2014

Regulating Cryptocurrencies in the United States: Current Issues and Future Directions

Sarah Jane Hughes
Indiana University Maurer School of Law, sjhughes@indiana.edu

Stephen T. Middlebrook
FSV Payment Systems

REGULATING CRYPTOCURRENCIES IN THE UNITED STATES: CURRENT ISSUES AND FUTURE DIRECTIONS

Stephen T. Middlebrook[†] and Sarah Jane Hughes[††]

---

† Stephen T. Middlebrook is the General Counsel of FSV Payment Systems, Inc., a prepaid processor and program manager. Prior to joining FSV, he was Senior Counsel at the U.S. Department of the Treasury, Financial Management Service. He is the current co-chair of the Electronic Payments and Financial Services Subcommittee of the Cyberspace Law Committee and a contributor to RFIDS, NEAR-FIELD COMMUNICATIONS, AND MOBILE PAYMENTS: A GUIDE FOR LAWYERS (2013). He can be reached at stm@aol.com. The views contained in this article are his and may not reflect the views of his employer.

†† Sarah Jane Hughes is the University Scholar and Fellow in Commercial Law at the Maurer School of Law at Indiana University. She is a graduate of Mount Holyoke College and of the University of Washington School of Law. She co-authored RESPONDING TO NATIONAL SECURITY LETTERS: A PRACTITIONER'S GUIDE (2009) (with David P. Fidler), and contributed to and edited RFIDS, NEAR-FIELD COMMUNICATIONS, AND MOBILE PAYMENTS: A GUIDE FOR LAWYERS (2013), with Mr. Middlebrook and Candace M. Jones as co-editors. She has also written articles on payments and banking law, policies and regulations related to the deterrence of money laundering, and data security and privacy, including *Red Skies in the Morning—Professional Ethics and the Dawn of Cloud Computing*, 38 WM. MITCHELL L. REV. 111 (2011) (with Roland L. Trope).

I. INTRODUCTION

Since virtual currencies first came into the marketplace in the 1990s, those responsible for monetary policy, federal anti-money-laundering and economic sanctions programs, along with federal and state consumer protection regulators, payment systems operators, businesses, and consumers have grappled with understanding how these "currencies" work, whether they should be deemed "lawful" payment methods in the United States, and, if so, the manner and extent to which they should be regulated. Regulatory activity related to offering virtual currencies has come in fits and starts, with a burst of intensity in 2013 spurred by the attention to and use of a special form of virtual currency known as a cryptocurrency.

This article reviews developments in 2013 that pertain to cryptocurrencies and their transactors and evaluates them against the backdrop of long-established and more recent federal and state licensure, payments systems, anti-money laundering, economic sanctions, and consumer protection regulation. It also touches upon transactors' desires for anonymity and security in their transactions and related information and discusses how the technologies upon which cryptocurrencies are based may be adapted to support both other payment methods and electronic commerce in general.

Part II describes cryptocurrencies in the market in 2013. Part III reviews the precursors to the current state of regulation in the United States, particularly the federal government's prosecution of

e-gold, Ltd. In Part IV, we evaluate FinCEN's initial guidance on virtual currencies, which it published in March 2013, and discuss industry reaction to the new rules. In Part V, we review recent actions by legislators, other federal regulators and some state actors. Part VI analyzes the federal government's 2013 enforcement actions against Mt. Gox Co. Ltd. ("Mt. Gox"), and Liberty Reserve, which closely followed FinCEN's March guidance. And, in Part VII, we ask—and make some modest efforts to answer—the core question: what does the future hold for cryptocurrency? The brief conclusion in Part VIII relies in part on the legal history of concepts of "money" and "legal tender" in the United States since 1862 and concludes that it is unrealistic to imagine that cryptocurrencies will not face regulation in the United States for some or all of the purposes mentioned in this article.

II. THE CURRENT STATE OF CRYPTOCURRENCIES

A. *Cryptocurrencies Gain Attention of Regulators and Legislators*

In the spring of 2013 the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) issued guidance on the compliance obligations of virtual currencies under the federal Bank Secrecy Act (BSA).[1] FinCEN's announcement was quickly followed by law enforcement action, including seizure of assets of cryptocurrency participants held at banks in Maryland and California.[2] In addition, federal indictments, accompanied by seizure orders, came down against the Costa Rica-based cryptocurrency known as Liberty Reserve.[3] Also, the State of California's Department of Financial Institutions issued a cease and

1. Bank Secrecy Act, tit. I–II, Pub. L. No. 91-508, 84 Stat. 1114, 1114–24 (codified as amended at 12 U.S.C. §§ 1829b, 1951–1959; 31 U.S.C. §§ 5311–5314, 5316–5332 (2012)) (authorizing the Secretary of the Treasury to issue regulations requiring financial institutions to keep and file reports that the Secretary determines have a "high degree of usefulness in criminal, tax, or regulatory investigations or proceedings, or in the conduct of intelligence or counterintelligence matters, including analysis to protect against terrorism" (quoting 12 U.S.C. § 1829b(a)(1)(A)); 31 C.F.R. §§ 1000–1099 (2013) (FinCEN's BSA regulations).

2. See Part VI.A for a discussion of the seizures conducted as part of the enforcement action against Mt. Gox, an offshore bitcoin exchange.

3. See Part VI.B for a discussion of the seizures conducted as part of the Liberty Reserve enforcement action.

desist letter to the Bitcoin Foundation charging the foundation with engaging in the business of money transmission without obtaining a license or other authorization required by California's Money Transmission Act.[4] The interests of federal and other state legislators and regulators have been piqued, and investigations and studies are underway on several fronts.[5]

Cryptocurrencies have the potential to challenge government supervision of monetary policy by the disruption of current payment systems and the avoidance of existing regulatory schemes. In particular, they offer, or at least are perceived as providing, the ability to cloak transactions with a level of anonymity that is currently found only with certain cash transactions. Consequently, cryptocurrencies are of special interest to those who value their privacy, whether that desire springs from personal or political views, a desire to evade taxes, or for other nefarious purposes such as money laundering, terrorism, child pornography, or human trafficking.[6]

Beyond these prospects, some charge that cryptocurrencies lack proper consumer protections, including consumers' rights to prompt and full redemption of funds on terms specified in contracts that consumers have with entities holding their virtual currency.[7] Additionally, cryptocurrencies are theoretically open to

---

4. Jon Matonis, *Bitcoin Foundation Receives Cease and Desist Order from California*, FORBES (June 23, 2013, 11:11 AM), http://www.forbes.com/sites/jonmatonis/2013/06/23/bitcoin-foundation-receives-cease-and-desist-order-from-california (describing and including a copy of the California Department of Financial Institutions' cease-and-desist letter to the Bitcoin Foundation, May 30, 2013, which references California Financial Code sections 2030 and 2151–2152, California Business & Professional Code sections 17200 and 17205–17206, 18 U.S.C. § 1960, and 31 U.S.C. § 5330). For a discussion of the letter, see Rick Fischer, Obrea O. Poindexter & Matthew Ly, *Bitcoin Receives Cease and Desist Order Evidencing Increased Regulatory Scrutiny of Virtual Currency*, MORRISON FOERSTER (July 18, 2013), http://www.mofo.com/files/Uploads/Images/130718-Bitcoin-Receives-Cease-and-Desist.pdf.

5. See Part V for a discussion of the state and federal initiatives related to cryptocurrencies.

6. For more extensive discussion of these privacy issues, see Danton Lee Bryans, Note, *Bitcoin and Money Laundering: Mining for an Effective Solution*, 89 IND. L.J. (forthcoming 2014) (manuscript at 38–39), *available at* http://ssrn.com/abstract=2317990.

7. An example of such a consumer protection problem arose on June 20, 2013 when Mt. Gox, a bitcoin exchange, suspended redemption in U.S. dollars for

use to transfer funds to persons who themselves are Specially Designated Nationals[8] or to nations that are covered by one of many economic sanctions programs under the supervision of the Treasury Department's Office of Foreign Asset Controls.[9] No wonder that they are attracting much attention from the United States government.

B. Bitcoin

Much of the recent media attention surrounding virtual currencies has been focused on bitcoins, due in large part to their extreme volatility, with prices for a single bitcoin moving from $13 in January 2013[10] to $1242 on November 29, 2013, just a few dollars short of the price of an ounce of gold.[11] Frequently described as a "cryptocurrency," bitcoins have no physical presence and no

---

two weeks. Press Release, Mt. Gox, Statement Regarding Temporary Hiatus on U.S. Dollar Withdrawals (June 20, 2013), https://mtgox.com/press_release_20130620.html. For a wonderful, early discussion of issues arising in connection with stored value and e-money in their infancy, see Task Force on Stored-Value Cards, *A Commercial Lawyer's Take on the Electronic Purse: An Analysis of Commercial Law Issues Associated with Stored-Value Cards and Electronic Money*, 52 BUS. LAW. 653 (1997).

8. *See Specially Designated Nationals List (SDN)*, U.S. DEP'T TREASURY, http://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx (last visited Nov. 18, 2013). The preamble to the website's coverage explains:

> As part of its enforcement efforts, OFAC publishes a list of individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries. It also lists individuals, groups, and entities, such as terrorists and narcotics traffickers designated under programs that are not country-specific. Collectively, such individuals and companies are called "Specially Designated Nationals" or "SDNs." Their assets are blocked and U.S. persons are generally prohibited from dealing with them.

Id.

9. For an explanation of the U.S. economic sanctions programs that the Treasury's Office of Foreign Assets Control enforces, see *Office of Foreign Assets Control—Sanctions Programs and Information*, U.S. DEP'T TREASURY, http://www.treasury.gov/resource-center/sanctions/Pages/default.aspx (last visited Nov. 17, 2013).

10. *The Mysterious World of Bitcoin: Does It Have Staying Power?*, WHARTON SCH. U. PENN. (Apr. 24, 2013), http://knowledge.wharton.upenn.edu/article/the-mysterious-world-of-bitcoin-does-it-have-staying-power.

11. Ben Rooney, *Bitcoin Worth Almost as Much as Gold*, CNNMONEY.COM (Nov. 29, 2013), *available at* LEXIS.

central authority in charge of the money supply, but instead, they rely upon a peer-to-peer network of participants to maintain a huge database of valid bitcoins used to verify transactions.[12] Each bitcoin is in essence a chain of digital signatures which, when decoded, provide the entire transactional history of the bitcoin.[13] The members of the network who verify new transactions, a process involving intense mathematical computations, are called "miners" and are rewarded for their service with additional bitcoins.[14]

The number of bitcoins slowly expands over time, but will reach a pre-announced limit of twenty-one million around the year 2040.[15] The supply of bitcoin "money" is not controlled by any government or central authority and cannot be manipulated for political purposes—a definite advantage to the currency in the eyes of some.[16] Bitcoin is frequently described as anonymous, because while every transaction is recorded in the public "block chain," parties are identified only by a bitcoin address.[17] It is possible to trace transactions although it may be difficult to associate a transaction with a particular individual.[18] To obtain bitcoins, you either need to be a "miner" or you must purchase them on a currency exchange.[19] Users keep their bitcoins in a wallet, which is stored either in the cloud or on their personal computer.[20]

Bitcoins may be used to make purchases from a growing number of merchants,[21] although the currency is still strongly

12. EUROPEAN CENTRAL BANK, VIRTUAL CURRENCY SCHEMES 21 (Oct. 2012), *available at* http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf.

13. *Id.* at 23.

14. *Id.* at 23–24.

15. *Id.* at 24–25 (explaining that the bitcoin protocol was designed to allow for the money supply to increase at a predictable pace, without the possibility of intervention by a central authority, in order to prevent inflation).

16. *See id.*

17. *See* Nicole Perlroth, *Unlike Liberty Reserve, Bitcoin Is Not Anonymous—Yet*, N.Y. TIMES (May 29, 2013), 2013 WLNR 13121843.

18. Andy Greenberg, *Follow the Bitcoins: How We Got Busted Buying Drugs on Silk Road's Black Market*, FORBES (Sept. 5, 2013, 10:36 AM), http://www.forbes.com/sites/andygreenberg/2013/09/05/follow-the-bitcoins-how-we-got-busted-buying-drugs-on-silk-roads-black-market; Perlroth, *supra* note 17.

19. EUROPEAN CENTRAL BANK, *supra* note 12, at 21, 24.

20. *Virtual Currency: Bits and Bob*, ECONOMIST.COM (June 13, 2011, 8:30 PM), *available at* Westlaw.

21. Bailey Reutzel, *Why Some Merchants Accept Bitcoin Despite the Risks*,

suspected of being associated with underground and illegal transactions.[22] In particular, it was the payment mechanism of choice on Silk Road, an online marketplace for drugs, erotica, fake IDs, and other illegal goods[23] before the government shut down the website.[24] Despite its current bad-boy reputation, traditional bankers have taken notice of bitcoin and are working on integrating it into more mainstream financial services.[25] Companies that provide bitcoin-related products and services—things like currency exchanges, wallets, mining equipment, and software—are also garnering attention from venture capitalists and other investors.[26]

C. Other Cryptocurrencies

Bitcoin may be the media darling of the moment, but it is not the only virtual currency in existence. Other cryptocurrencies such as Litecoin, GeistGeld, SolidCoin, BBQcoin, and PPCoin are similar in nature to Bitcoin but claim to offer technological improvements that will make them faster, safer, or more convenient than Bitcoin.[27] A modified version of the Bitcoin protocol

---

PAYMENTS SOURCE (May 21, 2013, 4:00 AM), *available at* LEXIS.

22. Arwa Mahdawi, *Bitcoin: More Than Just the Currency of Digital Vice*, GUARDIAN (Mar. 4, 2013), 2013 WLNR 5318040.

23. James Ball, *Silk Road: The Online Drug Marketplace That Officials Seem Powerless to Stop*, GUARDIAN (Mar. 22, 2013, 12:04 AM), http://www.guardian.co.uk/world/2013/mar/22/silk-road-online-drug-marketplace.

24. Andy Greenberg, *End of the Silk Road: FBI Says It's Busted the Web's Biggest Anonymous Drug Black Market*, FORBES (Oct. 2, 2013, 12:35 PM), http://www.forbes.com/sites/andygreenberg/2013/10/02/end-of-the-silk-road-fbi-busts-the-webs-biggest-anonymous-drug-black-market.

25. *See* Marc Hostein, *Lightning Fast, Dirt Cheap: Bitcoin Shows What Banking Could Be*, AM. BANKER (Aug. 24, 2012, 1:58 PM), http://www.americanbanker.com/bankthink/lightning-fast-dirt-cheap-bitcoin-shows-what-banking-could-be-1052108-1.html; Jon Matonis, *Bitcoin on the PayPal Network*, FORBES (May 4, 2013, 10:16 AM), http://www.forbes.com/sites/jonmatonis/2013/05/04/bitcoin-on-the-paypal-network.

26. Stacey Cowly, *The Winklevoss Twins Are Bitcoin Bulls*, CNNMONEY.COM (May 18, 2013, 11:35 AM), http://money.cnn.com/2013/05/18/investing/winklevoss-bitcoin/index.html; Jon Matonis, *New Bitcoin VC Fund Seeks Edge with Regulatory, Security Skills*, AM. BANKER (May 29, 2013, 2:24 PM), http://www.americanbanker.com/bankthink/new-bitcoin-vc-fund-seeks-edge-with-regulatory-security-skills-1059453-1.html.

27. *See* Andrew R. Johnson, *Promise and Peril of Virtual Currencies*, WALL ST. J.,

with enhancements to support increased anonymity, dubbed "Bitcoin 2," also has been proposed.[28] The rise of these so called "altcoins"[29] has been criticized by some as detrimental to cryptocurrencies[30] and doomed to failure.[31] In addition, virtual currencies like Liberty Reserve, WebMoney, Perfect Money, and CashU are designed to be totally anonymous,[32] although only time will tell whether such claims are true. These services are typically based outside of the United States, do little or nothing to verify the identity of their customers, and do not accept payment directly but require users to go through a third party to buy or sell their currency.[33]

D. Other Virtual Currencies

In addition to the products discussed above, there are virtual currencies in the market that do not rely on cryptography. The online role-playing game Second Life created by Linden Labs has been around since 2003 and allows players to participate in a virtual economy based on Linden Dollars.[34] Whereas Bitcoin lacks a central monetary authority, Second Life maintains control over its

---

May 29, 2013, at C2, *available at* LEXIS; Tom Simonite, *Bitcoin Isn't the Only Cryptocurrency in Town*, MIT TECH. REV. (Apr. 15, 2013), http://www.technologyreview.com/news/513661/bitcoin-isnt-the-only-cryptocurrency-in-town.

28. Danny Bradbury, *Bitcoin Activists Propose Hard Fork to Bitcoin to Keep It Anonymous and Regulation-Free*, COINDESK (July 25, 2013, 7:08 PM), http://www.coindesk.com/bitcoin-activists-suggest-hard-fork-to-bitcoin-to-keep-it-anonymous-and-regulation-free.

29. A listing of altcoins can be found at *List of Alternative Cryptocurrencies*, BITCOIN WIKI, https://en.bitcoin.it/wiki/List_of_alterantive_cryptocurrencies (last visited Oct. 15, 2013). Some commentators recognize Ripple as an "altcoin" and others do not. The cited list does not recognize Ripple as an altcoin, conceiving of Ripple more like a different payment system with similar concepts operating in a closed-source, centralized nature. *See id.*

30. David Gilson, *MasterCoin to Create New Altcoins in Bitcoin's Block Chain*, COINDESK (Aug. 25, 2013, 10:45 AM), http://www.coindesk.com/mastercoin-to-create-new-altcoins-in-bitcoins-block-chain.

31. Daniel Krawisz, *The Problem with Altcoins*, MISES CIRCLE (Aug. 22, 2013), http://themisescircle.org/blog/2013/08/22/the-problem-with-altcoins.

32. Nicole Perlroth, *Anonymous Payment Schemes Thriving on Web*, N.Y. TIMES, May 29, 2013, at B1, *available at* 2013 WLNR 13235067.

33. *Id.*

34. EUROPEAN CENTRAL BANK, *supra* note 12, at 28–29.

currency through a variety of mechanisms.[35] Players who earn a profit selling virtual land and goods to other players can even convert their Linden Dollars back into real money.[36]

In 2010, Facebook announced its virtual currency called Facebook Credits, which would facilitate payments in games and apps operating on the site.[37] Within two years, however, it abandoned the virtual currency[38] and is facing a class action lawsuit brought by parents of children who purchased Facebook Credits without parental consent.[39]

Although Facebook may be retreating, Amazon is marching forward, announcing Amazon Coins, a virtual currency for use on the company's Kindle Fire tablets.[40] Commentators are already criticizing Amazon Coins as being of limited value to consumers,[41] but that has not stopped Amazon from filing for a patent on its digital currency.[42]

In an interesting twist, the founder of the failed virtual currency e-gold[43] is involved in efforts to launch a new virtual currency backed by reserves of gold.[44]

---

35. *Id.* at 29.

36. *Id.*; Michael S. Rosenwald, *In the Virtual World, Making Actual Millions; Online Entrepreneurs Meet Avatars' Needs as Well as Their Own*, WASH. POST, Mar. 8, 2010, at A01, *available at* 2010 WLNR 26708271.

37. Dean Takahashi, *How Facebook Plans to Fuel the App Economy with Facebook Credits*, VENTUREBEAT (Apr. 21, 2010, 3:18 PM), http://venturebeat.com/2010/04/21/how-facebook-plans-to-fuel-the-app-economy-with-facebook-credits.

38. Tim Peterson, *Facebook Gives Up on Facebook Credits*, ADWEEK (June 20, 2012, 10:26 AM), http://www.adweek.com/news/technology/facebook-gives-facebook-credits-141237.

39. Tom Cheredar, *Can Minors Buy Facebook Credits? Parents Demand Refund in Class Action Suit*, VENTUREBEAT (Apr. 20, 2012, 10:27 AM), http://venturebeat.com/2012/04/20/facebook-credits-minors.

40. Bailey Reutzel, *Amazon Advances in Virtual Money Battle While Facebook Retreats*, AM. BANKER (Feb. 11, 2013), 2013 WLNR 3209781.

41. Lee Hutchinson, *Amazon's New "Virtual Currency" of Dubious Benefit to Customers*, ARS TECHNICA (May 13, 2013, 10:08 AM), http://arstechnica.com/business/2013/05/amazons-new-virtual-currency-of-dubious-benefit-to-customers.

42. *Amazon Applies for Patent on Digital Currency*, PAYMENTS J. (Apr. 29, 2013), http://paymentsjournal.com/Content/Featured_Stories/16200.

43. e-gold is discussed in depth in Part III, *infra*.

44. Stephen Foley, *E-gold Founder Backs New Bitcoin Rival*, FIN. TIMES (London) (Nov. 28, 2013, 2:44 PM), http://www.ft.com/cms/s/0/f7488616-561a-11e3-96f5-00144feabdc0.html; *see also* Stephen Foley, *Bitcoin Needs to Learn from*

III. PRECURSORS TO REGULATION—THE GOVERNMENT'S PROSECUTION OF E-GOLD

While recent interest in cryptocurrencies has been sparked by Bitcoin and related products, law enforcement first took notice of virtual currencies back in 2007 when the federal government charged e-gold, Ltd. and its owners with violating federal and state laws regarding "money transmission" services. This section of this article describes the e-gold, Ltd. business model, the criminal prosecution of the company, and the current status of the company and its assets. In addition, the section critiques the application of "money transmission" laws to e-gold and discusses what the court's decision may mean for cryptocurrencies.

A. *e-gold, Ltd. Built a Successful Business Facilitating Internet Payments*[45]

Before it was effectively shut down by law enforcement, e-gold, Ltd. was an Internet-based system that allowed individuals to make domestic and international payments denominated not in dollars or pounds or euros, but rather in gold and other precious metals.[46] e-gold promoted its product as unique because "every ounce is secured by actual gold bullion held in allocated storage at repositories certified by the London Bullion Market Association."[47] Title to the bullion was held by the e-gold Bullion Reserve Special Purpose Trust for the exclusive benefit of holders of e-gold, e-silver, e-platinum, and e-palladium.[48] In 1999, the *Financial Times* described e-gold as "the only electronic currency that has achieved

---

Past E-Currency Failures, FIN. TIMES (London) (Nov. 28, 2013, 8:45 AM), http://www.ft.com/intl/cms/s/2/6d51117e-5806-11e3-a2ed-00144feabdc0.html.

45. Part III.A is derived in part from an article previously published by the authors. *See* Sarah Jane Hughes, Stephen T. Middlebrook & Broox W. Peterson, *Developments in the Law Concerning Stored-Value Cards and Other Electronic Payments Products*, 63 BUS. LAW. 237, 255–57 (2007).

46. *See generally*, Kim Zetter, *Bullion and Bandits: The Improbable Rise and Fall of E-Gold*, WIRED (June 9, 2009, 12:00 AM), http://www.wired.com/threatlevel/2009/06/e-gold/.

47. Defendants' Status Report and Notice of Compliance with This Court's Seizure Warrants and Post-Indictment Restraining Order at 6, United States v. e-gold, Ltd., No. 07-109-RMC (D.D.C. May 17, 2007), ECF No. 28, *available at* http://cryptome.org/e-gold/028.pdf.

48. *Id.*

critical mass on the web. . . . For merchants, [e-gold] has a further bonus: unlike credit cards, which are liable to charge backs, the system guarantees payment once ordered."[49] Early write-ups in magazines such as *Barron's*[50] and *Wired*[51] gave e-gold both visibility and credibility.

B. The United States Government Indictment against e-gold for Money Laundering and Other Offenses[52]

On April 24, 2007, a federal grand jury in the District of Columbia handed down a four-count indictment against e-gold, Ltd; its affiliate Gold & Silver Reserve, Inc.; and their owners, Dr. Douglas L. Jackson, Reid Jackson, and Barry K. Downey.[53] The government alleged that "[e-gold] has been a highly favored method of payment by operators of investment scams, credit card and identity fraud, and sellers of online child pornography," and that e-gold facilitated its customers' payments "knowing that the funds involved were the proceeds of unlawful activity."[54]

Count one of the indictment charged the defendants with transmitting monetary instruments or funds involving the proceeds of illegal activity with the intent of promoting that illegal activity,

---

49. Tim Jackson, *When Gold Makes Cents*, FIN. TIMES (London), July 13, 1999, at 18.

50. Jack White & Doug Ramsey, *Making New Money*, BARRON'S, Apr. 23, 2001, at 59, *available at* LEXIS ("With the global explosion of the Internet and e-commerce, the world needs a new type of currency. It needs an asset-backed, high-tech monetary standard, without the political machinations that hobble the euro, the dollar, the yen and all other traditional currencies. . . . One company, [e]-gold, already allows online users to settle payments using its currency, which is 100% backed by gold.").

51. Julian Dibbell, *In Gold We Trust*, WIRED (Jan. 2002), http://www.wired.com/wired/archive/10.01/egold.html ("Invulnerable to government manipulation and subject to the kinds of market forces only a worldwide, 24/7, open-ended network can bring to bear, e-gold promises not simply better money but the best: a money supply kept so straight and narrow that it has room for neither bubbles nor crashes.").

52. The first four paragraphs of Part III.B are derived from an article previously published by the authors. *See* Hughes et al., *supra* note 45, at 257–59.

53. Indictment at 1, United States v. e-gold, Ltd., No. 07-109 (D.D.C. Apr. 24, 2007), 2007 WL 2988241 [hereinafter "e-gold Indictment"].

54. Press Release, Dep't of Justice, Digital Currency Business E-Gold Indicted for Money Laundering and Illegal Money Transmitting (Apr. 27, 2007), http://www.justice.gov/opa/pr/2007/April/07_crm_301.html.

knowing that the transactions were designed to conceal the source of the proceeds of the illegal activity.[55] At issue were transfers of e-gold from one account to another that the government alleged facilitated the sale of child pornography, stolen credit and debit card information, and various types of investment fraud, such as Ponzi schemes and illegal high-yield investment programs.[56] The indictment identified thirty-six specific e-gold transactions taking place between August 2000 and December 2005 with dollar values ranging from $40 to $725,000 that the government asserted were made in support of such illegal activity.[57]

The remaining three counts of the indictment alleged that e-gold operated as a money transmitter without an appropriate state license, failed to comply with federal money transmitter regulations, and transmitted funds known to have been derived from a criminal offense.[58] According to the government, e-gold failed to obtain a money transmitter's license in the District of Columbia,[59] as is required by law.[60] Prosecutors further alleged that e-gold ignored federal requirements to implement an anti-money-laundering program[61] and to file Suspicious Activity Reports with the Treasury.[62] The indictment alleged that e-gold failed to verify the identity of its customers,[63] allowed accounts with obviously bogus names such as "Mickey Mouse" and "Anonymous Man,"[64] hired employees with no experience in financial services and provided them with little or no training,[65] allowed transactions with suspicious notations such as "child porn" and "CC fraud," and did little or nothing to stop transactions tied to illegal behavior.[66] As

55. e-gold Indictment, *supra* note 53, ¶ 29 (alleging violations of 18 U.S.C. §§ 1956(a)(1)(A)(i), 1956(a)(1)(B)(i), 1956(a)(2)(B)(i), and 1957).

56. *Id.* ¶¶ 23–26.

57. *Id.* ¶¶ 42–47.

58. *Id.* ¶ 50.

59. *Id.* ¶ 68.

60. *See id.* at 26 (citing D.C. CODE § 26-1001(10)).

61. *Id.* ¶ 11 (citing 31 U.S.C. § 5318(h) and its implementing regulations, 31 C.F.R. § 103.125).

62. *Id.* ¶ 12 (citing 31 U.S.C. § 5318(g) in conjunction with 31 C.F.R. § 103.20 (current version at 31 C.F.R. § 1022.320 (2013))).

63. *Id.* ¶ 31.

64. *Id.* ¶¶ 20–21.

65. *Id.* ¶ 32.

66. *Id.* ¶¶ 34–35.

well as being independent violations of the law, these offenses constituted criminal offenses under 18 U.S.C. § 1960.[67]

In August 2007, the federal court ordered the seizure of all of the assets of e-gold, including bank accounts, precious metals, and accounts receivable both in the United States and abroad.[68] Subsequently, e-gold entered into a plea agreement resolving the charges against it.[69] Its remaining assets are being distributed to users under a court-approved plan.[70]

Prior to entering into the plea agreement, defendants unsuccessfully sought to have most of the indictment dismissed, asserting the government had failed to allege adequate facts to support the charges.[71] Defendants' primary argument was the statute they were charged under, 18 U.S.C. § 1960, applied only to a "money transmitting business" and that in order to be a money transmitting business an entity must engage in cash transactions.[72] They argued that because they do not deal in cash, the indictment must be dismissed.[73] The court rejected e-gold's argument, concluding, "Section 1960 defines what it means to be unlicensed and what it means to engage in money transmitting. By those definitions, a business can clearly engage in money transmitting without limiting its transactions to cash or currency and would commit a crime if it did so without being licensed."[74] The court read § 1960 as providing an expansive definition of money transmission: "Section 1960 defines 'money transmitting' broadly to

67. *See* 18 U.S.C. § 1960(a) (2006) ("Whoever knowingly conducts, controls, manages, supervises, directs, or owns all or part of an unlicensed money transmitting business, shall be fined in accordance with this title or imprisoned not more than 5 years, or both.").

68. Post-Indictment Restraining Order at 3–4, United States v. e-gold, Ltd., No. 07-109 (D.D.C. Apr. 25, 2007), ECF No. 33, *available at* http://ia600202.us.archive.org/16/items/gov.uscourts.dcd.125293/gov.uscourts.dcd.125293.33.0.pdf.

69. Plea Agreement of e-gold, Ltd., United States v. e-gold, Ltd., No. 07-109-01 (D.D.C. July 21, 2008), 2008 WL 4234436.

70. *See* Douglas Jackson, *e-gold Value Access Plan Overview*, E-GOLD BLOG (Aug. 12, 2011, 7:45 PM), http://blog.e-gold.com/2011/08/vap-overview.html.

71. *e-gold, Ltd.*, 550 F. Supp. 2d at 84.

72. *Id.*

73. *Id.*

74. *Id.*

including transferring 'funds,' not just currency, by 'any and all means;' it is not limited to cash transactions."[75]

Defendants argued that within federal law, the term "money transmitting business" is only defined at 31 U.S.C. § 5330, which provides that a business can be considered a "money transmitting business" only if it is required to file cash transaction reports under 31 U.S.C. § 5313.[76] Section 5313, in turn, places a reporting requirement only upon domestic financial institutions involved in transactions of "United States coins or currency (or other monetary instruments the Secretary of the Treasury prescribes)."[77] Accordingly, e-gold argued that because § 5330 applies only if § 5313 is triggered, and § 5313 requires the handling of cash or coin, § 5330 also must require the handling of cash or coin.[78]

The court was not persuaded, concluding that in fashioning § 1960, Congress did not borrow from § 5330, but rather relied upon 18 U.S.C. § 1955, which makes it a federal crime to operate a gambling business in violation of state law.[79] Looking at the legislative history[80] of § 1955, the court found that Congress used the term "gambling business" to indicate that it sought to criminalize only large-scale illegal gambling operations: "Because Section 1960 was modeled from Section 1955, it can be inferred that Congress employed the term 'business' after 'money transmitting' in subsections (a) and (b)(1) of Section 1960 to indicate that Section 1960 was designed to tackle large-scale operations as opposed to small-scale or individual money transmitters."[81]

---

75. *Id.* at 88 (citing 18 U.S.C. § 1960(b)(2) (2006)).

76. *Id.* at 87–88.

77. 31 U.S.C. § 5313(a) (2006).

78. *e-gold, Ltd.*, 550 F. Supp. 2d at 87–88.

79. *Id.* at 89.

80. Anticipating that its reliance on the legislative history of § 1955—a statute not at issue in the case—might trouble some readers, the court preemptively defended its analysis:

> The Court recognizes that reliance on the legislative history of a separate, albeit historically related, statute may not by itself eliminate all ambiguity from the phrase "money transmitting business" in Section 1960 (assuming *arguendo* that any ambiguity existed at the outset). The structure of the statute as well as the relevant canons of statutory construction, however, guide the Court to the same conclusion.

Id. at 90.

81. *Id.*

The day before oral argument was held on defendants' motion to dismiss,[82] the government filed a superseding indictment that buttressed the large-scale nature of e-gold's "money transmitting business" by alleging it maintained "a cadre of employees" and transferred "approximately $145,535,374.26" in funds.[83] With these facts included in the indictment, the court concluded that e-gold constituted a "money transmitter" and a "business" and, thus, was also a "money transmitter business."[84] The court also held that even though e-gold had never handled currency or coin, it was still subject to the currency reporting requirements: "A money transmitting business is no less a transmitter of money just because it does not deal in currency. Rather, Section 5313 comes into force and will require a report if, when, and as the transmitter does engage in currency transactions."[85] In conclusion, the court was very clear in its view that handling cash is not the touchstone of being a money transmitting business under federal law. "The term 'money transmitting business' as used in Section 5330 includes all financial institutions that fall outside of the conventional financial system (and that are not a 'depository institution'), not just those that engage in cash transactions."[86]

The court's decision, however, raises as many questions as it answers. If all entities could theoretically handle cash at some time in the future and thus be subject to § 5313, how could being subject to § 5313 possibly serve as a limiting factor in the application of § 1960(a)? What limitations, if any, are there on the application of money transmitter business laws? What does the expansion of money transmission from cash and currency to the more general term "funds" mean for virtual currencies? If e-gold—an Internet-based system that allowed users to transfer among themselves electronic warehouse receipts for precious metals—was required to comply with federal money transmitter laws, then do other similar Internet systems also need to come into compliance? And if transactions in virtual currencies do constitute money transmission, does the court's reliance on the legislative history of § 1955 and its focus on large-scale versus small-scale enterprises

82. *Id.* at 85 n.1.
83. *Id.* at 90.
84. *Id.* at 93.
85. *Id.* at 95.
86. *Id.* at 93.

mean that only major participants would fall under the regulations while small players and mere users would be free from government oversight?

IV. FINCEN SPEAKS—INITIAL GUIDANCE ON VIRTUAL CURRENCIES

On March 18, 2013, FinCEN issued interpretive guidance clarifying the application of the BSA to virtual currencies ("FinCEN Guidance").[87] The guidance interprets FinCEN's recently amended regulations governing money services businesses (MSBs), which includes currency exchanges and money transmitters ("MSB Rule"),[88] and regulations governing providers and sellers of prepaid access ("Prepaid Access Rule").[89] The guidance attempts to clarify if and when a participant in a virtual currency scheme might be engaged in "money transmission," which would require the entity to comply with the MSB Rule requirements to register, file reports, and maintain records.

FinCEN began its analysis by distinguishing "real" currency from "virtual" currency. Real currency is the coin and paper money of the United States or another country that has status of legal tender in the country of issue.[90] Virtual currency does not have legal tender status and thus is not currency. Some virtual currency, however, has an equivalent value in real currency or may be used as a "substitute" for real currency, and FinCEN deems this "convertible virtual currency."[91] FinCEN is not explicit on this point, but presumably a virtual currency, such as Bitcoin, that can be exchanged for real currency would constitute a convertible virtual currency. FinCEN concludes that the Prepaid Access Rule only applies to real currency and thus is not applicable to virtual

87. FIN. CRIMES ENFORCEMENT NETWORK, DEP'T OF THE TREASURY, FIN-2013-G001, APPLICATION OF FINCEN'S REGULATIONS TO PERSONS ADMINISTERING, EXCHANGING, OR USING VIRTUAL CURRENCIES (2013), *available at* http://www.fincen.gov/statutes_regs/guidance/pdf/FIN-2013-G001.pdf.

88. Bank Secrecy Act Regulations; Definitions and Other Regulations Relating to Money Services Businesses, 76 Fed. Reg. 43,585 (July 21, 2011) (codified at 31 C.F.R. pt. 1010, 1021–1022).

89. Bank Secrecy Act Regulations—Definitions and Other Regulations Relating to Prepaid Access, 76 Fed. Reg. 45,403 (July 29, 2011) (codified at 31 C.F.R. pt. 1010, 1022).

90. FIN. CRIMES ENFORCEMENT NETWORK, *supra* note 87, at 1 (citing 31 C.F.R. § 1010.100(m) (2012)).

91. *Id.*

currencies.[92] Likewise, the regulations governing foreign exchange only cover currencies issued by other countries and thus do not apply to virtual currencies.[93]

Because a convertible virtual currency may "substitute" for real currency, it may qualify as a form of money transmission. FinCEN defines money transmission as "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."[94] Whether a particular entity is or is not a money transmitter is "a matter of facts and circumstances," and the rules include a number of exemptions from the general rule.[95] Under this guidance, a person who accepts a convertible virtual currency from one person and then transmits that convertible virtual currency to another person or location would be a money transmitter for FinCEN's purposes.[96]

In the next step of its analysis, FinCEN divides the participants in virtual currency arrangements into three categories: users, exchangers, and administrators.[97] Users obtain virtual currency in order to purchase real or virtual goods and services.[98] An exchanger is a person engaged as a business in the exchange of virtual currency for real or virtual currency.[99] An administrator is a person engaged as a business in issuing and redeeming virtual currency.[100] FinCEN quickly concludes users are not MSBs because they do not transmit the value of funds to another person or location.[101] "An administrator or exchanger that (1) accepts and transmits a convertible virtual currency or (2) buys or sells convertible virtual currency," however, is a money transmitter unless an exemption applies.[102] One exemption carves out an entity that accepts and transmits funds solely for the purpose of affecting a bona fide

92. *Id.* at 5.
93. *Id.* at 5–6.
94. 31 C.F.R. § 1010.100(ff)(5)(i)(A) (2012).
95. *Id.* § 1010.100(ff)(5)(ii).
96. *Id.* § 1010.100(ff)(5)(i).
97. FIN. CRIMES ENFORCEMENT NETWORK, *supra* note 87, at 2.
98. *Id.*
99. *Id.* at 3.
100. *Id.*
101. *See id.*
102. *Id.*

purchase or sale of currency—real or virtual—from the entity accepting the funds.[103] In that case, the person is not acting as a money transmitter.[104]

In an arrangement with a centralized administrator, the administrator will be a money transmitter to the "extent that it allows transfers of value between persons or from one location to another."[105] In addition, an intermediary exchange that accepts funds from a user and then transmits those funds to the user's account with the administrator would also be engaged in money transmission.[106] FinCEN acknowledges that the third-party exchange might appear to be conducting a bona fide purchase and thus entitled to an exemption, but notes that the safe harbor does not apply when the only service being provided is money transmission.[107]

In a decentralized arrangement, a person who creates units of the virtual currency (a "miner" in Bitcoin parlance) and uses it to purchase real or virtual goods would not be a money transmitter.[108] FinCEN notes, however, "a person that creates units of convertible virtual currency and sells those units to another person for real currency or its equivalent is engaged in transmission to another location and is a money transmitter."[109]

Although the FinCEN Guidance is not a model of clarity, it appears that individuals who merely use a virtual currency to purchase goods or services are not deemed money transmitters and are not required to register as an MSB.[110] Users who attempt to sell their virtual currency, however, may become money transmitters.[111]

An administrator or an exchange that transmits convertible virtual currency to another person or location would be required to register as an MSB.[112] FinCEN's description of both an exchanger and an administrator contain the phrase "engaged as a business,"

---

103. *Id.*
104. *Id.*
105. *Id.* at 4.
106. *Id.*
107. *See id.*
108. *Id.* at 5.
109. *Id.*
110. *Id.*
111. *Id.*
112. *Id.*

which is not defined.[113] The inclusion of this limiting descriptor seems to echo the large-scale-versus-small-scale dichotomy that the court in *United States v. e-gold* incorporated in its analysis of money transmission.[114] It is unclear at what point an entity participating in the virtual currency scheme would be deemed to be acting as a business, and thus, it is difficult to advise such an entity as to when its obligation to register begins. The guidance appears to be designed to apply to Bitcoin and similar virtual currencies, although it is less clear whether it would apply to an in-game currency like Linden Dollars or to a merchant-sponsored program like Amazon Coins.

At least three exchanges that traded bitcoin shut down shortly after the new guidance was issued.[115] Patrick Murck, legal counsel for the Bitcoin Foundation, which promotes use of the virtual currency, said that rules "would be infeasible for many, if not most, members of the bitcoin community to comply with."[116]

The spring 2013 actions by the federal government prompted changes beyond bitcoin. For example, Linden Labs announced that it was modifying terms of service for Second Life to prohibit third-party currency exchanges and require all Linden Dollar transactions to take place on its own exchange.[117] Treasury Undersecretary David Cohen stated, however, that virtual currency exchanges that comply with the law "have nothing to fear from Treasury."[118]

---

113. *Id.* at 2.

114. See *supra* text accompanying footnotes 76–81.

115. Jon Matonis, *Fincen's New Regulations Are Choking Bitcoin Entrepreneurs*, AM. BANKER (Apr. 25, 2013, 10:00 AM), http://www.americanbanker.com/bankthink/fincen-regulations-choking-bitcoin-entrepreneurs-1058606-1.html.

116. Jeffrey Sparshott, *Web Money Gets Laundering Rules*, WALL ST. J., Mar. 22, 2013, at C1, *available at* LEXIS.

117. Linden Lab, *Updated Second Life Terms of Service*, SECOND LIFE (May 7, 2013, 11:55 AM), http://community.secondlife.com/t5/Featured-News/Updated-Second-Life-Terms-of-Service/ba-p/1996185.

118. *U.S.: Liberty Reserve Case No Comment on E-Currency Exchangers*, UNITED PRESS INT'L (May 29, 2013), *available at* LEXIS.

V. ADDITIONAL FEDERAL AND STATE REGULATORS TAKE AN INTEREST IN VIRTUAL CURRENCIES

Perhaps inspired by FinCEN's issuance of guidance, in 2013 Congress and other federal agencies, along with some state regulators, began to show an interest in Bitcoin and virtual currencies.

At the federal level, there was a suggestion that the Commodity Futures Trading Corporation should consider regulating virtual currencies as a form of commodity trading.[119] The Government Accountability Office prepared a report for the Senate Committee on Finance, which concluded that transactions "using virtual currencies could produce taxable income in various ways" and recommended that the IRS issue guidance to tax payers of the "tax consequences of virtual economy transactions."[120] In August 2013, the Senate Homeland Security Committee sent letters to several federal agencies asking them to disclose their policies with regard to virtual currencies, explain how those policies were developed, and describe any future actions the agencies plan to take in this area.[121] In addition, the House Committee on Appropriations noted that "Bitcoins and other forms of peer-to-peer digital currency are a potential means for criminal, terrorist, or other illegal organizations and individuals to illegally launder and transfer money."[122] The committee then directed the Federal Bureau of Investigation to prepare a report "on the nature and scale of the risk posed by such ersatz currency, both in financing illegal enterprises and in undermining financial institutions."[123]

The Senate then moved into high gear in November 2013, holding two separate hearings on virtual currencies. First, the Homeland Security and Governmental Affairs Committee held a hearing entitled "Beyond Silk Road: Potential Risks, Threats, and

119. Tracey Alloway et al., *U.S. Regulators Eye Bitcoin Supervision*, FIN. TIMES (London) (May 6, 2013), *available at* LEXIS.

120. U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-13-516, VIRTUAL ECONOMIES AND CURRENCIES: ADDITIONAL IRS GUIDANCE COULD REDUCE TAX COMPLIANCE RISKS 10, 15 (2013), *available at* http://www.gao.gov/assets/660/654620.pdf.

121. Zachary Warmbrodt, *Congress Starts Looking into Bitcoin*, POLITICO.COM (Aug. 13, 2013, 12:08 AM) http://www.politico.com/story/2013/08/congress-starts-looking-into-bitcoin-95464.html.

122. H.R. REP. NO. 113-171, at 45 (2013).

123. *Id.*

Promises of Virtual Currencies," which featured witnesses from law enforcement and industry addressing the risks and potential rewards of virtual currencies.[124] The Senate Banking Committee followed with its own hearing entitled "The Present and Future Impact of Virtual Currency," which also featured the perspectives of law enforcement, state regulators, industry, and academics.[125] The hearings were widely viewed as positive developments for virtual currencies and were described by one reporter as "lovefests."[126] Law enforcement officials went on record describing Bitcoin as having a legitimate purpose and constituting a legal means of exchange.[127]

State officials are also looking at virtual currency providers.[128] Several states have written to virtual currency exchanges and other businesses suggesting that if the companies do not come into compliance with state money transmitter rules, they will be shut down.[129] In New York, the Department of Financial Services (NYDFS) opened an investigation into virtual currencies and subpoenaed twenty-two companies providing Bitcoin-related services[130] as well as a number of venture capital firms that have

124. *Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies: Hearing on S.D. 342 Before the S. Comm. on Homeland Sec. and Gov't Affairs*, 113 Cong. (2013), http://www.hsgac.senate.gov/hearings/beyond-silk-road-potential-risks-threats-and-promises-of-virtual-currencies.

125. *The Present and Future Impact of Virtual Currency: Hearing Before the Subcomm. on Nat'l Sec. & Int'l Trade & Fin. of the S. Comm. on Banking, Housing, & Urban Affairs*, 113 Cong. (2013), http://www.banking.senate.gov/public/index.cfm?FuseAction=Hearings.LiveStream&Hearing_id=955322cc-d648-4a00-a41f-c23be8ff4cad.

126. Timothy B. Lee, *Here's How Bitcoin Charmed Washington*, WASH. POST. (Nov. 21, 2013), 2013 WL 29385308.

127. Max Raskin, *U.S. Agencies to Say Bitcoins Offer Legitimate Benefits*, BLOOMBERG (Nov. 18, 2013, 4:08 PM), http://www.bloomberg.com/news/2013-11-18/u-s-agencies-to-say-bitcoins-offer-legitimate-benefits.html; Ryan Tracy, *Authorities See Worth of Bitcoin*, WALL ST. J, Nov. 19, 2013, at C1, *available at* LEXIS.

128. Robin Sidel & Andrew R. Johnson, *'Virtual' Currencies Draw State Scrutiny*, WALL ST. J., June 1, 2013, at A1, *available at* LEXIS.

129. Robin Sidel & Andrew R. Johnson, *States Put Heat on Bitcoin: Letters Warn Exchanges to Follow Money-Transmission Laws or Be Closed Down*, WALL ST. J., June 26, 2013, at C1, *available at* LEXIS.

130. Emily Spaven, *New York State Financial Regulator Issues Subpoenas to 22 Bitcoin Companies*, COINDESK (Aug. 12, 2013, 5:55 PM), http://www.coindesk.com/new-york-state-financial-regulator-issues-subpoenas-to-bitcoin-companies.

invested in Bitcoin businesses.[131] In a public statement, the NYDFS said, "If virtual currencies remain a virtual Wild West for narcotraffickers and other criminals, that would not only threaten our country's national security, but also the very existence of the virtual currency industry as a legitimate business enterprise."[132] NYDFS stated that based on its preliminary investigation, it was concerned that virtual currency exchangers may be engaging in money transmission (as defined under New York state law) without posting collateral, undergoing periodic safety and soundness examinations, and complying[133] with applicable anti-money-laundering laws.[134] Some state actions underscore how little officials understand cryptocurrency. For example, the California Department of Financial Institutions sent a cease and desist letter to the Bitcoin Foundation, a nonprofit organization registered in Washington, D.C. with the mission of standardizing and promoting the Bitcoin protocol.[135] The letter charged the foundation with engaging in money transmission in the state without a license, apparently in reaction to the group hosting a conference in the state.[136] In response to all of the activity at the state level, a group of Bitcoin companies and advocates formed the Digital Asset Transfer Authority, a self-regulatory body for the industry, tasked with developing common risk management and compliance standards for members.[137]

131. Bailey Reutzel, *What NY's Bitcoin Crackdown Means for Emerging Payments Companies*, PAYMENTS SOURCE (Aug. 12, 2013, 3:13 PM), *available at* LEXIS.

132. Memorandum from Benjamin M. Lawsky, Superintendent of Fin. Servs., Notice of Inquiry on Virtual Currencies 1 (Aug. 12, 2013), http://www.dfs.ny.gov/about/press2013/memo1308121.pdf.

133. *Id.*

134. *Id.* at 2.

135. Matonis, *supra* note 4.

136. *Id.*

137. Danny Bradbury, *Bitcoin Industry Leaders Launch DATA, A Self-Regulatory Body for Digital Currencies*, COINDESK (July 30, 2013, 10:04 AM), http://www.coindesk.com/bitcoin-industry-leaders-launch-data-a-self-regulatory-body.

VI. THE GOVERNMENT ACTS—ENFORCEMENT ACTIONS AGAINST MT. GOX AND LIBERTY RESERVE

A. Homeland Security Seizes Funds Held by Bitcoin Exchange Mt. Gox

On May 14, 2013, the Department of Homeland Security obtained a seizure warrant directed to Dwolla, an Iowa-based Internet payments company, ordering the seizure and forfeiture of an account belonging to Mutum Sigillum, L.L.C.[138] According to the federal agent's affidavit filed with the warrant application, Mutum Sigillum is the U.S.-based subsidiary of Mt. Gox, the world's largest Bitcoin exchange, which is based in Japan.[139] The affidavit stated that a confidential informant residing in Maryland established an account at Dwolla that he used to fund an account at Mt. Gox and to purchase bitcoins.[140] In addition, the informant also exchanged bitcoins for U.S. dollars, which were transmitted back to him through Mutum Sigillum and Dwolla accounts.[141] The application asserted these transactions demonstrate that Mutum Sigillum is engaged in money transmission but has failed to register with FinCEN as required by 31 U.S.C. § 5330.[142] The affidavit did not cite the FinCEN Guidance issued on March 18, 2013, but it is apparent from the document that the federal agent relied upon it. By failing to register as required by § 5330, the government asserted that Mt. Gox is in violation of 18 U.S.C. § 1960 and subject to criminal penalties.[143] In addition, the forfeiture of property involved in a transaction in violation of § 1960 is authorized by 18 U.S.C. § 981(a)(1)(A).[144] The affidavit noted that Mutum Sigillum

138. Seizure Warrant at 1, *In re* Seizure of the Contents of One Dwolla Account, No. 13-1162-SKG (D. Md. May 14, 2013), *available at* http://cdn.arstechnica.net/wp-content/uploads/2013/05/Mt-Gox-Dwolla-Warrant-5-14-13.pdf; *see also* Joe Mullin, *Feds Seize Money from Dwolla Account Belonging to Top Bitcoin Exchange Mt. Gox*, ARS TECHNICA (May 14, 2013, 5:55 PM), http://arstechnica.com/tech-policy/2013/05/feds-seize-money-from-top-bitcoin-exchange-mt-gox.

139. Affidavit in Support of Seizure Warrant at 2, *In re Seizure of the Contents of One Dwolla Account*, No. 13-1162-SKG, *available at* http://cdn.arstechnica.net/wp-content/uploads/2013/05/Mt-Gox-Dwolla-Warrant-5-14-13.pdf.

140. *Id.* at 3.

141. *Id.*

142. *Id.*

143. *Id.* at 1.

144. *Id.* at 4–5.

funds were also transmitted through an account at Wells Fargo and that a separate warrant was issued to seize funds in that account.[145] Although law enforcement executed warrants to seize the funds of Mt. Gox located in the United States, as of December 31, 2013, no indictments of Mt. Gox or its subsidiary Mutum Sigillum have been handed down. Perhaps in an effort to prevent criminal charges from being brought against it, Mt. Gox implemented a new policy requiring identity verification before it would perform currency deposits or withdrawals.[146] According to press reports, a total of five million dollars was seized from Mt. Gox accounts.[147]

B. Department of Justice Indicts Liberty Reserve for Money Laundering

On May 28, 2013, the U.S. Attorney for the Southern District of New York unsealed a criminal indictment charging Liberty Reserve and seven of its principals and employees with operating an unlicensed money transmitter and engaging in money laundering.[148] The indictment charges the defendants under 18 U.S.C. § 1960 with conspiracy to operate and operating an unlicensed money transmitting business in violation of 31 U.S.C. § 5330 and its accompanying regulations.[149] Defendants were also charged with conspiracy to commit money laundering in violation

145. *Id.* at 4; *see also* Brian Browdie, *Bitcoin Exchange in U.S. Crosshairs Banked at Wells Fargo*, AM. BANKER (May 16, 2013), 2013 WL 12019270 (noting that their Wells Fargo account had been seized).

146. Press Release, Mt. Gox Co., Statement Regarding Account Verifications (May 30, 2013), https://mtgox.com/press_release_20130530.html. For more information about these new procedures see Andy Greenberg, *Not So Anonymous: Bitcoin Exchange Mt. Gox Tightens Identity Requirements*, FORBES (May 30, 2013, 12:03 PM), http://www.forbes.com/sites/andygreenberg/2013/05/30/not-so-anonymous-bitcoin-exchange-mt-gox-tightens-identity-requirement.

147. Greg Schvey, *Additional $2.1M Seized from Mt. Gox Accounts—Now Over $5M Total*, GENESIS BLOCK (Aug. 22, 2013), http://thegenesisblock.com/warrant-for-mt-gox-wells-fargo-accounts-shows-additional-2-1m-seized.

148. Press Release, U.S. Attorney's Office, S.D.N.Y., Manhattan U.S. Attorney Announces Charges Against Liberty Reserve, One of World's Largest Digital Currency Companies, and Seven of Its Principals and Employees for Allegedly Running a $6 Billion Money Laundering Scheme (May 28, 2013), http://www.justice.gov/usao/nys/pressreleases/May13/LibertyReservePR.php.

149. Indictment ¶¶ 33–42, United States v. Liberty Reserve, No. 13-CR-368 (S.D.N.Y. May 20, 2013), *available at* http://www.justice.gov/usao/nys/pressreleases/May13/LibertyReservePR/Liberty%20Reserve,%20et%20al.%20Indictment%20-%20Redacted.pdf.

of 18 U.S.C. §§ 1956(a)(1)(B)(i) and 1956(a)(2)(B)(i).[150] Liberty Reserve is alleged to have been a "financial hub of the cyber-crime world" facilitating identity theft, credit card fraud, computer hacking, child pornography, and drug trafficking.[151] It had 200,000 users in the United States and processed over twelve million transactions a year with a value of more than $1.4 billion.[152] Criminals were drawn to Liberty Reserve because it did not require users to validate their identity with the service and criminals could create accounts under false names such as "Russian Hackers."[153] The government alleges that Liberty Reserve, in an effort to add an additional layer of anonymity, did not permit users to transmit funds directly to Liberty Reserve but instead required them to make deposits and withdrawals through third-party exchanges.[154] These exchangers were themselves unlicensed money transmitters operating without government oversight from Malaysia, Russia, Nigeria, and Vietnam.[155]

Pursuant to 18 U.S.C. § 982(a)(1), the government sought forfeiture of "at least $6 billion" held in accounts in Costa Rica, Cyprus, Russia, Hong Kong, China, Morocco, Spain, Latvia, Australia, and one account at SunTrust Bank in the United States.[156] In a declaration filed in support of the indictment, a Secret Service agent stated that the investigation included execution of "one of the first-ever 'cloud'-based search warrants, directed to a service provider used to process Liberty Reserve's Internet traffic."[157] The government also sought an injunction preventing Amazon Web Services from providing services to support Liberty Reserve's web site.[158]

---

150. *Id.* ¶¶ 30–32.
151. *Id.* ¶ 9.
152. *Id.* ¶ 10.
153. *Id.* ¶¶ 14, 19.
154. *Id.* ¶ 16.
155. *Id.* ¶ 18.
156. *Id.* ¶ 43.
157. Declaration of Special Agent [] in Support of Ex Parte Application for Post-Indictment Restraining Order, Seizure Warrant and Injunction Exhibit B, ¶ 9, United States v. Liberty Reserve, No. 13-CR-368 (S.D.N.Y. May 23, 2013), *available at* http://www.justice.gov/usao/nys/pressreleases/May13/LibertyReservePR/Liberty%20Reserve,%20et%20al.%20Redacted%20AUSA%20Appln%20with%20exhibits.pdf.
158. *Id.* ¶ 74.

On the same day that indictment was unsealed, FinCEN issued a notice of proposed rulemaking to declare Liberty Reserve an institution of primary money laundering concern under section 311 of the Patriot Act.[159] The designation would prohibit U.S. financial institutions from maintaining correspondent relationships with foreign banks that do business with Liberty Reserve.[160] The measure "would effectively cut off Liberty Reserve from the U.S. financial system."[161]

Although the Mt. Gox forfeiture order and the e-gold and Liberty Reserve criminal indictments are quite different on a number of levels, all three enforce regulatory business requirements through a criminal process and rely on the often-criticized penalty [162] of asset forfeiture.

While this may be a convenient and effective way for law enforcement to deal with money launderers, it has significant collateral effect on small companies and start-ups who wish to operate within the confines of the law but lack the resources or the expertise to navigate such tricky regulatory waters. Establishing appropriate compliance obligations without stifling innovation in emerging payments technology is always a concern. With regard to virtual currencies, it remains to be seen whether the government has found the proper balance.[163]

VII. FUTURE PARADIGMS FOR THE REGULATION OF CRYPTOCURRENCY

Cryptocurrencies face efforts to regulate their existence and the manner in which they are transferred and redeemed by both state and federal authorities in the United States as well as by foreign governments.[164] In order for future regulation to be

159. Imposition of Special Measure Against Liberty Reserve S.A. as a Financial Institution of Primary Money Laundering Concern, 78 Fed. Reg. 34,008 (proposed June 6, 2013) (to be codified at 31 C.F.R. pt. 1010).

160. *Id.* at 30,009–10.

161. Chris Cumming, *Fincen Seeks to Deputize Banks in $6B Laundering Case*, AM. BANKER (May 29, 2013), 2013 WLNR 13105120.

162. *See, e.g.*, Sarah Stillman, *Taken*, NEW YORKER, Aug. 12, 2013, at 48, *available at* 2013 WLNR 20611866.

163. For a discussion of the potential "chilling effect" of California's money transmitter statute, see Bryans, *supra* note 6 (manuscript at 34–35).

164. *See* Deepak Tiwari, *Bitcoin Dealers Realize a Regulated Market Is Better for Growth and Development*, FOREXMINUTE (Sept. 8, 2013, 5:00 AM), http://www.forexminute.com/bitcoin/bitcoin-dealers-realize-a-regulated-market-is-better-for

successful and foster a new monetary technology that appropriately weighs both the needs of citizens and governments, a number of paradigmatic questions will require answers. In this part of the article, we raise those questions that have occurred to us that we feel deserve serious thought and exploration by industry participants, regulators, and legislators. We also take the liberty of suggesting for some of these questions the direction in which we think the analysis should advance. We make no claim, however, to have thought of all of the possible questions or to have answers to the majority of them. We offer these thoughts in the spirit of fostering a robust debate on the future of cryptocurrencies.

What Is Cryptocurrency?

Proponents can't easily explain what a cryptocurrency is. If you can't explain what you are and how you fit into the current legal and regulatory scheme, you are at the mercy of the ignorant. The "what this is" answer needs to address not just things like "is it money transmission?" but more mundane yet important questions like "where is a bitcoin located?" and "where and when does a transaction take place?"

Cryptocurrency supporters should address whether cryptocurrency is a currency/store of value or a payment system or a hybrid of both. They should also be prepared to explain if and when these products should be treated like securities or commodities or prepaid access.

It is also important for proponents to separate the different "brands" of cryptocurrency (Bitcoin, Litecoin, Ripple, etc.) from each other and the larger concept of a cryptographically-secured value transfer system. Given that the different protocols will likely develop along divergent pathways, some choosing to emphasize certain attributes (like anonymity), the industry is going to have to decide how it wishes to treat players who take a minority position. It may be that certain protocols will evolve to support different business models, introducing changes so significant that the

-growth-and-development-14540 (reporting on a meeting between U.K. policy makers and Bitcoin dealers that recently took place at Downing Street at which the participants concluded that the U.K. government should introduce regulation for bitcoins).

modified product should be treated as a different species subject to a different regulatory scheme.

What Is the Proper Regulatory Scheme for Cryptocurrency?

Among the most probable possibilities are:

- None. Cryptocurrency will not be regulated. We think this option has no chance of being adopted.
- Unique cryptocurrency regulatory scheme. While this could be the ideal solution, this currently seems an unlikely outcome. The law has a tendency to address new products and technologies by analogizing to existing regulatory schemes. We suggest that this outcome is not wholly impossible, however, and note that with its e-money directive, the European Union demonstrated that if legislators are willing to make hard policy choices, they can craft a regulatory scheme uniquely tailored to a new technology.[165]
- Cryptocurrency as money transmission. This seems to be the current direction based on recent actions by FinCEN and the states. It is unclear that this route is optimal, but for those entities that can comply with federal and state money transmitter requirements, this option provides a safe haven. One example of a payments innovator that used this option to enormous benefit is PayPal.
- Cryptocurrency as bank product. Banks are currently standing on the sidelines as other entities develop and market cryptocurrency. This might change, however, especially if the innovators are successful in navigating the regulatory waters and at turning a profit. We believe that in the future, banks may become involved in the cryptocurrency market, which would have interesting regulatory implications. Banks are exempt from state money transmitter laws and registration requirements. Banks, however, have come under heavy pressure to police their business partners that offer innovative products.[166] Given recent communications that banks and other depository institutions have received about facilitating providers of certain consumer payments, banks may well take a

165. Council Directive 2009/110/EC, 2009 O.J. (L267) 7, 7 (EC).

166. *See* Memorandum from Benjamin M. Lawsky, *supra* note 132.

"wait-and-see" attitude before deciding how or how much to participate in or with cryptocurrencies. If cryptocurrency establishes itself more firmly in the future, then banks are likely to become players by buying participants. This was the strategy that several banks used with prepaid cards.

- Cryptocurrency as multiple activities. We could see cryptocurrency regulation varying significantly based on the role taken by participants. Administrators and exchanges, for example, might be subjected to the full panoply of state and federal money transmitter rules, while an individual merely using a cryptocurrency to make a purchase would remain unregulated.[167] One can see the beginnings of such an approach in the FinCEN Guidance.

Are Cryptocurrencies Intended to Provide Anonymous Transactions?

A business model that is predicated on providing anonymity is going to face a very high level of scrutiny. Entities that provide payment services designed to provide anonymity are going to find themselves cut off from the rest of the financial system, making it difficult if not impossible for users to engage the service. Federal regulators have already used section 311 of the Patriot Act to isolate and effectively close Liberty Reserve.[168] It's important to understand that anonymity is not binary, meaning that the choice isn't between absolute anonymity and completely open transactions. The questions are (1) what degree of anonymity is provided, (2) what is the process for breaking anonymity, and (3) who controls the process. An important question will be whether current law that prevents financial institutions from providing customer records to federal agencies except in certain limited circumstances will be extended to cover newer technology like cryptocurrency that is not offered by a traditional financial institution.[169]

---

167. For discussion of this "regulation-in-part" concept, as well as one view of the optimal manner of regulating exchanges, see Bryans, *supra* note 6 (manuscript at 34–35).

168. *See supra* note 159 and accompanying text.

169. See provisions prohibiting government access to financial records included in the Right to Financial Privacy Act, 12 U.S.C. §§ 3401–3422 (2012). For an analysis of the application of the Right to Financial Privacy Act to prepaid cards, *see* Stephen T. Middlebrook, *What's in Your Wallet? Could It Be the Department of Homeland Security?*, BUS. L. TODAY, Nov. 2013, at 1.

One solution, already used in the prepaid industry, is to allow anonymous users and transactions with certain lower velocity limits and to require customer identification when dollar volumes (or rather, coin volumes) exceed a certain threshold.

It is also important to note that anonymity is incongruous with consumer protections.

Will Future Regulation Be Driven by Payments Policy Concerns or Law Enforcement Demands?

The 2013 FinCEN Guidance came out after the Mt. Gox and Liberty Reserve investigations were underway, but before public law enforcement actions were taken. It's tempting to ask whether FinCEN was pressured by law enforcement to issue the guidance and whether FinCEN's analysis was influenced by law enforcement's immediate needs. We have no answers to these questions.

Assuming Anonymity Is Resolved, What Is the Appropriate Level of Consumer Protection for Cryptocurrency Users?

It appears that users of e-gold, Liberty Reserve, and perhaps Mt. Gox have lost funds entrusted with those providers. What recourse should users, and particularly consumers, have in such situations? The current state of regulatory uncertainty imperils not just cryptocurrency businesses and their investors, but also their users. Although the finality of transactions that cannot be disputed or reversed may appeal to sellers on the Silk Road,[170] ordinary, law-abiding individuals eventually will expect the same kinds of protections from unauthorized or fraudulent transactions they receive on credit and debit cards.

To demonstrate the prospective dollar value of transactions that might arise on Bitcoin or another cryptocurrency that ordinary

170. For a useful discussion on finality of payments, see Katy Jacob & Kristin E. Wells, *Evaluating the Potential for Immediate Funds Transfer for General-Purpose Payments in the United States*, CHI. FED. LETTER (Fed. Reserve Bank, Chi., Ill.) Nov. 2011, *available at* http://www.chicagofed.org/digital_assets/publications/chicago_fed_letter/2011/cfInovember2011_292a.pdf (identifying "immediate funds transfer" (IFT) as bank-to-bank transfers "with no or minimal delay in receiver's receipt and use of funds" and citing the growing availability of IFT abroad). For discussion of the use of bitcoins in Silk Road transactions, see Ball, *supra* note 23.

individuals would care about, we cite the fact that bitcoins are touted as a cost-effective alternative for individuals wanting to make remittance payments to their home countries.[171] Should (does?) the federal Remittance Transfer Rule[172] apply to cryptocurrency transactions?

Which Government Will Have Jurisdiction over Cryptocurrencies for Purposes Such as Escheat?

Assuming that the "location" of a bitcoin is resolved, regulators will have to address abandoned property issues. This might strike readers as a silly concern, but there are billions of dollars at stake and states will fight to escheat abandoned bitcoins or other cryptocurrencies or virtual currencies.[173]

Looking at other regulatory paradigms might help us predict how federal, state, and foreign governments might regulate cryptocurrencies. In particular, reviewing past regulatory approaches for the following products might prove instructive:

- online gaming;[174]

171. Joshua Brustein, *Will Migrant Workers Drive Bitcoin's Mundane Future?*, BUSINESSWEEK (Oct. 8, 2013), http://www.businessweek.com/articles/2013-10-08/will-migrant-workers-drive-bitcoins-mundane-future.

172. 12 C.F.R. pt. 1005 (2012).

173. For decisions involving the escheat of funds in gift cards, see N.J. Retail Merchs. Ass'n v. Sidamon-Eristoff, 669 F.3d 374, 396–98 (3d Cir. 2012) (affirming the district court's injunction against a "place of purchase" presumption for its jurisdictional claim to escheat priority); Am. Express Travel Related Servs. Co. v. Sidamon-Eristoff, 755 F. Supp. 2d 556, 563 (D.N.J. 2010). For discussions of these decisions, see Sarah Jane Hughes, *L'Embarras du Choix: A Year of Developments in the Laws Affecting Remittance Transfers, Credit Cards, and Certain Prepaid Cards*, 68 BUS. LAW. 233, 234, 241–42 (2012); Sarah Jane Hughes & Stephen T. Middlebrook, *Developments in the Laws Governing Electronic Payments Made Through Gift Cards, Debit and Prepaid Cards, Credit Cards, and Direct Deposits of Federal Benefits*, 66 BUS. LAW. 159, 159 (2010). For an extensive analysis of state escheat laws and their application to e-payments, see Anita Ramasastry, *State Escheat Statutes and Possible Treatment of Stored Value, Electronic Currency, and Other New Payment Mechanisms*, 57 BUS. LAW. 475, 475 (2001).

174. In particular, we note that the Unlawful Internet Gambling Enforcement Act of 2006, 31 U.S.C. §§ 5361–5367, defines a "financial transaction provider" as

> a creditor, credit card issuer, financial institution, operator of a terminal at which an electronic fund transfer may be initiated, money transmitting business, or international, national, regional, or local payment network utilized to effect a credit transaction, electronic fund

- electronic financial services that can be provided only by banks because they involve "deposits" that are subject to core banking regulations;
- electronic financial services not provided by banks and that state and federal regulators would deem to be "money transmission" under their respective statutes;[175]
- electronic financial services that do not qualify as money transmissions or as "deposits" under the definition in the Federal Deposit Insurance Corporation Act;[176] and
- forms of fractional-value "notes"—often called "shinplasters"—subject to the Stamp Payments Act of 1862 and thus, prohibited in the United States.[177]

Other reasons why governments—national governments and, in the United States, state governments—regulate media of exchange relate to ancient concerns that apply just as much to cryptocurrencies as they did to the earlier 1990s styles of "virtual currencies."[178] These concerns include widely found protections such as (1) safe storage of value; (2) redemption on predictable terms without interruptions such as those experienced by users of the Mt. Gox Bitcoin exchange in 2013; (3) protections against counterfeits or re-use or replications of the same unique "tokens"

---

transfer, stored value product transaction, or money transmitting service, or a participant in such network, or other participant in a designated payment system.

Id. § 5362(4). The gist of the Act is to make payments processing illegal if the law of the state in which the gambling occurred makes the wager or bet illegal. *Id.* § 5363.

175. *See supra* text accompanying notes 74–86.

176. *See* 12 U.S.C. § 1813(l) (2012).

177. *See* 18 U.S.C. § 336 (2006). The constitutionality of the Stamp Payments Act (which only applies to values under one dollar) and of the National Currency Act of 1863, ch. 58, § 1, 12 Stat. 665 (authorizing issuance of "greenbacks" not backed by specie), *replaced by* National Bank Act of 1864, ch. 106, 13 Stat. 99 (codified as amended in scattered sections of 12 U.S.C.), were tested in a series of United States Supreme Court decisions beginning shortly after the Civil War ended, including *United States v. Van Auken*, 96 U.S. 366 (1877) (reviewing claim of violation of the Stamp Payments Act, but holding act was not violated because the scrip was explicitly only redeemable in goods, and was not intended to circulate as money).

178. For a discussion of early e-payments products, see Sarah Jane Hughes, *A Call for International Legal Standards for Emerging Retail Electronic Payment Systems*, 15 ANN. REV. BANKING L. 197, 206–15 (1996) (describing products offered by First Virtual Holdings, Inc., DigiCash BV, and Mondex, among others).

that coins, paper currency, and even "electronic instruments" should have; and (4) seigniorage. Depending on the nature of the transaction, the federal government and the states have had widely varying regulations governing error resolution, including on the reversibility of payments, for users of credit and debit cards, payroll cards, checks, and even funds transfers.

VIII. CONCLUSION

No cryptocurrency issuer, exchanger, or user should have expected that the government of the United States—or any other government for that matter—would allow any significant storage of value in its "currency" without deciding to regulate the issuer or central exchange involved in some manner.

Why? Because that is what governments have been doing to protect both trade and their own seigniorage rights for at least the past 500 years. By 1605, for example, the English courts were already convinced of the Crown's right to control what constituted "legal tender" and who could issue "legal tender."[179] The federal government's exclusive right to issue "coins" is expressed in the U.S. Constitution.[180] When Congress enacted the Stamp Payments Act of 1862,[181] the National Currency Act of 1863,[182] and then the National Bank Act of 1864,[183] it expressed its conviction that it alone had authority to declare what qualifies as "legal tender."

---

179. *See* The Case of Mixed Money, [1605] 80 Eng. Rep. 507 (P.C.) (upholding the right of Elizabeth I of England to devalue the currency, as she had in 1601, even if it caused great suffering among the people of Ireland), *translated in* JOHN DAVIES, A REPORT OF CASES AND MATTERS IN LAW: RESOLVED AND ADJUDGED IN THE KING'S COURTS IN IRELAND [1604–1612], at 48 (1762). A key sentence from the opinion in that case proclaimed: "That it appertaineth only to the [K]ing of England, to make or coin money within his dominions; [King's prerogative in making or coining money.]" *Id.* at 51. The court also announced its conviction that there were three attributes of "money" and "legal tender" that distinguished them: the prince, the stamp, and the value. *Id.* at 52.

180. U.S. CONST. art. 1, § 8, cl. 5 ("To coin Money, regulate the Value thereof, and of foreign Coin . . . .").

181. Stamp Payments Act of 1862, ch. 196, § 2, 12 Stat. 592 (codified at 18 U.S.C. § 336 (2012)).

182. National Currency Act of 1863, ch. 58, § 1, 12 Stat. 665, *replaced by* National Bank Act of 1864, ch. 106, 13 Stat. 99 (codified as amended in scattered sections of 12 U.S.C.).

183. National Bank Act, § 1, 13 Stat. 99.

The Supreme Court agreed with Congress in a series of famous decisions beginning shortly after the National Bank Act was enacted.[184] In *Veazie Bank v. Fenno*,[185] the Supreme Court upheld Congress's imposition of a tax of ten percent imposed on state and national banks paying out "notes" of individuals or state banks used for circulation, likening this tax to the payment of duties. The Court specifically recited a number of facts about the manner in which Congress has taken charge of legal tender, including (1) denying the quality of legal tender to foreign coins, (2) providing a law against counterfeits and base coin on the community, (3) restraining the issue of notes not issued under its own authority, and (4) observing that without the power to control these aspects of legal tender, Congress's "attempts to secure a sound and uniform currency for the country must be futile."[186]

The Supreme Court was even more forceful in holding the 1860s "legal tender" acts constitutional, both as to contracts entered into before and after their passage.[187] The Court's opinion discussed the powers of the sovereign and noted that the Court would have to reverse course for its growing body of canons of

184. *See* United States v. Van Auken, 96 U.S. 366 (1877) (reviewing claim of violation of the Stamp Payments Act (which only prohibits issuance of notes with values under one dollar), but holding that the act was not violated because the scrip was explicitly only redeemable in goods and was not intended to circulate as money); Legal Tender Cases, 79 U.S. 457, 549–55 (1870), *abrogated by* Tahoe-Sierra Pres. Council, Inc. v. Tahoe Reg'l Planning Agency, 535 U.S. 302 (2002) (upholding the constitutionality of the legal tender acts as to contracts entered into both after and before their enactment, with much interesting discussion of the powers of the sovereign over currency and coinage, and holding the National Currency Act of February 25, 1863 to be valid to pay most government obligations).

185. Veazie Bank v. Fenno, 75 U.S. 533 (1869).

186. *Id.* at 549 (describing the federal government's rights under the Constitution, the claim of direct but non-apportioned taxation, and the ninth section of the Act of July 13, 1866 that imposed a ten percent tax on notes issued by banking associations chartered by the states). For additional discussion of that decision, see Nikolei M. Kaplanov, *Nerdy Money: Bitcoin, the Private Digital Currency, and the Case Against Its Regulation*, 25 LOY. CONSUMER L. REV. 111 (2012).

187. *Legal Tender Cases*, 79 U.S. at 549–55 (holding that "greenbacks" issued under the authority of the National Currency Act of February 25, 1863 were valid to pay most government obligations).

statutory construction if it did not uphold Congress's acts concerning legal tender.[188]

A government's interests are no less when one considers the authority to tax transactions and profits[189] and to impose duties on foreign transactions.[190] Thus, following its announcement that it would not require Bitcoin exchanges to register as a "money service" or "money transmitter" in the United Kingdom, Her Majesty's representatives still warned Bitcoin users about paying attention to the tax implications of their Bitcoin transactions.[191] Those representatives, however, predicted that regulation "will definitely come into play" and "so it is in the best interests of businesses that think they are transacting as a money services business to still keep anti-money laundering and know-your-customer practices in play so they're prepared for when HMRC does come knocking."[192] Soon afterwards, Her Majesty's representatives did an about-face and, following a meeting with Bitcoin U.K. representatives, announced their intention to issue regulations.[193]

Considering the different possible regulatory paradigms and the questions we raised in Part VII of this article, we find ample evidence of governments' interests in regulating cryptocurrencies in one fashion or another and of several possible ways to determine which of the competing federal-versus-state and payments-versus-securities-versus-commodities paradigms should be considered. Even among the paradigms that apply to different payments systems, options abound. The participants in transactions of this type have long had regulations governing their rights and have

188. *Id.* at 491–96.

189. For an interesting discussion of the authority to tax and the reasons for exercising that authority, see Omri Marian, *Are Cryptocurrencies Super Tax Havens?*, 112 MICH. L. REV. FIRST IMPRESSIONS 38 (2013).

190. U.S. CONST. art. 1, § 8, cl. 3.

191. *See* Emily Spaven, *HMRC: UK Bitcoin Exchanges Don't Have to Register Under Money Laundering Regulations*, COINDESK (July 8, 2013, 2:39 PM), http://www.coindesk.com/hmrc-uk-bitcoin-exchanges-dont-have-to-register-under-money-laundering-regulations/ (explaining that although there is "no specific regulation relating to digital currency" in the U.K., "standard tax rules apply" and, thus, "those who receive bitcoin in return for goods and services will have to pay tax on any profits they make").

192. *Id.*

193. Tiwari, *supra* note 164.

had, in greater and lesser degrees, government regulation of depositories and exchange/payment systems rules. Some of these regulations grew out of informal self-regulation, at least as the subjects suitable for resolution by private law or system rules—as opposed to public law—are concerned.

The federal government's action against e-gold and its 2013 regulatory guidance and law enforcement actions against Liberty Reserve and Mt. Gox persuade us that the government will exercise regulatory authority over cryptocurrencies and other virtual currencies to some extent.

Despite the tendency of new Internet-based entrants to imagine themselves to be entitled to exist and operate without regulations, a kind of unregulated Wild West attitude, the old-fashioned notions of why we regulate payments and value-storage media that we discuss in this article suggest to us that regulation will happen, and that its challenges will be similar to those faced since kings and princes first issued coins and then issued other indicia of stored value such as paper "money" that qualified for use as "legal tender."

The idea that governments issue "money" and declare what qualifies as "legal tender" is an ancient notion. The history of regulating money and legal tender suggests that it is not likely that governments will surrender their privileges to regulate cryptocurrency issuers, exchanges, administrators, or users. The real questions are which paradigm(s) governments will use, how much enforcement energy they will spend on regulating cryptocurrencies, and whether and how they will compete with each other to offer regulatory schemes that do not send cryptocurrency entrepreneurs, investors, and users running offshore.