodov, *Venezuelan Police Bust Bitcoin Mining Farm for Stealing Electricity; Authorities Claim Operators Linked to Polish Organized Crime Syndicate*, RAZOR-FOREX (Jan. 28, 2017), https://www.razor-forex.com/2017/01/venezuelan-police-bust-bitcoin-mining.html.

[118] U.S. DEP'T OF JUST., NATIONAL TERRORIST FINANCING RISK ASSESSMENT 57–58 (2015), https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/National%20Terrorist%20Financing%20Risk%20Assessment%20%E2%80%93%2006-12-2015.pdf. Liberty Reserve was accused of money laundering and of "illegally operating as an unlicensed money transmitter," and was, thus, charged in federal court in New York. *Id.* at 58. In fact:

> The Secret Service estimates that Liberty Reserve had *more than one million users worldwide*, with more than 200,000 in the United States, and processed more than $1.4 billion of transactions annually. The transactions processed through Liberty Reserve involved payments associated with credit card fraud, identity theft, investment fraud, computer hacking, drug trafficking, and child pornography.

Id. (emphasis added).

[119] Popper, *supra* note 8.

[120] *Id.*

[121] *Id.*

stolen coins into real cash.[122] because this type of online extortion activity had become so widespread, in 2015 the Financial Industry Regulatory Authority ("FINRA") warned its members to immediately contact the FBI if they received messages from a criminal group working under the pseudonym "DD4BC."[123]

Organized crime and its involvement with cryptocurrency has also touched the banking sector, despite banks' overall distrust of virtual currency.[124] Commonwealth Bank provided millions of dollars in mortgages to a notorious Italian mafia kingpin to launder from his drug and extortion conglomerate whilst banning its customers from buying Bitcoin due to the "unregulated and highly volatile nature of virtual currencies."[125] Similarly, the Netherlands' Rabobank rejects Bitcoin for like reasons, while its California branch pled guilty to conspiracy for cooperating in Mexican drug money laundering efforts.[126] These are a just handful of examples of

---

[122] *Id.* ("'The criminal underground very much likes Bitcoin,' said Curt Wilson, a senior threat intelligence analyst at Arbor Networks. 'It's enabled a greater sense of obfuscation.'").

[123] FIN. INDUS. REG. AUTH., DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACKS ON MEMBER FIRMS (June 19, 2015), https://www.finra.org/industry/information-notice-061915 ("In these incidents, DD4BC first sends the firm an email announcing that the firm will be a target for a DDoS attack, but that the firm can avoid the attack by paying a ransom in Bitcoin. DD4BC conducts a short 'demonstration' attack, typically lasting about one hour, with the threat of further attacks if the ransom is not paid. DD4BC requests payment within 24 hours to prevent further attacks.").

[124] Rkeca, *Banks' Hypocrisy: Ban Bitcoin but Mafia Boss is Ok to Work with*, TOKENTHUSIAST (Mar. 31, 2018), https://tokenthusiast.com/2018/03/31/bank-hypocrisy-ban-bitcoin-but-mafia-boss-is-ok-to-work-with/.

[125] *Id.*; *see also* Roberto Saviano, *Where the Mob Keeps Its Money*, N.Y. TIMES (Aug. 25, 2012), https://www.nytimes.com/2012/08/26/opinion/sunday/where-the-mob-keeps-its-money.html ("American banks have profited from money laundering by Latin American drug cartels . . . .").

[126] Rkeca, *supra* note 124; *see also* Janene Pieters, *Dutch Banks Refuse Accounts for Cryptocurrency Businesses*, NL TIMES (Feb. 2, 2018), https://nltimes.nl/2018/02/02/dutch-banks-refuse-accounts-cryptocurrency-businesses; Elliot Spagat, *Rabobank to Pay $369 Million in Money-laundering Case*, AP NEWS (Feb. 8, 2018), https://www.apnews.com/25204f3ee9fa4e948ea74a0e82249258/Rabobank-to-pay-$369-million-in-money-laundering-case.

a global trend among banks to turn a blind eye to organized criminal activity when these institutions benefit from it.[127]

Cryptocurrency has also appealed to terrorists.[128] In 2015, the Department of Treasury issued a National Money Laundering Risk Assessment ("NMLRA") and a National Terrorist Risk Assessment ("NTRA").[129] The NMLRA reiterated the general concerns surrounding cryptocurrency, using the Silk Road and Liberty Reserve prosecutions as examples;[130] the NTRA explained how

---

[127] *See* Saviano, *supra* note 125. The article goes on to state that, although:

> Mutually beneficial relationships between bankers and gangsters aren't new . . . what's remarkable is their reach at the highest levels of global finance. In 2010, Wachovia admitted that it had essentially helped finance the murderous drug war in Mexico by failing to identify and stop illicit transactions. The bank, which was acquired by Wells Fargo during the financial crisis, agreed to pay $160 million in fines and penalties for tolerating the laundering, which occurred between 2004 and 2007. [In July 2012], Senate investigators found that HSBC [Bank] had for a decade improperly facilitated transactions by Mexican drug traffickers, Saudi financiers with ties to Al Qaeda and Iranian bankers trying to circumvent United States sanctions. The bank set aside $700 million to cover fines, settlements and other expenses related to the inquiry, and its chief of compliance resigned. ABN Amro, Barclays, Credit Suisse, Lloyds and ING have reached expensive settlements with regulators after admitting to executing the transactions of clients in disreputable countries like Cuba, Iran, Libya, Myanmar and Sudan.

Id.

[128] U.S. DEP'T OF JUST., *supra* note 118.

[129] Press Release, U.S. Dep't of Treas., Treasury Department Publishes National Money Laundering Risk Assessment and National Terrorist Financing Risk Assessment (June 12, 2015), https://www.treasury.gov/press-center/press-releases/Pages/jl0072.aspx.

[130] U.S. DEP'T OF TREAS., NATIONAL MONEY LAUNDERING RISK ASSESSMENT 62 (2015), https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/National%20Money%20Laundering%20Risk%20Assessment%20%E2%80%93%2006-12-2015.pdf ("[T]he rapid evolution of the market, the development of new business models and entry of new virtual currency payments developers and providers—many from a non-financial services environment (e.g., the technology sector), where industry is not as highly regulated as in the financial sector—together with the potential to operate without a domestic presence, is leading to service providers entering the market that do not comply with BSA obligations. The Secret Service observes that criminals are looking for and finding virtual currencies that offer: [a]nonymity for both users and transactions[;] [t]he ability to move illicit proceeds from one country to

terrorists around the world have backed away from utilizing traditional American banks and opted to embrace Bitcoin and its anonymity in the pursuit of their ventures.[131]

A. *RICO: An Overview*

The Racketeer Influenced and Corrupt Organizations Act[132] is a federal law enacted in 1970 as Title IX of the Organized Crime Control Act.[133] At its inception, RICO was written to target the Mafia and other organized crime families in the United States, and did so by tying mob bosses to the crimes of their subordinates by holding all the parties involved accountable as part of "criminal enterprises."[134] The Act also allows multiple crimes going back several years to be sweepingly prosecuted in a single case; the Act's language contains a long list of crimes that constitute "racketeering activity," the repetition of which triggers a RICO suit.[135] Such "predicate" crimes include: homicide, kidnapping, extortion, witness tampering, robbery, arson, money laundering, counterfeiting, securities violations, and mail and wire fraud.[136] Defendants, however, must have engaged in a "pattern" of racketeering activity, requiring at least two acts of racketeering

---

another quickly[;] [l]ow volatility, which results in lower exchange risk[;] [w]idespread adoption in the criminal underground[; and] [t]rustworthiness.").

[131] U.S. DEP'T OF JUST., *supra* note 118, at 57–58. ("[T]he U.S. Secret Service has observed that criminals are looking for and finding virtual currencies that offer anonymity for both users and transactions; the ability to move illicit proceeds from one country to another quickly; low volatility, which results in lower exchange risk; widespread adoption in the criminal underground; and trustworthiness . . . . [A] posting on a blog linked to ISIL has proposed using Bitcoin to fund global jihadist efforts.").

[132] 18 U.S.C. §§ 1961–68 (2012).

[133] Michael Beshears, *The Fight Against Organized Crime: RICO Stands the Test of Time*, IN PUB. SAFETY, (Apr. 11, 2014), https://inpublicsafety.com/2014/04/the-fight-against-organized-crime-rico-stands-the-test-of-time/.

[134] *See* § 1961; *see also* Nathan Koppel, *They Call it RICO, and It Is Sweeping*, WALL ST. J. (Jan. 20, 2011), https://www.wsj.com/articles/SB10001424052748704881304576094110829882704; 18 U.S.C. § 1961(4) (2012).

[135] *See, e.g.*, *RICO Law*, HG.ORG (last visited Oct. 13, 2018), https://www.hg.org/rico-law.html; Koppel, *supra* note 134; § 1961.

[136] *See RICO Law*, *supra* note 135; § 1961.

activity within a ten-year window.[137] As this Recent Development will explain, this may be one of the least flexible elements of the RICO statute.

Over the decades since RICO's codification, however, Congress has broadened the Act's scope of applicability beyond the Mafia, turning it into one of the most powerful (and controversial)[138] laws the government utilizes to this day against white collar crimes.[139] The statute's wide adaptability is due to its accommodating language and the broad interpretations of it that followed.[140] First,

---

[137] § 1961(5).

[138] Koppel, *supra* note 134 ("Over time . . . the law has become controversial. RICO is often criticized because of its use in civil cases to deal with business disputes that have nothing to do with mob activity . . . .") (internal quotations omitted).

[139] *Id.*; Peck, *supra* note 97 at 195. But Congress, in fact, never intended for RICO to have a narrow scope in the first place. Robert Blakey, adviser to the United States Senate Government Operations Committee who drafted the act, stated in 1989 that "[w]e don't want one set of rules for people whose collars are blue or whose names end in vowels, and another set for those whose collars are white and have Ivy League diplomas." Alain L. Sanders, *Law: Showdown at Gucci*, TIME (Aug. 21, 1989).

[140] Much has changed for RICO in recent years, as:

> Businesses can be considered enterprises subject to the law, said Peter Henning, a law professor at Wayne State University, in Michigan. Victims of an alleged fraud can use RICO to file civil suits and recover triple the amount of damages they suffered. The Gulf of Mexico oil disaster has prompted civil racketeering suits. Some alleged conspirators of Ponzi schemer Bernard Madoff have been charged under RICO, as have tobacco companies and prominent political figures.

Koppel, *supra* note 134. Additionally, RICO has been used against the Fédération Internationale de Football Association ("FIFA"), *id.*, pro-life activists, Nat'l Org. for Women, Inc. v. Scheidler, 510 U.S. 249 (1994) ("Women's rights organization and abortion clinics brought action against coalition of antiabortion groups alleging that defendants were members of nationwide conspiracy to shut down abortion clinics through a pattern of racketeering activity in violation of . . . []RICO[]."), and even President Trump prior to his election to office, Cohen v. Trump, 10-CV-0940-GPC-WVG, 2014 WL 690513, at *1 (S.D. Cal. Feb. 21, 2014) ("Plaintiff alleges that, but for misrepresentations made by Trump University, he would not have paid for Trump University programs. Specifically, Plaintiff alleges the following misrepresentations: that the programs would give access to Donald Trump's real estate investing secrets; that Donald Trump had a meaningful role in selecting the instructors

RICO itself explicitly calls for a generous reading, providing that it "be liberally construed to effectuate its remedial purpose."[141] This has given courts ample latitude in deciding and interpreting RICO-related cases. For example, in *Boyle v. United States*,[142] the Supreme Court allowed for a broad understanding of the word "enterprise" in the statute.[143] There, the Court decided that RICO claims can be brought against "enterprises-in-fact," meaning an informal group of individuals working around a common structure that contains three main features: a common purpose, relationships among the participating individuals, and longevity sufficient enough to effectively pursue the group's purposes.[144] In essence, this decision

---

for Trump University programs; and that Trump University was a 'university.'") (citation omitted).

[141] Pub. L. No. 91-452, § 904(a) 84 Stat. 922 (1970); *see also* J. KELLY STRADER, UNDERSTANDING WHITE COLLAR CRIME 347 (Carolina Academic Press, 4th ed. 2017).

[142] Boyle v. United States, 556 U.S. 938 (2009).

[143] *Id.* at 948; *see also* 18 U.S.C. § 1962(c) (2012) ("[I]t includes any . . . group of individuals associated in fact although not a legal entity . . . ."). The defendants were part of a "group [that] was loosely and informally organized," and had participated in a string of bank heists across various states in the 1990s. *Boyle*, 556 U.S. at 940.

[144] *Boyle*, 556 U.S. at 944–45. The Supreme Court emphasizes the flexibility of RICO's language in its opinion:

> The statute does not specifically define the outer boundaries of the 'enterprise' concept but states that the term 'includes any individual, partnership, corporation, association, or other legal entity, and any union or group of individuals associated in fact although not a legal entity.' . . . This enumeration of included enterprises is obviously broad, encompassing '*any* . . . group of individuals associated in fact.' . . . The term 'any' ensures that the definition has a wide reach, . . . and the very concept of an association in fact is expansive.

Id. The *Boyle* decision was also crucial because it resolved a four-to-five circuit split regarding what criteria are necessary for a group to constitute an enterprise. STRADER, *supra* note 141, at 138, 355. Additionally, unlike most criminal statutes, RICO is exceptionally flexible because it:

> [C]ontains a civil component that allows it to be used to turn ordinary business disputes that would be filed in state courts into federal cases. Proving a violation results in the award of triple damages plus attorney's fees, so plaintiffs have an incentive to look for ways to turn their grievances into a RICO suit.

made it so that the government was no longer required to show proof of a structured enterprise separately from the criminal activity at bar to bring forth a satisfactory RICO suit.[145]

RICO's flexibility is also apparent in its ability to prosecute a leader of a syndicate for crimes he or she delegated to be performed, even though he or she may not have actually acted,[146] while referring back to years of the defendant's criminal and civil history as long as it is within a ten-year window.[147] Past convictions are not necessary—rather, the prior criminal activity need only be "chargeable," "indictable," or "punishable" under their respective state or federal statutes.[148] This section of RICO also transcends the statutes of limitation for the respective crimes; so long as the predicate acts fall within RICO's five-year statute of limitations, they are sufficient.[149]

To understand RICO is to understand the ongoing dispute surrounding it, as:

> [f]or some commentators, Congress's original focus on organized crime shows that RICO has been stretched beyond its intended targets, and is an inappropriate vehicle for prosecuting white collar cases. Others contend, however, that RICO was never intended to be limited to

---

Peter J. Henning, *RICO Lawsuits Are Tempting, but Tread Lightly*, N.Y. TIMES (Jan. 16, 2018), https://www.nytimes.com/2018/01/16/business/dealbook/harvey-weinstein-rico.html. This Recent Development, however, will focus exclusively on RICO's criminal components.

[145] *See Boyle*, 556 U.S. at 948.

[146] 18 U.S.C. § 1962(c) (2012); *see also* U.S. DEP'T OF JUST., ORGANIZED CRIME AND GANG SECTION, CRIMINAL RICO: 18 U.S.C. §§ 1961-1968 A MANUAL FOR FEDERAL PROSECUTORS, 169–70 (6th rev. ed. May 2016), https://www.justice.gov/usam/file/870856/download ("A Defendant May Be Liable for a RICO Conspiracy Offense even if the Defendant Did Not Participate in the Operation or Management of the Enterprise."). The manual further iterates, citing *Salinas v. United States*:

> [A] defendant may be liable for a conspiracy to violate a law even if he may not be liable for a substantive violation of the law because he does not fall within the category of persons who could commit the substantive offense directly . . . . [And] may be liable for conspiracy even though he was incapable of committing the substantive offense.

Id. (citation omitted).

[147] *See* 18 U.S.C. §§ 1961–68 (2012); Koppel, *supra* note 134.

[148] *See* § 1962(a)–(c); *see also* STRADER, *supra* note 141, at 364.

[149] *See* § 1962(a)–(c); *see also* STRADER, *supra* note 141, at 364.

> "organized crime" and that its use is entirely proper in white collar cases.[150]

Despite the conjectures, however, it is undisputed that RICO's application has remained broad and versatile, and that seems unlikely to change.[151]

B. *RICO: A Qualitative Analysis*

By its own text, RICO is well-equipped to tackle issues in cryptocurrency, or at least the troubles virtual currency has encountered quite recently;[152] specifically, it is RICO's proven versatility that bodes well for the Act's ability to curb virtual currency-related crimes. As seen above, cryptocurrency laws have struggled to find elasticity and expand their power to impact cryptocurrency. RICO, however, has been applied to a wide gamut of crimes, straying away from its original mob family target. This versatility could translate into an ability to shapeshift alongside the ever-changing world of virtual currency and keep holding criminals accountable, no matter how innovative their efforts. In brief, RICO's elasticity may be adequate to keep up with the changing nature of cryptocurrency.

Another characteristic of RICO that would particularly benefit the realm of cryptocurrency is that it mandates asset forfeiture from the defendant.[153] Specifically with regard to the monetary value of virtual currency itself, this would ensure that the crime would not allow any amount of Bitcoin or currency to get lost in cyber-ether—unlike the thousands upon thousands of Bitcoin lost to hacks. However, this resolution likely pivots directly on the yet-to-be-

---

[150] STRADER, *supra* note 141, at 346. This is not to be construed to mean that RICO is wielded liberally as a legal weapon. In fact, the Department of Justice ("DOJ") enforces guidelines that impose restrictions on RICO's use, so as not to allow "'imaginative' prosecutions . . . which are far afield from the congressional purpose of the RICO statute. The [g]uidelines also seek to limit RICO's application in cases where the matter is best left to state and local law enforcement." *Id.* at 347.

[151] *Id.* at 346 n.10 ("[T]he legislative history actually glitter with resolve to strike at enterprise criminality in all its forms.") (citation omitted).

[152] *See* 18 U.S.C. § 1961 (2012)*; see also* Koppel, *supra* note 134.

[153] § 1963.

determined issue about whether cryptocurrency constitutes property.

Although RICO's territorial scope is not unlimited,[154] it is far-reaching. Recently confirmed by the United States Supreme Court, RICO applies extraterritorially and can be used against foreign enterprises whose actions directly affect American commerce.[155] Subsequently, federal prosecutors have ample room to target foreign criminal activity pertaining to RICO's criminal provisions.[156] With cryptocurrency involving online transactions, it is unlikely that large-scale online crimes do not touch American commerce. However, when it comes to issues that on their face appear isolated to foreign countries (such as mining devices missing in Iceland[157]), it might be more difficult for RICO to extend its reach.

In contrast, a major problem RICO may face with regards to prosecuting crypto-criminals may be exactly where its strength has lain for the past half century: its definition of "pattern of racketeering,"[158] requiring the finding of two racketeering crimes within the span of ten years.[159] Outside of the cryptocurrency realm, federal courts have struggled to come to a consensus on how to interpret this provision.[160] In *Sedima, S.P.R.L. v. Imrex Co.*,[161] the Supreme Court noted in a footnote that the two-crime requirement was necessary, but not sufficient, for a successful RICO claim.[162] Then, the Supreme Court echoed its holding in *Sedima* when it decided *H.J. Inc. v. Nw. Bell Tel. Co.*[163] There, the Court rejected the Eighth Circuit's narrow reading of the provision (stating the plaintiff had failed to prove a "pattern") and called for an additional

---

[154] *Id.*

[155] *Supreme Court Clarifies Extraterritorial Reach of RICO*, BALLARD SPAHR LLP (June 21, 2016), https://www.ballardspahr.com/alertspublications/legalalerts/2016-06-21-supreme-court-clarifies-extraterritorial-reach-of-rico.aspx.

[156] *Id.*

[157] Koppel, *supra* note 134.

[158] 18 U.S.C. § 1961(5) (2012).

[159] *See id.*

[160] STRADER, *supra* note 141, at 369.

[161] Sedima, S.P.R.L. v. Imrex Co., 473 U.S. 479 (1985).

[162] *Id.* at 496 n.14.

[163] H.J. Inc. v. Nw. Bell Tel. Co., 492 U.S. 229 (1989).

requirement to the two-crime minimum for establishing a "pattern": the "relationship plus continuity" test.[164] The Court held that "relationship" entailed a commonality of factors. This included "purposes, results, participants, victims, or methods of commission" as among the predicate acts that would indicate that they were not isolated incidents.[165] It also held that "continuity" can be proven in two ways: through a finding of a defined sequence of criminal acts over a period of time longer than a "few weeks or months" (also known as a "closed-ended pattern"), or through a finding of, if the activity occurred over a short period of time, continuity demonstrated via implicit or explicit threat of continued repetition into the future (an "open-ended pattern").[166] While helpful, this opinion was too vague to offer actionable guidance to lower federal courts as to how to identify a pattern of racketeering activity.[167] As a result, lower courts have differed in their respective approaches on the matter.[168]

While this ambiguity is daunting, the "closed-ended" and "open-ended" pattern dichotomy might still be optimistic. On one hand, it probably remains difficult to determine whether isolated racketeering incidents, even at the international level, could be prosecuted under RICO if there is a lack of proof of intent to commit another racketeering offense by the same defendant. It is especially difficult to enforce RICO where, in the presence of a provable offense, the pattern occurs over a short span of time.[169] On the other

---

[164] *Id.* at 239.

[165] *Id.* at 240.

[166] *Id.* at 241–42; *see also* STRADER, *supra* note 141, at 370.

[167] STRADER, *supra* note 141, at 370. In *Nw. Bell*, Justice Scalia, although concurring in the judgment, opined the "relationship plus continuity" test was so vague it violated due process. *Nw. Bell*, 492 U.S. at 255–56 (Scalia, J., concurring). Thus far, the Supreme Court has not faced due process challenges to RICO. STRADER, *supra* note 141, at 370.

[168] STRADER, *supra* note 141, at 370.

[169] *Id.* at 373 ("[C]ourts are likely to find that the pattern requirement is not met where the alleged predicate acts extended over a relatively short and finite period, often defined as less than one year.") Hypothetically, in one-off international syndicate heist situations, it is easy to imagine a scenario where the enterprise involved in the execution of the crime may have committed a pattern of crimes in preparation of the heist within a one-year window. For all intents and purposes, those instances would be difficult for RICO to touch.

hand, relying on the Supreme Court's generous "open-ended pattern" approach may suffice. Undoubtedly, it may be hard to imagine a first-time criminal successfully delegating subordinates to execute a highly sophisticated, cross-continental heist. However, the realm of cryptocurrency specifically posits unique threats that should encourage such a generous reading of RICO to preemptively avoid future syndicate-led crypto-crimes. As seen above, virtual currency provides all users, law-abiding and delinquent, a cloud of anonymity. It also provides consumers a loophole for avoiding banks and their respective regulations. Even where evidence of a continued threat is weak at best, the hypothetical risk of repeated future activity is heightened by the fact that these actors have anonymity and a lack of regulations on their side. Thus, the prospect of delving deeper into the wild west of crypto anarchy could, and definitely should, be enough to successfully trigger RICO action.

It is important to remember another key aspect of cryptocurrency: its ability to transcend geographical boarders. Online crimes that have involved organized syndicates to date have demonstrated sophisticated, international efforts, raising the stakes so high as to have governments actively concerned about unlawful uses of virtual currency.[170] The risk of a repeated threat to a country or its government alone, even where the evidence of such risk is weak, should be egregious enough to successfully trigger a RICO action.[171] Additionally, RICO, with its power to expose a defendant's criminal and civil history,[172] could take down even the lowest member of the organizational hierarchy.

The FTC's actions echo the above concerns and ambitions: when charging Butterfly Labs,[173] the settlement pivoted on the element of likelihood of continued harm. There, a sustained pattern

---

[170] Lujan, *supra* note 112.

[171] This notion is echoed in *Uniroyal Goodrich Tire Co. v. Mut. Trading Corp.*, where the Seventh Circuit found that a pattern of criminal activity may be shown even if directed against a single victim. Uniroyal Goodrich Tire Co. v. Mut'l Trading Corp., 63 F.3d 516, 524 (7th Cir. 1995). Hypothetically, under this ruling, a country or government may constitute a single victim of a pattern of misconduct, creating the potential for a successful RICO action.

[172] Beshears, *supra* note 133.

[173] MURPHY ET AL., *supra* note 22.

of deceit toward its consumers led the court to believe that, without intervention, Butterfly Labs would continue its violations. Of course, the element of the found pattern which led Butterfly Labs to its demise cannot be ignored. However, though the case ended in a settlement, the FTC's action and the court's willingness to grant the initial *ex parte* restraining order, even where the proof of continued harm was not explicit, encapsulate a sentiment that is essential for dealing with the unwieldy nature of cryptocurrency and related crimes. Perhaps future RICO applications will take heed.

In summary, RICO's claim to fame (or notoriety) that has led it to endure decades of law-making lies in its generous application. RICO and cryptocurrency are alike—they are serpentine, often amorphous, and sometimes difficult to define. If it really does "take one to know one," we are hard-pressed to identify a law better equipped than RICO to deal with the turbulent enigma that is the world of Bitcoin and other virtual currency.

V. CONCLUSION

When cryptocurrency gained traction, new crimes came along with it. But the spark of cryptocurrency is also responsible for stoking the once-dwindling flame of mob and syndicate crimes. Gone may be the days of Gotti and Hollywood-worthy heists—but mob syndicates, old and new, have shown no intention of leaving. Only time will tell what new and creative ways criminals around the world will leverage virtual currency to avoid the law.

The United States is home to the world's largest financial system and plays a central role in the global economy.[174] The onus remains on American law enforcement to ensure that mobs and syndicates across the world do not re-enter the forefront of our economy. Without a doubt, federal law has gone to great lengths to wrangle the crypto-world. Although these efforts have not resulted in a sweeping success, the government's willingness to creatively come up with new solutions to regulate cryptocurrency is promising. RICO, however, may be the best legal recourse to keep crypto-crimes at bay. By its very nature, RICO demands a liberal

[174] Treasury Department Publishes National Money Laundering Risk Assessment and National Terrorist Financing Risk Assessment, *supra* note 129.

application, which courts have dutifully carried out. And because of these broad, liberal applications, RICO has stood the test of time, adapting to changing crimes and legal demands with the passing of the decades. While not a flawless remedy, RICO's versatility is likely to allow the law to endure and to continue to stretch its scope to include crimes in cryptocurrency, with particular emphasis on organized crime that leverages virtual currency. Despite popular conjectures claiming that RICO's evolution has strayed too far from Congress's original intent behind its codification, not only does RICO appear to state the exact opposite, but it would be unhelpful to our modern state of affairs if we started to tighten the scope of RICO now—at least for the time being. It might be more helpful to consider RICO as means to an end, rather than the end itself: because many branches of the federal government have understandably struggled with the task of regulating cryptocurrency, RICO could be the interim remedy, keeping nationwide and global syndicates at bay while other federal laws continue to plan and prepare for a world in which cryptocurrency may dominate the market.

In these fast-paced times, at the mercy of ever-changing modern technology, perhaps a law that has been consistently inconsistent is exactly the tool justice needs. To civilize cyberspace, it is in the United States government's best interest to rely on RICO.