ARTICLES

WHACK-A-MOLE: WHY PROSECUTING DIGITAL CURRENCY EXCHANGES WON'T STOP ONLINE MONEY LAUNDERING

by
Catherine Martin Christopher[*]

Law enforcement efforts to combat money laundering are increasingly misplaced. As money laundering and other underlying crimes shift into cyberspace, U.S. law enforcement focuses on prosecuting financial institutions' regulatory violations to prevent crime, rather than going after criminals themselves. This Article will describe current U.S. anti-money laundering laws, with particular criticism of how attenuated prosecution has become from crime. The Article will then describe the use of Bitcoin as a money-laundering vehicle, and analyze the difficulties for law enforcement officials who attempt to choke off Bitcoin transactions in lieu of prosecuting underlying criminal activity. The Article concludes with recommendations that law enforcement should look to digital currency exchangers not as criminals, but instead as partners in the effort to eradicate money laundering and—more importantly—the crimes underlying the laundering.

---

[*] Visiting Professor of Legal Skills and Director of Bar Preparation Resources Office, Texas Tech University School of Law. J.D., University of Pittsburgh. The author wishes to thank Elizabeth Caulfield, Brie D. Sherwin, and DeLeith Duke Gossett for their assistance and support in the writing of this Article.

Introduction

In the United States, law enforcement is constantly playing catch-up with criminals, and in no arena is this more evident than that of cybercrime. Money is moved around the globe at the click of a mouse or the tap on a smartphone screen, both spending and earning proceeds from crime. In response, U.S. legislators pile on more laws and regulations, increasing compliance burdens on law-abiding actors while failing to prevent criminal actors from operating.

Though only thinly understood, either by prosecutors or academics, a digital currency called Bitcoin has emerged as a boon to money launderers worldwide—it allows for the instantaneous transfer of vast amounts of money from one anonymous account to another, whether to purchase illegal drugs or weapons, or to fund organizations of questionable political endeavors.

This Article specifically addresses the crime of money laundering and its related criminal activities. In Part I, the structure of U.S. anti-money laundering laws is described and is criticized as not only ineffective but burdensome to the wrong parties. In Part II, the mechanics of Bitcoin are explored, along with its strengths and weaknesses as a measure of value and medium of exchange. Part III outlines the difficulties in prosecuting crimes committed via Bitcoin transfers and recommends that the current strategy, that of prosecuting currency exchangers for viola-

tions of reporting requirements, be abandoned in favor of using these entities as partners in law enforcement.[1]

I. U.S. Anti-Money Laundering Regime Explained and Critiqued

A. Statutes

Money laundering is criminalized by the intersection of a pair of relatively young statutory schemes: the Money Laundering Control Act of 1986[2] and the Bank Secrecy Act of 1970.[3] These statutes and their implementing regulations act in concert to deter and criminalize money laundering, which is essentially the process by which individuals disguise the source of illegally obtained funds.[4] Criminals must obscure the origin of criminally derived income so they may spend it without drawing the attention of law enforcement.[5]

Money laundering is a crime because lawmakers sought to make underlying criminal activity more difficult to engage in.[6] Initially, anti-money laundering statutes were enacted in order to hamper the illegal drug trade,[7] though anti-money laundering laws are also used to fight

---

[1] It is inherently difficult to write about developing technology. By the time a sentence is written, cite-checked, edited, and published, it's out of date. While great pains have been taken to make this Article as up-to-date as possible, by the time it is read, it will undoubtedly contain information that has been eclipsed by new developments. Even if (when) the details change, however, the larger issues are still at play. It is the author's hope that this Article will continue to be useful and interesting for its elucidation of the mechanics of Bitcoin transactions, the difficulties of prosecuting online crimes, and the themes of criminal and law enforcement priorities.

[2] Anti-Drug Abuse Act of 1986, Pub. L. No. 99-570, 100 Stat. 3207 (Subtitle H–Money Laundering Control Act of 1986) (codified in various sections of 12 U.S.C., 18 U.S.C., 21 U.S.C., and 31 U.S.C.).

[3] Bank Secrecy Act of 1970, Pub. L. No. 91-508, 84 Stat. 1114 (codified as amended in various sections of 12 U.S.C, 18 U.S.C., and 31 U.S.C.).

[4] M. Michelle Gallant, Money Laundering and the Proceeds of Crime: Economic Crime and Civil Remedies 11 (2005); Shawn Turner, Note, *U.S. Anti-Money Laundering Regulations: An Economic Approach to Cyberlaundering*, 54 Case W. Res. L. Rev. 1389, 1391 (2004).

[5] Robert Stokes, *Anti-Money Laundering Regulation and Emerging Payment Technologies*, Banking & Fin. Servs. Pol'y Rep., May 2013, at 1, 1.

[6] *See* Turner, *supra* note 4, at 1398 ("money laundering itself is not 'reprehensible'") (quoting Guy Stessens, Money Laundering: A New International Law Enforcement Model 84–85 (2000)).

[7] Anti-Drug Abuse Act of 1986, Pub. L. No. 99-570, 100 Stat. 3207, 3207, pmbl. (Subtitle H–Money Laundering Control Act of 1986) (codified in various sections of 12 U.S.C., 18 U.S.C., 21 U.S.C., and 31 U.S.C.) ("An Act [t]o strengthen Federal efforts to encourage foreign cooperation in eradicating illicit drug crops and in halting international drug traffic, to improve enforcement of Federal drug laws and enhance interdiction of illicit drug shipments, to provide strong Federal leadership in establishing effective drug abuse prevention and education programs, to expand Federal support for drug abuse treatment and rehabilitation efforts, and for other purposes.").

"corruption, organized crime and transnational criminal activity."[8] Theoretically, individuals will be less likely to engage in criminal enterprises if they cannot safely (that is, without law enforcement detection) spend the proceeds of their crimes.

The Money Laundering Control Act of 1986 criminalizes financial transactions (or attempted financial transactions) that "conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activit[ies]."[9] Such "specified unlawful activities" are enumerated in a mind-numbingly long list[10] ranging from dealing controlled substances,[11] murder,[12] and human trafficking,[13] to copyright infringement and violence against maritime fixed platforms.[14] Thus, in order to be guilty of money laundering under the Money Laundering Control Act, an individual must first have committed one of these specified unlawful activities.

In addition to any penalties assessed for the underlying crime, the money laundering crime carries criminal penalties of 20 years' imprisonment and fines of up to "$500,000 or twice the value of the property involved in the transaction, whichever is greater."[15] Criminal money laundering also subjects an individual to *civil* liability to the United States of fines of $10,000 or "the value of the property, funds, or monetary instruments involved in the transaction," whichever is greater.[16]

Significantly, law enforcement has begun to rely far more extensively on civil punishment rather than criminal.[17] Although the penalties are lower—disgorgement of ill-gotten funds, rather than fines of twice that amount plus jail time—prosecutors appear to believe civil penalties are sufficient. On the other hand, civil penalties may have become the preferred law enforcement mechanism because the government's burden of proof is much lower: preponderance of the evidence, rather than beyond a reasonable doubt.[18]

---

[8] GALLANT, *supra* note 4, at 7–8.

[9] 18 U.S.C. § 1956(a)(1)(B)(i) (2006). This section also criminalizes financial transactions intended "to promote the carrying on of specified unlawful activity." *Id.* § 1956 (a)(1)(A)(i).

[10] *Id.* § 1956(c)(7).

[11] *Id.* § 1956(c)(7)(B)(i).

[12] *Id.* § 1956(c)(7)(B)(ii).

[13] *Id.* § 1956(c)(7)(B)(vii).

[14] *Id.* § 1956(c)(7)(D).

[15] *Id.* § 1956(a)(1)(B). Conspiracy to launder money carries the same penalties. *Id.* § 1956(h).

[16] *Id.* § 1956(b)(1).

[17] GALLANT, *supra* note 4, at 75.

[18] The government's extremely broad authority for civil forfeiture is found in 18 U.S.C. § 981(a) (2006), and general rules for civil forfeiture (including burden of proof) are found in 18 U.S.C. § 983. Civil forfeiture has a long history in American law enforcement and is rooted in the legal fiction that the property itself is the criminal. *See* GALLANT, *supra* note 4, at 82–88 (discussing the historical roots and procedural distinctions of criminal forfeiture and civil forfeiture in United States law enforcement).

In more recent years, especially after the terrorist attacks of September 11, 2001, anti-money laundering laws are also relied upon to prevent terrorism.[19] Terrorism is, in several senses, a very different crime from illegal drug distribution, the initial target of anti-money laundering laws. Individuals who deal in drugs are paid *after* the illegal conduct has occurred—with those crimes, law enforcement can use anti-money laundering laws to trace the movement of funds back to the individuals who have already committed some other crime.[20] With terrorist financing, however, the movement of funds occurs *before* the intended crime has been committed.[21] Funds are transacted to prepare for a terroristic act that has not yet occurred—to purchase supplies, for instance, or to train would-be terrorists. In these instances, anti-money laundering laws are used to aid in detective work that will allow law enforcement to disrupt a crime that has not yet occurred.[22] In the case of terrorism, therefore, money is laundered to obscure not its source, but its destination.

Another important distinction between terrorism and other crimes such as drug trafficking is the legality of the origins of the funds in question. Drug traffickers obtain large sums of money (usually in cash) through their illegal endeavors, and the money laundering process is designed to disguise the source of those ill-gotten funds. With terrorism, however, the money may have been obtained from perfectly lawful sources; for example, individuals with lawful, respectable jobs may decide

---

[19] William Hett, *Digital Currencies and the Financing of Terrorism*, 15 RICH. J.L. & TECH. 4, ¶ 23 (2008), http://jolt.richmond.edu/v15i2/article4.pdf (citing Laura K. Donohue, *Anti-Terrorist Finance in the United Kingdom and United States*, 27 MICH. J. INT'L L. 303, 304–05 (2006)). The Bank Secrecy Act was amended to specify that "given the threat posed to the security of the Nation on and after the terrorist attacks against the United States on September 11, 2001," financial institutions' recordkeeping and reporting requirements could be used "in the conduct of intelligence or counterintelligence activities, including analysis, to protect against international terrorism." Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272, 326–27.

[20] *See The Financial War on Terrorism and the Administration's Implementation of Title III of the USA Patriot Act: Hearing Before the S. Comm. on Banking, Hous., & Urban Affairs*, 107th Cong. 53 (2002) (prepared statement of Kenneth W. Dam, Deputy Sec'y, Dep't of the Treasury) [hereinafter Dam Statement], *available at* http://www.gpo.gov/fdsys/pkg/CHRG-107shrg86403/pdf/CHRG-107shrg86403.pdf ("Stopping terrorist financing is perhaps more nuanced than money laundering because terrorist financing could be described as 'reverse money laundering.' In money laundering, the proceeds of crime are laundered for legitimate use or for use in perpetrating more crimes. If you find evidence of the original crime, you are likely to be placed on the trail of some money laundering. In terrorist finance, it is often the other way around. Proceeds of legitimate economic activity are used for illicit purposes. The money can come from almost anywhere.").

[21] *Id.*

[22] The full name of the Patriot Act, passed shortly after September 11, 2001, tacitly acknowledges that the law is designed to stop crimes before they occur: Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act.

to donate a portion of their salary to terrorist causes.[23] In such instances, it is the intended use of the funds—and the desire to conceal the intended use—that makes the transactions criminal.

Whether related to terrorism, drugs, or other forms of crime, though, money laundering is criminalized only because it is the outgrowth of some underlying crime. Spending income is perfectly legal so long as the funds were legally obtained; only where the funds were earned by (or destined for, in the case of terrorism) illegal means does the "shell" crime of money laundering occur.

B. Regulations

Anti-money laundering laws are in turn enforced through a complex scheme of regulations that require financial institutions to confirm customer identities,[24] maintain certain records,[25] and report certain transactions to government agencies.[26] The Bank Secrecy Act delegates to the Secretary of the Treasury broad authority to require financial institutions to maintain records and make reports that have "a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings" or "a high degree of usefulness in the conduct of intelligence or counterintelligence activities . . . to protect against international terrorism."[27]

Broadly, there are three types of regulations that impact American anti-money laundering efforts: know your customer, recordkeeping, and reporting requirements.[28]

Know your customer, or KYC,[29] regulations require that banks implement "risk-based procedures for verifying the identity of each customer to the extent reasonable and practicable."[30] Although the regulations allow for some flexibility based on the institution's size, customer base, types of accounts offered, etc., banks' policies must include collection of a customer's name, date of birth, address, and an identification number

---

[23] *See* Dam Statement, *supra* note 20, at 53.

[24] 31 U.S.C. § 5318(*l*) (2006).

[25] 12 U.S.C. § 1953(a) (2006).

[26] 31 U.S.C. § 5313 ("a domestic financial institution . . . shall file a report on the [specified] transaction at the time and in the way the Secretary prescribes").

[27] 12 U.S.C. § 1953. This language is also found in 31 U.S.C. § 5311.

[28] Regulations promulgated under the Bank Secrecy Act have been transferred and reorganized. Transfer and Reorganization of Bank Secrecy Act Regulations, 75 Fed. Reg. 65806 (Oct. 26, 2010) (effective Mar. 1, 2011). Previous literature often cites regulations found in 31 C.F.R. § 103 (2010), but regulations are cited herein using the updated citations, found in 31 C.F.R. §§ 1000–1099 (2013). A conversion table providing previous and current regulation citations is available at Transfer and Reorganization of Bank Secrecy Act Regulations, 75 Fed. Reg. at 65808–11.

[29] "KYC" is the standard acronym used in the financial services industry to refer to customer identity verification, although the applicable Treasury regulations refer to a "Customer Identification Program (CIP)." 31 C.F.R. § 1020.220(a) (2013). Less common is the phrase "customer due diligence," or CDD. *E.g.*, Stokes, *supra* note 5, at 4.

[30] 31 C.F.R. § 1020.220(a)(2).

(such as a taxpayer ID).[31] Typically, this means checking the drivers' licenses of customers who present themselves at a physical office.[32] Confirming customer identities becomes murkier, though, when the customer conducts business at an ATM or drive-through teller service, or—most ominously—conducts business online. Even if the bank has complied with the KYC requirements when opening an account, in these non-face-to-face situations, it is more difficult to confirm that the person authorizing the transaction is the actual account holder; the authentication (such as a PIN or online password) may be forged or stolen.

Also of note, other countries have different (read: more lax) KYC requirements.[33] It is possible for an individual in the United States to open a bank account in another country that does not require meaningful customer due diligence, then obtain a bank card that works at American ATMs. Money can be funneled into the foreign bank account with little or no identifying customer information, then accessed as cash in the United States.[34]

The regulations require that financial institutions maintain records of certain transactions as well. Nonbanks are required to maintain records of all transactions over $3,000, while the record retention threshold for banks is $10,000.[35] Such records must be retained for five years.[36]

Moreover, certain transactions trigger a financial institution's obligation to report the transaction to the government. For instance, all financial institutions (other than casinos) are required to report any "deposit, withdrawal, exchange of currency or other payment or transfer" exceeding $10,000.[37] These reports must be filed within 15 days of the transaction,[38] and any financial institution making such a transaction must verify and record the transacting customer's name and address, as well as record the beneficiary's identity, account number, and social security or taxpayer identification number.[39]

---

[31] *Id.* KYC requirements are similar for "money services businesses," entities such as check cashers and issuers of money orders, which are entities distinct from banks. *Id.* § 1010.100(ff). Money services businesses that provide or sell "prepaid access" are required to obtain a prepaid access customer's name, date of birth, address, and identification number. *Id.* § 1022.210(d)(1)(iv).

[32] Customer identification via a driver's license or passport is specifically authorized by 31 C.F.R. § 1020.220(a)(2)(ii)(A)(1). The regulations permit customer identity verification through non-documentary methods, but offer only suggestions as to how that might be accomplished; development of specific procedures is left to the financial institution(s). *Id.* § 1020.220(a)(2)(ii)(B).

[33] *See* Madelyn J. Daley, *Effectiveness of United States and International Efforts to Combat International Money Laundering*, 2000 ST. LOUIS-WARSAW TRANSATLANTIC L.J. 175, 199 (discussing "haven jurisdictions" for money laundering).

[34] *See* Hett, *supra* note 19, at ¶¶ 15–17.

[35] 31 C.F.R. § 1010.410(a)–(e) (2013).

[36] *Id.* § 1010.430(d).

[37] *Id.* § 1010.311.

[38] *Id.* § 1010.306(a)(1).

[39] *Id.* § 1010.312.

More vaguely, financial institutions must report "suspicious" transactions.[40] Regulations describe a "suspicious" transaction as one that involves at least $5,000 where the bank "knows, suspects, or has reason to suspect" that the funds are being laundered, the transaction is designed to evade regulation, or "[t]he transaction has no business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage."[41] For money services businesses, the dollar threshold drops to $2,000.[42] Suspicious transactions must be reported using a Suspicious Activity Report (SAR) filed with the Treasury Department's Financial Crimes Enforcement Network within 30 days of the transaction.[43]

Taken altogether, the regulations are confusing and burdensome. Willful failure to comply with regulations promulgated under the Bank Secrecy Act exposes the financial institution and its employees—not the customer actually making or receiving an illegal transaction—to criminal penalties of up to one year in prison and a $1,000 fine,[44] while willful or grossly negligent failure to comply may lead to civil liability to the United States of up to $10,000.[45] Failure to report coin or currency transactions, failure to report the import or export of monetary instruments over $10,000, or structuring transactions to avoid reporting requirements can result in the financial institution forfeiting "all property, real or personal, involved in the offense and any property traceable thereto."[46]

Potential violations exist everywhere. For example, money transmitting businesses are required to register with the Financial Crimes Enforcement Network,[47] and failure to do so is a punishable offense. Beyond that, operating a money transmitting business without obtaining a license required by the home state *also* constitutes a federal crime[48] punishable by five years imprisonment or a fine.[49]

These regulations place a heavy burden on financial institutions to perform criminal detection and law enforcement work. In fact, some have suggested that this shifting of police work was intentional, because financial institutions are in a better position and are better capable of detecting criminal activity.[50]

---

[40] *E.g.*, *id.* § 1020.320 (requirements for banks), § 1022.320 (requirements for money services businesses).

[41] *Id.* § 1020.320(a). The regulations do not provide guidance as to how a financial institution would come to "know" or "suspect" the illegality of a particular transaction.

[42] *Id.* § 1022.320(a)(2).

[43] *Id.* §§ 1020.320(b), 1022.320(b).

[44] 12 U.S.C. § 1956 (2006).

[45] *Id.* § 1955(a).

[46] 31 U.S.C. § 5317(c)(1)–(2) (2006) (including criminal and civil forfeiture provisions).

[47] 31 C.F.R. § 1022.380.

[48] 18 U.S.C. § 1960(b)(1)(A) (2006).

[49] *Id.* § 1960(a).

[50] Hett, *supra* note 19, at ¶ 26 (citing Donohue, *supra* note 19, at 356–57).

Legislators have thus created another shell in the Russian nesting doll of anti-money laundering laws: it is illegal for financial institutions to fail to report suspicious activity, because that suspicious activity is indicative of money laundering, while money laundering in turn is only illegal because it indicates the commission of an underlying crime.[51] The crime of failing to make SARs is thus significantly attenuated from the root problem: the drug trade, terrorism, or other criminal activity.

Moreover, by requiring KYC and SAR compliance and criminalizing the failure to comply with those regulations, legislators have now shifted the criminal activity (and law enforcement attention) away from the drug dealers, terrorists, and other criminals onto the financial institutions that take those individuals' deposits and effect their financial transactions.[52] To be sure, financial institutions benefit from the transaction fees imposed on money laundering activities, but the institutions themselves may not be wittingly contributing to the underlying criminal activity.

Even more frustrating is the very real possibility that the burdensome reporting requirements are ineffective. The regulations promulgated pursuant to the Patriot Act would likely not have prevented, or even raised suspicion about, the financial transactions that funded the September 11 terrorist attacks.[53] Loopholes in the reporting requirements are constantly being found and exploited by money launderers so the launderers can continue to use the financial system to obscure the source (or purpose) of their funds, while regulators are constantly playing catch-up.[54] For instance, money launderers conducted business by wire transfers for some time before regulators realized it and, in 1995, included wire transactions in the reporting requirements.[55] Large transactions have long been broken down into multiple smaller increments in order to fall beneath the reporting requirements—a process known by the hilarious name of "smurfing"[56]—until legislators specifically criminalized this evasive behavior.[57]

Moreover, a SAR is filed long after the horse is out of the barn. Although useful in creating a paper trail,[58] there may be considerable delay (up to 30 days[59]) between the suspicious transaction itself and the filing

---

[51] *See* GALLANT, *supra* note 4, at 13–14.

[52] *See* Turner, *supra* note 4, at 1404–05.

[53] Hett, *supra* note 19, at ¶ 23 (citing Donohue, *supra* note 19, at 396).

[54] *See* Turner, *supra* note 4, at 1402–06 (evolution of the Bank Secrecy Act and Money Laundering Control Act).

[55] *Id.* at 1403 (citing Lisa A. Barbot, Comment, *Money Laundering: An International Challenge*, 3 TUL. J. INT'L & COMP. L. 161, 193 (1995)).

[56] *Id.* The term is apparently a reference to drug dealers' "minions (like the cartoon Smurfs)" who would take smaller amounts of cash and scatter to various banks to make deposits. Steven Biskupic & Eric J. Klumb, *10 Things to Know About the Federal Money Laundering Law*, WIS. LAW., July 1994, at 12, 13.

[57] 31 U.S.C. § 5324 (2006).

[58] Hett, *supra* note 19, at ¶ 22.

[59] *E.g.*, 31 C.F.R. § 1020.320(b)(3) (2013).

of the report. Even among those transactions that do raise suspicion, most are not halted[60]—indeed, a suspicious transaction cannot be halted if it is reported days and weeks after it has been completed. If the reporting requirements do not raise sufficient red flags to garner law enforcement attention and allow prevention of terroristic crimes, the utility of SARs is reduced to investigation after the commission of a crime.[61]

II. Laundering with Bitcoin

Money launderers constantly seek new ways to disguise the origins and destinations of their funds. Those seeking to launder money would obviously like to do so without getting caught or breaking existing laws, so they constantly exploit loopholes in existing regulations and new ways of confusing regulators. Transactions that take place across international borders are appealing because of the potential to confuse and hide from the authorities of any one jurisdiction.[62] Emerging payment technologies also appeal to money launderers because such new technologies are "unlikely to be well understood by regulated business, financial intelligence units, or, indeed, governments."[63]

Criminals can utilize both these techniques—international transactions and emerging payment technologies—by moving money online. The internet provides a wealth of opportunities for individuals to move money. "[O]nline casinos, virtual worlds (such as Second Life), multiplayer online role-playing games (such as World of Warcraft), and the use of digital precious metals (such as e-gold [L]td[.])" provide many ways to move money while making it difficult for law enforcement to follow the movement of the funds.[64] One of the most exciting developments for money launderers in recent years has been the advent of Bitcoin.[65]

A. How Does Bitcoin Work?

Bitcoin is a digital currency: it exists only online,[66] it is not backed by any country or government, and its users operate anonymously. The Bitcoin software was published on January 3, 2009, by a computer pro-

---

[60] Hett, *supra* note 19, at ¶ 22.

[61] *See id.* ¶ 23.

[62] *See* Turner, *supra* note 4, at 1398 (citing Stessens, *supra* note 6, at 87) ("[L]aundered money travels across political borders because individuals seeking to launder dirty money logically will introduce the money into an economy that presents the lowest detection risk."); *see also id.* at 1403.

[63] Stokes, *supra* note 5, at 1.

[64] *Id.* (footnotes omitted).

[65] Literature on this subject typically capitalizes the word "Bitcoin" when referring to the software and the network it creates, but does not capitalize "bitcoin" when discussing individual units of currency themselves. The custom is followed herein.

[66] Physical bitcoins are minted by at least one private entity, *e.g.*, Physical Bitcoins by Casascius, http://www.casascius.com, but tangible coins are completely unnecessary to the function of the currency.

grammer named Satoshi Nakamoto[67] and operates via a peer-to-peer (P2P) network.[68] P2P networks are created when multiple individuals run the necessary software on their individual computers and connect to each other; P2P networks do not have a centralized website, server, or organizer.

Many other online entities operate from a centralized location; Google, for instance, is a publicly traded company with a management team and computer servers that store information on behalf of the users.[69] Even online communities such as Reddit, which runs on open-source software and gave up its physical servers for geographic-less "cloud computing" in 2010,[70] still have some physical manifestations: Reddit has a physical office,[71] a management team,[72] and a CEO.[73]

Bitcoin, on the other hand, has no management team and no physical manifestation whatsoever. Once written, the Bitcoin software became entirely self-sufficient, and it does not require oversight or tech support; even if it did, the software's author is an anonymous individual who has reportedly lost interest in the project.[74] Moreover, Bitcoin has no centralized location, either geographic or virtual.[75] Because of the P2P nature of the software, Bitcoin operates connectedly from each computer running the software, making it resistant to centralized attack[76]—or regulation.[77]

---

[67] "Satoshi Nakamoto" is widely believed to be a pseudonym for an individual or group of individuals. Reuben Grinberg, *Bitcoin: An Innovative Alternative Digital Currency*, 4 HASTINGS SCI. & TECH. L.J. 159, 162 (2012); Joshua Davis, *The Crypto-Currency*, NEW YORKER, Oct. 10, 2011, at 62, 62.

[68] Stokes, *supra* note 5, at 1.

[69] *See Investor Relations–Frequently Asked Questions*, GOOGLE, http://investor.google.com/corporate/faq.html (containing headquarters location information, links to SEC filings, ticker symbol, etc.); Mark Prigg, *Inside the Internet: Google Allows First Ever Look at the Eight Vast Data Centres That Power the Online World*, DAILY MAIL (U.K.) (Oct. 19, 2012), http://www.dailymail.co.uk/sciencetech/article-2219188/Inside-Google-pictures-gives-look-8-vast-data-centres.html (identifying major data centers in six U.S. and two European locations).

[70] *About Reddit*, REDDIT, http://www.reddit.com/about (scroll down to "history").

[71] *See* Jeremy Edberg, *Moving to the Cloud*, REDDIT BLOG (Nov. 10, 2009, 10:29 AM), http://blog.reddit.com/2009/11/moving-to-cloud.html (scroll down for photo of decommissioned server panels "back at the office").

[72] *See About the Reddit Team*, REDDIT, http://www.reddit.com/about/team/#sort/random ("we spend our days building reddit.").

[73] Yishan Wong became CEO of Reddit the week of March 8, 2012. Yishan Wong, *New Reddit CEO Reporting for Duty*, REDDIT BLOG (Mar. 8, 2012, 1:24 PM), http://blog.reddit.com/2012/03/new-reddit-ceo-reporting-for-duty.html.

[74] Davis, *supra* note 67, at 62 ("Then, in April, 2011, [Nakamoto] sent a note to a developer saying that he had 'moved on to other things.' He has not been heard from since.").

[75] *See* James C. Smith, Comment, *Online Communities as Territorial Units: Personal Jurisdiction over Cyberspace After* J. McIntyre Machinery, Ltd. v. Nicastro, 57 ST. LOUIS U. L.J. 839, 849 (2013).

[76] Grinberg, *supra* note 67, at 163.

This self-sufficient computer program is thus run on any computer on which it is installed. To simplify, the program is designed to solve a complicated math problem, the result of which is the creation of individual bitcoins, which are each merely long strings of numbers.[78] Computers running the Bitcoin software contribute their computing power to the solving of the math problem, and users are rewarded by being given the newly created bitcoins.[79] This process is known as "mining" the bitcoins,[80] but mining occurs rather slowly, and is getting slower. In late 2011 and early 2012, approximately 50 bitcoins were distributed every 10 minutes,[81] but the rate of bitcoin production slows by half every few years.[82] (By June of 2011, more than seven million bitcoins were in circulation,[83] and two years later, there were approximately eleven million.[84])

Ultimately, there will be approximately 21 million bitcoins in circulation,[85] a maximum expected to be reached in about 2025.[86] Even as more computer processing power is devoted to the Bitcoin software, the program adjusts the difficulty of the math problem over time so bitcoins are released at a predetermined rate.[87] Because mining occurs more slowly and requires more computing power over time, some commentators have criticized the Bitcoin system as being biased in favor of early adopters.[88]

Thus, anyone can mine bitcoins by downloading the Bitcoin software and letting the software run on his or her computer. Some people have even set up entire computers devoted solely to mining bitcoins, such as Kevin Groce of Kentucky, who built a room-size computer in 2011 that

---

[77] *See* Davis, *supra* note 67, at 66 ("There is no company in control, no office to raid, and nobody to arrest.").

[78] Stokes, *supra* note 5, at 2.

[79] *Id.*; Grinberg, *supra* note 67, at 163.

[80] Stokes, *supra* note 5, at 1.

[81] Grinberg, *supra* note 67, at 163; Davis, *supra* note 67, at 62.

[82] Grinberg, *supra* note 67, at 163 ("Currently, about 50 bitcoins are issued every ten minutes, although the rate will halve to 25 bitcoins in about two years and will halve every four years after that.").

[83] Davis, *supra* note 67, at 62.

[84] Nathaniel Popper & Peter Lattman, *Never Mind Facebook; Winklevoss Twins Rule in Digital Money*, N.Y. TIMES, Apr. 12, 2013, at A1.

[85] Grinberg, *supra* note 67, at 163. The Bitcoin software is designed so that this maximum is approached but never reached. Bitcoins are divisible to eight decimal points, however, so it is conceivable that deflation would allow for transactions in minute fractions of bitcoins. *On the Potential Adoption and Price Appreciation of Bitcoin in the Long Run*, CS702 BLOG (May 29, 2011, 8:57 PM), http://cs702.wordpress.com/2011/05/29/on-the-potential-adoption-and-price-appreciation-of-bitcoin-in-the-long-run/.

[86] Noam Cohen, *Speed Bumps on the Road to Virtual Cash*, N.Y. TIMES, July 4, 2011, at B3.

[87] Stokes, *supra* note 5, at 2.

[88] *E.g.*, Derek A. Dion, Comment, *I'll Gladly Trade You Two Bits on Tuesday for a Byte Today: Bitcoin, Regulating Fraud in the E-conomy of Hacker-Cash*, 2013 U. ILL. J.L. TECH. & POL'Y 165, 187.

mined about $1,000 worth of bitcoins every month.[89] More malicious actors have been able to hack into computers without the owners' knowledge and harness the hacked computers' processing power to mine for bitcoins: the FBI has received reports of malware and botnets that can hijack infected computers' processing power, and there have also been reports that at least two colleges' computer labs were compromised in pursuit of bitcoin mining.[90]

Because the pace of bitcoin release is slowing, mining becomes less time- and cost-effective as time goes on.[91] Mining bitcoins is not the only way to obtain them, however; they can also be purchased.

Bitcoins can be purchased from any current holder, just as any other commodity can be purchased: the buyer pays money to the seller, and the seller transfers the purchased bitcoins to the buyer's Bitcoin address.[92] Purchases may be more easily made, however, by going to a Bitcoin exchange.[93] The leading Bitcoin exchange has been Mt. Gox,[94] based in Japan.[95] In April 2013, Mt. Gox claimed to process 80% of all Bitcoin currency exchanges[96] for a fee of 0.65% per transaction.[97]

Although Mt. Gox is the most well-known site on which to exchange national currencies for bitcoins, it is far from the only site: as of this writing, at least 29 other digital currency exchangers offer real-time trading in bitcoins, 18 of which deal in U.S. dollars.[98] Still, other digital currency exchange sites offer fixed-rate Bitcoin trades; or specialize in bulk trades, exchanges for gift or debit cards, or exchanges for precious metals; or help users arrange in-person exchanges.[99]

Each bitcoin is merely a chunk of computer code, specially designed to be unique and un-replicate-able.[100] This means that bitcoins can be

---

[89] Davis, *supra* note 67, at 69.

[90] FED. BUREAU OF INVESTIGATION, BITCOIN VIRTUAL CURRENCY: UNIQUE FEATURES PRESENT DISTINCT CHALLENGES FOR DETERRING ILLICIT ACTIVITY (2012).

[91] *See* Davis, *supra* note 67, at 66.

[92] Dion, *supra* note 88, at 168. Websites such as https://localbitcoins.com connect users with one another to make person-to-person Bitcoin transactions.

[93] Dion, *supra* note 88 at 168.

[94] Grinberg, *supra* note 67, at 166.

[95] Marc Hochstein, *Lightning Fast, Dirt Cheap: Bitcoin Shows What Banking Could Be*, AM. BANKER (Aug. 24, 2012), http://www.americanbanker.com/bankthink/lightning-fast-dirt-cheap-bitcoin-shows-what-banking-could-be-1052108-1.html.

[96] Popper & Lattman, *supra* note 84.

[97] Jack Hough, *The Currency That's Up 200,000%*, MARKET WATCH (June 3, 2011), http://www.marketwatch.com/story/the-currency-thats-up-200000-1307029053200. Mt. Gox collapsed in February 2014, filing for bankruptcy in Japan on February 28, 2014 amidst the scandalous news that it had lost 850,000 bitcoins, valued at approximately $450 million. Chris O'Brien, *Mt. Gox Fulfills Worst Fears*, L.A. TIMES, March 1, 2014, at B1.

[98] *Trade*, BITCOIN WIKI, https://en.bitcoin.it/wiki/Trade (scroll down to "Currency [E]xchanges" and "Real-time Trading").

[99] *Id.*

[100] *See* Smith, *supra* note 75, at 848–49.

neither forged nor counterfeit. Whether the bitcoins are mined or purchased, users who possess bitcoins store them in digital wallets on their computers or other electronic storage devices.[101] Securing the digital wallet is the responsibility of the user,[102] meaning that bitcoins can be stolen if the digital wallet is hacked.

In order to spend bitcoins, the user must have the Bitcoin *address* of the intended recipient, and must use his or her own private Bitcoin *key* to authorize the transaction.[103] A Bitcoin address is akin to an e-mail address[104]—a destination in cyberspace to which transactions are directed—but because it is merely a string of numbers, it contains no identifying information about the account owner.[105] "[I]ndividuals can create unlimited accounts instantly and for free."[106] A Bitcoin key is a string of numbers that functions like a PIN at an ATM, in that it allows the user to authorize the transaction.[107]

When a transaction is made, the recipient's Bitcoin address and the transaction amount are recorded within the Bitcoin code itself,[108] and transactions are "published across the entire network."[109] Thus, a public record exists of all Bitcoin transactions,[110] albeit with no identifying information about the transferor or the transferee.[111]

Because Bitcoin accounts are free and there is no limit to the number that can be established, a Bitcoin address can be essentially disposable. Individuals can use a Bitcoin address once and then create a new one, hampering or defeating a third party's ability to extract identifying information from a pattern of transactions.[112]

---

[101] *See* Grinberg, *supra* note 67, at 163. The Winklevoss twins, the largest publicly-identified Bitcoin users, with approximately $11 million invested, store their bitcoins on flash drives locked in safety deposit boxes in three cities. Popper & Lattman, *supra* note 84.

[102] Grinberg, *supra* note 67, at 163; Davis, *supra* note 67, at 70.

[103] Stokes, *supra* note 5, at 2.

[104] *Id.* For example, 1PFgAJWLJZGSaVDg2rX3XDfTcyd6CpXXXX is one receiving address. Hochstein, *supra* note 95.

[105] Dion, *supra* note 88, at 168.

[106] Grinberg, *supra* note 67, at 164–65 (citing *Introduction*, BITCOIN WIKI, https://en.bitcoin.it/wiki/Introduction#Anonymity (subsection "Anonymity")).

[107] *See* Stokes, *supra* note 5, at 2.

[108] Smith, *supra* note 75, at 849.

[109] Davis, *supra* note 67, at 65.

[110] Other digital currencies have even greater anonymity. Liberty Reserve, for instance, allows for anonymous transactions without the "public ledger" that the Bitcoin software generates. Nicole Perlroth, *Anonymous Payment Schemes Thriving on Web*, N.Y. TIMES, May 30, 2013, at B1. The operators of Liberty Reserve were indicted by the U.S. Attorney for the Southern District of New York in May 2013, and Liberty Reserve's operations were shut down. *Id.*; *see also infra* Part III.A.2.

[111] Dion, *supra* note 88, at 168; Stokes, *supra* note 5, at 3; Davis, *supra* note 67, at 65 ("Buyers and sellers remain anonymous, but everyone can see that a coin has moved from A to B.").

[112] *See* Stokes, *supra* note 5, at 3.

The software also prevents an individual bitcoin from being spent in duplicate—a single bitcoin can be transferred only to one recipient at a time, just as a dollar bill can be handed only to one person.[113] The recipient is certainly able to pass that bitcoin on again, but a holder of a bitcoin cannot pay two recipients with the same bitcoin unless he receives that coin again between the two payments. This feature of the software keeps the supply of bitcoins strictly controlled. On the other hand, it also prevents the fractional reserve banking[114] that allows government-backed currencies to be lent by financial institutions to their borrowers.

So, what's a bitcoin worth? In short, it's worth whatever someone else will trade for it. As discussed in more detail below, bitcoins can be exchanged for goods and services, or can be exchanged for U.S. dollars or other national currencies.

B. Why Use Bitcoin?

At this point, the reader may be asking why anyone would wish to possess bitcoins. Why exchange your salary or savings, (presumably) obtained and held in the form of a national, government-backed currency, with an intangible digital currency? After all, without the backing of a government or other guarantor, bitcoins have no intrinsic value—bitcoins are valuable only because users believe them to be valuable.[115]

Historically, currencies have either been *specie* (backed by a valuable commodity, such as gold or other precious metal) or *fiat* (backed by the assurances of a government).[116] The U.S. dollar, for instance, had been redeemable for a certain quantity of gold bullion until the United States went off the gold standard.[117] By doing so, the dollar went from being a specie currency to being a fiat currency.

Bitcoin, unusually, is neither specie nor fiat. Nevertheless, Bitcoin is capable of serving the two main functions of a currency: that it be a medium of exchange and also a measure of value.[118]

1. Spending Power

It is perfectly possible to buy goods and services with bitcoins, both in the United States and abroad. Bitcoins can be used to buy electronics,

---

[113] Davis, *supra* note 67, at 65.

[114] Grinberg, *supra* note 67, at 165.

[115] Stokes, *supra* note 5, at 2. Of course, U.S. dollars are also only valuable because of public trust; the U.S. dollar is not tied to the value of gold or any other commodity. Grinberg, *supra* note 67, at 162 ("Like the U.S. Dollar, Bitcoin is not redeemable for another type of money or for a certain amount of a commodity, such as an ounce of gold.").

[116] *See* Claire Priest, *Currency Policies and Legal Development in Colonial New England*, 110 YALE L.J. 1303, 1318 n.34 (2001).

[117] *See* John J. Chung, *Money as Simulacrum: The Legal Nature and Reality of Money*, 5 HASTINGS BUS. L.J. 109, 137–45 (2009) (explaining the history of the United States' departure from the gold standard).

[118] CS702 BLOG, *supra* note 85; *see also* Chung, *supra* note 117, at 114–21.

jewelry, paintball equipment, and clothing, and to pay for health care, technical support, hotel rooms, and restaurant meals.[119] Merchants are not required to accept bitcoins for payment, but among those who choose to, bitcoins serve as a viable medium of exchange. Institutions such as Wikileaks accept contributions in bitcoins.[120]

Infamously, bitcoins can also be used to purchase illegal items. A website called Silk Road offers hundreds of narcotics and hallucinogenic drugs for sale, deliverable via the U.S. Postal Service, purchasable in bitcoins.[121] Bitcoins can also be used to buy weapons[122] and pornography.[123] The lack of identifying information connected to a Bitcoin address insulates the criminal from the crime.

2. Speculation

Individuals also invest in Bitcoin to take advantage of price fluctuations: buying up bitcoins when the exchange rate makes them inexpensive to purchase, and selling them when the exchange rate rises. Exchange rates for Bitcoin have been known to fluctuate wildly, and the old standby of "buy low, sell high" applies to Bitcoin as well as it does to anything else.

For example, in May 2010, one bitcoin was worth about half a cent.[124] The dollar–bitcoin exchange rate rose to $30 per bitcoin in June 2011,[125] then dropped to $2 per bitcoin in October 2011.[126] At the time, commentators were describing this kind of volatility in dramatic language,[127] but prices have risen so much that this early hand-wringing seems ridiculous. In April 2013, the price of a single bitcoin rose to an intraday high of

---

[119] *Trade*, *supra* note 98 (list of retailers currently accepting payment in bitcoin). Interestingly, a warning on this page provides that "[p]roducts or services illegal in [the] US or Japan are not fit to be listed here—such links will be removed immediately." *Id.*

[120] Dion, *supra* note 88, at 169.

[121] Adrian Chen, *The Underground Website Where You Can Buy Any Drug Imaginable*, GAWKER (June 1, 2011, 4:20 PM), http://gawker.com/5805928/the-underground-website-where-you-can-buy-any-drug-imaginable. The original Silk Road website was shut down by federal authorities in October 2013, but a new Silk Road 2.0 site was up and running a month later. Andy Greenberg, *'Silk Road 2.0' Launches, Promising a Resurrected Black Market for the Dark Web*, FORBES (Nov. 6, 2013), http://www.forbes.com/sites/andygreenberg/2013/11/06/silk-road-2-0-launches-promising-a-resurrected-black-market-for-the-dark-web/.

[122] Adrian Chen, *Now You Can Buy Guns on the Online Underground Marketplace*, GAWKER (Jan. 27, 2012, 1:45 PM), http://gawker.com/5879924/now-you-can-buy-guns-on-the-online-underground-marketplace.

[123] *Buy Porn from the Biggest Sites Using Bitcoin*, REDDIT (May 15, 2013), http://www.reddit.com/r/Bitcoin/comments/1ee728/buy_porn_from_the_biggest_sites_using_bitcoins/.

[124] Grinberg, *supra* note 67, at 164.

[125] *Id.*

[126] *Id.* at 160, 164.

[127] *E.g.*, *id.* at 164 (describing the October 2011 price as "crashing"); CS702 BLOG, *supra* note 85 (questioning whether a $9 high was a price "bubble").

$266,[128] "plummet[ting]" 60% to about $120 before trading was suspended on one currency exchange due to price volatility.[129] The roller coaster continues: a bitcoin valued at over $1,100 on December 4, 2013, dropped to $522 two weeks later.[130]

Individual users each have their own stories about the speculative risks and rewards of Bitcoin. The Winklevoss twins (vilified in the movie *The Social Network* for suing Facebook founder Mark Zuckerberg) have publicly announced an $11 million investment in bitcoins, seeking to gain a return on their investment as the value and usage of Bitcoin expands in coming years.[131] Gavin Andresen, chief scientist at the Bitcoin Foundation, is paid in bitcoins—because of fluctuations in value, his salary in the first few months of 2013 increased more than tenfold.[132] Users such as Jefferson Kim, on the other hand, who operates a Howard Johnson hotel near Disneyworld and accepts payment in bitcoin, exchange earned bitcoins immediately for dollars to avoid exchange rate fluctuations.[133]

Income earned from Bitcoin transactions is presumably taxable,[134] though the Internal Revenue Service is struggling to identify and explain Bitcoin-derived tax liability to taxpayers.[135]

3. Trust in Algorithms

In the white paper introducing the currency, Nakamoto wrote, "We have proposed a system for electronic transactions without relying on trust."[136] Some individuals find comfort in the Bitcoin currency precisely because it is mathematically driven and not manipulated by central bankers. Such Bitcoin users mistrust central banking institutions and their authority to print more money,[137] and instead prefer a currency op-

---

[128] Matthew Boesler, *Wall Street Analyst: Hackers Are Attacking Bitcoin So They Can Scoop It Up for Lower Prices*, BUS. INSIDER (Apr. 11, 2013), http://www.businessinsider.com/colas-hackers-manipulating-bitcoin-down-2013-4.

[129] Popper & Lattman, *supra* note 84.

[130] *See Bitcoin Price Index Chart*, COINDESK, http://www.coindesk.com/price/.

[131] Popper & Lattman, *supra* note 84.

[132] Noam Cohen, *Bubble or No, this Virtual Currency Is a Lot of Coin in Any Realm*, N.Y. TIMES, Apr. 8, 2013, at B3.

[133] Davis, *supra* note 67, at 66, 68.

[134] Mandi Woodruff, *Yes, You Have to Pay Taxes on Your Bitcoin Profits*, BUS. INSIDER (Apr. 2, 2013), http://www.businessinsider.com/do-you-have-to-pay-taxes-on-bitcoins-2013-4.

[135] *See* U.S. GOV'T ACCOUNTABILITY OFFICE, REPORT TO THE COMM. ON FIN., U.S. SENATE, VIRTUAL ECONOMIES AND CURRENCIES: ADDITIONAL IRS GUIDANCE COULD REDUCE TAX COMPLIANCE RISKS 10–13 (May 2013).

[136] SATOSHI NAKAMOTO, BITCOIN, BITCOIN: A PEER-TO-PEER ELECTRONIC CASH SYSTEM, at 8, *available at* http://bitcoin.org/bitcoin.pdf.

[137] Grinberg, *supra* note 67, at 172.

erated with computerized, pre-determined precision to a currency backed by a government but regulated by fallible humans.[138]

Relatedly, some individuals feel a libertarian pleasure in utilizing Bitcoin—they feel that storing wealth in Bitcoin rather than, say, U.S. dollars is somehow subverting the U.S. government.[139]

In some sense, Bitcoin users' enthusiasm is also related to some people's faith in gold. Historically, gold has been more than just a scarce commodity, it has been *money*.[140] Bitcoin appeals to these goldbugs' "libertarian politics" because, as in societies that used gold as currency, more money cannot simply be created by governmental decision.[141]

4. Dearth of National Currency

Bitcoins have proven useful in countries and times when government-backed currency is difficult to come by, such as in Iran,[142] Cyprus,[143] and parts of Africa.[144] If there is simply not enough fiat currency available for citizens to make transactions for goods and services, access to another form of trustworthy currency can supplement as a new means of exchange. Commentators have speculated that access to Bitcoin can shield people from the effects of hyperinflation—citizens can convert their savings and salary from their national currency into bitcoins, and when the value of the national currency plummets, the individual's net worth is thus stored in a different currency that shielded from the hyperinflation of the national currency.[145] (As discussed above, however, Bitcoin is subject to its own wild swings of exchange rate.) Because Bitcoin exists online and can be transacted from anywhere in the world with an internet connection, citizens of the hyperinflationary state need not be able to physically locate fiat currencies of another country; instead, they can make the conversion online via digital currency exchanges like Mt. Gox.[146]

---

[138] *See* Popper & Lattman, *supra* note 84 (quoting Tyler Winklevoss as saying, "We have elected to put our money and faith in a mathematical framework that is free of politics and human error").

[139] *See* Dion, *supra* note 88, at 169 ("The currency may also have been favored by those who viewed American monetary policy as unconstitutional and therefore illegitimate. Their investment in Bitcoin is a political demonstration of the feasibility of a private legal currency.") (footnote omitted).

[140] Floyd Norris, *One Man's Currency Is Another Man's Bet*, N.Y. TIMES, Apr. 19, 2013, at B1.

[141] Paul Krugman, Op-Ed., *The Antisocial Network*, N.Y. TIMES, Apr. 15, 2013, at A19.

[142] Dion, *supra* note 88, at 182 (citing Max Raskin, *Dollar-Less Iranians Discover Virtual Currency*, BLOOMBERG BUSINESSWEEK (Nov. 29, 2012), http://www.businessweek.com/articles/2012-11-29/dollar-less-iranians-discover-virtual-currency).

[143] *Marketplace Morning Report: Bitcoin Continues to Spike in the Wake of Cyprus*, AM. PUB. MEDIA (Apr. 3, 2013), http://www.marketplace.org/topics/economy/bitcoin-continues-spike-wake-cyprus.

[144] James Smith, *Bitcoin Fuels Africa's Banking Revolution*, CONVERSATION (July 12, 2013), http://theconversation.com/bitcoin-fuels-africas-banking-revolution-16044.

[145] *See, e.g.*, Hough, *supra* note 97.

[146] *Id.*

5. Crime

Of course, because Bitcoin transactions are made anonymously, the currency has a natural appeal for criminals. Bitcoins can be used as the medium of exchange for drug trafficking and making financial contributions to causes and projects of interest.[147] In addition to those underlying crimes, Bitcoin can also be used for the "shell" crime of money laundering.[148]

> Dirty money is typically laundered in three steps: (1) placing money derived from criminal activities into a legitimate enterprise; (2) layering the money through multiple transactions to "obscure the original source"; and (3) integrating the clean funds into the "legitimate financial world 'in the form of bank notes, loans, letters of credit,' or other recognizable financial instruments."[149]

Funds can be converted to bitcoins quickly and cheaply. Any examples offered here are likely to be out of date by the time they are read, given that internet sites and traffic patterns can change from moment to moment; nevertheless, a few methods of converting national currency to bitcoins are described here for illustrative purposes.

Mt. Gox, one of the most famous currency exchange dealing in Bitcoin, did not accept credit or debit transactions, but other exchanges do. Liberty Reserve, for instance, accepts (or at least, accepted for a time)[150] transfers of U.S. dollars and trades those funds on a Bitcoin exchange.[151] Even if such digital currency exchangers were shut down, though, new exchangers would pop up, and could be based in jurisdictions with minimal banking regulation and U.S. jurisdictional contacts. (As discussed in more detail *infra*, several of the individuals involved with Liberty Reserve were part of a previous virtual currency, e-gold, which was functionally shut down by U.S. officials.)

Transacting funds from a bank to a digital currency exchange potentially puts such a transaction on the government radar, as the bank would be subject to KYC and reporting requirements.[152] If a would-be Bitcoin user is unable or unwilling to purchase bitcoins directly with dollars, it is possible to take intermediary steps. For instance, credit cards can be used easily (and legally) to purchase Linden Dollars, the currency used in the online video game Second Life.[153] Linden Dollars can be spent in the

---

[147] *See supra* text accompanying notes 120–22.

[148] *See supra* Part I.A.

[149] Turner, *supra* note 4, at 1392 (quoting *Money Laundering*, 39 AM. CRIM. L. REV. 839, 840 (2002)); *see also* Stokes, *supra* note 5, at 1.

[150] *See infra* Part III.A.2.

[151] Dion, *supra* note 88, at 187.

[152] *See supra* Part I.B.

[153] *See Shop: Learn*, SECOND LIFE, http://secondlife.com/shop/learn/.

Second Life games on virtual clothing, houses, trees, or pets,[154] or they can be sold on digital currency exchanges for bitcoins.[155]

Exchangers' creativity continues: although refusing to take credit or debit card transactions, Mt. Gox has accepted personal checks by mail, drawn on U.S. banks and made out to "Morpheus."[156]

If this process sounds increasingly bizarre, it is at least a demonstration of the solutions individuals will develop to avoid detection of their transactions.

In any of these ways, the first, "placement" portion of the money laundering scheme is accomplished. The second step, "layering," can be accomplished by transferring bitcoins between accounts held by one or more users. Because Bitcoin accounts contain no identifying information about the user, and because users can have an infinite number of accounts,[157] such layering transactions could obliterate any record of ownership.[158]

The third step, "integration," or returning the funds to the legitimate financial world, is simply the reverse of "placement." Thus, the criminal actor has obtained funds, obscured their source, yet retained the ability to use them.

C. Strengths and Weaknesses

Physical cash has long been the ideal medium of money laundering: it's "anonymous, untraceable, requires no intermediary, is widely accepted, and provides for immediate settlement."[159] On the other hand, cash presents several significant difficulties, namely the physical, logistical, and geographic problems of possessing and transporting large amounts of cash.[160] Digital currencies eliminate the physical and logistical problems associated with cash; the more of the positive cash-like assets a digital currency possesses—anonymity, immediacy of settlement, wide acceptance,

---

[154] *Id.*

[155] Dion, *supra* note 88, at 188.

[156] *Id.* at 187–88. The name is presumably a reference to Laurence Fishburne's character in *The Matrix* movie franchise.

[157] *Supra* note 106.

[158] Bitcoin transactions also record the Internet Protocol (IP) address of any computer linked to the transaction, though a user can artificially anonymize and randomize an IP address. Some researchers have demonstrated that transaction patterns can give clues to a transactor's identity, and other parties (such as currency exchanges) may have access to additional information that could identify a party, such as bank account information or shipping addresses. FED. BUREAU OF INVESTIGATION, *supra* note 90 (asking "How Anonymous is Bitcoin?").

[159] Hett, *supra* note 19, ¶ 11 (quoting FIN. ACTION TASK FORCE, REPORT ON NEW PAYMENT METHODS 10 n.22 (2006), *available at* http://www.fatf-gafi.org/dataoecd/30/47/37627240.pdf) (internal quotation mark omitted).

[160] *Id.* Cash may be stolen, but so, too, may digital currency accounts be hacked.

lack of intermediary, untraceability—the more appealing that digital currency is to launderers.[161]

Bitcoin, of course, has many of these attributes.[162] Most importantly, Bitcoin transactions can be effected anonymously.[163] Bitcoin addresses and wallets have no identifying information about the owner, and encryption and IP randomizers can be used to further obscure any facts that would lead to the discovery of the owner's identity. Peer-to-peer Bitcoin transactions occur instantaneously[164] and do not run through regulated financial institutions. Moreover, charge-backs (akin to disputing a credit card charge) are impossible.[165] Exchanges made through services such as Mt. Gox have low transaction costs,[166] so bitcoins can be exchanged for other currencies cheaply and easily.

Of course, Bitcoin is not perfect. Bitcoins are susceptible to theft, via good old-fashioned hacking. Hackers can obtain a Bitcoin user's private key and use it to transfer some or all of the bitcoins in the user's wallet to another location.[167] The private key is a validation process to ensure that Bitcoin transactions are authorized, but there is no way to ensure that the e-wallet's owner is the one doing the authorizing.[168] The potential for hacking is not helped by the facts that (1) encryption and protection of an e-wallet is left to the user and (2) transactions are irreversible.[169] Just as with physical cash, once bitcoins have been stolen, they are untraceable and unreturnable.

Along with theft of bitcoins, hacker attacks on digital currency exchanges drive down the price of bitcoins across the system.[170] If bitcoins can be stolen, or if transactions cannot be completed, what is a bitcoin worth? A massive hacker attack on Mt. Gox in June 2011 resulted in the theft of 25,000 bitcoins, valued at the time at approximately $8.75 million, and drove the exchange value of a bitcoin from $17.50 to a single penny.[171] (Worth noting, however, is the fact that although Bitcoin wallets

---

[161] *Id.* ¶¶ 12–13.

[162] Turner, *supra* note 4, at 1407–08 (describing "attractive" attributes for cyberlaundering: "[s]peed, anonymity, and the ability to transfer unlimited value").

[163] Stokes, *supra* note 5, at 3.

[164] Dion, *supra* note 88, at 182.

[165] Peter C. Tucker, Note, *The Digital Currency Doppelganger: Regulatory Challenge or Harbinger of the New Economy?*, 17 CARDOZO J. INT'L & COMP. L. 589, 607 (2009).

[166] Dion, *supra* note 88, at 182.

[167] *Id.* at 184.

[168] *Id.*

[169] *See* Grinberg, *supra* note 67, at 165.

[170] *See* Boesler, *supra* note 128.

[171] Jason Mick, *Inside the Mega-Hack of Bitcoin: The Full Story*, DAILY TECH (June 19, 2011), http://www.dailytech.com/Inside+the+MegaHack+of+Bitcoin+the+Full+Story/article21942.htm. Interestingly, subsequent attacks on major Bitcoin associates have actually increased the price of bitcoins: After Silk Road was shut down on October 1, 2013, and after Mt. Gox declared bankruptcy on February 28, 2014, the price of bitcoins actually increased. *See Bitcoin Price Index Chart*, *supra* note 130. This may reflect speculators' belief that negative news coverage would result in bargain prices for bitcoins.

can be hacked, bitcoins themselves have thus far been proved impervious to counterfeiting.[172])

The volatility of the exchange rate is its own susceptibility of the Bitcoin system. Just as speculators and arbitrageurs can take advantage of the fluctuating exchange rate to buy low and sell high,[173] so does the risk exist that the exchange rate will drop, devaluing any bitcoins held by users. Hacking scandals contribute to this drop in exchange rate, as does a dip in demand for any other reason. Until the exchange rate of bitcoins to other currencies stabilizes, bitcoins present significant risk as a store of value.

Bitcoin also has liquidity problems that other currencies do not. U.S. dollars are universally accepted within the United States[174] (and many places overseas, as well), but Bitcoin has a significantly smaller number of users.[175] Bitcoin advocates crow about thousands of vendors accepting bitcoins as payment,[176] but bitcoins still cannot be used generally to pay for things like rent.[177] Bitcoin's association with infamous vendors, such as Silk Road (selling illegal drugs and weapons) and WikiLeaks (an organization flirting with the distinction between heroic whistleblowers and criminal anarchists), may contribute to legitimate, lawful retailers' reluctance in adopting Bitcoin as a viable means of payment.

III. Prosecuting Digital Currencies

As the public becomes aware of criminal activity being conducted via Bitcoin, naturally, thoughts turn to how legislators can prevent, curtail, and criminalize such behavior. Some commentators treat regulation of Bitcoin as a foregone conclusion.[178] Of course, regulation is more easily said than done.

It is important to understand at this juncture that Bitcoin itself almost certainly cannot be regulated.[179] Bitcoin is the currency—when U.S. dollars are involved in money laundering, it is not the dollars themselves

---

[172] Cohen, *supra* note 132.

[173] *See supra* Part II.B.2.

[174] *See* Chung, *supra* note 117, at 113–14 (discussing the related concepts of fiat money and legal tender).

[175] *See* Kashmir Hill, *21 Things I Learned About Bitcoin from Living on It for a Week*, Forbes (May 9, 2013), http://www.forbes.com/sites/kashmirhill/2013/05/09/25-things-i-learned-about-bitcoin-from-living-on-it-for-a-week/ ("Living on Bitcoin is a great way to lose weight. As it is not widely accepted, you are prevented from spontaneous snacking.").

[176] *See Trade*, *supra* note 98.

[177] *See* Hill, *supra* note 175.

[178] *E.g.*, *Marketplace Morning Report*, *supra* note 143 ("I imagine that as [Bitcoin] gains popularity, it will be regulated very closely.").

[179] *See* Nikolei M. Kaplanov, Comment, *Nerdy Money: Bitcoin, the Private Digital Currency, and the Case Against Its Regulation*, 25 Loy. Consumer L. Rev. 111, 167–68 (2012) (discussing the impossibility of "outlawing" Bitcoin).

that are regulated; rather, it is the *transactions* that are regulated, along with those entities or individuals making or facilitating those transactions. Regulating Bitcoin *transactions* would require regulation of the digital currency exchangers, such as Mt. Gox, that effectuate the transfer of bitcoins from one party to another.[180]

U.S. law enforcement is increasingly turning to regulation and prosecution of financial institutions to enforce anti-money laundering laws, and existing anti-money laundering laws are being stretched to include digital currency exchanges in the group of institutions subject to reporting requirements.[181] In March 2013, the Financial Crimes Enforcement Network (FinCEN) announced that it would begin applying anti-money laundering laws to virtual currencies.[182]

This attention is misplaced. While debate is certainly possible regarding whether financial institutions are complicit in money laundering schemes and deserve to be prosecuted,[183] prosecuting digital currency exchanges is simply not worth law enforcement time. Sites pop up and disappear so quickly that by the time law enforcement can shut down one exchange, more will have appeared elsewhere, happy to serve needy customers.[184] This never-ending game of whack-a-mole cannot be won, and it is a waste of investigative and prosecutorial effort to try.

Instead, digital currency exchanges should be embraced as partners in law enforcement. With the assistance and support of digital currency exchanges, which may have access to more information about transacting parties than just their Bitcoin addresses, law enforcement can return its efforts to the more significant, nested crimes: money laundering and the underlying criminal activities such as terrorism and drug trafficking.

A. Previous "Successes"

Prosecuting digital currency providers and exchanges is in its infancy. Few charges have been filed, and no cases have yet proceeded through trial to verdict.[185] This section discusses the few prosecutorial

---

[180] The Bitcoin software does not have the ability to exchange bitcoins for other currencies; it does, however, permit bitcoins to be exchanged directly between users, just as cash can be handed from one person to another. *See infra* text accompanying notes 214–17.

[181] *See generally* Hett, *supra* note 19, at Part III (analyzing the application of anti-money laundering regulations to digital currency providers and currency exchangers).

[182] Perlroth, *supra* note 110.

[183] *See* GALLANT, *supra* note 4, at 4.

[184] *See id.* at 3 ("Incarceration or fines fail to deter when the potential rewards of criminal pursuits are substantial.").

[185] A famous conviction occurred in 2011, when Bernard von NotHaus was convicted for crimes related to the printing and distribution of Liberty Dollars. Liberty Dollars were not a digital currency, however—they were tangible dollar bills and coins designed to be an alternative to U.S. currency. Liberty Dollars were designed to have at least some resemblance to U.S. dollars and were slipped into circulation sometimes without the knowledge of the recipients. NotHaus was

moves that have been made to date. Each digital currency has individual characteristics, however, that impact the legality and prosecutability of the currency and its servicers.

1. E-gold

The most successful law enforcement effort to date has been the prosecution related to e-gold,[186] a digital currency purportedly backed by physical stockpiles of gold.[187] The e-gold currency was created by a company called e-gold, Ltd., incorporated in the Caribbean nation of St. Kitts and Nevis, but operated in Melbourne, Florida.[188] Accounts could be created on the e-gold website with only a valid e-mail address; other identifying information was requested but unverified.[189] (Indeed, accounts existed with the names "Mickey Mouse," "Anonymous Man," "bud weiser," and "No Name."[190]) Units of e-gold could be purchased with a credit card and could be exchanged directly with other users on the e-gold site or via digital currency exchanges[191] such as OmniPay—an entity owned by e-gold, Ltd.'s parent company Gold & Silver Reserve, Inc.[192]

The currency became a haven for criminals and money laundering.[193] The FBI and Secret Service raided the e-gold offices in December of 2005, and an indictment was filed on April 24, 2007.[194] The indictment charged five defendants—e-gold, Ltd.; Gold & Silver Reserve, Inc.; founder Douglas L. Jackson; co-founder Barry K. Downey; and employee Reid A. Jackson—with conspiracy to launder monetary instruments, conspiracy to operate an unlicensed money transmitting business, and operation of an unlicensed money transmitting business under Federal and D.C. laws.[195]

After losing motions to stay the prosecution[196] and dismiss the charges,[197] the defendants each pled guilty to one or more of the charges in July, 2008.[198]

---

convicted of counterfeiting and related crimes, not money laundering. Grinberg, *supra* note 67, at 191–94.

[186] Capitalization of "e-gold" is inconsistent throughout the literature, with some authors writing "E-Gold" or "E-gold." The currency creators do not capitalize any of the letters in the currency's name, *see* E-GOLD, http://www.e-gold.com, and that custom will be followed here, except where the name begins a sentence.

[187] Tucker, *supra* note 165, at 591. For a detailed description of how e-gold transactions work, see Hett, *supra* note 19, at ¶¶ 38–41.

[188] Indictment at 6, United States v. e-gold, Ltd., No. 07-109 (D.D.C. Apr. 24, 2007) [hereinafter e-gold Indictment].

[189] *Id.* at 7.

[190] *Id.*

[191] Brian Grow, *Gold Rush*, BUSINESSWEEK, Jan. 9, 2006, at 69, 69.

[192] e-gold Indictment, *supra* note 188, at 6.

[193] *Id.* at 8; Grow, *supra* note 191, at 69.

[194] Tucker, *supra* note 165, at 590.

[195] e-gold Indictment, *supra* note 188, *passim*.

[196] United States v. e-gold, Ltd., No. 07-109, 2007 WL 2103602, at *1 (D.D.C. July 20, 2007).

E-gold differs from the Bitcoin ecosystem in several important respects. First, e-gold was created by three identifiable people who lived and worked in the United States. There were offices to raid, people to arrest. None of this is true with Bitcoin, since the software was developed by an anonymous individual, and it is operated across a global P2P network of individual computers, instead of from central servers in a headquarters.

Second, the digital currency provider, e-gold, Ltd., shared common ownership with the primary digital currency exchanger, OmniPay—both entities were owned by Gold & Silver Reserve, Inc. This has two implications:

(1) The e-gold creators were making money from the transactions. OmniPay, like other digital currency exchanges, charged transaction fees to users,[199] and because OmniPay was related to e-gold, Ltd., the same entities and individuals were benefitting from these transaction fees. The Bitcoin system, on the other hand, significantly separates the digital currency provider (the Bitcoin software) from the exchangers (entities such as Mt. Gox). Although some exchanges do happen via the Bitcoin software itself, when users transact directly with one another,[200] no transaction fees are assessed during this type of transfer. The significant number of Bitcoin transactions that occur via digital currency exchanges do incur transaction fees, but those fees are accumulated by the exchangers themselves, not the Bitcoin software or its creator.

(2) The interrelatedness of e-gold, Ltd.; Gold & Silver Reserve, Inc.; OmniPay; and the individual defendants meant that the entire e-gold ecosystem could be effectively shut down in a very few number of prosecutorial moves. After the indictment was issued to five defendants, the Department of Justice seized 58 e-gold accounts and obtained a restraining order that prohibited the defendants from dissipating assets.[201] By contrast, the Bitcoin system is far more disparate. The number of users is impossible to determine, as each Bitcoin address is anonymous and individuals may have multiple ad-

---

[197] United States v. e-gold, Ltd., 550 F. Supp. 2d 82, 84–85 (D.D.C. 2008).

[198] *Digital Currency Business E-Gold Pleads Guilty to Money Laundering and Illegal Money Transmitting Charges*, DEP'T OF JUSTICE (July 21, 2008), http://www.justice.gov/opa/pr/2008/July/08-crm-635.html.

[199] e-gold Indictment, *supra* note 188, at 20; Tucker, *supra* note 165, at 599–600.

[200] *See infra* text accompanying notes 214–17.

[201] Defendants' Status Report and Notice of Compliance with this Court's Seizure Warrants and Post-Indictment Restraining Order at 13–14, United States v. e-gold, Ltd., No. 07-109 (D.D.C. May 17, 2007).

> dresses;[202] the numerous digital currency exchangers dealing in Bitcoin are unaffiliated with each other or the currency provider, and new digital currency exchangers can be created at any time by any individual willing to take the business risks.[203]

2. Liberty Reserve

Another significant digital currency-related prosecution is currently unfolding. In an indictment unsealed on May 28, 2013, the U.S. Attorney for the Southern District of New York filed charges against Liberty Reserve, a digital currency provider and exchange based in Costa Rica.[204] The indictment charges the company, Liberty Reserve S.A., and seven individuals associated with it, with conspiracy to commit money laundering, conspiracy to operate an unlicensed money transmitting business, and operation of an unlicensed money transmitting business.[205] Government authorities seized six domain names, including libertyreserve.com, and the indictment identifies 45 specific bank accounts subject to forfeiture.[206]

The indictment hammers home the defendants' knowledge and intent that Liberty Reserve be used to facilitate crime: alleging the defendants "intentionally created, structured, and operated Liberty Reserve as a criminal business venture, one designed to help criminals conduct illegal transactions and launder the proceeds of their crimes."[207] Also prominently featured are allegations that Liberty Reserve lied to Costa Rican financial regulators[208] and that one of the defendants admitted in an obtained online chat that Liberty Reserve's activities were "illegal" and that "everyone in USA" knows "LR is [a] money laundering operation that hackers use."[209]

Although Bitcoin is certainly being used to conduct illegal activities, the creator demonstrated no intent that it be used in such a way.[210] The white paper introducing the currency focuses on the importance of transparency and "cryptographic proof instead of trust."[211]

---

[202] *See, e.g.*, *How Many Bitcoin Users Are There?*, BITCOIN TALK (June 6, 2011, 10:30 AM), https://bitcointalk.org/index.php?topic=12574.0 (forum discussion on how many estimated Bitcoin users exist and methodologies for calculating those estimates).

[203] GALLANT, *supra* note 4, at 3 ("[C]riminal sanctions become a cost of doing business, an expense that is easily absorbed by the revenues.").

[204] Marc Santora et al., *Firm Accused in Laundering of $6 Billion*, N.Y. TIMES, May 29, 2013, at A1.

[205] Verified Complaint at 8, United States v. Liberty Reserve S.A., No. 13-3565 (S.D.N.Y May 28, 2013).

[206] Indictment ¶ 43, United States v. Liberty Reserve S.A., No. 13-368 (S.D.N.Y. May 20, 2013) [hereinafter Liberty Reserve Indictment].

[207] *Id.* ¶ 8.

[208] *Id.* ¶¶ 23–25.

[209] *Id.* ¶ 22 (alteration in original).

[210] *See* Nakamoto, *supra* note 136, at 1, 8.

[211] *Id.* at 1.

Interestingly, two of the individual Liberty Reserve defendants had been previously convicted of operating Gold Age, Inc., a currency exchange for e-gold.[212] The indictment notes that after his conviction, one of these individuals "set about building a digital currency that would succeed in eluding law enforcement where E-Gold had failed, by, among other ways, locating the business outside the United States."[213] Although the two have been caught and indicted again, it is noteworthy that one conviction was not enough deterrent for these individuals, who were so determined to develop digital currency systems that they emigrated to Costa Rica and set up a new digital currency exchange,[214] which they operated successfully—and lucratively—until 2013.

Although the ending of Liberty Reserve's prosecution has not yet been written, it is illustrative to see that the whack-a-mole game continues; after the government effectively shut down e-gold, the individuals returned underground, only to pop up again with a new digital currency exchange.

3. Closing in on Bitcoin?

a. Mt. Gox

Mt. Gox is a Japan-based digital currency exchange service that has long been the most popular place to exchange bitcoins for other currencies.[215] In May 2013, a seizure warrant was issued to the Department of Homeland Security, authorizing the seizure of one of Mt. Gox's payment processing accounts, this one with Dwolla, a digital currency exchange based in Iowa.[216] The Department of Homeland Security alleges that Mt. Gox failed to register as a money transmitting business.[217]

As of this writing, no charges have been filed, and no further developments have been made in the case. The pending warrant may be moot, however, as the Mt. Gox business collapsed and the company filed for bankruptcy in February 2014, admitting that it lost 750,000 of its customers' bitcoins and 100,000 of its own, totaling $450 million in value.[218]

---

[212] Liberty Reserve Indictment, *supra* note 206, ¶ 11.

[213] *Id.* ¶ 12.

[214] *Id.*

[215] *See* Grinberg, *supra* note 67, at 166; Davis, *supra* note 67, at 66, 68.

[216] Adrian Chen, *Feds Seize Assets of World's Largest Bitcoin Exchange*, GAWKER (May 15, 2013, 1:31 PM), http://gawker.com/feds-seize-assets-of-worlds-largest-bitcoin-exchange-506790294.

[217] *Id.*

[218] O'Brien, *supra* note 97. The currency exchange had been criticized for months over its slow processing of Bitcoin withdrawals, and withdrawals were suspended completely on February 7; the site disappeared altogether on February 24 before Mt. Gox filed for bankruptcy in Japan on February 28. *See also* Jose Pagliery, *Mt.Gox Site Disappears, Bitcoin Future in Doubt*, CNNMONEY (Feb. 25, 2014), http://money.cnn.com/2014/02/25/technology/security/mtgox-bitcoin/index.html; Mark Thompson, *Bitcoin Market Mt.Gox Files for Bankruptcy*, CNNMONEY (Feb. 28, 2014), http://money.cnn.com/2014/02/28/investing/mt-gox-bankruptcy/index.html.

b. First Seizure of Bitcoins

In June 2013, the U.S. Drug Enforcement Agency made what appears to be the first seizure of bitcoins, in connection with an online purchase of illegal substances.[219] Though there is speculation,[220] there is no indication of exactly how the agency took control of the bitcoins. The seizure was fairly small, however, consisting of 11.02 bitcoins, worth approximately $814.22 at the time.[221]

Although details are few, it is noteworthy that this particular seizure appears to be targeting a drug trafficker, rather than a digital currency exchange. The seizure is small but commendable.

B. Additional Headaches for Would-Be Bitcoin-Related Prosecutions

Part III.A., *supra*, discusses a few instances of the anti-money laundering regime being applied to digital currencies, with emphasis on how the Bitcoin ecosystem differs from the digital currencies under consideration. With one set of guilty pleas (relating to e-gold) and all the other matters pending (indictment for Liberty Reserve, seizures but no charges for Mt. Gox, and one small Bitcoin account), no patterns of prosecutorial success or failure have yet emerged.

Nor can Bitcoin be shut down the way law enforcement has been able to close down operations of e-gold and Liberty Reserve. Bitcoin cannot be shut down because there is no central source to close—because the entire Bitcoin institution operates on a P2P network, it operates simultaneously on unknowable numbers of private computers. The Bitcoin code is open-source, visible to anyone who looks for it, and is available free of charge. A global, public computer code simply cannot be shuttered by U.S. law enforcement efforts.

In addition to the differences in digital characteristics highlighted above, several other important hurdles must be cleared before significant law enforcement of digital currency providers and/or exchangers can take place.

1. What Is the Crime?[222]

Prosecutions can be based on any of the shells in the Russian nesting doll of anti-money laundering laws discussed in Part I: failure to comply

---

[219] George Dvorsky, *U.S. Feds Make Their First-Ever Bitcoin Seizure*, io9 (June 28, 2013, 6:40 AM), http://io9.com/u-s-feds-make-their-first-ever-bitcoin-seizure-607748728.

[220] *See id.*

[221] *Id.*

[222] The analysis here is limited to violations of U.S. anti-money laundering laws and regulations. While analysis of violations of other statutory schemes, such as the Securities and Exchange Acts (*see* Dion, *supra* note 88, at 192; Kaplanov, *supra* note 179, at 145–47), the Stamp Payments Act (*see* Dion, *supra* note 88, at 192; Grinberg, *supra* note 67, at 182–83), or the counterfeiting statutes (like the Liberty Dollars case, discussed *supra* note 185), are possible, they are beyond the scope of this Article.

with KYC or reporting requirements, or money laundering itself, or on the underlying criminal activity.

The anti-money laundering regulatory scheme, including KYC and reporting requirements, applies to "financial institutions," a term that includes banks and "money services businesses."[223] If digital currency providers and exchangers are not "financial institutions," they cannot be prosecuted for regulatory violations because the regulations do not apply to them.

If, on the other hand, the current regulations *are* applicable to digital currency providers and exchangers, it will be because those entities constitute money services businesses.[224] The definition of money services businesses encompasses "money transmitters"—those that engage in "the acceptance of currency, funds, or other value that substitutes for currency from one person *and* the transmission of currency, funds or other value that substitutes for currency to another location or person by any means."[225]

Bitcoin transactions can either occur peer-to-peer, via the Bitcoin software itself, or through third-party digital currency exchanges. It seems impossible that peer-to-peer transactions could trigger reporting requirements: this could only be the case if every Bitcoin user constituted a "money transmitter." By analogy, then, every person who came in contact with a dollar bill would become a "money transmitter" and would be subject to KYC and reporting requirements.[226] It seems unrealistic to consider each user of cash to be a "money transmitter," just as it seems unrealistic (and impractical, from a regulatory standpoint) to consider each Bitcoin user to be a "money transmitter."

On the other hand, digital currency exchanges probably do fall within the definition of "money transmitter" in the regulations, given the plain meaning of the definition. The definition hinges on "the acceptance of currency, funds, or other value that substitutes for currency."[227] Even taking a skeptic's perspective that Bitcoin is not "currency" or "funds," it almost certainly is "value that substitutes for currency."[228] As such, digital currency exchanges would be required to register with Fin-

---

[223] 31 C.F.R. § 1010.100 (2013). The related statutory language in 31 U.S.C. § 5312(a) is not identical, but the Secretary of the Treasury is authorized to extend the reach of regulations to entities engaging in similar or related activities. § 5312(a)(2)(Y).

[224] Hett, *supra* note 19, at ¶¶ 24–25.

[225] 31 C.F.R. § 1010.100(ff)(5)(i)(A) (emphasis added).

[226] Certain private fund transfers—whether in dollars or bitcoins—may trigger the application of other regulations, such as estate and gift tax implications, but not the anti-money laundering regulations.

[227] 31 C.F.R. § 1010.100(ff)(5)(i)(A).

[228] *Accord* Joshua J. Doguet, Comment, *The Nature of the Form: Legal and Regulatory Issues Surrounding the Bitcoin Digital Currency System*, 73 LA. L. REV. 1119, 1147–48 (2013).

CEN as money services businesses[229] and comply with regulations. Even here, however, compliance is problematic.

First, many digital currency exchanges are located overseas and are arguably not subject to U.S. anti-money laundering laws. Even if digital currency exchanges have U.S. customers, because of the anonymity of digital currencies, the exchange may not know the customer is in the United States. Thus, even if an exchange wanted to comply with U.S. laws regarding its U.S. customers, it likely would not be able to ascertain which customers are in the U.S. Complying with KYC regulations would be extremely difficult, since these exchanges operate online and worldwide, making face-to-face identification next to impossible. Moreover, it would be extremely difficult for an exchange to verify the authenticity of any identification documents provided by a customer.

Furthermore, compliance with recordkeeping requirements would be confounded by the volatile exchange rates of digital currencies. Threshold dollar amounts that trigger recordkeeping are problematic at best (and meaningless at worst) when the dollar-to-bitcoin exchange rate is capable of fluctuating 60% in a single day.

Suspicious activity reports, a tremendously important part of anti-money laundering regulation, are also meaningless in a new and rapidly evolving currency ecosystem like Bitcoin's. How can law enforcement know what a "suspicious" Bitcoin transaction looks like, when we hardly know what a typical transfer looks like?[230] This problem may be solved over time, as Bitcoin transactions happen with more frequency and regularity, but given the lack of information about any one transfer and the likelihood of criminals using disposable Bitcoin addresses, patterns of normalcy may not emerge in a meaningful timeframe. Without patterns of normalcy, abnormality cannot be detected.[231]

2. Jurisdiction

Serious questions exist regarding whether U.S. courts have jurisdiction for crimes that occur in cyberspace. In some ways, cyberspace has become a location of its own, territorial in its ability to support communities with distinct cultures and rules of conduct.[232] Any number of events giving rise to criminal or civil liability may occur exclusively in cyberspace: defamation,[233] distribution of child pornography, breach of contract, or money laundering. Yet current personal jurisdiction jurispru-

---

[229] 31 C.F.R. § 1022.380(a).

[230] Stokes, *supra* note 5, at 5.

[231] The scope of this Article does not allow for discussion of the crime of conspiracy as related to Bitcoin transactions; of note, however, both the e-gold and Liberty Reserve prosecutions involved charges of conspiracy to launder money and conspiracy to operate unlicensed money transmitting businesses. Verified Complaint, *supra* note 205, at 8; e-gold Indictment, *supra* note 188, at 9, 18.

[232] *See* Smith, *supra* note 75, at 846.

[233] *See id.* at 849–50.

dence remains yoked to the idea of geography.[234] Courts and commentators seek desperately to determine where on Earth a cybercrime (or cybertort, etc.) occurs, so that legal proceedings can commence in the correct physical courthouse.

The geographic context of personal jurisdiction is becoming harder and harder to justify as more of modern life is conducted online. To begin with a tangible example, when an individual orders a book from Amazon.com, jurisdiction over the customer is obviously proper in the customer's home state. Are other locations also proper? The customer likely ordered a book online specifically to avoid going to a physical bookstore. The customer can hardly be said to be purposefully availing himself of the jurisdiction where Amazon's headquarters, warehouses, or information servers are located. More likely, such an individual does not know—or care!—where those places are.[235] Even more problematic, sites such as Amazon employ multiple warehouses and duplicative information servers in numerous locations, each with redundant information; details of an Amazon transaction are likely stored in multiple geographic locations "typically both unknown and irrelevant to the user."[236] Does it not *offend traditional notions of fair play and substantial justice* to subject an Amazon customer to personal jurisdiction in one or more states that happen to contain Amazon warehouses or servers, without the customer being aware of those locations?

The foregoing example assumes that a tangible good is being purchased and shipped to an end user. The jurisdictional problems become even more complicated when the transaction is for a digital good. Assume the Amazon customer above purchases an e-book and downloads it to a Kindle e-reader.[237] Where does this transaction take place? If Amazon's computers store identical e-book files on servers in several states (unknown and unimportant to the user), those states cannot fairly provide jurisdiction. The customer's physical location may be a source of jurisdiction, but the Kindle, unlike the customer's front porch, is mobile. The customer can download an e-book while at home in Texas, on vacation in Florida, or while visiting grandparents in Australia. (What if the book is purchased from a customer sitting on a cruise ship or airplane, located in an undeterminable—or, egads, nonexistent—jurisdiction?)

Moreover, digital goods such as e-books can be multiple places at once—the customer can be reading an e-book on a smartphone during a business trip while the customer's spouse uses the Kindle at home to read the same book. In fact, because these kinds of devices typically store information in "the cloud," the e-book is essentially *everywhere*.

---

[234] *See id.* at 848 ("The fact that online activities are not fixed at a particular point in space frustrates attempts to analyze online interactions as if they take place in a forum state.").

[235] *Id.*

[236] *Id.*

[237] *Id.* at 850.

Downloading an e-book from cyberspace onto a mobile device ought to be the same transaction, regardless of the accident of geography. Individuals who transact business online have made a conscious decision to do so in a place separate and apart from their geographic locations.[238]

Until recently, even online transactions have been grounded by *something*—headquarter offices or places of incorporation,[239] physical delivery addresses, or the brick and mortar financial institutions through which parties pay and are paid. With the advent of digital currencies such as Bitcoin,[240] however, attempts to tie online transactions to a physical location seem even more incredulous.[241]

The same issues plague a potential prosecution of a digital currency exchange. Users of digital currency exchanges do not know or care in which country the exchange is located—all the user cares about is that the exchanger will effect the requested transaction promptly, and without asking too many questions. The digital currency exchanger's services are sought out by legitimate users and criminals alike simply because they are available and easily accessible online. A Bitcoin user may be aware that Mt. Gox is based in Japan, but the user can hardly be said to be availing herself of Japanese jurisdiction—the transaction is made solely in cyberspace.

A new jurisdictional model must be adopted to conform with the realities of cyberspace, but unfortunately, a comprehensive proposal for such a model is beyond the scope of this Article. Instead, this Article's thesis avoids the cyberjurisdiction problem by reframing and refocusing: law enforcement should partner with digital currency exchangers to extract what information is available in order to prosecute the money laundering and underlying crimes, rather than seek to prosecute the attenuated violations of KYC, recordkeeping, and reporting requirements.

3. Other Difficulties

The prosecutorial problems continue to add up. Which law enforcement agent will be responsible for, or at least spearhead, prosecutions of digital currency exchanges? The Patriot Act authorized the Secretaries of the Treasury and Department of Homeland Security, the Federal Reserve, the Internal Revenue Service, and even the Postmaster General to investigate money laundering crimes.[242] In announcing the e-gold indictment, the Department of Justice acknowledged that the case was investigated by the Secret Service (a division of the Treasury Depart-

---

[238] *See id.* at 848.

[239] *See, e.g.*, *supra* text accompanying notes 69–73 (physical locations for Google and Reddit); Part III.A.1 (discussing e-gold's physical headquarters).

[240] Similar issues are raised with Linden Dollars, the online currency used in the Second Life video game. Smith, *supra* note 75, at 849–50.

[241] *Id.* at 849.

[242] 18 U.S.C. § 1956(e) (2006).

ment), the IRS, and the FBI.[243] In the few short years that digital currencies have been in existence, these agencies appear to have had a cooperative relationship, but as potential criminal defendants continue to multiply, conflicts of interest and turf wars are certainly conceivable.

All of the foregoing discussion has assumed that law enforcement has been able to detect a crime in the first place. The hallmark of digital currencies, however, is anonymity, and Bitcoin's anonymity protections seem to be particularly robust. If law enforcement continues to view everyone in the digital economy as a potential defendant, the game of whack-a-mole is unwinnable, as individuals will retreat into anonymity and reemerge in another part of the digital currency ecosystem. Instead, by bringing digital currency exchanges into the law enforcement fold as partners, law enforcement can develop a better understanding of the cyberlaundering landscape and make more informed decisions about which entities to target for laundering and underlying crimes.

Additional questions of which parties to charge, whether to pursue civil or criminal penalties, and whether to seek jail time or forfeiture, will have to be left to prosecutorial discretion. Because no digital currency prosecutions have yet gone to trial, it is unknown whether any viable defenses can be raised by defendants. Most attorneys and commentators who have addressed the question have focused on definitions—that a particular digital currency entity does not fall within, say, the definition of "money transmitter," and as such, the regulatory scheme does not apply.[244] By retreating from prosecutions of reporting requirement violations, the government can avoid litigation focused on hair-splitting (and fact-intensive) analysis of particular wording of a regulation. (Hair-splitting analysis of regulations may even encourage innovation—would-be online criminals could develop new technologies that specifically avoid the characteristics of former digital currencies.) This would also relieve the Executive branch of the ongoing obligation to update and itemize the digital entities subject to the regulations.

C. Alternatives and Recommendations

Commentators have proposed various solutions—or, at least, modifications—to existing U.S. anti-money laundering laws to improve law enforcement's ability to prevent and prosecute crimes committed via Bitcoin. Taken together, these changes would improve a prosecutor's ability to bring digital currency providers to court, but would not reduce the hair-splitting, fact-specific analysis that would be required for every digital currency provider that debuts with a few different features.

---

[243] *Digital Currency Business E-Gold Indicted for Money Laundering and Illegal Money Transmitting*, DEP'T OF JUSTICE (Apr. 27, 2007), http://www.justice.gov/opa/pr/2007/April/07_crm_301.html.

[244] *See, e.g.*, Hett, *supra* note 19, ¶¶ 44–45.

Instead, the better approach would be for law enforcement to partner with the digital currency exchanges to extract additional identifying information about the individuals conducting the actual money laundering or the underlying crimes, such as drug trafficking.

1. Revise Statutes and Regulations

Federal statutes and Treasury regulations, particularly ones defining which entities are subject to the regulations, can be amended to specifically include entities dealing in digital currencies. Hett recommends amending the definition of "money transmitter" in 31 C.F.R. § 1010.100(ff)(5)[245] to include "any person engaged in maintaining an online funds transfer system."[246] However, any attempt to itemize entities subject to regulation necessarily leaves some entities outside the definition. Given the speed and flexibility with which criminals—particularly those active online—have demonstrated their ability to modify their businesses to avoid falling within existing regulations, regulators and legislators will be required "to constantly revisit regulations to make sure the regulations are technologically updated."[247]

Dion goes further, proposing that "Congress . . . explicitly create a comprehensive set of statutes" relating to digital currencies.[248] He suggests that such laws would "require Bitcoin to maintain a database of registered wallets."[249] Bitcoin operates without leadership, however, and it is unclear to whom such a requirement could be directed or who would develop and maintain such a database. While a comprehensive list of Bitcoin wallets would certainly be more data than is currently available, it is uncertain how this information, without more, could lead to the apprehension of criminals.

The regulations as written are probably (or at least arguably) sufficiently broad to include digital currency providers and exchanges.[250] Given this, law enforcement can make a plausible threat of prosecution in order to secure a digital currency exchange's cooperation in law enforcement investigation. This is the better course of action with Bitcoin-related crimes, where the digital currency provider is the un-prosecuteable P2P network of users. Instead, law enforcement would have greater success expending its energies using the digital currency exchanges' information to detect money laundering and underlying criminal activity.

---

[245] Hett's article, published before the reorganization of the Title 31 Treasury regulations, utilizes the prior numbering scheme; the current citation is used here. *See, e.g.*, Hett, *supra* note 19, ¶ 24 n.84.

[246] *Id.* ¶ 62.

[247] Turner, *supra* note 4, at 1410.

[248] Dion, *supra* note 88, at 197.

[249] *Id.*

[250] *See supra* text accompanying notes 221–22.

2. Broaden Jurisdiction

If cyberspace is its own location,[251] Congress could simply authorize a specific court or courts to have jurisdiction over causes of action that accrue online.[252] Precedent exists for the establishment of jurisdiction over entities involved in a widespread common endeavor: the Federal Interpleader Act gives district courts jurisdiction over specific situations in which residents of multiple states have claims on the same insurance policy.[253] Other types of cases are heard in specific courts regardless of the state in which the cause of action accrued, such as those cases heard by the U.S. Court of International Trade.[254]

In his otherwise excellent article, Smith recommends "that Congress mandate that the operators of an online community hub . . . select one or more federal districts as the community's designated forum district(s) for jurisdictional purposes."[255] While this would satisfy several interests served by personal jurisdiction jurisprudence—convenience of forum for the defendant, for example—it is difficult to imagine online organizations devoted to money laundering stepping forward to volunteer locations where they would be amenable to lawsuits. Furthermore, Congress may lack authority to make (and the Executive branch may lack authority to enforce) such requirements applicable to websites operated offshore. Even if such forums are selected and publicized in a website's terms and conditions governing use of the service,[256] the efficacy of an end user's acceptance of those terms and conditions is not a surety.

3. Cooperation

Digital currency exchanges frequently possess more information about their users, even Bitcoin users, than the Bitcoin software retains. Bitcoin transactions are recorded in the code of the bitcoins themselves, but the only information retained is the recipient's Bitcoin address and the amount of the transfer. Although this transaction ledger is essentially public, considering Bitcoin addresses can be anonymous and disposable, the published information is quite minimal.

Other exchange mediums, however, may collect and retain significant amounts of other information; these clues can be used, along with

---

[251] *See* Smith, *supra* note 75, at 845.

[252] *Id.* at 860.

[253] *Id.* at 859 (citing 28 U.S.C. §§ 1335, 1397, 2361 (2006)).

[254] *See* 28 U.S.C. § 1581; *About the Court*, U.S. COURT OF INT'L TRADE, http://www.cit.uscourts.gov/AboutTheCourt.html#jurisdiction ("The geographical jurisdiction of the United States Court of International Trade extends throughout the United States. The court can and does hear and decide cases which arise anywhere in the nation. The court is also authorized to hold hearings in foreign countries.").

[255] Smith, *supra* note 75, at 861.

[256] *Id.*

transaction patterns, to identify individuals.[257] Purchases of Linden Dollars require credit or debit cards. E-gold accounts required valid email addresses. In fact, after the significant outlay of time and resources to bring charges against e-gold, the company's files provided a wealth of information to investigators, allowing them to pursue credit card thieves and hackers[258]—those criminals committing the underlying crimes, not just the financial institution processing their payments. By treating digital currency exchanges as partners, this information may be divulged to law enforcement without the significant capital outlay involved in actually prosecuting the exchanger.

Conclusion

United States anti-money laundering laws have become a complicated mess of statutes and regulations. Initially designed to hamper drug trafficking, and later used to attempt to disrupt planned acts of terrorism, anti-money laundering laws are now enforced when law enforcement cracks down on financial institutions for failure to comply with reporting requirements and know-your-customer protocols.

In response, as they have always done, criminals seek new ways of transacting business to avoid violating existing laws and out-maneuver law enforcement. Crime has moved online: ordering drugs through the mail and laundering money by moving funds from one anonymous digital currency account to another.

By focusing attention on prosecuting digital currency exchangers, law enforcement is engaging in the never-ending uphill battle of locating, asserting jurisdiction over, and prosecuting online companies conducting global business that may or may not be subject to—or be violating—existing U.S. laws. Amending regulations to incorporate such online entities would require constant revisions as new entities with new characteristics appeared.

Instead, law enforcement should be partnering with such digital currency exchanges to wring what information can be wrung in order to prosecute the launderers and criminals themselves.

---

[257] *See* Kaplanov, *supra* note 179, at 171 n.379 (quoting Katherine Mangu-Ward, *Buy Illegal Drugs Anonymously on the Internet. Finally. UPDATED: Too Good to Be True*, Hit & Run Blog (June 1, 2011, 4:36 PM), http://reason.com/blog/2011/06/01/buy-illegal-drugs-anonymously) ("Attempting major illicit transactions with bitcoin, given existing statistical analysis techniques deployed in the field by law enforcement, is pretty damned dumb.").

[258] Kim Zetter, *Liberty Reserve Founder Indicted on $6 Billion Money-Laundering Charges*, Wired (May 28, 2013), http://www.wired.com/threatlevel/2013/05/liberty-reserve-indicted/.