VIRTUAL CURRENCIES; BITCOIN & WHAT NOW AFTER LIBERTY RESERVE, SILK ROAD, AND MT. GOX?

Lawrence Trautman*

Cite as: Lawrence Trautman, *Virtual Currencies Bitcoin & What Now After Liberty Reserve, Silk Road, and Mt. Gox?*, 20 RICH. J.L. & TECH. 13 (2014), http://jolt.richmond.edu/v20i4/article13.pdf.

I. OVERVIEW

[1] During 2013, the U.S. Treasury Department evoked the first use of the 2001 Patriot Act[1] to exclude virtual currency provider Liberty Reserve from the U.S. financial system.[2] This article will discuss: the regulation of virtual currencies, cybercrimes and payment systems, darknets, Tor and the "deep web," Bitcoin; Liberty Reserve, Silk Road, and Mt. Gox. Virtual currencies have quickly become a reality, gaining significant traction in a very short period of time, and are evolving rapidly. Virtual

* Thanks to the following for their assistance in the research and preparation of this article: Timothy Bauman, Edward W. Felten, Urs Gasser, Reuben Grinberg, Alvin Harrell, Tomas Olov Larsson, Vili Lehdonvirta, Tyler Moore, John Palfrey, Nicholas Plassaras, Ariel Rabkin, Mina Rady, Ulrike Schultz, Robin Teigland, John Trautman, François Velde, Ruoke Yang, Zeynep Yetis and Jonathan Zittrain. All errors and omissions are my own.

[1] *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001, Pub. L. No. 107-56, § 224(b), 115 Stat. 272, 295; *see also* Orin S. Kerr, *Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't*, 97 NW. U. L. REV. 607 (2003), *available at* http://ssrn.com/abstract=317501.

[2] Press Release, Department of the Treasury, Treasury Identifies Virtual Currency Provider Liberty Reserve as a Financial Institution of Primary Money Laundering Concern under USA Patriot Act Section 311 (May 28, 2013), *available at* http://www.treasury.gov/press-center/press-releases/Pages/jl1956.aspx; *see also* Press Release, Department of Justice, Co-founder of Liberty Reserve Pleads Guilty to Money Laundering in Manhattan Federal Court, (Oct. 31, 2013), *available at* http://www.justice.gov/opa/pr/2013/October/13-crm-1163.html.

currencies present particularly difficult law enforcement challenges because of their ability to transcend national borders in the fraction of a second, unique jurisdictional issues and anonymity due to encryption. Due primarily to their anonymity, virtual currencies have been linked to numerous types of crimes, including facilitating marketplaces for: assassins, attacks on businesses, the exploitation of children (including pornography), corporate espionage, counterfeit currencies, drugs, fake IDs and passports, high yield investment schemes (Ponzi schemes and other financial frauds), sexual exploitation, stolen credit cards and credit card numbers, and weapons.

[2] Innovation in the pace of developing new currencies and technologies continues to create ongoing challenges for responsible users of technology and regulators alike. While technological advances create great opportunities to improve the health, living conditions, and general wellbeing of mankind; new technologies also create great challenges for nation states. Reminiscent of Lawrence Lessig's comment that "code is law,"[3] James Grimmelman observes, "[u]nlike the rule of law, the rule of software is simple and brutal: whoever controls the software makes the rules. And if power corrupts, then automatic power corrupts automatically."[4]

A. Structure of This Paper

[3] This paper is organized as follows. In Section II, a background describing virtual currencies, cybercrimes and payment systems is presented. Section III depicts the regulation of Internet payments. Section IV discusses and explores the mechanism, promise, ecosystem, and vulnerabilities of Bitcoin. In Section V, Liberty Reserve is discussed, with

[3] *See generally* LAWRENCE LESSIG, CODE (Basic Books 2d ed. 2006), *available at* http://codev2.cc/download+remix/Lessig-Codev2.pdf (discussing how code is cyberspace's law).

[4] James Grimmelmann, *Anarchy, Status Updates, and Utopia*, 34 PACE L. REV. (forthcoming 2014), *available at* http://ssrn.com/abstract=2358627.

the implications from Silk Road presented in Section VI. In Section VII, the demise of Mt. Gox is described. Section VIII depicts the collateral impact on Bitcoin from the failures of Liberty Reserve, Silk Road and Mt. Gox, and posits scenarios for Bitcoin's likely future. Implications for further research are then presented.

II. VIRTUAL CURRENCIES, CYBERCRIMES & PAYMENT SYSTEMS

What is a Virtual Currency?

[4] The U.S. Government Accountability Office (GAO) observes that "[t]here are no legal definitions for a virtual economy or currency."[5] However, "[a] virtual currency is, generally, a digital unit of exchange that is not backed by a government-issued legal tender. Virtual currencies can be used entirely within a virtual economy, or can be used in lieu of a government-issued currency to purchase goods and services in the real economy."[6]

[5] FinCEN defines *virtual currency* as "those currencies that operate like a currency in some environments, but does not have legal tender status in any jurisdiction."[7] Mythili Raman defines *virtual currency* as "a

[5] *See* U.S GOV'T ACCOUNTABILITY OFFICE, GAO-13-516, VIRTUAL ECONOMIES AND CURRENCIES: ADDITIONAL IRS GUIDANCE COULD REDUCE TAX COMPLIANCE RISKS 3 (2013).

[6] *Id.*

[7] *Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies: Hearing Before the S. Comm. on Homeland Security & Governmental Affairs*, 113th Cong. (Nov. 18, 2013) (statement of Edward W. Lowery III, Special Agent in Charge, Criminal Investigative Division, U.S. Secret Service) (citing DEPARTMENT OF TREASURY FINANCIAL CRIMES ENFORCEMENT NETWORK, GUIDANCE FIN-2013-G0001, APPLICATION OF FINCENS'S REGULATIONS TO PERSONS ADMINISTERING, EXCHANGING, OR USING VIRTUAL CURRENCIES (Mar. 18, 2013)).

medium of exchange circulated over a network, typically the Internet, which is not backed by a government."[8] Moreover

> Early centralized models, where the currency is controlled by a single private entity, have expanded and now encompass a wide range of business concepts. Some centralized virtual currencies take the form of digital precious metals, such as e-Gold and Pecunix, where users exchange digital currency units ostensibly backed by gold bullion or other precious metals. Others exist within popular online games or virtual worlds, such as Farmville, Second Life, or World of Warcraft. Still others are online payment systems such as WebMoney and Liberty Reserve, which are available generally outside of specific online communities and denominate users' accounts in virtual currency rather than U.S. Dollars, Euros, or some other national currency. Decentralized systems such as Bitcoin, which have no centralized administrating authority and instead operate as peer-to-peer transaction networks, entered the scene relatively recently but are growing rapidly. A network of sites and services, including exchangers who buy and sell virtual currencies in exchange for national currencies or other mediums of value, have developed around virtual currency systems, as well.[9]

[8] Press Release, Department of Justice, Acting Assistant Attorney General Mythili Raman Testifies Before the Senate Committee on Homeland Security and Governmental Affairs (Nov. 18, 2013), *available at* http://www.justice.gov/criminal/pr/speeches/2013/crm-speech-131118.html.

[9] *Id.*

[6] The forerunner to today's virtual currency may be found in a 1982 paper by computer scientist David Chaum.[10] In 1990, Mr. Chaum founded DigiCash which unfortunately failed during 1999.[11] Aleksandra Bal notes that unlike electronic money, where the "traditional money format is preserved, as the stored funds are expressed in the same unit of account (for example US dollars or euros). In virtual currency schemes, the unit of account is changed into a virtual one (for example, Linden Dollars or Bitcoins)."[12] Indeed, the genesis of virtual currency appears to result from the massive popularity of online games.[13] Boston University's Mark

[10] *See* David Chaum, *Blind Signatures for Untraceable Payments*, In ADVANCES IN CRYPTOLOGY: PROCEEDINGS OF CRYPTO 82 (1982), *available at* http://link.springer.com/chapter/10.1007%2F978-1-4757-0602-4_18.

[11] *FM Interviews: David Chaum*, FIRST MONDAY (July 1999), *available at* http://firstmonday.org/ojs/index.php/fm/rt/article/view/683/593.

[12] Aleksandra Bal, *Stateless Virtual Money in the Tax System*, 53 EUROPEAN TAXATION 351, 351 (July 2013), *available at* http://ssrn.com/abstract=2298537.

[13] *See generally* David A. Bray & Benn Konsynski, *Virtual Worlds: Multi-Disciplinary Research Opportunities*, 38 THE DATA BASE FOR ADVANCES IN INFORMATION SYSTEMS, Nov. 2007, at 17, *available at* http://ssrn.com/abstract=1016485 (discussing how virtual worlds offer significant opportunities for research in many fields of research); Hiroshi Yamaguchi, *An Analysis of Virtual Currencies in Online Games* (Sep. 1, 2004), *available at* http://ssrn.com/abstract=544422 (analyzing the economic and monetary system of online games and discussing its implications in the real economy); Jun-Sok Huhh, *An Economic Analysis on Online Game Service* (Aug. 28, 2009), *available at* http://ssrn.com/abstract=1335120 (investigating economic problems of a firm providing online game services); Levent V. Orman, *Virtual Money in Electronic Markets and Communities* (Cornell University, Johnson School Research Paper Series No. 27-2010, June 2010), *available at* http://ssrn.com/abstract=1621725 (asserting that virtual money can benefit money semantics and management); Matthew Elias, *Bitcoin: Tempering the Digital Ring of Gyges or Implausible Pecuniary Privacy* (Oct. 3, 2011), *available at* http://ssrn.com/abstract=1937769 (comparing different forms of digital currencies to Bitcoin); Sukwon Thomas Kim, *Why Bitcoin?: Structure and Efficiency of Markets for Online Game Currency* (Dec. 18, 2013), *available at* http://ssrn.com/abstract=2334000 (analyzing markets for online game currencies); Sulin Ba & Dan Ke, *Optimal Pricing and Permissions Strategy for Virtual Good Creators in Second Life* (Sept. 15, 2008), *available at* http://ssrn.com/abstract=1271684 (discussing the impact of virtual worlds on "the way people cooperate, communicate, and conduct business"); Vili Lehdonvirta,

Williams observes that "Bitcoin has not been recognized by any of the G20 countries as meeting the definition of currency as it lacks price stability and does not provide a stable store of value. As a result it is a speculative virtual commodity with no tangible value."[14]

A. Illicit Use of Virtual Currencies

[7] In his testimony before the U.S. Senate Committee on Homeland Security and Governmental Affairs, Mythili Raman observes that virtual currencies present two primary law enforcement interests to the Department of Justice (DOJ),

> (1) deterring and prosecuting criminals using virtual currency systems to move or hide money that is used to facilitate, or is derived from, criminal or terrorist acts, *i.e.*, money laundering; and (2) investigating and prosecuting those virtual currency services that themselves violate laws aimed at illegal money transmission and money laundering.[15]

Virtual Item Sales as a Revenue Model: Identifying Attributes that Drive Purchase Decisions, 9 ELECTRONIC COMMERCE RESEARCH 97 (2009), *available at* http://ssrn.com/abstract=1351769 (analyzing the what drives virtual spending); Vili Lehdonvirta, *Real-Money Trade of Virtual Assets: New Strategies for Virtual World Operators*, *in* VIRTUAL WORLDS 113 (Mary Ipe ed., Icfai University Press 2008), *available at* http://ssrn.com/abstract=1351782 (exploring the implications of trading virtual currencies for real money).

[14] *Hearing Regarding Virtual Currencies Before the New York State Department of Financial Services* (Jan. 28-29, 2014) (statement of Mark T. Williams, Banking Specialist, Commodities and Risk Management Expert, Finance Department, Boston University), *available at* http://www.dfs.ny.gov/about/hearings/vc_01282014/williams.pdf. *See generally* David Yermack, *Is Bitcoin a Real Currency?* (Dec. 1, 2013), *available at* http://ssrn.com/abstract=2361599 (discussing whether bitcoin is a real currency).

[15] Raman, *supra* note 8, at 1.

[8] Digital currencies are believed by the U.S. Secret Service to be preferred by criminals because they offer

> 1. The greatest degree of anonymity for both users and transactions.
> 2. The ability to quickly and confidently move illicit proceeds from one country to another.
> 3. Low volatility, which results in lower exchange risk, increasing the digital currency's ability to be an efficient means to transmit and store wealth.
> 4. Widespread adoption in the criminal underground.
> 5. Trustworthiness.[16]

Mythili Raman further explains

> Criminals are nearly always early adopters of new technologies and financial systems, and virtual currency is no exception. As virtual currency has grown, it has attracted illicit users along with legitimate ones. . . . [S]ome criminals have exploited virtual currency systems because of the ability of those systems to conduct transfers quickly, securely, and often with a perceived higher level of anonymity than that afforded by traditional financial services. The irreversibility of many virtual currency transactions additionally appeals to a variety of individuals seeking to engage in illicit activity, as does their ability to send funds cross-border.[17]

[16] Lowery, *supra* note 7. *But see* E-mail from Ariel Rabkin, Postdoctoral Researcher, Computer Science Department, Princeton University (Feb. 23, 2014, 16:59 CST) (on file with author) (observing that Bitcoin prices have been famously volatile); *and* Danton Bryans, Note, *Bitcoin and Money Laundering: Mining for an Effective Solution*, 89 IND. L.J. 441, 441 (2014), *available at* http://ilj.law.indiana.edu/articles/19-Bryans.pdf.

[17] Raman, *supra* note 8, at 2.

[9] Virtual currencies, due primarily to their anonymity, have been linked to numerous types of crimes, including facilitating marketplaces for: assassins, attacks on businesses, exploiting children (including pornography), corporate espionage, counterfeit currencies, drugs, fake IDs and passports, high yield investment schemes (Ponzi schemes and other financial frauds), sexual exploitation, stolen credit cards and credit card numbers, and weapons.[18]

B. Marketplace for Assassins

[10] The diversity of illicit content available on underground message boards is truly astonishing. Trend Micro, a member of the Digital Economy Task Force reports "privately maintained sites that offer specific types of goods and services. Some are pages with prices and contact information for anonymous orders and others provide a full order and payment management system . . . include[ing] hired assassins."[19] A New York Times article regarding the website Silk Road and alleged exploits of

[18] *See Beyond Silk Road: Potential Risks, Threats and Promises of Virtual Currencies: Hearings Before the S. Comm. on Homeland Sec. & Governmental Affairs*, 113th Cong. (2013) (statement of Ernie Allen, President & CEO, The International Centre for Missing & Exploited Children); *see also* Christopher Bronk, Cody Monk & John Villasenor, *The Dark Side of Cyber Finance,* 54 Survival: Global Politics & Strategy 129 (2012); Raman, *supra* note 8; Fernando M. Pinguelo & Bradford W. Muller, *Virtual Crimes, Real Damages: A Primer on Cybercrimes in the United States and Efforts to Combat Cybercriminals*, 16 VA. J.L. & TECH. 116, 119 (2011); Malte Möser, Rainer Böhme & Dominic Breuker, *An Inquiry into Money Laundering Tools in the Bitcoin Ecosystem, in Proceedings of the APWG eCrime Researchers Summit*, San Francisco (ECRIME 2013), *available at* http://maltemoeser.de/paper/money-laundering.pdf; William Hett, *Digital Currencies and the Financing of Terrorism,* 15 RICH. J.L. & TECH. 4, ¶ 10 (2008), http://law.richmond.edu/jolt/v15i2/article4.pdf.

[19] *Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies: Hearings Before the S. Comm. on Homeland Sec. & Governmental Affairs,* 113th Cong. (2013) (statement of Ernie Allen, President & CEO, The International Centre for Missing & Exploited Children).

Ross William Ulbricht, a/k/a "Dread Pirate Roberts," points to a Baltimore criminal complaint depicting the solicitation of several killings.[20]

C. Attacks on Businesses

[11] Examples of hacking attacks on businesses are recited daily by virtually every major news source. Pinguelo and Muller observe that "[a]ttacks on businesses include such things as the theft of intellectual property, seizing bank accounts, generating and distributing malware, and other disruptive activity."[21] Cybersecurity experts from the law enforcement community observe that many of these illicit cyber services are routinely available and purchased with virtual currencies.[22]

D. Child Exploitation

[12] In his November 18, 2013 testimony before the U.S. Senate Committee on Homeland Security and Governmental Affairs, Ernie Allen, President & CEO of the International Center for Missing and Exploited Children (ICMEC), expresses concern about "the apparent migration of commercial child sexual exploitation, including sex abuse images, child exploitation and sex trafficking, along with other criminal enterprises to a new unregulated digital economy, made up of digital currencies;

[20] David Segal, *Eagle Scout. Idealist. Drug Trafficker?*, N.Y. TIMES (Jan. 18, 2014), http://www.nytimes.com/2014/01/19/business/eagle-scout-idealist-drug-trafficker.html.

[21] Pinguelo & Muller, *supra* note 18, at 119; *see also* Lawrence J. Trautman, *E-Commerce and Electronic Payment System Risks: Lessons from PayPal*, 17 SMU SCIENCE & TECHNOLOGY LAW REVIEW (2014), *available at* http://www.ssrn.com/abstract=2314119; Lawrence J. Trautman, Jason Triche & James C. Wetherbe, *Threats Escalate: Corporate Information Governance Under Fire*, 8 JOURNAL OF STRATEGIC & INTERNATIONAL STUDIES 105 (2013), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2171026; Lawrence J. Trautman & Kara Altenbaumer-Price, *The Board's Responsibility for Information Technology Governance*, 28 J. MARSHALL J. COMPUTER & INFO. L., 313 (2011).

[22] Raman, *supra* note 8, at 2.

anonymous online payment systems; anonymous internet tools; and file hosting companies."[23] Examples of large scale providers of child pornography are numerous. Accordingly,

> In August 2013 the Irish founder/owner/operator of Freedom Hosting, which the FBI called 'the largest facilitator of child pornography on the planet,' was arrested. Freedom Hosting maintained servers for a number of Tor-based, so-called 'deep web' child pornography sites and others. The best-known child pornography sites included Lolita City, the Love Zone and PedoEmpire, all of which accept Bitcoins for payment.
>
> To shut down Freedom Holdings, law enforcement exploited a 'java script exploit,' a vulnerability in the site, enabling law enforcement to penetrate Tor and expose the IP addresses of the users of Freedom Hosting. Interestingly, in 2011 the hacktivist group, Anonymous, hacked into Tor to shut down Lolita City. However, Lolita City has reemerged with an estimated 15,000 members and 1.5 million child pornography images.[24]

[23] *See* Allen, *supra* note 19; *see generally* Mark Latonero, *Technology and Human Trafficking: The Rise of Mobile and the Diffusion of Technology-Facilitated Trafficking* (Nov. 13, 2012), *available at* http://ssrn.com/abstract=2177556 (discussing the role of modern technologies in facilitating and combating human trafficking); Mark Latonero, *Human Trafficking Online: The Role of Social Networking Sites and Online Classifieds* (Sept. 1, 2011), *available at* http://ssrn.com/abstract=2045851 (examining the "role of social networking cites and online classified ads in facilitating human trafficking"); Danah Boyd, Heather Casteel, Mitali Thakor & Rane Johnson, *Human Trafficking and Technology: A Framework for Understanding the Role of Technology in the Commercial Exploitation of Children in the U.S., available at* http://research.microsoft.com/en-us/collaboration/focus/education/htframework-2011.pdf (discussing the role technology plays in human trafficking).

[24] Allen, *supra* note 19.

[13] In another case known as Dreamboard, various measures were employed to conceal the sale of child exploitation images and videos over the Internet, including: the use of screen names or aliases rather than actual names, all links to pornography were encrypted requiring passwords only available to members, and all Internet access traffic was routed through proxy servicers and sent through a pathway involving multiple nodes designed to "disguise a user's actual location and prevent law enforcement from tracing Internet activity. Dreamboard members also encouraged the use of encryption programs on their computers, which password-protect computer files to prevent law enforcement from accessing them in the event of a court-authorized search."[25]

[14] In addition to those already cited, other child pornography sites mentioned by ICMEC as accepting payment in digital currencies include Hard Candy, Jailbait and others.[26] During December 2013, Acting Assistant Attorney General Raman announced the creation of a task force to counter online child exploitation, observing that "[s]exual predators are using technology to exploit and harm children, and we need to consider whether technology-based solutions can help curb this abuse . . . we know that the help and support of the innovators in the tech community are critical."[27]

E. Corporate Espionage

[15] Corporate espionage is rampant. Technology provides sophisticated tools to those who would seek to steal the intellectual

[25] Press Release, Department of Justice, Dreamboard Member Sentenced to 45 Years in Prison for Participating in International Criminal Network Organized to Sexually Exploit Children (Jan. 8, 2013), *available at* http://www.justice.gov/opa/pr/2013/January/13-crm-034.html.

[26] *See* Allen, *supra* note 19.

[27] Press Release, Department of Justice, U.S., U.K. Law Enforcement Launch Task Force to Counter Online Child Exploitation (Dec. 11, 2013), *available at* http://www.justice.gov/opa/pr/2013/December/13-crm-1299.html.

property assets that represent future economic stability, jobs for our children, and the promise of a society that moves forward in peace. Assistant Director Richard McFeely states, "[t]he FBI will not stand by and watch the hemorrhage of U.S. intellectual property to foreign countries who seek to gain an unfair advantage for their military and their industries . . . Since 2008, our economic espionage arrests have doubled; indictments have increased five-fold; and convictions have risen eight-fold."[28] Testimony reveals that many of the illicit cyber services involved with corporate espionage are routinely available and purchased with virtual currencies.[29]

F. Drugs

[16] Having started as an organized, illicit, cross-border activity, drug trafficking now constitutes a serious threat to nation states because of its close alliance with worldwide terrorist groups.[30] Silk Road, described as the "Amazon for Drugs," is perhaps the most significant example of a site reported to have been responsible for major sales, "[y]et, barely one month later the site is back up and is operating again."[31] Liberty Reserve, the

[28] Press Release, Department of Justice, Sinovel Corporation and Three Individuals Charged in Wisconsin with Theft of Amsc Trade Secrets (June 27, 2013), *available at* http://www.justice.gov/opa/pr/2013/June/13-crm-730.html*; see also* Pinguelo & Muller, *supra* note 18 at 126; Joshua Nathan Aston, *Narco-Terrorism – A Critical Study* (Jan. 29, 2013), *available at* http://ssrn.com/abstract=2221590.

[29] *See generally* Raman, *supra* note 8 (noting the appeal of virtual currencies to criminals); Trautman, Triche & Wetherbe, *supra* note 21(examining cyber security threats).

[30] *See generally* Aston, *supra* note 28 (observing that transnational organized crime is considered as one of the major threats to human security, impeding the political, social, economic, and cultural development of societies worldwide).

[31] Allen, *supra* note 18. *But see* Jose Pagliery, *Drug Site Silk Road Wiped Out by Bitcoin Glitch*, CNN MONEY (Feb. 14, 2014, 11:16 AM) http://money.cnn.com/2014/02/14/technology/security/silk-road-bitcoin/ (reporting Silk Road victim of hacking loss of $2.7 million).

other major digital currency service to receive focus in this paper, "allegedly laundered more than $6 billion in suspected proceeds of crimes."[32] The DOJ's announcement of Vladimir Kats' guilty plea reports that before operations were stopped during May 2013, "Liberty Reserve had more than one million users worldwide, including more than 200,000 users in the United States who conducted approximately 55 million transactions through its system and allegedly laundered more than $6 billion in suspected proceeds of crimes, including . . . narcotics trafficking."[33] Other arrests have been reported. For example, "in February [2013] Australian police arrested a cocaine dealer operating on Silk Road and being paid in Bitcoins. In May [2013] Israeli police broke up a drug distribution ring operating in Bitcoins."[34]

G. Fake IDs and Passports

[17] Just one of many cases involving the use of and sale of false identities and counterfeit certificates of title, the U.S. Department of Justice reported in October, 2013 that Romanian fugitive Nicolae Popescu and his criminal syndicate held non-existent high-value items such as boats, cars, and motorcycles − priced generally between $10,000 to $45,000 − and "produced and used high-quality fake passports . . . as identification by co-conspirators in the United States to open bank accounts."[35] In this and similar cases, the DOJ reported that "the illicit

[32] Press Release, Department of Justice, Co-Founder of Liberty Reserve Pleads Guilty to Money Laundering in Manhattan Federal Court (Oct. 31, 2013), *available at* http://www.justice.gov/opa/pr/2013/October/13-crm-1163.html.

[33] *Id.*

[34] Allen, *supra* note 18; *see* Segal, *supra* note 20, ¶ 2 (citing $1.2 billion of transactions, many for cocaine, heroin and LSD).

[35] Press Release, Department of Justice, Indictment Unsealed and "Wanted" Posters Issued for Fugitives Charged With Multimillion Dollar International Cyber Fraud Scheme (Oct. 24, 2013), *available at* http://www.justice.gov/opa/pr/2013/October/13-crm-1128.html.

proceeds were then withdrawn from the U.S. bank accounts and sent to the defendants in Europe by wire transfer and other methods [often virtual currencies]."[36]

H. High Yield Investment Schemes

[18] Ponzi schemes and other forms of financial frauds seem to find virtual currencies attractive. Observing that "cyber criminals were among the first illicit groups to take widespread advantage of virtual currency," Acting Assistant Attorney General Raman stated that "high-yield investment schemes" are among the types of crimes conducted with the use of virtual currencies.[37]

I. Sexual Exploitation

[19] Recent Congressional hearings produced testimony revealing that "[w]hile much of the evidence is still anecdotal, there is consensus that . . . sexual exploitation, sex trafficking and other criminal enterprises are increasingly moving to a new unregulated, unbanked digital economy."[38]

[36] *Id.*

[37] Raman, *supra* note 8. *See generally* Tyler Moore, Jie Han & Richard Clayton, *The Postmodern Ponzi Scheme: Empirical Analysis of High-Yield Investment Programs*, *in* FINANCIAL CRYPTOGRAPHY AND DATA SECURITY 41 (Angelos D. Keromytis, Ed., 2012), *available at* http://link.springer.com/book/10.1007%2F978-3-642-32946-3 (describing an extensive online ecosystem that has developed in support of these HYIPs, including discussion websites, digital currencies, and third-party aggregator websites that track HYIP performance); Reuben Grinberg, *Bitcoin: Today Techies, Tomorrow* the World?, MILKEN INST. REV. 22, 24 (First Quarter 2012), *available at* http://www.milkeninstitute.org/publications/review/2012_1/22-31MR53.pdf (discussing the criminal use of Bitcoin).

[38] Allen, *supra* note 18; *see also* Latonero, *supra* note 23.

J. Stolen Credit Cards

[20] Just one of the many examples of the sale of credit card or personally identifiable information (PII) involving hundreds of thousands of American's accounts is found in the DOJ's 15-count indictment of Vietnamese national, Hieu Minh Ngo, age 24, "charging him with conspiracy to commit wire fraud, substantive wire fraud, conspiracy to commit identity fraud, substantive identity fraud, aggravated identity theft, conspiracy to commit access device fraud, and substantive access device fraud."[39] The DOJ further states that "Ngo and his co-conspirators created one or more accounts with a digital currency service and used those accounts to receive funds for the stolen payment card data, 'fullz' and other PII that they sold."[40]

K. Darknets, Tor & the "Deep Web"

[21] Although not the specific cryptographic tool used to produce virtual currencies such as (potentially anonymous) Bitcoin, a number of "deep web" tools exist to ensure privacy and deserve brief mention here. These cryptographic tools may be used for both good and evil acts. For example, many sites dealing in illegal drugs and other illicit goods and

[39] Press Release, Department of Justice, Vietnamese National Charged in Widespread International Scheme to Steal and Sell Hundreds of Thousands of U.S. Persons' Personally Identifiable Information (Oct. 18, 2013), *available at* http://www.justice.gov/opa/pr/2013/October/13-crm-1116.html.

[40] *Id.*; *see also* Press Release, Department of Justice, Romanian National Sentenced to 21 Months in Prison for Role in Multimillion-Dollar Scheme to Remotely Hack into and Steal Payment Card Data from Hundreds of U.S. Merchants' Computers (Jan. 7, 2013), *available at* http://www.justice.gov/opa/pr/2013/January/13-crm-028.html; Press Release, Department of Justice, International Cybercriminal Extradited from Thailand to the United States (May 3, 2013), *available at* http://www.justice.gov/opa/pr/2013/May/13-crm-502.html; Trautman, Triche & Wetherbe, *supra* note 21 (providing a recent account of credit card fraud and corporate cybersecurity risk); Trautman & Altenbaumer-Price, *supra* note 21.

services such as Silk Road and Black Market Reloaded rely on anonymous proxy network *Tor* "to prevent law enforcement from identifying the sites' operator and users."[41]

[22] Anonymizing tools such as *Tor* have provided significant benefits to enable secure communications for: governments, law enforcement agencies, businesses; journalists as they work to communicate with dissidents and send confidential news, enabled oppressed peoples during the "Arab Spring" to overthrow oppressive regimes, and influenced governmental change recently in Egypt in large measure by enabling individuals and political activist groups to communicate privately with reduced fear of reprisals.[42] Other groups such as "the Electronic Frontier Foundation (EFF) recommend Tor as a mechanism for maintaining civil liberties online. Corporations use Tor as a safe way to conduct competitive analysis, and to protect sensitive procurement patterns from eavesdroppers."[43]

[23] Tor in its present form is an outgrowth of "[T]he [O]nion [R]outing" (TOR) project, (as in pealing back the layers of an onion), originally funded and nurtured by the U.S. Naval Research Laboratory.[44] To mask a users identity disclosed by a senders or receivers' header information (traffic analysis), the Tor system distributes a transaction

[41] Timothy Bauman, Commerce and Reputation in Online Illegal Drug Markets (Apr. 3, 2013) (unpublished Senior Thesis, Woodrow Wilson School of Public and International Affairs, Princeton University) *available at* http://arks.princeton.edu/ark:/88435/dsp01sq87bt70p.

[42] *See generally* Mina Rady, *Anonymity Networks: New Platforms for Conflict and Contention* 22 (MIT Political Science Department, Research Paper No. 2013-5), *available at* http://ssrn.com/abstract=2241536 (discussing the various consequences of anonymity network).

[43] *Tor: Overview*, TOR PROJECT, *available at* https://www.torproject.org/about/overview.html.en (last visited April 10, 2014).

[44] *Id.*

"over several places on the Internet, so that no single point can link you to your destination."[45] Bauman observes that *Tor*

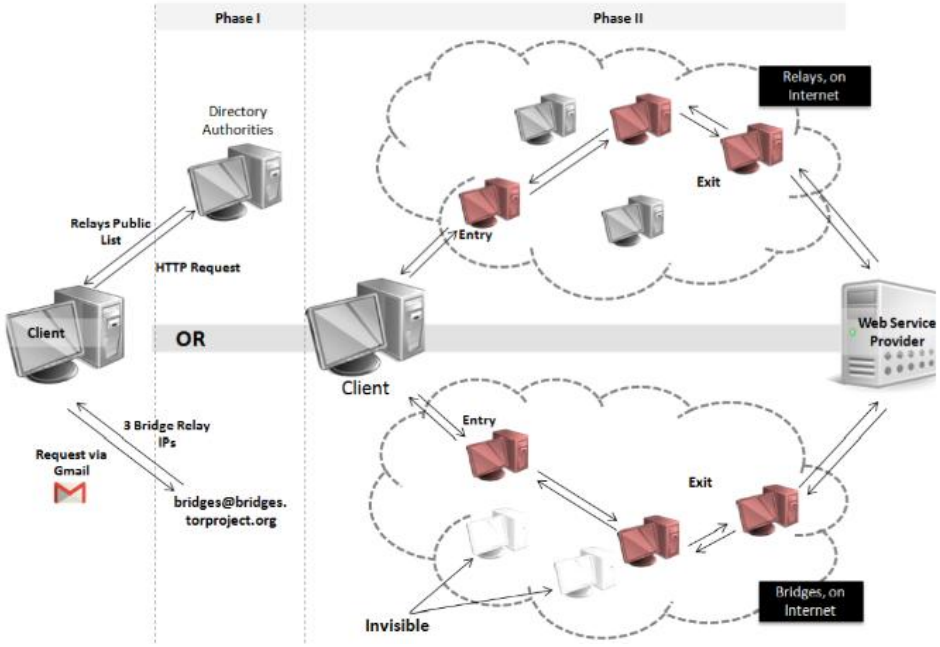
> Prevents traffic analysis by encrypting both the header and the content and sending them both through a series of proxy servers, known as nodes, each of which knows only the identities of the adjacent proxies in the chain. Every node in the chain would have to be compromised for an attacker to discover both the originator and the recipient of a packet. This allows for a near-guarantee of anonymity as long as at least one node in the chain is trusted, and as long as there are enough other users of the Tor network that an individual's traffic is hard to identify . . . Tor relays exist all over the world, which helps them effectively anonymize traffic. The two countries with the most relays are the United States, with about 800, followed by Germany with about 500. More than 300 list their country code as "zz," which does not correspond to a real country, thereby attempting to hide the country of that relay.[46]

A graphic depiction of a Tor network is presented at Figure 1.

[45] *The Solution: A Distributed, Anonymous Network*, TOR PROJECT, *available at* https://www.torproject.org/about/overview.html.en (last visited April 10, 2014) [hereinafter *The Solution*].

[46] Bauman, *supra* note 41 at 12 (*citing* Roger Dingledine, Nick Mathewson & Paul Syverson, *Tor: The Second-generation Onion Router*, Naval Research Lab, Wash. D.C. (2004); *see also Tor Metrics Portal: Network*, TOR PROJECT, *available at* https://metrics.torproject.org/network.html (last viewed April 10, 2014)).

Overview of Tor Mechanism[47]



[24] The Tor network directs message packets to take a random path through numerous difficult-to-identify interim relays rather than the most direct route, thereby covering a messenger's "tracks so no observer at any single point can tell where the data came from or where it's going."[48] Tor works by constructing a circuit of encrypted network relay connections to create a unique secured private pathway for information or transaction flow. According to the Tor project

> The circuit is extended one hop at a time, and each relay along the way knows only which relay gave it data and

[47] Rady, *supra* note 42 at 6.

[48] *The Solution*, *supra* note 45.

> which relay it is giving data to. No individual relay ever knows the complete path that a data packet has taken. The client negotiates a separate set of encryption keys for each hop along the circuit to ensure that each hop can't trace these connections as they pass through.
>
> Once a circuit has been established, many kinds of data can be exchanged and several different sorts of software applications can be deployed over the Tor network. Because each relay sees no more than one hop in the circuit, neither an eavesdropper nor a compromised relay can use traffic analysis to link the connection's source and destination. Tor only works for TCP [Transmission Control Protocol] streams and can be used by an application with SOCKS [Socket Secure] support.[49]

[25] Tor hidden services offers an environment where users may instant message or publish materials and keep their locations anonymous by "[u]sing Tor 'rendezvous points,' other Tor users can connect to these hidden services, each without knowing the other's network identity . . . . Nobody [is] able to determine who [is] offering the site, and nobody who offered the site would know who [is] posting to it."[50]

[26] It should come as no surprise that criminals are attracted to the ability to communicate and conduct financial transactions on an anonymous basis. These "[o]nline black markets capitalize on Tor's

[49] *Id.*

[50] The Tor Project, *Hidden Services, available at* https://www.torproject.org/about/overview.html.en; *see also* Nassim Nazemi, *Note and Comment: DMCA § 512 Safe Harbor for Anonymity Networks Amid a Cyber-Democratic Storm: Lessons from the 2009 Iranian Uprising,* 106 NW. U.L. REV. 855, 868-70 (2012). *But see* Nicholas Hopper, *Short Paper: Challenges in Protecting Tor Hidden Services From Botnet Abuse, available at* http://ifca.ai/fc14/papers/fc14_submission_152.pdf (describing the potential for a decrease in the privacy of hidden service users).

anonymizing features to offer a wide selection of illicit goods and services . . . ."[51]

III. REGULATION OF INTERNET PAYMENTS

[27] With the volume of online transactions achieving tremendous growth during the past two decades, the ability to securely accept online payments has become profoundly important for global business.[52] Unfortunately, as Fred Chang observes, "[o]ur trust in cyberspace has been taken from us by hackers, cybercriminals and sophisticated cyber attackers who intend to do us harm . . . . Attacks on both the public sector and the private sector are rampant. Denial of service, identity theft, and cyber extortion are now all too common."[53] Therefore, "[c]reating and protecting trust . . . becomes a crucial issue in the regulation of payment services . . . . It is generally accepted that adequate regulation is a key pre-cursor to consumer acceptance of new payment methods, including mobile banking and payments."[54] Regulation should reflect the ethical

[51] Raman, *supra* note 8, at 2. *But see* Andrew Grossman, *Federal Agents Pierce Tor Web-Anonymity Tool*, WALL ST. J. (Mar. 31, 2014), http://online.wsj.com/news/articles/SB10001424052702303949704579461641349857358 (contending that Tor's anonymity shield isn't impenetrable).

[52] *See, e.g.*, Paul Benjamin Lowry, Taylor Michael Wells, Greg Moody, Sean Humphreys & Degan Kettles, *Online Payment Gateways Used to Facilitate E-Commerce Transactions and Improve Risk Management*, 17 Comm. of the Ass'n for Info. Sys. (CAIS) 1, 3 (2006) *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=879797; *see also* Brian Mantel & Timothy McHugh, *Competition and Innovation in the Consumer e-Payments Market? Considering the Demand, Supply, and Public Policy Issues* 33 (Emerging Payments Occasional Working Paper Series, Paper No. EPS-2001-4, 2001) *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=298388.

[53] *Hearing on Cyber R&D Challenges and Solutions Before the Subcomm. on Tech., Subcomm. on Research, & H. Comm. on Sci., Space & Tech.*, 113th Cong. (2013) (statement of Frederick R. Chang, President & COO, 21CT, Inc.).

[54] Rhys Bollen, *The Legal Status of Online Currencies: Are Bitcoins the Future?*, J. BANKING & FIN. L. & PRAC. 1, 38 (2013), *available at* http://ssrn.com/abstract=2285247.

implications of payment systems and virtual currencies such as Bitcoin. For example, Angel and McCabe observe that:

> Proponents of the use of the bitcoin system view it as a workaround for their lack of trust in the existing payment infrastructure, dependent as it is on a fallible central bank or other payment intermediary . . . . The continuing evolution in the technology of payments raises interesting ethical questions for businesses as well as public policy considerations . . . . Situations in which the bargaining power of one of the parties is limited raise questions about the fairness of the result . . . . A new payment system such as bitcoin, like any tool, is neither good nor evil on its own, but it is the ethical or unethical use of the payment system that matters.[55]

[28] Lowry, Wells, Moody, Humphreys and Kettles observe that the academic literature about electronic internet payment systems proposes models,[56] protocols,[57]and architectures[58] to facilitate online payments.

[55] JAMES J. ANGEL & DOUGLAS MCCABE, THE ETHICS OF PAYMENTS: PAPER, PLASTIC, OR BITCOIN? 14-16 (2014), *available at* http://ssrn.com/abstract=2379233.

[56] *See* Lowry et al., *supra* note 52, at 5 (citing X. Hou & C. H. Tan, *A New Electronic Cash Model* 374-79, Paper presented at the Int'l Conference on Info. Tech.: Coding and Computing, Las Vegas, NV, April 4-6, 2005; S. F. Mjølsnes & C. Rong, *On-line e-Wallet System with Decentralized Credentials Keepers*, 8 MOBILE NETWORKS AND APPLICATIONS 87 (2003) *available at* http://dl.acm.org/citation.cfm?id=603909).

[57] *Id.* (citing A.R. Dani, P.R. Krishna & V. Subramanian, *An Electronic Payment System Architecture for Composite Payment Transactions*, Paper presented at the International Conference on e-Technology, e-Commerce, and e-Service, Hong Kong, China, March 29-April 1 2005 at 552-555; M. Kinateder & K. Rothermel, *Bringing Confidence to the Web-Combining the Power of SET and Reputation Systems*, Paper presented at the First IEEE Consumer Communications and Networking Conference, Las Vegas, NV, Jan. 5-8, 2004 at 545-550; B. Meng & Q. Xiong, *SOCPT: A Secure Online Card Payment Protocol*, Payment presented at the 8th International Conference on Computer Supported Cooperative Work in Design, Xiamen, China, May 26-28, 2004 at 679-684; V. Varadharajan & Y. Mu, *On the Design of secure Electronic Payment Schemes for*

Other studies provide mathematical proofs of specific protocols.[59] These models, protocols and architectures focus on providing security, accountability, atomicity, anonymity, non-repudiation, and fairness to transactions.[60] For online payment systems, the most vital of these may be security,[61] identified identification, confidentiality, authentication, data integrity, non-repudiation, and customer solvency as key levels of security surrounding payment alternatives.[62]

Internet, Paper presented at the 12th Annual Computer Security Applications Conference, San Diego, CA, Dec. 9-13, 1996 at 78-87).

[58] *Id.* (citing H. Knospe & S. Schwiderski-Grosche, *Future Mobile Networks: Ad-hoc Access Based on Online Payment with Smartcards*, Paper presented at the 13th IEEE International Symposium on Personal, Indoor, and Mobile radio Communications, Lisbon, Portugal, Sept. 15-18, 2002 at 197-200; A. Liu, V.Y. Shen & J.K. Muppala, *Security Issues on Server-Side Credit-Based Electronic Payment Systems*, Paper presented at the 3rd International Symposium on Electronic Commerce, Research Triangle Park, NC, Oct. 18-19 at 47-57; J. ZHANG ET AL., MIGRATION TO WEB SERVICES ORIENTED ARCHITECTURE – A CASE STUDY 1624 (2004)).

[59] *Id.* (citing M. Backes & M. Dürmuth, *A Cryptographically Dound Dolev-Yao Style Security Proof of an Electronic Payment System*, Paper presented to the 18th IEEE Computer Security Foundations Workshop, June 20-22 Axin-en-Provence, France at 78; G. Bella, F. Massicci & L.C. Paulson, *The Verification of an Industrial Payment Protocol: The SET Purchase Phase*, Paper presented at the 9th ACM Conference on Computer and Communications Security, Washington, DC, Nov. 18-22 at 12 *available at* http://www.cl.cam.ac.uk/~lp15/papers/Bella/purchase.pdf).

[60] *Id.* (citing Meng & Xiong, *supra* note 57).

[61] Lowry et al., *supra* note 52, at 5 (citing I. Mavridis, G. Pangalos, T. Koukouinos & S. Muftic, *A Secure Payment System for Electronic Commerce*, Paper presented at the 10th International Workshop on Database and Expert Systems Applications, Florence, Italy, Sept. 1-3, 1999 at 832; J. Sahut & M. Galuszewska, *Electronic Payment Market: A Non-optimal Equilibrium*, Paper presented at the 2004 International Symposium on Applications and the Internet Workshops, Tokyo, Jan. 26-30, 2004 at 3).

[62] *Id.* at 5-6 (quoting J. Sahut & M. Galuszewska, *Electronic Payment Market: A Non-optimal Equilibrium*, Paper presented at the 2004 International Symposium on Applications and the Internet Workshops, Tokyo, Jan. 26-30, 2004 at 3).

A. Regulatory Fabric

[29] The schematic for regulation of money transmission in the United States involves both State and Federal laws. Primarily, an anti-money laundering statute, the Bank Secrecy Act ("BSA") regulates transmission at the Federal level.[63]

B. U.S. State Money Transmission Laws

[30] By contrast with federal statutes, "State money transmitter laws vary by jurisdiction and focus on consumer protection concerns."[64] Accordingly, state money transmitter laws are essentially 'safety and soundness' statutes designed to ensure that consumer funds are protected from loss.[65] These state "statutes historically regulated money transfer businesses like Western Union with an eye toward preventing consumer harm. The plain language of such statutes, however, purports to broadly regulate the receipt of money or monetary value for the purpose of transmitting it to another place or location by any means."[66] It appears

[63] Kevin V. Tu, *Regulating the New Cashless World*, 65 ALA L.REV. 77, 86 (2013), (citing 31 U.S.C. § 5311 (2011); *FinCEN's Mandate from Congress*, FINANCIAL CRIMES ENFORCEMENT NETWORK, http://www.fincen.gov/statutes_regs/bsa/ (last visited May 18, 2014); Lawrence J. Trautman & Alvin Harrell, *Bitcoin vs. Regulated Payment Systems: What Gives?*, 68 CONSUMER FIN. L. Q. REP. (2014).

[64] *Id.* at 85 (citing UNIF. MONEY SERV. ACT, prefatory note, 7A U.L.A. 163-64 (2004), *available at* http://www.uniformlaws.org/shared/docs/money%20services/umsa_final04.pdf (last visited Aug. 18, 2013) (noting that state laws are 'extremely varied'); *see, e.g.*, CAL. FIN. CODE § 2002 (Deering 2014) (the purpose is to protect the interests of consumers); VA CODE ANN. § 6.2-1902(B) (2010) (the statute shall be construed for the purpose of protecting, against financial loss, citizens of Virginia who purchase money orders or control of their funds or credit into the custody of another person for transmission).

[65] *See* UNIF. MONEY SERV. ACT, *supra* note 64.

[66] Kevin V. Tu, *supra* note 63, at 77.

that both enforcement and clear guidance by some states has been inconsistent, and "in the face of such uncertainty, Amazon, Google, and PayPal have all become licensed money transmitters under state law. Even Facebook has become licensed in advance of launching a payments product in order to mitigate the risk of sanctions as the development of their payments product continues to evolve."[67]

[31] A license is required in most states before a money transmitter may conduct business.[68] Therefore, any entity operating as a money transmitter that fails to obtain the necessary state licensing or to register with FinCEN may become subject to criminal prosecution under 18 U.S.C. §1960.[69]

> Many virtual currency systems, exchangers, and related services operate as money transmitters, which are part of a larger class of institutions called money services businesses. Money transmitters are required under 31 U.S.C. §5330 to register with the Financial Crimes Enforcement Network (FinCEN). . . . Additionally, the general money laundering and spending statutes, 18 U.S.C. §§ 1956 and 1957, cover financial transactions involving virtual currencies. Finally, where virtual currencies are used in furtherance of underlying criminal activity, the Department [of Justice] can rely on traditional criminal statutes proscribing that activity, such as narcotics, cybercrime, child exploitation, and firearms laws.[70]

[67] *Id.* at 78*; see also* Trautman, *supra* note 21, at 22.

[68] Raman, *supra* note 8.

[69] *Id.*

[70] *Id.*

[32] During the early part of 2014, FinCEN published two administrative rulings regarding virtual currencies, providing much needed guidance. Accordingly,

> The first ruling states that, to the extent a user creates or "mines" a convertible virtual currency solely for a user's own purposes, the user is not a money transmitter under the BSA. The second states that a company purchasing and selling convertible virtual currency as an investment exclusively for the company's benefit is not a money transmitter.[71]

[33] In addition to money transmission statutes, states have also adopted cybercrime statutes. Because Virginia is the home state to many Internet service providers including America OnLine, "it has been dubbed 'the epicenter of Internet traffic,' and has adopted some of the toughest cybercrime legislation in the country."[72] Pinguelo and Muller provide a forty-nine state survey of cyberlaw legislation as of 2013.[73]

[34] The New York State Department of Financial Services announced in August 2013 that it has launched a fact-finding effort regarding guidelines for regulating virtual currencies with a view toward exploring the potential NYDFS issuance of a 'BitLicence'.[74] In his opening statement for Hearings on the Regulation of Virtual Currency, New York

[71] Press Release, FinCEN, FinCEN Publishes Two Rulings on Virtual Currency Miners and Investors (Jan. 30, 2014), *available at* http://www.fincen.gov/news_room/nr/pdf/20140130.pdf.

[72] Pinguelo & Muller, *supra* note 18, at 149.

[73] *See id.* at 150-55.

[74] *See* Press Release, N.Y. Dep't of Fin. Serv., NYDFS Outlines Additional Details on Witnesses and Panels for Virtual Currency Hearing on January 28 and 29 in New York City (Jan. 23, 2014), *available at* http://www.dfs.ny.gov/about/panels_witnesses_virtual_currency_hearing.pdf.

Superintendent of Financial Services, Benjamin M. Lawsky, stated that "[i]t's hard to say precisely what the future holds for virtual currency and its associated technology. Currently, there is not widespread adoption of virtual currencies among the general public. And some doubt whether there will ever be."[75] Moreover,

> [S]erious people – in the technological and investment community – are taking virtual currencies seriously. They are putting significant amounts of time, attention, and capital behind them. We, as a regulator, cannot turn a blind eye to something like that. We don't really have a choice. Moreover, the Department of Financial Services – like many other state financial regulators – has a specific legal responsibility to license and regulate money transmission. And to the extent that some virtual currency service providers are engaged in money transmission, we do have an important role in writing and enforcing the rules of the game for financial firms . . . . [V]irtual currency could ultimately have a number of benefits for our financial system. It could force the traditional payments community to "up its game" in terms of the speed, affordability, and reliability of financial transactions . . . . Fashioning appropriate guardrails for virtual currencies presents challenging questions for regulators. Virtual currency is not easily categorized within the divisions we traditionally think about when it comes to the financial system (such as banks, insurers, or money transmitters). It's neither fish nor fowl.[76]

[75] Benjamin M. Lawsky, Superintendent of Fin. Serv., N.Y. Dep't of Fin. Serv., Opening Statement to Hearings on the Regulation of Virtual Currency (Jan. 28, 2014), *available at* http://www.dfs.ny.gov/about/hearings/vc_01282014/lawsky_vchearing.pdf.

[76] *Id.*

Indeed, Superintendent Lawsky suggests that the term "money transmission" connotes an image of "firms that were formed more than 150 years ago when our country was still exploring the western frontier."[77] The challenge to regulators everywhere is to determine "what type of licensing, examination, and collateral requirements for the virtual currency industry will provide appropriate guardrails to protect consumers and our national security − without stifling beneficial innovation."[78] Moreover,

> Safety and soundness requirements help build greater confidence among customers that the funds that they entrust to virtual currency companies won't get caught in a virtual black hole. Indeed, some consumers have expressed concerns about how quickly their virtual currency transactions are processed. There have also been public reports of virtual currency lost – perhaps irretrievably – through hacking and other cyber security vulnerabilities. Addressing those issues through enhanced safety and soundness requirements would be important to building greater confidence in this technology among the general public and promoting wider adoption.[79]

C. Implications for Tax Revenues

[35] Virtual transactions, virtual economies and transactions within these virtual economies are often very different.[80] Cryptocurrencies

[77] *Id.*

[78] *Id.*

[79] *Id.*; *accord* Cameron Winklevoss & Tyler Winklevoss, Written Testimony of Cameron and Tyler Winklevoss to the New York State Department of Financial Services NYDFS Virtual Currency Hearing (Jan. 28 2014), *available at* http://www.dfs.ny.gov/insurance/hearing/vchearing/winklevoss.pdf.

[80] *See* Leandra Lederman, *'Stranger than Fiction': Taxing Virtual Worlds*, 82 N.Y.U. L. REV. 1620, 1670-72 (2007); Theodore P. Seto, *When is a Game Only a Game?: The*

present difficult challenges to taxing authorities worldwide.[81] A discussion of global tax issues and implications is beyond the scope of this paper; however, with a focus on the United States, general comments are provided to outline some of the major issues and suggest topics for further research. Aleksandra Bal observes that "the question as to whether or not virtual currency may constitute taxable income is likely to vary from country to country."[82] Moreover, tax administrators worldwide face the challenge of "how to approach a system that is outside the traditional streams of commerce and finance and for users to understand the tax consequences of their transactions in virtual currencies."[83] Bal postulates that taxable income may be generated from the following: "the creation of virtual money ('mining'), the receipt of virtual currency as a gift (or reward for some achievements within the game), the receipt of virtual currency in exchange for (real or virtual) goods and services and the sale of digital money for real currency."[84] In their May 2013 report to the U.S. Senate Finance Committee, the GAO concluded that

---

Taxation of Virtual Worlds, 77 U. CIN. L. REV. 1027, 1031, 1037-38, 1040 (2009), *available at* http://ssrn.com/abstract=1220923.

[81] *See* Sarah Gruber, Note, *Trust, Identity, and Disclosure: Are Bitcoin Exchanges the Next Virtual Havens for Money Laundering and Tax Evasion?,* 32 QUINNIPIAC L. REV. 135, 196 (2013); Jennifer Isom, *As Certain as Death and Taxes: Consumer Considerations of Bitcoin Transactions for When the IRS Comes Knocking* 12-13 (Dec. 9, 2013) (unpublished note), *available at* http://ssrn.com/abstract=2365493; Steven S. Chung, Note, *Real Taxation of Virtual Commerce*, 28 VA. TAX REV. 101, 131-34 (2008), *available at* http://ssrn.com/abstract=1097793 (proposing that virtual currencies integrating real cash into their economies through internal currency exchange systems behave like foreign currencies and should be taxed under the foreign currency rules of the Internal Revenue Code (Code); Bryan Camp, *The Play's the Thing: A Theory of Taxing Virtual Worlds*, 59 HASTINGS L.J. 1, 61-62 (2007), *available at* http://ssrn.com/abstract=980693.

[82] Bal, *supra* note 12, at 354.

[83] *Id.* at 351.

[84] *Id.* at 354.

> Virtual economies and the use of virtual currencies intended as alternatives to government-issued currencies are a recent phenomenon, and the extent to which their use results in tax noncompliance is unknown. Given this uncertainty, available funding, and other priorities, IRS made a reasoned decision not to implement a compliance approach specific to virtual economies and currencies.[85]

[36] Internal IRS research beginning during 2007 looked at virtual economies and "did not find strong evidence of the potential for tax noncompliance related to virtual economies, such as the number of U.S. taxpayers involved in such activity or the amount of federal tax revenue at risk."[86] After consulting with academics, tax practitioners, the IRS and others, the GAO reports that the following tax compliance risks germane to virtual currencies and virtual economies include: tax evasion, mischaracterization, and underreporting.[87] However, the GAO is quick to observe that "[t]hese risks are not unique to virtual economies and currencies, as they also exist for other types of transactions, such as cash transactions, where there are not always clear records or third-party tracking and reporting of transactions."[88] Accordingly, the GAO identifies the following virtual currencies and economies compliance risks: lack of taxpayer knowledge regarding tax requirements; uncertainty over how to characterize income; uncertainty over how to calculate basis for gains; challenges with third-party reporting; and tax evasion.[89] Akins, Chapman and Gordon conclude that "creating, or mining, bitcoin should be

[85] U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 5, at 16.

[86] *Id.* at 15.

[87] *See id.* at 12.

[88] *Id.*

[89] *Id.* at 12-14.

characterized as income for services and reported as such. At the same time, transactions involving the exchange of bitcoin for legal currency, goods, or services should be reported as a capital gain or loss transaction."[90] On March 25, 2014, the IRS provided guidance stating that "[f]or federal tax purposes, virtual currency is treated as property. General tax principles applicable to property transactions apply to transactions using virtual currency."[91]

[37] Omri Marian suggests that "[c]ryptocurrencies offer, at least theoretically, a near-perfect alternative to tax-evaders who can no longer find a safe haven in tax-haven jurisdictions."[92] Marian further observes that "[c]ryptocurrencies possess the traditional characteristics of tax havens: earnings are not subject to taxation and taxpayers' anonymity is maintained. Cryptocurrencies, however, also possess one added value: their operation is not dependent on the existence of financial institutions."[93]

D. Financial Crimes Enforcement Network (FinCEN)

[38] A bureau of the U.S. Treasury Department, FinCEN, reports directly to the Office of Terrorism and Financial Intelligence. Consisting

[90] Benjamin Akins et al., *A Whole New World: Income Tax Considerations of the Bitcoin Economy*, PITT. TAX REV. (forthcoming 2015), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2394738##.

[91] INTERNAL REVENUE SERVICE, NOTICE 2014-21, VIRTUAL CURRENCY GUIDANCE (2014); *see also* John D. McKinnon & Ryan Tracy, *Bitcoin Investors Face the Real IRS*, WALL ST. J. (Mar. 26, 2014), http://online.wsj.com/news/articles/SB10001424052702303949704579461502538024502.

[92] Omri Y. Marian, *Are Cryptocurrencies 'Super' Tax Havens?*, 112 MICH. L. REV. FIRST IMPRESSIONS 38, 47 (2013), *available at* http://ssrn.com/abstract=2305863.

[93] *Id.* at 39.

of only approximately 340 employees,[94] FinCEN's "mission is to safeguard the financial system from illicit use, combat money laundering and promote national security through the collection, analysis, and dissemination of financial intelligence and strategic use of financial authorities."[95] Among FinCEN's responsibilities is to issue regulations and administer the Bank Secrecy Act (BSA).[96] The BSA requires that a wide range of financial institutions assist FinCEN by having effective anti-money-laundering (AML) programs and by filing periodic reports with FinCEN and by maintaining appropriate records. Examples of these financial institutions include: securities and futures broker/dealers, insurance companies, banks, casinos, other money services businesses, and certain trades or businesses such as automobile dealers.[97]

[39] In March 2013, FinCEN provided interpretive guidance for those individuals and businesses offering virtual currencies and those engaged in providing money transmittal.[98] While acknowledging that there are some troublesome virtual currency providers, FinCEN Director Jennifer Shasky Calvery observes that the impact of troublesome providers are mitigated by the positive innovative contributions provided by virtual currencies, and the financial inclusion that they might offer society. A whole host of

[94] *See Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies: Hearings Before the S. Comm. on Homeland Sec. & Gov't Affairs*, 113th Cong. (2013) (statement of Jennifer Shasky Calvery, Director, Fin. Crimes Enforcement Network, United States Department of the Treasury).

[95] *Id.*

[96] *Id.*

[97] *See* Jennifer Shasky Calvery, Director, Fin. Crimes Enforcement Network, Remarks at the Independent Armored Car Operators Association Cash in Transit Networking Conference (May 18, 2014).

[98] FINANCIAL CRIMES ENFORCEMENT NETWORK, 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/html/FIN-2013-G001.html.

emerging technologies "in the financial sector have proven their capacity to empower customers, encourage the development of innovative financial products, and expand access to financial services. We want these advances to continue."[99] Observing that financial institutions have the responsibility to ensure transparency and integrity, Director Calvery states

> FinCEN's guidance explains that administrators or exchangers of virtual currencies have registration requirements and a broad range of AML program, recordkeeping, and reporting responsibilities. Those offering virtual currencies must comply with these regulatory requirements, and if they do so, they have nothing to fear from Treasury.
>
> The guidance explains how FinCEN's 'money transmitter' definition applies to certain exchangers and system administrators of virtual currencies depending on the facts and circumstances of that activity. "Those who use virtual currencies exclusively for common personal transactions like buying goods or services online" are not affected by this guidance.
>
> Those who are intermediaries in the transfer of virtual currencies from one person to another person, or to another location, are money transmitters that must register with FinCEN as MSB [money service business], unless an exception applies. Some virtual currency exchangers have already registered with FinCEN as MSBs, though they have not necessarily identified themselves as money transmitters.[100]

[99] Calvery, *supra* note 94 at 10-11.

[100] Calvery, *supra* note 94; *see also* FINANCIAL CRIMES ENFORCEMENT NETWORK, 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/html/FIN-2013-G001.html.

E. Digital Economy Task Force

[40] The Digital Economy Task Force is an outgrowth of a conference held on June 14, 2013 at the World Bank and included officials from the European Central Bank, ICMEC, International Monetary Fund, Thomson Reuters, the U.S. Federal Reserve, U.S. Department of the Treasury's Office on Terrorist Financing and Financial Crimes, and others. With a view toward exploring "reasonable, constructive solutions, including best practice models to address the challenge of anonymity," the Task Force issued its findings during March 2014 on the working group topics of: "Defining the Problem; Regulation; Law Enforcement; Human Rights/Financial Inclusion; and Interagency Cooperation and Coordination."[101]

F. Virtual Currency Emerging Threats Working Group (VCET)

[41] The FBI founded the Virtual Currency Emerging Threats Working Group (VCET) during early 2012 to address and "mitigate the cross-programmatic threats arising from illicit actors' use of virtual currency systems."[102] Membership of VCET consists of an interagency assortment of U.S. government, including within the DOJ: multiple U.S. Attorney's offices; the Criminal Division's sections of Asset Forfeiture and Money Laundering and Computer Crime and Intellectual Property; the Drug

[101] *See* Allen, *supra* note 18; *see generally* INT'L CTR. FOR MISSING & EXPLOITED CHILDREN, *Preface* to THE DIGITAL ECONOMY: POTENTIAL, PERILS, AND PROMISES: A REPORT OF THE DIGITAL ECONOMY TASK FORCE (Thomson Reuters 2014), *available at* http://thomsonreuters.com/business-unit/legal/digital-economy/digital-economy-task-force-report.pdf (proposing regulations to frame the policy discussion in a manner that enables the digital economy to grow while creating an inhospitable environment for those who seek to abuse it).

[102] Raman, *supra* note 8, at 6.

Enforcement Administration and the FBI.[103] Many other law enforcement groups have a mission concerning emerging payment systems and virtual currencies. Far too numerous and clandestine to list them all, these include: local, state, federal and international law enforcement agencies, "the Secret Service and U.S. Immigration and Customs Enforcement's Homeland Security Investigations (ICE/HSI) partner through the Secret Service's Electronic Crimes Task Forces (ECTFs), which leverage the private sector, academia, and state and local law enforcement to support cyber crime investigations."[104] The "New Payment Methods Ad Hoc Working Group, a subgroup of the Terrorist Finance Working Group, led by the State Department. The FBI specifically has issued numerous intelligence products related to virtual currency, many . . . co-authored with other members of the U.S. Intelligence Community."[105]

G. Regulation of International Foreign Currencies

[42] The Great Depression of the 1930s highlighted the need for an international institution to provide the stability of exchange rates, international monetary cooperation and balanced growth of trade among nations. Therefore, in July 1944, the International Monetary Fund (IMF) was conceived by 45 countries meeting at Bretton Woods, New Hampshire.[106] During December 1945, the IMF came into formal existence when its *Articles of Agreement* were adopted by its initial 29 members.[107] While virtual currencies were not contemplated during 1945, of relevance to our discussion is the fact that the IMF is the international

[103] *Id.*

[104] Lowery, *supra* note 7, at 1.

[105] Raman, *supra* note 8.

[106] International Monetary Fund, *About the IMF: History, Cooperation and Reconstruction (1944-71), available at* http://www.imf.org/external/about/histcoop.htm (last visited Apr. 9, 2014).

[107] *Id.*

organization consisting of almost every signatory nation state (except for perhaps North Korea), and has the principal responsibility of coordinating foreign currency exchange, as noted by the following stated purposes of the IMF:

> (i) To promote international monetary cooperation through a permanent institution which provides the machinery for consultation and collaboration on international monetary problems.
>
> (ii) To facilitate the expansion and balanced growth of international trade, and to contribute thereby to the promotion and maintenance of high levels of employment and real income and to the development of the productive resources of all members as primary objectives of economic policy.
>
> (iii) To promote exchange stability, to maintain orderly exchange arrangements among members, and to avoid competitive exchange depreciation.
>
> (iv) To assist in the establishment of a multilateral system of payments in respect of current transactions between members and in the elimination of foreign exchange restrictions which hamper the growth of world trade. . . . [108]

[108] Articles of Agreement of the International Monetary Fund, 2011 ed., *available at* http://www.imf.org/External/Pubs/FT/AA/pdf/aa.pdf; *see* Articles of Agreement of the International Bank for Reconstruction and Development, Dec. 27, 1945, 2 U.N.T.S. 134 ; Participants, Articles of Agreement of the International Monetary Fund, U.N.T.S., https://treaties.un.org/Pages/showDetails.aspx?objid=0800000280165965 (last visited Apr. 9, 2014) (listing the countries who participate in the International Monetary Fund).

H. Regulatory Challenges

[43] The desire to formulate an enlightened and productive regulatory environment for virtual currencies has been the subject of Congressional hearings during recent months.[109] Professor Sarah Jane Hughes offers her vision of a future regulatory fabric with her recommendation that Congress

> 1. Retain the current division of regulation between the States and Federal Government − with prudential regulation of the non-depository providers of new payments systems with the States and retaining the anti-money-laundering, anti-terrorism and economic sanctions regulations with the Federal Government.
>
> 2. Make providers of virtual currencies comply with the customer-identification program and AML compliance program requirements of Sections 326 and 352 of the USA PATRIOT Act, and with the economic sanctions regulations enforced by OFAC, just as other payments systems providers do. Virtual currency customers will have to reveal their identities to issuers of the currencies they use. As a corollary, customers should get the same federal financial privacy rights that users of other payments products have under the Right to Financial Privacy Act of 1978 and Title V of the Gramm-Leach-Bliley Act.
>
> 3. Encourage FinCEN to clarify the manner in which customer-identification and AML compliance requirements apply to virtual currencies. This is needed

[109] *See Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies*: *Hearing Before the S. Comm. on Homeland Security & Governmental Affairs*, 113th Cong. (2013), *available at* http://www.hsgac.senate.gov/hearings/beyond-silk-road-potential-risks-threats-and-promises-of-virtual-currencies.

to help banks ensure that they can do business with providers and users of virtual currencies and other payments innovators. Second-stage innovations from distributed computing and database technologies could offer benefits to payments and commerce far beyond those that virtual currencies now offer. If banks cannot determine how to comply with FinCEN regulations, for example, they may continue to terminate their relationships with payments innovators before the innovators can attract investors and users to make it to the second-stage technologies their current work may generate.

4. Encourage payments systems innovators to adopt and publicize transparent payment systems rules for their own systems and even to compete for customers on the basis of the system rules they adopt. It is too early to enact user protections for virtual currencies.

5. Ignore the claims that
   a. additional regulation of virtual currencies will halt innovations,
   b. innovators deserve freedom from regulations that apply to other payments systems and their providers, and
   c. virtual currencies deserve a single federal licensure system that preempts State prudential regulation and licensure.

6. Monitor the development of virtual currency providers in case they transform their products into commodities or securities and, if this happens, then decide whether regulating their products under the applicable regulations makes more sense.

7. Leave room for non-depository and depository providers of payments products to innovate in the virtual currency space.

8. Authorize and fund a study of virtual currencies to be carried out by the Federal Reserve Board or pursuant to the Federal Advisory Committees Act by an inter-agency task force and industry participants.[110]

I. Unique Enforcement Challenges & Monetary Stability

[44] Virtual currencies present particularly difficult law enforcement challenges because of its: ability to transcend national borders in the fraction of a second; unique jurisdictional issues; and anonymity due to encryption. Gabriel Michael observes that "Bitcoin is a disruptive technology that undermines the regulatory capacity of the state."[111] Mark Williams observes that

[110] *The Present and Future Impact of Virtual Currency*: Hearing Before the Subcomms. on Econ. Policy and on Nat'l Sec. and Int'l Trade and Fin. of the S. Banking Comm., 113th Cong. 2-3 (2013) (statement of Sarah Jane Hughes, University Scholar and Fellow in Commercial Law, Indiana University Maurer School of Law), *available at* http://www.banking.senate.gov/public/index.cfm?FuseAction=Files.View&FileStore_id=12e58649-d425-428f-a52c-b7938051536b.

[111] Gabriel J. Michael, Note, *Anarchy and Property Rights in the Virtual World: How Disruptive Technologies Undermine the State and Ensure that the Virtual World Remains a "Wild West,"* 21 (March 1, 2013), *available at* http://ssrn.com/abstract=2233374. *See generally* Shawn J. Bayern, *Of Bitcoins, Independently Wealthy Software, and the Zero-Member LLC*, 109 NW. L. REV. COLLOQUY (forthcoming 2014), *available at* http://ssrn.com/abstract=2366197 (discussing the consequences of Bitcoin as an independently wealthy software); Harri Lahdenpera, *Payment and Financial Innovation, Reserve Demand and Implementation of Monetary Policy* (Bank of Finland, Working Paper No. 26/2001, 2001) (observing that private substitutes for central bank money are available for the settlements of transactions, showing that effective monetary control by the central bank indeed be compromised in those circumstances), *available at* http://ssrn.com/abstract=315479; *and* Malte Möser, Ranier Böhme & Dominic Breuker,

> There are significant risks and uncertainties associated with virtual currencies that need to be fully measured before they are allowed to proliferate further or be adopted into the financial system. Bitcoin presents numerous market-related risks as it is decentralized, volatile, untraceable, unregulated, and provides no legal protection to customers. If Bitcoin, in its embryonic stage, were to replace the U.S. dollar, it would be economically disastrous causing trade to plummet, GDP to fall and unemployment levels and bartering to surge. Bitcoin is an experiment that needs to remain in the laboratory until it can meet the basic standards required to become a beneficial transactional currency. As a virtual commodity, Bitcoin remains extremely risky and needs to be closely watched. To transform Bitcoin into a virtual currency would require regulation, centralization, creation of a legal framework and strong regulatory oversight. However, these steps alone would not necessarily guarantee that chronically high price volatility would drop low enough to allow Bitcoin to become a trusted transactional currency.[112]

J. International & Jurisdictional Issues

[45] The international reach and clientele of those engaged in virtual currency transactions present obvious law enforcement compliance problems. Mythili Raman states that "transnational organized crime networks are increasingly involved in cybercrime, and can imperil consumers' faith in emerging digital systems" and "[i]nvestigations into illicit virtual currency businesses therefore often require considerable

Towards Risk Scoring of Bitcoin Transactions, available at http://fc14.ifca.ai/bitcoin/papers/bitcoin14_submission_15.pdf.

[112] Mark T. Williams, *supra* note 14 at 1.

cooperation from international partners."[113] The investigation and takedown of Liberty Reserve, involved coordination of the law enforcement agencies in 17 nations.[114]

[46] The practical inability to obtain customer transaction records remains one of the most significant problems confronting law enforcement efforts:

> Because decentralized systems lack any sort of administering authority to collect user information or receive legal process, investigators must rely on information collected by other sources, such as exchangers. Even if the target used a centralized system or exchanger, however, accurate customer records may still be difficult to obtain, or may not exist at all.[115]

[47] Incongruent regulatory schemes present difficulty in regulating transactions and technology that appear to move at the speed of light.[116]

---

[113] Raman, *supra* note 8. *See generally* Joel Reidenberg, *Technology and Internet Jurisdiction*, 153 U. PA L. REV. 1951 (2005) (discussing the struggle to adapt existing regulatory standards to new technologies and the Internet).

[114] *See* Raman, *supra* note 8.

[115] *Id. See generally* Christopher Kuner, *Data Protection Law and International Jurisdiction on the Internet (Part 1)*, 18 INT'L J. L. & INFO. TECH. 176 (2010), *available at* http://ssrn.com/abstract=1496847 (discussing the increasing complexity of data protection law); Christopher Kuner, *Data Protection Law and International Jurisdiction on the Internet (Part 2)*, 18 INT'L J. L. & INFO. TECH. 227 (2010), *available at* http://ssrn.com/abstract=1689495 (examining international jurisdiction and its relationship to data protection law).

[116] *See generally* Gargi Rajvanshi, Tapas K. Badhyopadhyay & Rajeev Gupta, *Intricacies of Privacy Protection in Electronic Commercial Transactions: Critical Analysis* (April 9, 2012), *available at* http://ssrn.com/abstract=2036935 (analyzing the issue of data protection and privacy as it relates to electronic transactions); Franziska Boehm & Paulina Pesch, *Bitcoin: A First Legal Analysis – With Reference to German & US-American Law* (2014), *available at*

Virtual currencies, which facilitate the movement of money across the globe without involving a traditional financial services institution, exist in a legal and regulatory environment that may not address virtual currencies at all.[117] Those countries having substandard anti-money laundering or know-your-customer regulatory oversight or those jurisdictions hostile to the United States attract these illicit operations. Even in those jurisdictions having a cooperative regulatory environment, "the legal process for obtaining foreign records is relatively slow when compared to the near-instantaneous speed at which the virtual currency user can send the funds to another jurisdiction."[118]

K. Anonymity Due to Encryption

[48] The link between sophisticated encryption and virtual currency presents yet another difficult technical challenge for regulators, investigators, and others in the enforcement process such as prosecutors.[119] Because virtual currencies lack a centralized authority for administration (such as a central bank or financial institution), the decentralized command and control functions of a virtual currency rely typically on an encryption algorithm.[120] Therefore, "[t]hese encryption-

http://fc14.ifca.ai/bitcoin/papers/bitcoin14_submission_7.pdf (observing that current laws are not designed to handle decentralized virtual currencies like Bitcoin and that the criminal and civil law systems in Germany particularly are not prepared for the challenges arising outside the traditional understanding of physically existent objects).

[117] *See* Niels Vandezande, *Mobile Wallets and Virtual Alternative Currencies Under the EU Legal Framework on Electronic Payments*, ICRI Working Paper 16 (Sept. 12, 2013), *available at* http://ssrn.com/abstract=2325410; D.C. Kennedy, *In Search of a Balance Between Police Power and Privacy in the Cybercrime Treaty*, 9 RICH. J.L. & TECH. 3 (2002), *at* http://jolt.richmond.edu/v9i/article3.html. *See generally* Raman, *supra* note 8 (discussing law enforcement interests related to virtual currencies).

[118] Raman, *supra* note 8.

[119] *See* Peter Swire & Kenesa Ahmad, *Encryption and Globalization*, 23 COLUM. SCI. & TECH. L. REV. 416, 453 (2012), *available at* http://ssrn.com/abstract=1960602.

[120] *See* Raman, *supra* note 8.

based currencies, also known as cryptocurrencies, lack a central administering authority that might otherwise possess valuable evidence. In addition, users of these currencies often encrypt their digital wallets, complicating our efforts to seize and forfeit criminal proceeds."[121] Moreover,

> To be clear, virtual currency is not necessarily synonymous with anonymity. A convertible virtual currency with appropriate anti-money laundering and know-your-customer controls, as required by U.S. law, can safeguard its system from exploitation by criminals and terrorists in the same way any other money services business could. As virtual currency systems develop, it is imperative to law enforcement interests that those systems comply with applicable anti-money laundering and know-your-customer controls.[122]

IV. BITCOIN

[49] Based on ideas from b-money[123] and Hashcash,[124] "[a] Bitcoin is a fixed-value cryptographic object represented as a chain of digital

[121] *Id.*

[122] *Id.*

[123] Joshua A. Kroll, Ian C. Davey, & Edward W. Felten, *The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries,* THE TWELFTH WORKSHOP ON THE ECONOMICS OF INFORMATION SECURITY (WEIS 2013) 3, *available at* http://www.weis2013.econinfosec.org/papers/KrollDaveyFeltenWEIS2013.pdf (citing Wei Dai, *b-money*, http://www.weidai.com/bmoney.txt (1998) (last visited May 13, 2014).).

[124] *See* Kroll, Davey & Felten, *supra* note 123, at 3 (citing Adam Back, *Hashcash - A Denial of Service Counter-Measure*, HASHCASH.ORG (Aug. 1, 2002), http://www.hashcash.org/papers/hashcash.pdf).

signatures over the transactions in which the coin was used."[125] Bitcoin "aims to be completely distributed, free of central authorities or points of control, and at least somewhat anonymous."[126] Bitcoin is a virtual currency based on a decentralized peer-to-peer (P2P) network, much like BitTorrent, the popular protocol for sharing files over the Internet, such as music, games and video.[127] Boston University's Mark Williams observes that "[s]ince 2009, over seventy-five virtual currencies have been created and are traded globally representing about $11 billion in stated market value."[128] As shown in Figure 2, Bitcoin has grown rapidly since 2009 from a mere idea to a legitimate currency by mid-2013, with bitcoins in circulation, its market capitalization having total value in excess of $14 billion (U.S.) during December 2013.[129] One 2013 estimate states that

[125] Kroll, Davey & Felten, *supra* note 123, at 3; *see also* Robert McMillan, *The Fierce Battle for the Soul of Bitcoin*, WIRED (Mar. 26, 2014, 6:30 AM), http://www.wired.com/2014/03/what-is-bitcoin.

[126] Kroll, Davey & Felten, *supra* note 123, at 3.

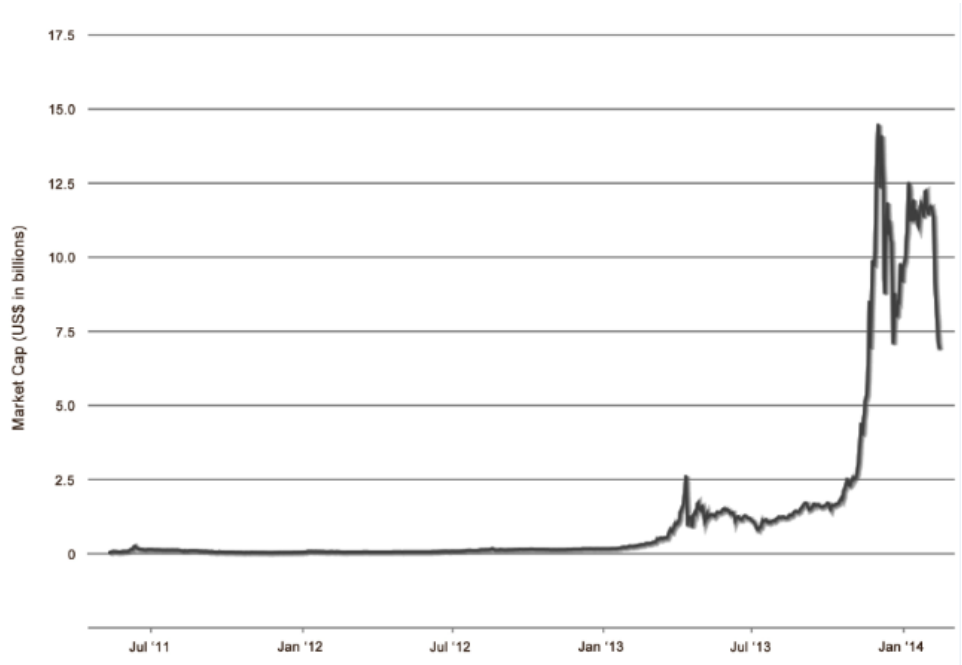
[127] *See* EUROPEAN CENTRAL BANK, VIRTUAL CURRENCY SCHEMES 42-43 (Oct. 2012), *available at* http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf. *See generally* Rostislav Skudnov, *Bitcoin Clients*, TURKU UNIVERSITY OF APPLIED SCIENCES 1, http://publications.theseus.fi/bitstream/handle/10024/47166/Skudnov_Rostislav.pdf?sequence=1 (exploring the different features of Bitcoin); David Allen Bronleewe, *Bitcoin NFC*, UNIVERSITY OF TEXAS AT AUSTIN 1, http://repositories.lib.utexas.edu/bitstream/handle/2152/ETD-UT-2011-08-4150/BRONLEEWE-MASTERS-REPORT.pdf?sequence=1 (discussing the use of Bitcoin).

[128] Williams, *supra* note 14, at 1 (citing *Crypto-Currency Market Capitalizations*, COINMARKETCAP, http://coinmarketcap.com/mineable.html (last visited Apr. 16, 2014)).

[129] *Bitcoin Market Capitalization*, BLOCKCHAIN, https://blockchain.info/charts/market-cap?timespan=all&showDataPoints=false&daysAverageString=1&show_header=true&scale=0&address (last visited (Apr. 16, 2014). *See generally* Robin Teigland, Zeynep Yetis & Tomas Larsson, *Breaking Out of the Bank in Europe - Exploring Collective Emergent Institutional Entrepreneurship Through Bitcoin*, SWEDISH NETWORK FOR EUROPEAN STUDIES IN ECONOMICS & BUSINESS, at 3, *available at*

Bitcoin transactions reportedly average about 30 transactions per minute, contrasted with about 200,000 transactions per minute for VISA.[130]

Figure 2: Bitcoin Market Capitalization[131]



[50] By Thanksgiving of 2013, an increase in media attention and publicity surrounding U.S. Senate hearings resulted in Bitcoin increasing

http://ssrn.com/abstract=2263707 (discussing the implications of the rapid growth of Bitcoin).

[130] François R. Velde, *Chicago Fed Letter, Bitcoin: A Primer*, 317 THE FEDERAL RESERVE BANK OF CHICAGO (Dec. 2013), *available at* http://www.chicagofed.org/digital_assets/publications/chicago_fed_letter/2013/cfldecember2013_317.pdf.

[131] BLOCKCHAIN.INFO, https://blockchain.info/charts/market-cap (last visited Sept. 11, 2014).

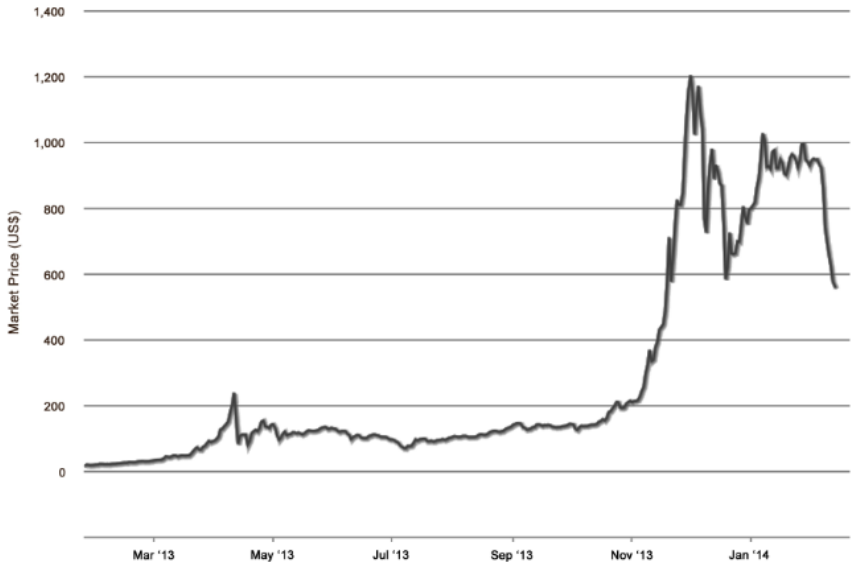
in value during one seven-day period from $615 per Bitcoin to more than $1,000 per Bitcoin on the Mt. Gox exchange, resulting in a total market capitalization in excess of $11 billion in US dollars.[132] Figure 3 illustrates the volatility of Bitcoin market price in US dollars during 2013, and through mid-February 2014.[133] On Tuesday, February 24, 2014, following the failure of the online marketplace, the price of Bitcoin, in what must be regarded as "an astonishing price recovery immediately following bad news," stood at $525 per Bitcoin, not far from where it was when the Mt. Gox news emerged on Monday night.[134]

[132] *See* Nick Bilton, *N.Y. Times Bits: A Surge in Value for Bitcoin and Currencies Similar to It,* N.Y. TIMES BITS BLOG (Nov. 27, 2013, 4:16 PM), http://bits.blogs.nytimes.com/2013/11/27/a-rise-in-attention-and-price-for-crypto-currencies/?_r=0; *see also* Marie Brière, Kim Oosterlinck & Ariane Szafarz, *Virtual Currency, Tangible Return: Portfolio Diversification with Bitcoins* (Working Paper, Sept. 2013), *available at* http://ssrn.com/abstract=2324780.

[133] *Bitcoin Market Price in US Dollars*, BLOCKCHAIN, *available at* https://blockchain.info/charts/market-price (last visited Apr. 16, 2014).

[134] Hiroko Tabuchi & Ben Protess, *Bitcoin Investors See Bright Side in Site's Failure*, INT'L N.Y. TIMES, Feb. 27, 2014, at 15, *available at* http://ihtbd.com/ihtuser/print/old%20THT/27-02-2014/a2702x15xxxxxxxxx.pdf.

Figure 3: Bitcoin Market Price[135]
(0,000,000s omitted)



[51] Approximately 90% ($10 billion) of the total virtual currency market value is represented by Bitcoin; but, "[b]ased on its volatile price behavior, Bitcoin is not a virtual currency but a high-risk virtual commodity, in a hyper-asset bubble that has begun to pop" and "Bitcoin the pseudo currency and Bitcoin the low-cost payment system are dependent on each other and inseparable."[136] Barber, Boyen, Shi, and

[135] BLOCKCHAIN.INFO, *supra* note 131.

[136] Williams, *supra* note 14, at 1; *see also id.* at n. 2 (observing "Bitcoin is the equivalent of the locomotive while the payment system is the rails that allow it to move. If the engine does not work no matter how well built the rails, they won't be used."). *See generally* George Selgin, *Synthetic Commodity Money* (Univ. of Ga. Dept. of Econ., Working Paper, Apr. 10, 2013), *available at* http://ssrn.com/abstract=2000118 (discussing Bitcoin as a synthetic commodity currency); David Groshoff, *Kickstarter My Heart: Extraordinary Popular Delusions and the Madness of Crowdfunding Constraints and Bitcoin Bubbles*, 5 WM. & MARY BUS. L. REV. (forthcoming 2014), *available at* http://ssrn.com/abstract=2313396 (proposing a re-regulatory scheme that may provide a solution to combat the excessive volatility of Bitcoin bubbles); Joseph Chen-Yu Wang, *A*

Uzun observe that "Bitcoin assumes that the majority of nodes in its network are honest, and resorts to a majority vote mechanism for double spending avoidance, and dispute resolution. In contrast, most e-cash schemes require a centralized bank who is trusted for purposes of e-cash issuance, and double-spending detection."[137] Hammad Siddiqi contends that the market for Bitcoin is a "complex system without a stable equilibrium."[138]

[52] Bitcoin was created during 2009 by Satoshi Nakamoto, believed by many to be a pseudonymous hacker or hackers.[139] Moreover

> Nakamoto was inspired by an article written back in 1998 by Wei Dai, a graduate from the University of Washington. Dai envisioned a system in which "untraceable pseudonymous entities . . . [could] cooperate with each other more efficiently, by providing them with a medium of exchange and a method of enforcing contracts." He sought to create a medium of exchange that avoided the need for

Simple Macroeconomic Model of Bitcoin (Bitquant Research Laboratories, Working Paper No. 1, Feb. 11, 2014), *available at* http://ssrn.com/abstract=2394024 (suggesting that bitcoin will not fall victim to the liquidity trap suggested by some economists).

[137] Simon Barber, Xavier Boyen, Elaine Shi & Ersin Uzun, *Bitter to Better – How to Make Bitcoin a Better Currency*, *in* FINANCIAL CRYPTOGRAPHY AND DATA SECURITY; 16TH INTERNATIONAL CONFERENCE, FC 2012 399, 400 (Angelos D. Keromytis ed., 2012), *available at* http://crypto.stanford.edu/~xb/fc12/bitcoin.pdf.

[138] Hammad Siddiqi, *The Routes to Chaos in the Bitcoins Market,* (Working Paper, Feb. 17, 2014), *available at* http://ssrn.com/abstract=2396997.

[139] *See* Barber, Boyen, Shi & Uzun, *supra* note 137, at 1. *But see* Julianne Pepitone, *Bitcoin Creator Satoshi Nakamoto Found, Newsweek Says,* NBC NEWS (Mar. 6, 2014), http://www.nbcnews.com/tech/tech-news/bitcoin-creator-satoshi-nakamoto-found-newsweek-says-n45871 (identifies 64-year-old California resident as the author), *and* Nathaniel Popper & Rachel Abrams, *Bitcoin's Mysterious Creator Is Said to Be Identified,* N.Y. TIMES (Mar. 6, 2014, 3:51 PM), http://dealbook.nytimes.com/2014/03/06/newsweek-unmasks-bitcoin-founder-stirring-ire/?_php=true&_type=blogs&_r=0 (raising doubts about the Newsweek report).

> intermediaries in electronic transactions, and one in which government involvement "[was] not [only] temporarily destroyed but permanently forbidden and permanently unnecessary. "
>
> Drawing on Dai's vision, Nakamoto created Bitcoin, the world's first private, decentralized digital currency. Unlike traditional fiat currencies, whose value is determined by law and underwritten by the state, Bitcoin is not backed by a government or legal entity. Bitcoin does not have a central authority in charge of the money supply or a central clearing house. Indeed, no traditional financial institutions are involved in Bitcoin transactions. Instead, users perform all steps of the transactions themselves.[140]

A. How Bitcoin Works

[53] Bitcoin can be described as a "Proof-of-Work (PoW) based currency that allows users to generate digital coins by performing computations."[141] Dorit Ron and Adi Shamir report that "[p]articipants begin using bitcoin by first acquiring a program called a Bitcoin wallet

[140] Nicholas Plassaras, *Regulating Digital Currencies: Bringing Bitcoin Within the Reach of the IMF*, 14 CHI. J. INT'L L. 377, 383 (2013) (*quoting* Morgen Peck, *Bitcoin: The Cryptoanarchists' Answer to Cash*, IEEE Spectrum (June 2012), *available at* http://spectrum.ieee.org/computing/software/bitcoin-the-cryptoanarchists-answer-to-cash (last visited Apr. 14, 2014); Wei Dai, *B-Money* (1998), http://weidai.com/bmoney.txt (last visited Apr. 14, 2014)); *see also* EUROPEAN CENTRAL BANK, *supra* note 127, at 6; J.P., *Virtual Currency: Bits and Bob*, THE ECONOMIST (June 13, 2011, 8:30 PM), http://www.economist.com/blogs/babbage/2011/06/virtual-currency (last viewed Apr. 14, 2014).

[141] Elli Androulaki, Ghassan O. Karame, Marc Roeschlin, Tobias Scherer & Srdjan Capkun, *Evaluating User Privacy in Bitcoin*, *in* FINANCIAL CRYPTOGRAPHY AND DATA SECURITY; 17TH INTERNATIONAL CONFERENCE, FC 2013 34, 34 (Ahmad-Reza Sadeghi ed., 2013), *available at* http://book.itep.ru/depository/bitcoin/User_privacy_in_bitcoin.pdf.

and one or more Bitcoin addresses."[142] Stored on a computer's hard drive as electronic files, Bitcoins "can be accumulated or transferred just like an e-mail. Software algorithms embedded in the online Bitcoin network protect against fraud and ensure that the files are not counterfeited."[143] By using a peer-to-peer network to distribute a master transparent public ledger called the Blockchain, each Bitcoin transaction is registered for all to see. The Blockchain is used to verify that the identical Bitcoins haven't been used in a previous transaction, thereby preventing "double spending" of the same Bitcoins.[144] Brito and Castillo observe

> [T]ransactions on the Bitcoin network are not denominated in dollars or euros or yen as they are on PayPal, but are instead denominated in bitcoins. This makes it a virtual currency in addition to a decentralized payments network. The value of the currency is not derived from gold or government fiat, but from the value that people assign to it.

[142] Dorit Ron & Adi Shamir, *Quantitative Analysis of the Full Bitcoin Transaction Graph*, *in* FINANCIAL CRYPTOGRAPHY AND DATA SECURITY; 17TH INTERNATIONAL CONFERENCE, FC 2013 6, 8 (Ahmad-Reza Sageghi ed., 2013), *available at* https://eprint.iacr.org/2012/584.pdf.

[143] Plassaras, *supra* note 140, at 379. *See generally* Jörg Becker, Dominic Breuker, Tobias Heide, Justus Holler, Hans Peter Rauer & Rainer Böhme, *Can We Afford Integrity by Proof-of-Work? Scenarios Inspired by the Bitcoin Currency* (Workshop on the Economics of Information Security WEIS 2012 Working Paper, Feb. 24, 2012), *available at* http://ssrn.com/abstract=2041492 (discussing the intricacies of the Bitcoin system); Sarah Jeong, *The Bitcoin Protocol as Law, and the Politics of a Stateless Currency* (Harv. L. Sch. Seminar "The Constitutional Law of Money" Working Paper, May 8, 2013), *available at* http://ssrn.com/abstract=2294124 (discussing the complex Bitcoin technology).

[144] Jerry Brito & Andrea Castillo, *Bitcoin: A Primer for Policymakers*, George Mason University Mercatus Center 4 (Dec. 19, 2013). *But see* Nicolas Houy, *It Will Cost You Nothing to 'Kill' a Proof-of-Stake Crypto-Currency* 2, 4 (University of Lyon-GATE Working Paper, 2014), *available at* http://ssrn.com/abstract=2393940. *But see generally* Androulaki et al., *supra* note 141 (describing several authors who contend that double-spending attacks can be successful).

> The dollar value of a bitcoin is determined on an open market, just as is the exchange rate between different world currencies.[145]

[54] Worldwide in scope, Bitcoin "can be used as a currency for all kinds of transactions (for both virtual and real goods and services), thereby competing with official currencies . . . [However,] it does not have a central clearing house, nor are there any financial or other institutions involved in the transactions."[146] Bitcoin exists with "no central authority in charge of the money supply [since] . . . the money supply is determined by a specific type of [data] 'mining' activity. It depends on the amount of resources (electricity and CPU time) that 'miners' devote to solving specific mathematical problems."[147] The Bitcoin *mining process* "involves repeatedly running a computationally intensive mathematical function (called a cryptographic hash function) on a set of randomly seeded inputs until a specific pattern pops up. . . . The results are publicized on the Internet for the rest of the Bitcoin network."[148] At the time of writing, March 2014, the Bitcoin network hash rate (total number of hashes per second made by all players) is estimated to be in the neighborhood of 30,000 trillion hashes per second (30,000 Thash/s), having increased at an astonishing rate due to "more efficient specialized mining hardware now available on the market."[149] At this rate, Bitcoin

[145] Brito & Castillo, *supra* note 144, at 4.

[146] EUROPEAN CENTRAL BANK, *supra* note 127, at 21; *see also* Marc Pilkington, *Bitcoin and Complexity Theory: Some Methodological Implications* (University of Burgundy Working Paper, Oct. 14, 2013), *available at* http://ssrn.com/abstract=2340007 (investigating the foundations of Bitcoin).

[147] EUROPEAN CENTRAL BANK, *supra* note 127, at 21.

[148] Paul Ford, *Marginally Useful*, MIT TECH. REV. (Feb. 18, 2014), http://www.technologyreview.com/review/524691/marginally-useful.

[149] E-mail from Edward W. Felten, Robert E. Kahn Professor of Computer Science and Public Affairs & Director, Center for Information Technology Policy, Princeton

has become one of the largest distributed computational efforts ever. Over a year earlier, with a hash rate of less than 1% the current rate, Kroll, Davey and Felten observed that "taken as a whole, the Bitcoin transaction verification network is more powerful than the combined computing power of the top 500 supercomputers in the world, giving pause to anyone concerned about whether the costs of transaction verification in Bitcoin are acceptable."[150] I have written this article to be readable by those not possessing an advanced degree in computer science. Therefore, while I present minimal math, a wealth of cryptographic rich research is available.[151] Babaioff, Dobzinski, Oren and Zohar present the following account:

University, to Lawrence J. Trautman (March 6, 2014) (on file with author); *see also Bitcoin Hash Rate*, BLOCKCHAIN, *available at* http://blockchain.info/charts/hash-rate.

[150] Kroll, Davey & Felten, *supra* note 123, at 8.

[151] *See generally* Androulaki, *supra* note 141 (analyzing the privacy guarantees of Bitcoin in a setting where Bitcoin is used as a primary currency for daily transactions of individuals); Marcin Andrychowicz et al., *Secure Multiparty Comnputations on Bitcoin* (2014), *available at* http://eprint.iacr.org/2013/784 (showing how the unique properties of Bitcoin can be used in the area of secure multiparty computation protocols (MPCs)); Marcin Andrychowicz et al., *Fair Two-Party Computations Via Bitcoin Deposits* (2014), *available at* https://eprint.iacr.org/2013/837 (explaining how Bitcoin can be used to obtain fairness in a two-party secure computation protocol); Marcin Andrychowicz et al., *How to Deal With Malleability of BitCoin Transactions* (2013), *available at* http://arxiv.org/abs/1312.3230 (discussing the malleability of Bitcoin transactions); Moshe Babaioff et al., *On Bitcoin and Red Balloons*, ACM Conference on Electronic Commerce (EC'12) (2012), *available at* http://www.cs.huji.ac.il/~avivz/pubs/12/Bitcoin_EC0212.pdf (proposing a modification to the Bitcoin protocol to help eliminate various problems with the virtual currency scheme); Alex Coventry, *NooShare: A Decentralized Ledger of Shared Computational Resources* (2012), *available at* http://web.mit.edu/alex_c/www/nooshare.pdf (describing NooShare, a decentralized ledger similar to Bitcoin); Ittay Eyal & Emin Gün Sirer, *Majority is not Enough: Bitcoin Mining is Vulnerable*, (forthcoming in Proceeds of the 18th International Conference on Financial Cryptography and Data Security, March 2014), *available at* http://arxiv.org/abs/1311.0243 (presenting an attack on the Bitcoin protocol that would result in Bitcoin ceasing to be a decentralized currency); Ilja Gerhardt & Timo Hanke, *Homomorphic Payment Addresses and the Pay-to-Contract Protocol* (2012), *available at* http://arxiv.org/abs/1212.3257 (proposing the design of a

> The basic setup of electronic transactions relies on public key cryptography. When Alice wants to transfer 50 coins to Bob, she signs a transaction using her private key. Hence, everyone can verify that Alice herself initiated this transaction (and not someone else). Bob, in turn, is identified as the target of the transfer using his public key. For the money to be actually transferred from Alice's account to Bob's account, some entity has to keep track of the last owner of the coins, and to mark Bob as the new owner. Otherwise, Alice could "double spend" her money. First transfer the coins to Bob, then transfer the same coins again to Charlie. Traditionally, this role was fulfilled by banks. In return, banks tended to charge high fees, for example in international transfers.[152]

[55] A report by the European Central Bank states that "[b]itcoins are divisible to eight decimal places enabling their use in any kind of transaction, regardless of the value. . . . [T]ransactions are carried out faster and more cheaply than with traditional means of payment. Transaction fees, if any, are very low and no bank account fee is charged."[153] Luther and Olson note that crypto-currency Bitcoin "functions as a public record-keeping device. As such, it serves as an

deterministic bitcoin wallet); Fergal Reid & Martin Harrigan, *An Analysis of Anonymity in the Bitcoin System*, *available at* http://arxiv.org/abs/1107.4524 (investigating an alleged theft of Bitcoins using various techniques); Ron & Shamir, *supra* note 142; Meni Rosenfeld, *Analysis of Hashrate-based Double-spending* (2014), *available at* http://arxiv.org/abs/1402.2009 (analyzing the stochastic processes of Bitcoin, which underlie typical attacks and assessing the resulting probabilities of success); Emily Shen, Elaine Shi & Brent Watters, *Predicate Privacy in Encryption Systems* (2008), *available at* https://www.cs.umd.edu/users/elaine/docs/sympredenc.pdf (analyzing predicate encryption).

[152] Babaioff et al., *supra* note 151, at 16-17.

[153] EUROPEAN CENTRAL BANK, *supra* note 127, at 21.

alternative to historically accepted monies while enabling transactions in much the same way."[154] Teigland, Yetis, and Larsson report that "[a] deal in December 2012 with French financial firms Aqoba and Credit Mutuel led to Bitcoin-Central, a currency exchange, being awarded an International Bank ID number and becoming a Payment Services Provider equal to services such as PayPal."[155]

B. Bitcoin Vulnerabilities

[56] Any discussion of virtual currencies must acknowledge that any such mathematically devised protocol is vulnerable to superior future cryptography advances that trump our present understanding of the boundaries of cybersecurity. Kroll, Davie, and Felten observe that "[s]uccess of the Bitcoin economy requires that Bitcoin's distributed protocols operate and remain stable."[156] Assuming that those involved behave as incentivized and in their own perceived best interest, three types of consensuses are required (each depending mutually on the other two) for Bitcoin to remain a success:

1. Consensus about Rules*:* Players must agree on criteria to determine which transactions are valid. Only valid

[154] William J. Luther & Josiah Olson, *Bitcoin is Memory* 2 (Kenyon College Working Paper, June 7, 2013), *available at* http://ssrn.com/abstract=2275730.

[155] Teigland et al., *supra* note 129, at 3.

[156] Kroll, Davey & Felten,, *supra* note 123, at 6; *see also* Mitsuru Iwamura, Yukinobu Kitamura & Tsutomu Matsumoto, *Is Bitcoin the Only Cryptocurrency in the Town*? *Economics of Cryptocurrency and Fredrich A. Hayek* 12 (Hitotsubashi University Institute of Economic Research Working Paper, Feb. 28, 2014), *available at* http://ssrn.com/abstract=2405790 (concluding that Bitcoin will be taken over by other cryptocurrencies with similar but somewhat improved technical as well as security structures); Tetsuya Saito, *Bitcoin: A Search-Theoretic Approach*, INT'L J. INNOVATION IN THE DIGITAL ECON. 16 (forthcoming 2014), *available at* http://ssrn.com/abstract=2405013 (assessing the stability of Bitcoin in the market as a payment method).

transactions will be memorialized in the Bitcoin log; but this requires agreement on how to determine validity.

2. *Consensus about State:* Players must agree on which transactions have actually occurred, that is, they must agree on the history of the Bitcoin economy, so that there is a common understanding of who owns which coin at any given time.

3. *Consensus that Bitcoins are Valuable:* Players must agree that Bitcoins have value so that players will be willing to accept Bitcoins in payment.[157]

[57] For purposes of our Bitcoin vulnerabilities discussion, I suggest that the following issues are among the most significant threats: (1) the 51% attack, (2) The Goldfinger attack, (3) privacy concerns, and (4) loss of confidence due to a significant decline in the price of Bitcoin resulting in a disincentive to mine. Many other potential threats exist such as: a deflationary spiral; denial-of-service attacks; or hoarding of Bitcoin due to its appreciation potential.[158]

[58] Among attacks intended to "destabilize consensus about the rules or state of Bitcoin,"[159] the 51% attack arises when Bitcoin's miners (or a single individual or cartel acting in concert) hold a majority of the network's capacity for puzzle-solving (mining).[160] This is a known design

[157] Kroll, Davey & Felten, *supra* note 123, at 6.

[158] *See* Barber, Boyen, Shi & Uzun, *supra* note 137, at 6; *and* Marie Vasek, Micah Thornton & Tyler Moore, *Empirical Analysis of Denial-of-Service Attacks in the Bitcoin Ecosystem* 1, *available at* http://fc14.ifca.ai/bitcoin/papers/bitcoin14_submission_17.pdf.

[159] Kroll, Davey & Felten, *supra* note 123, at 11.

[160] *See* Barber, Boyen, Shi & Uzun, *supra* note 137, at 6. *See also* Vasek et al., *supra* note 158, at 11; *See also* Philipp Güring & Ian Grigg, *Bitcoin & Gresham's Law – The Economic Inevitability of Collapse* 5 (Oct.-Dec. 2011), *available at* http://iang.org/papers/BitcoinBreachesGreshamsLaw.pdf (contending that botnets can

problem because the Bitcoin developers made the assumption that an effective cartel of miners would never develop. Kroll et al.. observe:

> [A] cartel can change any rules which are enforced by consensus and players who are not in the cartel will likely be obliged to follow. . . An interesting facet of mining cartels is that they can censor certain transactions. The cartel can choose to ignore any transaction it does not want appended to the log . . . [However,] a 51% cartel attack is unlikely to generate enough reward within the Bitcoin economy to be worthwhile to the attacker.[161]

[59] In a highly controversial paper, Cornell University computer scientists Ittay Eyal and Emin Gün Sirer warn that "[t]he Bitcoin ecosystem is open to manipulation, and potential takeover by miners seeking to maximize their rewards . . . [because] [h]igher revenues can lead new rational miners to join selfish miner pools, leading to a collapse of the decentralized currency."[162] Eyal and Gün Sirer further contend that

operate at a zero cost of power- therefore, stolen electricity will drive out honest mining, resulting in inevitable collapse of Bitcoin).

[161] Kroll et al., *supra* note 123 at 11-13.

[162] Eyal & Gün Sirer, *supra* note 151 at 15. *Compare* Ed Felton, *Game Theory and Bitcoin*, FREEDOM TO TINKER (Nov. 11, 2013), https://freedom-to-tinker.com/blog/felton/game-thory-and-bitcoin/ (disagreeing with the findings of the Eyal and Gün Sirer paper), *and* Ed Felton, *Bitoin Isn't So Broken After All,* FREEDOM TO TINKER (Nov. 7, 2013), https://freedom-to-tinker.com/blog/felton/bitcoin-inst-so-broken-after-all (finding contrary to the Eyal and Gün Sirer paper that a group of minors will not be stable) *with* Eyal & Gün Sirer, *Response to Feedback on Selfish Mining*, HACKING DISTRIBUTED (Nov. 14, 2013, 9:45 AM), https://hackingdistributed.com/2013/11/14/response-to-feedback-on-selfish-mining *and* E-mail from Ittay Eyal, post-doc, Systems and Networking Group. Dep't of Computer Science, Cornell University to Lawrence J. Trautman (Mar. 10, 2014, 7:58 CST) (on file with author) (contending Felton's main comment arises from a misunderstanding of a blog post published by Eyal & Gün Sirer and not with the actual paper). *But cf.*, Arvind Narayanan & Andrew Miler, *Why the Cornell Paper on Bitcoin Mining is Important,* FREEDOM TO TINKER (Nov. 9, 2013), https://freedom-to-

> [T]he upper bound on threshold size is 1/3: the protocol will never be safe against attacks by a selfish mining pool that commands more than 33% of the total mining power of the network. This upper bound is substantially lower than the 50% figure currently assumed, and difficult to achieve in practice.[163]

[60] The Goldfinger attack is named after the James Bond novel by Ian Flemming and movie of the same name. The novel's villain attempts to ruin the gold-backed U.S. currency by causing the underlying gold held at Fort Knox to become radioactive and therefore worthless.[164] Accordingly, in a Bitcoin Goldfinger attack, a 51% majority of miners seeks to "destroy the Bitcoin economy in order to achieve utility *outside* the Bitcoin economy."[165] Kroll et al. identify at least three potential (and expensive) motivations for such an attack: (1) a sovereign or institution may determine to disrupt Bitcoin for its own purposes (2) attack by a non-state actor (public protest such as an *Occupy Bitcoin*, etc.); and (3) an attacker may be motivated by an investment gain such as one derived by selling-short the underlying Bitcoin and closing the position at a gain.[166]

---

tinker.com/blog/randomwalker/why-the-cornell-paper-on-bitcoin-mining-is-important/ (observing that Eyal & Gün Sirer's paper is the first time a serious issue has been raised with Bitcoin's consensus mechanism and has exploited the peer-to-peer aspect of the system).

[163] Eyal & Gün Sirer, *supra* note 151 at 3.

[164] IAN FLEMING, GOLDFINGER (Thomas & Mercer 2012); *see also* GOLDFINGER (Eon Productions 1964).

[165] Kroll et al., *supra* note 123 at 13.

[166] Kroll et al., *supra* note 123 at 13 (citing J. Becker et al., *Can We Afford Integrity by Proof-of-Work? Scenarios Inspired by the Bitcoin Currency*, *in* WORKSHOP ON THE ECONOMICS OF INFORMATION SECURITY(2012) (emphasizing proposition two i.e. non-state actors)).

[61] Privacy concerns constitute another significant threat to the future viability of Bitcoin. Research conducted by Androulaki, Karame, Roeschlin, Scherer and Capkun find:

> [T]he current measures adopted by Bitcoin are not enough to protect the privacy of users if Bitcoin were to be used as a digital currency in realistic settings . . . [I]f Bitcoin is used as a digital currency to support the daily transactions of users in a typical university environment, then behavior-based clustering techniques can unveil, to a large extent, the profiles of 40% of Bitcoin users, even if these users try to enhance their privacy by manually creating new addresses.[167]

[62] The last on our abbreviated list of selected threats lies in the potential "death spiral"[168] that will likely be created if the price of Bitcoin declines to a point where there is no longer an economic incentive to mine

[167] Androulaki et al., *supra* note 141 at 15. *See also* Joseph Bonneau et al., *Mixcoin Anonymity for Bitcoin with Accountable Mixes*, Financial Cryptography & Data Conference (Mar. 307, 2014), *available at* https://eprint.iacr.org/2014/077 (last updated April 21, 2014) (proposing a protocol to facilitate anonymous payments utilizing the Bitcoin system); Philip Koshy, Diana Koshy & Patrick McDaniel, *An Analysis of Anonymity in Bitcoin Using P2P Network Traffic*, Financial Cryptography & Data Conference (Mar. 3-7, 2014), *available at* http://ifca.ai/fc14/papers/fc14_submission_71.pdf; (developing "heuristics for identifying ownership relationships between Bitcoin addresses and IP addresses"); Malte Möser, *Anonymity of Bitcoin Transactions*: *An Analysis of Mixing Services*, Münster Bitcoin Conference (July 17-18, 2013), https://www.wi.uni-muenster.de/sites/default/files/public/department/itsecurity/mbc13/mbc13-moeser-paper.pdf (examining three types of services that claim to increase Bitcoin anonymity); Michele Spagnuolo, Frederico Maggi & Stefano Zanero, *BitIodine: Extracting Intelligence from the Bitcoin Network*, Financial Cryptography & Data Conference (Mar. 3-7, 2014), *available at* http://fc14.ifca.ai/papers/fc14_submission_11.pdf(presenting BitIodine, a modular framework that can be used to build a library for more complex Bitcoin forensic analysis tools).

[168] Kroll et al., *supra* note 123 at 8.

additional Bitcoin. For a currency of any type to maintain value it must sustain confidence in its ability to serve as a store of value. Kroll, Davey, and Felten depict the following scenario:

> [L]oss of confidence in Bitcoin could cause the Bitcoin price to go down, a falling price lowers the incentive to mine and the equilibrium mining rate, lower mining rate leads to the currency being easier to subvert, and this leads to a further loss of confidence in the currency. Such a death spiral reflects the perceived loss of consensus in the value game . . .[169]

C. The Promise of Bitcoin

[63] Brito and Castillo in their report, *Bitcoin: A Primer for Policymakers,* highlight the many ways in which Bitcoin may be used to "improve the quality of life for the world's poorest. Improving access to basic financial services is a promising antipoverty technique."[170] The authors state "[t]o better understand why people might want to use Bitcoin, it helps to think of it, not necessarily as a replacement for traditional currencies, but rather as a new payments system."[171] The lower cost of Bitcoin assists small businesses by providing an alternative to expensive credit cards, enabling migrants to make cheaper remittances of payments to their families in developing countries, helping to protect individuals from censorship and capital controls, providing oppressed groups with financial privacy, and facilitating innovation and micropayments.[172]

---

[169] *Id.*

[170] Brito & Castillo, *supra* note 144 at 14, (citing MUHAMMAD YUNUS, BANKER TO THE POOR: MICRO-LENDING AND THE BATTLE AGAINST WORLD POVERTY (Public Affairs, 2003).

[171] Brito & Castillo, *supra* note 144 at 10.

[172] *See, e.g., id.* at 10-16.

D. Lower Transaction Costs

[64] Bitcoin offers the promise of substantially lower transaction costs for small merchants worldwide. Because Bitcoin transactions do not involve a third party (financial intermediary or institution), costly credit card charges are avoided.

> Credit cards have greatly expanded the ease of transacting, but their use comes with considerable costs to merchants. Businesses that wish to offer the option of credit card payments to their customers must first pay for a merchant account with each credit card company. Depending on the terms of agreement with each credit card company, businesses must then pay a variety of authorization fees, transaction fees, statement fees, interchange fees, and customer-service fees, among other charges.[173]

Bitcoin makes lower transaction costs possible, thus enabling (1) financial services to those populations currently without access to financial services, and (2) a multitude of micropayment services. In addition, the ability to

[173] Brito & Castillo, *supra* note 144 at 10. *See generally* Wilko Bolt, *Retail Payment Systems: Competition, Innovation, and Implications* (De Nederlandsche Bank, Working Paper No. 362, 2012), *available at* http://ssrn.com/abstract=2192046 (assessing key factors that affect pricing, competition, and incentives to innovate in the payment market); Marc Bourreau & Marianne Verdier, *Interchange Fees and Innovation in Payment Systems*, (2013), *available at* http://ssrn.com/abstract=2244160 (analyzing the impact of interchange fees on consumers' and merchants' incentives to adopt a payment instrument); David S. Evans et al., *Interchange Fees: The Economics and Regulation of What Merchants Pay for Cards*, (Dec. 17, 2011), *available at* http://ssrn.com/abstract=1974023 (examining the economics and regulation of interchange fees); David S. Evans, *Payments Innovation and Interchange Fees Regulation: How Inverting the Merchant-Pays Business Model Would Affect the Extent and Direction of Innovation* (June 27, 2011), *available at* http://ssrn.com/abstract=1878825 (examining the possible impact of a reduction in interchange fees on innovation involving payment cards).

make the transfer of funds available with lower transaction costs bodes well for global poverty reduction "by improving access to capital."[174]

E. Remittances

[65] One of the major potential benefits provided by Bitcoin may be in the marketplace for remittances sent by immigrants in developed countries (where the jobs are) to their relatives back home in developing countries. According to World Bank estimates, "remittances totalled [sic] USD 440 billion in 2010, of which USD 325 billion went to developing countries, involving some 192 million migrants or 3.0% of world population. For some individual recipient countries, remittances can be as high as a third of GDP."[175] The World Bank reports that "[r]emittance prices are high for many reasons, including underdeveloped financial infrastructure in some countries, limited competition, regulatory obstacles, lack of access to the banking sector by remittance senders and/or receivers, and difficulties for migrants to obtain the necessary identification documentation to enter the financial mainstream."[176] In addition,

> [T]he single most important factor leading to high remittance prices is lack of transparency in the market. It is difficult for consumers to compare prices because there are several variables that compose remittance prices. Prices for remittances are frequently made up of a fee charged for sending a certain amount, a margin taken on the exchange rate when remittances are paid and received in different currencies, and, at times, a fee charged to the recipient of

[174] Brito & Castillo, *supra* note 144 at 10.

[175] *Remittance Market Outlook*, Financial & Private Sector Development, WORLD BANK, http://web.worldbank.org/WBSITE/EXTERNAL/TOPICS/EXTFINANCIALSECTOR/0,,contentMDK:22121552~menuPK:6127416~pagePK:210058~piPK:210062~theSitePK:282885~isCURL:Y,00.html (last visited Sept. 10, 2014).

[176] *Id.*

> the funds. These fee components may also vary according to how the receiver is paid (i.e. cash or by creating an account), the speed of the transfer, and the ability of the sender to provide information about the recipient (i.e. bank account number).
>
> In addition, a lack of transparency in the market has had the impact of reducing competition, as consumers tend to patronize traditional market players because they are not aware of other players, and/or cannot compare the services they usually buy against other product.[177]

[66] The average cost of remitting funds during the 4th quarter of 2013 from G20 nations is reported by the World Bank to be 8.16%, contrasted with a cost of 12.33% for using a commercial bank to send funds.[178] The cost of using post offices stands at 4.12% for the same time period; cash products are among the least expensive averaging 7.34%; and "[a]ccount-to-account products are among the most expensive, with an average cost of 12.74 percent; however, the cost of transferring money within the same bank or to a partner bank is significantly lower."[179] The cost of remitting funds varies widely from country to country with Italy, Russia, the United Kingdom and the United States below the average cost found among G8 countries of 8.20 percent during the 4th quarter of 2013.[180] Of particular note, "South Africa remains the costliest remittance sending country in the G20 group, with an average of 18.16 [percent], followed by Japan with an average of 15.73 percent. The least expensive sending country, together

[177] *Id.*

[178] World Bank, *An Analysis of Trends in the Average Total Cost of Migrant Remittance Services*, 8 REMITTANCE PRICES WORLDWIDE 8, 2 (Dec. 2013), *available at* https://remittanceprices.worldbank.org/sites/default/files/RPW_Report_Dec2013.pdf.

[179] *Id.*

[180] *Id.* at 5.

with Russia, is Saudi Arabia (4.19 [percent]), followed by Korea (6.08 [percent]) and the USA (6.18 [percent]).”[181] The market for remittances is most troubling in Africa, as “[t]he Sub-Saharan Africa region remains the most expensive region in the world to send money to, and has registered a further increase from 12.29 in 3Q 2013 to 12.55 in 4Q 2013 . . .”[182]

F. Censorship, Human Rights, and Financial Privacy

[67] Daniel Solove writes, “[w]e are in the midst of an information revolution, and we are only beginning to understand its implications. . . . [W]e have undergone a dramatic transformation in the way we shop, bank, and go about our daily business . . . .”[183] Professor Jack Balkin observes that “the most important decisions affecting the future of freedom of speech will not occur in constitutional law; they will be decisions about technological design, legislative and administrative regulations, the formation of new business models, and the collective activities of end-users.”[184] The interconnected culture of oppressive censorship, bribery, corruption and extortion “is an amorphous cancer eating away at our societies with the very real potential to destroy commerce between nations and produce destructive global civil unrest.”[185] Richard Alderman, Director of the U.K.’s Serious Fraud Office (SFO) observes:

> I have been following . . . the events of the Arab Spring with the very greatest of interest. I have also been looking

[181] *Id.* at 6.

[182] *Id.* at 8.

[183] Daniel J. Solove, *Privacy and Power: Computer Database and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1394 (2001).

[184] Jack M. Balkin, *The Future of Free Expression in a Digital Age*, 36 PEPP. L. REV. 427, 427 (2009).

[185] Lawrence J. Trautman & Kara Altenbaumer-Price, *Lawyers, Guns and Money - The Bribery Problem and U.K. Bribery Act*, 47 INT’L LAW 481, 483 (2013) *available at* http://ssrn.com/abstract=2276738.

> at what has been happening recently in India, China, Russia, and other countries. When I look, in particular, at the Arab Spring I see that corruption is one of the top issues raised by the citizens of these countries as one of their main grievances against the government or, indeed in some cases, the former government. Some say that bribery is part of the culture of those countries and that we must respect it. The citizens of those countries have demonstrated very clearly to my mind that this is not part of the culture that they are prepared to accept any longer.[186]

[68] Internet technology has gradually become a tool of dissidence in repressed nations all over the world − to spread information, plan and

[186] *Id.* at 483 (citing Richard Alderman, Director, U.K. Serious Fraud Office, Keynote Address at the Risk Advisory Dinner (Oct. 5, 2011), *transcript available at* http://www.sfo.gov.uk/about-us/our-views/director's-speeches/speeches-2011/risk-advisory-dinner,-washington-dc.aspx).

organize activists and conduct protests.[187] Not surprisingly, repressive regimes see the Internet as a threat."[188]

[69] Bendrath and Mueller observe that technological advances "now allow [I]nternet service providers to monitor the content of data packets in real-time and make decisions about how to handle them. If deployed widely this technology, known as deep packet inspection (DPI), has the potential to alter basic assumptions that have underpinned Internet governance to date."[189] Mina Rady presents an excellent account of how

[187] *See, e.g.*, Uyen P. Le, *Online and Linked In: 'Public Morals' in the Human Rights and Trade Networks*, 38 N.C.J. INT'L L. & COM. REG. 107, 109 (2012); Antonio A. Casilli & Paola Tubaro, *Why Net Censorship in Times of Political Unrest Results in More Violent Uprisings: A Social Simulation Experiment on the UK Riots* 10 (Aug. 14, 2011), *available at* http://ssrn.com/abstract=1909467; James D. Fielder, *Dissent Versus the (Online) Surveillance State: Measuring Authoritarian Control of the Internet* 21, APSA 2011 Annual Meeting Paper, *available at* http://ssrn.com/abstract=1901908 (finding while authoritarian regimes do have some success in mitigating Internet-driven dissent, increasing Internet user bases ultimately reduce the ability of regimes to control online communication); Philip N. Howard, Sheetal D. Agarwal & Muzammil M. Hussain, *When Do States Disconnect Their Digital Networks? Regime Responses to the Political Uses of Social Media* 6 (Aug. 9, 2011), *available at* http://ssrn.com/abstract=1907191; Muzammil M. Hussain & Philip Howard, *Democracy's Fourth Wave? Information Technologies and the Fuzzy Causes of the Arab Spring* 3 & 12 (Mar. 27, 2012); Aleksey Ponomarev, *Balancing Internet Regulation and Human Rights* (2010), *available at* http://ssrn.com/abstract=1990182; Courtney C. Radsch, *Digital Dissidence & Political Change: Cyberactivism and Citizen Journalism in Egypt* 6-7, Doctoral Dissertion, American University, School of International Service (Dec. 2013), *available at* http://ssrn.com/abstract=2379913.

[188] Ramesh Subramananian, Commuications of the International Information Management Association [CIIMA], *The Growth of Global Internet Censorship and Circumvention: A Survey*, Vol. 11, Iss. 2 at 69 (2011), *available at* http://www.iima.org/index.php?option=com_phocadownload&view=category&download=331:the-growth-of-global-internet-censorship-and-circumvention-a-survey&id=56:2011-volume-11-issue-2&Itemid=68. *See generally* Derek E. Bambauer, *Cybersieves*, 59 DUKE L.J. 377, 378 (2009).

[189] Ralf Bendrath & Milton Mueller, *The End of the Net as We Know it? Deep Packet Inspection and Internet Governance* 1 (Aug. 4, 2010), *available at* http://ssrn.com/abstract=1653259. *See* Hal Roberts, Ethan Zuckerman & John G.

cyber-based assets have proven significant to citizen activists as they organize against repressive regimes in Cairo, Egypt and Iran.[190] In the particular case of Egypt, Rady observes:

> 1. Social media played a critical role in calling for and mobilizing for collective action (either via passive strikes in 2008 or via active protests in 2011). However, the impact of proxies and social networking in January 2011 was [sic] critical sparks lead[ing] to the subsequent events. With access to proxy channels, Egyptian Internet users prolonged their communication span, so that when Government decided to shut down the Internet the situation had already worsened well beyond [the] tipping point.
>
> 2. This case is that of a repressive regime that can no longer enforce controls on the behavior of their citizens given their use of a communication technology initially based by a major power.[191]

G. Capital Controls

[70] Bitcoin has already proven to be an asset to those living in countries having strict restrictions on the movement of Capital. Financial

---

Palfrey, *2011 Circumvention Tool Evaluation* at 1-3 (Berkman Center Research Publication No. 2011-08), *available at* http://ssrn.com/abstract=1940455. *See generally* Hadi Asghari, Michel Van Eeten & Milton Mueller, *Unraveling the Economic and Political Drivers of Deep Packet Inspection*, GigaNet 7th Annual Symposium (2012), *available at* http://ssrn.com/abstract=2294434 (examining the role of economic and political drivers of Deep Packet Inspection technology on typical use-cases).

[190] *See generally* Rady, *supra* note 42 (discussing how anonymity networks have become terrains for government-population conflict by enabling citizens to overpower the government's conventional control mechanisms).

[191] *Id.* at 14.

and currency crises are a constant threat in many parts of the world.[192] Graciela Kaminsky identifies ninety-six currency crises between January 1970 and February 2002 (pre sub-prime mortgage crisis of 2007-08) in Argentina, Bolivia, Brazil, Chile, Colombia, Denmark, Finland, Indonesia, Israel, Malaysia, Mexico, Norway, Peru, Spain, Sweden, the Philippines, Thailand, Turkey, Uruguay, and Venezuela.[193] Other scholars have written about the impact of the Russian 1998 crisis on Latin American

[192] *See generally* Graham Bird & Ramkishen S. Rajan, *Restraining International Capital Movements: What Does It Mean?*(Centre for International Economic Studies, Working Paper No. 0014, 2000), *available at* http://ssrn.com/abstract=231207 (discussing Chile and Malaysia's experiences with restraining capital movements); Benedict Clements & Herman Kamil, *Are Capital Controls Effective in the 21st Century? The Recent Experience of Colombia* (International Monetary Fund, Working Paper No. WP/09/30, 2009), available at http://www.imf.org/external/pubs/ft/wp/2009/wp0930.pdf (assessing the effects of capital controls on capital flows and exchange rate dynamics in Colombia in 2007); Kristin J. Forbes & Michael W. Klein, *Pick Your Poison: The Choices and Consequences of Policy Responses to Crises* (MIT Sloan School, Working Paper No. 5062-13, 2013), *available at* http://ssrn.com/abstract=2364457 (assessing the different strategies employed by countries in responding to crises); Reuven Glick & Michael Hutchison, *Capital Controls and Exchange Rate Instability in Developing Economies* (Pacific Basin Working Paper Series, Working Paper No. PB00-05), *available at* http://www.frbsf.org/economic-research/pbcpapers/2000/pb00-05.pdf (investigating whether legal restrictions on international capital flows are associated with greater currency stability); Hiro Ito, *Is Financial Openness a Bad Thing? An Analysis on the Correlation Between Financial Liberalization and the Output Performance of Crisis-Hit Economies*, (Santa Cruz Center for International Economics, Working Paper No. 04-23, 2004), *available at* http://sciie.ucsc.edu/workingpaper/2004/Ch3.pdf (investigating the link between capital account openness and the output cost associated with a currency crisis); Carmen M. Reinhart & Kenneth S. Rogoff, *Financial and Sovereign Debt Crises: Some Lessons Learned and Those Forgotten* (International Monetary Fund, Working Paper No. WP/13/266, 2013), *available at* http://www.imf.org/external/pubs/ft/wp/2013/wp13266.pdf (discussing the tools that advanced countries should use to overcome economic crises).

[193] Graciela Kaminsky, *Varieties of Currency Crises* 1 (National Bureau of Economic Research, Working Paper No. 10193, 2003), *available at* http://www.nber.org/papers/w10193.pdf.

countries,[194] and other examples of currency restrictions and lost purchasing power.[195] Nikoloski reports that it is the *currency* crisis, as opposed to *banking* or *sovereign debt* crises, that most significantly exacerbates the depth and incidence of poverty in the near term.[196]

[71] Argentina is but one example of the plight facing individuals caught up in economic crisis.[197] Scholars point to the uneasy lack of

[194] Guillermo A. Calvo & Ernesto Talvi, *Sudden Stop, Financial Factors and Economic Collpase in Latin America: Learning from Argentina and Chile* 1 (National Bureau of Economic Research, Working Paper No. 11153, 2005), *available at* http://www.nber.org/papers/w11153.pdf.

[195] *See generally* Pablo Bustelo, *Capital Flows and Financial Crises: A Comparative Analysis of East Asia (1997-98) and Argentina (2001-02)* at 3 (Complutense University of Madrid, Economics, Working Paper No. 2004-017, 2004), *available at* http://ssrn.com/abstract=612784 (exploring financial crises in emerging economies; specifically East Asia and Argentina); Wei Li, *Dealing with Capital Flows: Thailand in 2006*, (University of Virginia, Darden Case, Working Paper No. UVA-BP-0511, 2007), *available at* http://ssrn.com/abstract=1276570 (presenting a case that examines the different policy choices faced by Thailand in 2006).

[196] Zlatko Nikoloski, *"Impact of Financial Crises on Poverty in Developing World: An Empirical Approach,"* (Nov. 2, 2010), *available at* http://ssrn.com/abstract=1701894.

[197] *See, e.g.*, *Don't Cry for Me Argentina: Economic Crises and the Restructuring of Financial Property*, 14 FORDHAM J. CORP. & FIN. L. 771, 774 (2009); Nicolás Cachanosky & Adrián O. Ravier, *A Proposal of Monetary Reform for Argentina: Flexible Dollarization and Free Banking* (Jan. 13, 2014), *available at* http://ssrn.com/abstract=2378541 (proposing a monetary reform for Argentina); Horacio Spector; Enrique Alberola, Humberto López & Luis Servén, *Tango with the Gringo: The Hard Peg and Real Misalignment in Argentina* (World Bank Policy Research, Working Paper No. 3322, 2004), *available at* http://ssrn.com/abstract=610367; Werner Baer, Pedro Elosegui & Andrés A. Gallo, *The Achievements and Failures of Argentina's Neo-Liberal Economic Policies* (University of Illinois, Research, Working Paper No. 01-0114, 2001), *available at* http://ssrn.com/abstract=279383; Gerard Caprio, Michael P. Dooley, Danny Leipziger & Carl E. Walsh, *The Lender of Last Resort Function Under a Currency Board: The Case of Argentina* (World Bank Policy Research, Working Paper No. 1648, 1996), *available at* http://ssrn.com/abstract=620520; Guillermo Perry & Luis Servén, *The Anatomy of a Multiple Crisis: Why was Argentina Special and What Can We Learn From It?* (World Bank Policy Research, Working Paper No. 3081, 2003),

"confidence in Argentina's domestic currency and the banking sector due to the continuous changes in regulations on interest rates and foreign exchange markets as well as the forced conversions of bank deposits in 1985, 1989, and 2001 as triggers of runs against the [Argentine] peso."[198] Kaminsky, et al. observe that, "[t]he period from the mid-1970s to 2002 was as tumultuous as that of the earlier era and characterized by booms and busts in international capital flows, crises, and failed stabilization programs. During this period, Argentina had eight currency crises, four banking crises, and two sovereign defaults."[199] Daniel Kostzer notes that at the end of 2001, the Argentine government limited daily "money withdrawals from the banking system to a maximum of 300 pesos (equal to US$300 [sic])."[200] Hector Maletta reports:

> At the end of 2001 . . . the Argentine President resigned, the interim Government declared it would not continue serving its debts, and a widespread economic crisis ensued. The currency collapsed, banks were ordered to freeze deposits, and the nation's output fell . . . . The crisis also

available at http://ssrn.com/abstract=636443; Brad Setser & Anna Gelpern, *Argentina's Pathway Through Financial Crisis* (Rutgers School of Law-Newark Research, GEG, Working Paper No. 2004/02, 2004), *available at* http://ssrn.com/abstract=884225; Augusto de la Torre, Eduardo Levy Yeyati & Sergio L. Schmukler, *Living and Dying with Hard Pegs: The Rise and Fall of Argentina's Currency Board* (World Bank Policy Research, Working Paper No. 2980, 2003), *available at* http://ssrn.com/abstract=352380.

[198] Graciela Kaminsky, Amine Mati & Nada Choueiri, *Thirty Years of Currency Crises in Argentina: External Shocks or Domestic Fragility?* 8 *(*National Bureau of Economic Research, Working Paper No. 15478, 2009), *available at* http://ssrn.com/abstract=1501503(citing M. Kiguel & P. Neumeyer, *Seigniorage and Inflation: The Case of Argentina*, 27 J. MONEY, CREDIT & BANKING 672 (1995).

[199] *Id.* at 1.

[200] Daniel Kostzer, *Argentina: A Case Study on the Plan* Jefes y Jefas de Hogar Desocupados, *or the Employment Road to Economic Recovery* 2 (Levy Economics Institute of Bard College, Working Paper No. 534, 2008), *available at* http://ssrn.com/abstract=1132772.

> caused a rise in joblessness to 26% in the wake of the enormous contraction of consumption, investment and output. After a decade of price stability, inflation returned with a rise of 40.9% along 2002, especially during the first half of the year, and a further 23.5% distributed along 2003-2005, ... Time deposits were kept frozen for a long time, and those denominated in dollars were forcibly converted to pesos at a loss (in dollars) of about one half of their previous worth.[201]

These tragic developments meant those who had been assured by the Argentine government "that a peso was as good as a dollar, suddenly realized this was not the case. Not only a peso was not a dollar but . . . people did not want to hold the Argentine Currency. Yet because deposits were frozen, they were unable to dispose of unwanted pesos."[202] Thus, in December 2001, "[a]ngry Argentines remembered how high inflation during similar freezes in 1982 . . . and 1989 had robbed them of the real value of their savings."[203]

H. Innovation, Micropayments and Reducing World Poverty

[72] Innovation in financial markets will, as always, provide benefits not now envisioned. Among recent developments, "a cloud culture fueled by new media formats, mobile computing, and flash mobs has shifted the global disruption out of the workplace and into the streets. . . . [and] [d]isruptive innovations essentially redefine the value proposition for the

[201] Hector E. Maletta, *A Catastrophe Foretold: Economic Reform, Crisis, Recovery and Employment in Argentina* 1 (2007), *available at* http://ssrn.com/abstract=903124.

[202] Sebastian Edwards, *The Great Exchange Rate Debate After Argentina* 4 (National Bureau of Economic Research, Working Paper No. 9257, 2002), *available at* http://ssrn.com/abstract=336373.

[203] Steve H. Hanke & Kurt Schuler, *What Went Wrong in Argentina?*, CENTRAL BANKING, Feb. 2002, at 43, 45, *available at* http://ssrn.com/abstract=2204682.

customer."[204] During recent years, rapid technological change has produced a significant increase in the use of mobile payments.[205] As William Luther observes, "the widespread adoption of smartphones [sic] has made it easier to make and receive payments in person with electronic bank accounts and digital wallets. More recently, the development of inexpensive card-reading devices has enabled virtually anyone to accept electronic payments."[206] Jon Garon writes:

> Particularly in the area of payment systems, the implications of network effects will have a highly disintermediating impact. One particular payment system will become more readily used than the others, and as more objects can be purchased using that system, it will become more valuable and disrupt other systems. . . .
>
> Two competing networks drive network effects: the network of consumers and the network of merchants. The cost, convenience, social relevance, and network for the merchant may have quite a different value proposition than for the consumer. Merchants struggling to reduce the fees

[204] Jon Garon, *Mortgaging the Meme: Financing and Managing Disruptive Innovation*, 10 NW. J. TECH & INTELL. PROP. 441, 442-43 (2012).

[205] *See, e.g.*, Marc Bourreau & Marianne Verdier, *Cooperation for Innovation in Payment Systems: The Case of Mobile Payments*, 79 COMM. & STRATEGIES 95 (2010), *available at* http://ssrn.com/abstract=1810892. *See generally* Silvia Monica Elaluf-Calderwood, Jonathan Liebenau & Patrik Karrberg, *Privacy, Identity and Security Concerns: Enterprise Strategic Decision Making and Business Model Development for Mobile Payments in NFC* 2 (Mar. 1, 2012), *available at* http://ssrn.com/abstract=2014205 (assessing the use of near field communications technology in the public transport system); Kevin V. Tu, *Regulating the New Cashless World*, 65 ALA. L. REV. 77 (2013) (exploring the intersection of technology and consumer protection in the context of new and emerging payment systems).

[206] William Luther, *Cryptocurrencies, Network Effects, and Switching Costs* 3 (Mercatus Center, George Mason University, Working Paper No. 13-17, 2013), *available at* http://ssrn.com/abstract=2295134.

> they pay to current credit card companies are motivated to find less expensive alternatives, so some are promoting competition. . . . In short, the battle over payment systems will decide the future of the Fortune 100.[207]

It is clear that the challenges of reducing world poverty is intimately tied to issues involving reducing the transaction costs of remittances and the threat of capital/currency controls discussed above.[208] In turn, issues of global poverty are directly related to the propensity for outbreaks of civil war and terrorism.[209] Bracking and Sachikonye find:

> [R]emittances are critical to household wellbeing in Zimbabwe. . . . Indeed, it has become a commonplace in the research area of migration and development, and its subfield of poverty reduction and remittance studies, that international migration can have a positive impact on poverty reduction through the generation of migrant remittances[,] and, for the vast majority of researchers, that remittances are positively associated with economic growth. Within international development, much hope has been invested that remittances provide an accessible pathway out of poverty, and an alternative to inter-

[207] Garon, *supra* note 204, at 457.

[208] *See* Robert L. Hutchings & Bart M.J. Szewczyk, *The Global Future and Its Policy Implications: Views from Leading Thinkers on Five Continents*, The Atlantic Council of the United States (2009), *available at* http://ssrn.com/abstract=1881953. *See generally* Michael S. Barr, *Banking the Poor*, 21 YALE J. ON REG. 121 (2004) (exploring the use of new technology to increase access to banking by low income individuals and households).

[209] *See generally* Susan Rice, Corinne Graff & Janet Lewis, *Poverty and Civil War: What Policymakers Need to Know* (Brookings Global Economy and Development, Working Paper No. 2, 2006), *available at* http://ssrn.com/abstract=1015091 (questioning whether there is a link between income poverty and the risk of civil war).

governmental and official systems of development assistance.[210]

I. Bitcoin in China

[73] During November 2013, China Daily reported that "China now transacts half of the global Bitcoin volume and is a leader in pushing up the exchange rate."[211] About a week later, China Daily observed that "[a]n estimated 1.8 million Bitcoins were traded on BTC China in November [2013], the platform with the highest trading volume in the world, according to statistics gathered by bitcoincharts.com, which provides financial and technical data related to the Bitcoin network."[212] This compares with second-ranked Mt. Gox, which accounted for nearly 700,000 Bitcoins traded during November, 2013.[213] On December 5, 2013, in a joint statement issued with four of China's major regulatory organizations (the China Banking Regulatory Commission, China Securities Regulatory Commission, Ministry of Industry and Information Technology, and the China Insurance Regulatory Commission), the People's Bank of China, China's central bank, "barred financial institutions from handling Bitcoin transactions after investors lost money

[210] Sarah Bracking & Lloyd Sachikonye, *Remittances, Poverty Reduction and Informalisation in Zimbabwe 2005-6: A Political Economy of Dispossession?* (Brooks World Poverty Institute, Working Paper No. 28, 2008), *available at* http://ssrn.com/abstract=1265516 (internal citations omitted).

[211] John Coulter, *Beware of the Baneful Bitcoin Bug*, CHINA DAILY, (Nov. 29, 2013, 7:02 AM), *available at* http://usa.chinadaily.com.cn/epaper/2013-11/29/content_17140806.htm.

[212] Xinhua, *China Becomes Largest Bitcoin Market*, CHINA DAILY, (Dec. 5, 2013, 10:09 AM), *available at* http://usa.chinadaily.com.cn/business/2013-12/05/content_17153413.htm.

[213] *Id.*

on fraudulent online platforms for the virtual currency."[214] Reasoning offered by the central bank was that "the virtual currency could be used for reckless speculation, money laundering, drug and gun transactions, gambling and other illegal activities. It could also be used by terrorists to fund attacks."[215] China Daily reported that "[w]ithin one hour following the warning, per Bitcoin price plunged by as much as 35 percent at BTC China, the main Bitcoin trading platform in the country."[216] Moreover, the regulatory agencies

> [D]emanded financial and payment institutions not to price their products or services with Bitcoins, or to engage in transactions involving Bitcoins, or to accept insurances related to Bitcoins. The notice also told Bitcoin-transaction online platforms to register at China's telecom industry regulator in accordance with laws, and to carry out anti-laundering obligations by identifying its consumers and reporting suspicious transactions . . . After the release of the notice, the price of one Bitcoin at BTC China dived from 6,970 yuan ($1,137) to as low as just over 4,500 yuan in about one hour, down by 35 percent.[217]

[74] Shortly thereafter, China's central bank ordered third-party payment companies "not to do business with Bitcoin exchanges in China, meaning that holders of the virtual currency would lack a channel to exchange their Bitcoins for such currencies as the Chinese yuan or US

[214] Wu Yiyao & Gao Changxin, *Banks Not Allowed to Use Bitcoin*, CHINA DAILY, (Dec. 5, 2013, 11:31 PM), *available at* http://usa.chinadaily.com.cn/business/2013-12/05/content_17157648.htm.

[215] *Id.*

[216] Xinhua, *Bitcoin Price Dives After China Warning*, CHINA DAILY (Dec. 6, 2013, 9:32 AM), http://usa.chinadaily.com.cn/business/2013-12/06/content_17156199.htm.

[217] *Id.*

dollar."[218] "Alipay, the payment unit of Alibaba . . . confirmed to China Daily . . . that it has not supported and will not support Bitcoin-based transactions."[219] On January 8, 2014, Taobao, China's "largest customer-to-customer site, banned the transaction of virtual currency exchanges . . . following a central bank notice."[220]

J. Theoretical Foundation, Open-Source Communities & Bitcoin

[75] The European Central Bank reports that the theoretical foundation of Bitcoin "can be found in the Austrian school of economics and its criticism of the current fiat money system and interventions undertaken by governments and other agencies, which, in their view, result in exacerbated business cycles and massive inflation."[221] According to the European Central Bank

> One of the topics upon which the Austrian School of economics, led by Eugen von Böhm-Bawerk, Ludwig von Mises and Friedrich A. Hayek, has focused is business cycles. In short, according to the Austrian theory, business cycles are the inevitable consequence of monetary interventions in the market, whereby an excessive expansion of bank credit causes an increase in the supply of money through the money creation process in a fractional-reserve banking system, which in turn leads to artificially

[218] Wu Yiyao, *Bitcoin Falls On 3rd-Party Pullback*, CHINA DAILY (Dec. 18, 2013, 7:01 AM), http://usa.chinadaily.com.cn/epaper/2013-12/18/content_17182528.htm.

[219] *Id.*

[220] He Wei, *Bitcoin Transactions Banned On Taobao*, CHINA DAILY (Jan. 8, 2014, 3:45 PM), http://usa.chinadaily.com.cn/business/2014-01/08/content_17224285.htm. *See generally* Derek E. Bambauer et al., *Internet Filtering in China in 2004-2005: A Country Study* (Berkman Center for Internet & Society at Harvard Law School Research Publication No. 2005-10, Apr. 15, 2005), *available at* http://ssrn.com/abstract=706681.

[221] EUROPEAN CENTRAL BANK, *supra* note 127, at 22.

low interest rates. In this situation, the entrepreneurs, guided by distorted interest rate signals, embark on overly ambitious investment projects that do not match consumers' preferences at that time relating to intertemporal consumption (i.e. their decisions regarding near-term and future consumption). Sooner or later, this widespread imbalance can no longer be sustained and leads to a recession, during which firms need to liquidate any failed investment projects and readapt (restructure) their production structures in line with consumers' intertemporal preferences. As a result, many Austrian School economists call for this process to be abandoned by abolishing the fractional-reserve banking system and returning to money based on the gold standard, which cannot be easily manipulated by any authority.

Another related area in which Austrian economists have been very active is monetary theory. One of the foremost names in this field is Friedrich A. Hayek. He wrote some very influential publications, such as *Denationalisation of Money* (1976), in which he posits that governments should not have a monopoly over the issuance of money. He instead suggests that private banks should be allowed to issue non-interest-bearing certificates based on their own registered trademarks. These certificates (i.e. currencies) should be open to competition and would be traded at variable exchange rates. Any currencies able to guarantee a stable purchasing power would eliminate other less stable currencies from the market. The result of this process of competition and profit maximisation would be a highly efficient monetary system where only stable currencies would coexist.

The following ideas are generally shared by Bitcoin and its supporters:

> — They see Bitcoin as a good starting point to end the monopoly central banks have in the issuance of money.
>
> — They strongly criticize the current fractional-reserve banking system whereby banks can extend their credit supply above their actual reserves and, simultaneously, depositors can withdraw their funds in their current accounts at any time.
> — The scheme is inspired by the former gold standard.
>
> Although the theoretical roots of the scheme can be found in the Austrian School of economics, Bitcoin has raised serious concerns among some of today's Austrian economists. Their criticism covers two general aspects: a) Bitcoins have no intrinsic value like gold; they are mere bits stored in a computer; and b) the system fails to satisfy the "Misean Regression Theorem," which explains that money becomes accepted not because of a government decree or social convention, but because it has its roots in a commodity expressing a certain purchasing power.[222]

[76] While Hayek "argued that traditional government-backed currencies are prone to a number of weaknesses, particularly susceptibility to inflation and political corruption [p]rivate currencies…. are more stable than traditional currencies because they do not share these weaknesses."[223] François Velde believes that Hayek is misguided in his thesis that the production of money should be the domain of the private sector and not remain a monopoly of the state. Velde believes that Bitcoin is far from

[222] *Id*. at 22-23; *see also* Nicholas Cachanosky & Alexander William Salter, *The View from Vienna: An Analysis of the Renewed Interest in the Mises-Hayek Theory of the Business Cycle* (Dec. 4, 2013), *available at* http://ssrn.com/abstract=2363560.

[223] Plassaras, *supra* note 140, at 382.

what Hayek imagined, in that Bitcoin fails to be disciplined by market forces to maintain stability of its value.[224] Accordingly, "[t]he Bitcoin network is an automaton, issuing currency at a predictable rate, perfectly incapable of providing 'good money' in Hayek's sense, i.e., a currency of stable value."[225] In addition, by virtue of its first-mover advantage, Bitcoin has laid claim to quasi-monopoly status, "and Hayek did not address whether currency is a natural monopoly."[226] Accordingly, as Luther observes, Bitcoin use benefits from the fact that "[s]uccessive rounds of quantitative easing in the United States have been met with opposition, as some users of the dollar fear the currency will be worth significantly less in the future. Similarly, instability in Europe prompts fears of the devaluation or outright collapse of the euro."[227]

[77] Bitcoin appears to have its basis as an open-source community. According to Teigland, Yetis and Larsson

> Over the past two decades, the wide adoption of the Internet and developments in information and communication technologies (ICT) have greatly boosted the development of online knowledge creation communities, with some of these collective and emergent environments now disrupting and transforming industries. For example, open source software (OSS) communities (e.g., LINUX, MySQL) demonstrate how a globally dispersed group of strangers self-organize online to challenge and disrupt the software industry's established norms for innovation and value creation. Money as a social

[224] François R. Velde, *Bitcoin: A Primer*, 317 CHI. FED. LETTER 3-4 (2013), *available at* http://www.chicagofed.org/digital_assets/publications/chicago_fed_letter/2013/cfldecember2013_317.pdf.

[225] *Id.* at 4.

[226] *Id.*

[227] Luther, *supra* note 206 at 3.

> institution has also been affected by the developments in Internet and ICT and has evolved to adapt to the online economy. In recent years, we have seen the rapid spread of online banking, new payment services such as PayPal and mobile payments, and even new virtual currencies such as Linden Dollars and Project Entropia Dollars. These virtual currencies are used by virtual communities to exchange goods and services within the community and even with others outside the community, thereby providing a medium of exchange and a unit of account for that particular virtual community (ECB, 2012) . . . .[228] Open source communities emerge when strangers from across the globe come together online to self-organize around a shared interest and to create value through sharing knowledge and innovating. Some scholars propose that these communities are challenging the firm-based approach to knowledge creation as the primary mechanism for innovation.[229]

K. Governance

[78] Kroll, Davey and Felten argue that "Bitcoin will require the emergence of governance structures, contrary to the commonly held view in the Bitcoin community that the currency is ungovernable."[230] Teigland, Yetis and Larsson describe the Bitcoin community's formal governance as follows:

> The Bitcoin Foundation was founded by seven of the community's most instrumental individuals, such as Gavin Andresen – a core Bitcoin developer. The Bitcoin Foundation has been registered under section 501c of the

[228] Teigland, *supra* note 129 at 3.

[229] *Id.* at 5.

[230] Kroll et. al, *supra* note 123, at 1.

> US Internal Revenue Code in Washington, D.C., and its bylaws were effective as of July 23, 2012. The Foundation is governed by a board with five seats split by membership class. Two seats elected by the Individual member class (annual membership costs .23 BTC), two seats by the Corporate member class (five different levels from 9.4 BTC for companies younger than two years and with less than 25 employees to 935.4 BTC for Platinum companies), and one seat by the Founding member class. The Individual member class currently has 426 members (of which 68 are anonymous) while the Corporate member class comprises two platinum and eight silver members. The Board has established the following requirements for its board members: 1) an Individual member in good standing, 2) any business is conducted openly using their real identity, and 3) they pass a background check for felony conviction.[231]

[79] As would be expected in such a diverse community as that associated with the technologically complex mining of Bitcoin, Kroll, Davey and Felten depict a number of pressing issues that require governance structure including: threats from actual adversaries; the need for a change in the minimum transaction size; protocol instabilities; and the resolution of inevitable software bugs and accidents such as the conflict between version 0.7 and 0.8 during March 2013.[232] Moreover

> We argue that such governance is already emerging, that it will take the form of the governance of an open source project (in the sense that leaders cannot take actions

[231] Teigland, *supra* note 129, at 10 (citing *Bylaws of the Bitcoin Foundation, Inc.*, GITHUB, https://github.com/pmlaw/The-Bitcoin-Foundation-Legal-Repo/blob/master/Bylaws/Bylaws_of_The_Bitcoin_Foundation.md (last visited May 13, 2014); *Governance Structure*, BITCOIN FOUNDATION, https://bitcoinfoundation.org/about/governance (last visited May 13, 2014)).

[232] Kroll et al., *supra* note 123, at 2, 15.

> contrary to the interests and will of the community without naturally losing legitimacy), and that the emergence of formal governance structures will ultimately subject Bitcoin itself (and not merely particular players) to influence by government regulators around the world.[233]

L. Ecosystem

[80] Bitcoin enjoys a growing ecosystem "including exchanges, transaction services providers, market information and chart providers, escrow providers, joint mining operations and so on. Absent from this ecosystem at present are futures markets and entities offering legitimate investment returns, such as fractional reserve banks, although some individuals have announced plans to build these."[234] Reuben Grinberg observes

> Individuals holding this currency represent a number of interests, including technology early adopters, privacy and cryptography enthusiasts, government-mistrusting "gold bugs," criminals, and speculators. A large number of online merchants accept bitcoins, catering to individuals with these interests, including web hosts, online casinos, illicit drug marketplaces, auction sites, technology consulting firms, and adult media and sex toy merchants.[235]

---

[233] *Id.* at 2.

[234] Reuben Grinberg, *Bitcoin: An Innovative Alternative Digital Currency*, 4 HASTINGS SCI. & TECH. L. J., 159, 165 (2012) (citing Gigabytecoin, *Where To Create Your Own Bank For Less Than $25K???*, BITCOIN FORUM (Mar. 24, 2011, 5:22 AM), http://bitcointalk.org/index.php?topic=4871.0; Nefario, *Investors for Bitcoin Stock Market and Credit Rating Agrency, Dev Started!*, BITCOIN FORUM (Feb. 25, 2011, 3:01 AM), http://bitcointalk.org/index.php?topic=3844.0).

[235] *Id.* (citing Peter C. Tucker, *The Digital Currency Doppelganger: Regulatory Challenge or Harbinger of the New Economy*, 17 CARDOZO J. INT'L & COMP. L. 589, 602–08 (2009) (describing users generally interested in digital currencies); Reubgr, *Why Do You Use Bitcoin?*, BITCOIN FORUM (Mar. 14, 2011, 10:27 PM),

[81] Considerable press and commercial interest grows in Bitcoin as its use increases. Teigland, Yetis and Larsson report that "[o]ne area of interest is the range of start-ups entering the Bitcoin ecosystem. For example, BitPay, an electronic payment processing system for the Bitcoin currency, enables merchants to accept bitcoins as a form of payment."[236] San Francisco-based Coinbase was founded in June of 2012 as "a Bitcoin wallet and platform where merchants and consumers can transact."[237] During late 2013, Coinbase received a vote of confidence and $25 million investment infusion, led by venture capital firm Andreessen Horowitz, which was subsequently doubled at the failure of Mt. Gox.[238] Accordingly, Coinbase lists its current metrics as "1,100,000 consumer wallets, 29,000 merchants, 5,000 API applications, and U.S. bank integration."[239] New entrants appear almost daily in the Bitcoin ecosystem. As would be expected, Bitcoin seems to have inspired several other cryptocurrencies such as iOwe, which is "based on promises for

http://bitcointalk.org/index.php?topic=4465.0; Ryepdx, *What if One Bitcoin Was Worth the Same as One Share Berkshire Hathaway?*, BITCOIN FORUM (Mar. 12, 2011, 02:00 AM), http://bitcointalk.org/index.php?topic=4390.0 (discussing whether a single Bitcoin would ever equal in worth a share of Berkshire Hathaway); *Trade*, WIKIPEDIA, https://en.bitcoin.it/wiki/Trade (last modified Apr. 14, 2014) (identifying merchants that accept bitcoins)).

[236] Teigland, *supra* note 129, at 8.

[237] *About Coinbase*, COINBASE, https://coinbase.com/about (last visited May 13, 2014).

[238] Jason Del Rey, *Bitcoin's Biggest Bet: Andreessen Horowitz Leads $25 Million Investment in Coinbase*, ALL THINGS D (Dec. 12, 2013, 2:19 AM), http://allthingsd.com/20131212/bitcoins-biggest-bet-andreessen-horowitz-leads-25-million-investment-in-coinbase/; Gregory Zuckerman, *Web Pioneer Keeps Faith, and Cash, in Bitcoin*, WALL ST. J. (Mar. 21, 2014, 7:13 PM), http://online.wsj.com/news/articles/SB10001424052702304026304579453501821936252.

[239] *About Coinbase*, *supra* note 237.

future work."[240] Coinmarketcap.com lists one hundred different cryptocurrencies as of mid-May 2014, having a total market capitalization of approximately $6.178 US billion.[241] The top ten of these cryptocurrencies ranked by market capitalization as of May 13, 2014 are: Bitcoin ($6.604 billion), Litecoin ($294 million), Ripple ($47 million); Peercoin ($44.6 million); Dogecoin ($34.9 million), Nxt ($30 million); Namecoin ($17.7 million); Mastercoin ($16.7 million); Darkcoin ($11.2 million); and Blackcoin ($8.4 million).[242] For example, Litecoin describes itself as "a peer-to-peer Internet currency that enables instant payments to anyone in the world. [Litecoin] is based on the Bitcoin protocol but differs from Bitcoin in that it can be efficiently mined with consumer-grade hardware."[243]

[82] Peercoin boasts that "[t]hrough an innovative minting algorithm, the Peercoin network consumes far less energy, maintains stronger security, and rewards users in more sustainable ways than other cryptocurrencies."[244] Other Bitcoin-related or inspired projects of note include: the Bitcoin Investment Trust, Gyft, BitPremier, Coinsetter, itBit, Ripple Labs, CommitCoin, Mave and MavePay, Korbit and BitPagos;[245]

---

[240] DAVE LEVIN, AARON SCHULMAN, KATRINA LACURTS, NEIL SPRING & BOBBY BHATTACHARJEE, MAKING CURRENCY INEXPENSIVE WITH IOWE 6 (2011), http://www.cs.umd.edu/~dml/papers/iowe_netecon11.pdf.

[241] *Crypto-Currency Market Capitalizations*, COINMARKETCAP, http://coinmarketcap.com/ (last updated May 13, 2014).

[242] *Id.*

[243] *What Is Litecoin?*, LITECOIN, https://litecoin.org/ (last visited May 13, 2014).

[244] PEERCOIN, *Why Peercoin?*, http://www.peercoin.net (last visited May 13, 2014).

[245] *See generally* Jeremy Clark & Aleksander Essex, *CommitCoin: Carbon Dating Commitments With Bitcoin*, *in* A.D. Keromytis (Ed). Financial Cryptography 2012, LNCS 7397, 390 (2012), *available at* http://eprint.iacr.org/2011/677; Sergio Demian Lerner, *MavePay, A New Lightweight Payment Scheme for Peer to Peer Currency Networks* (2012), *available at* http://bitslog.files.wordpress.com/2012/04/mavepay1.pdf; Sergio Demian Lerner, *Mave, New Lightweight Digital Signature Protocols for Massive*

and the effort by Cameron and Tyler Winklevoss to launch a Bitcoin exchange-traded fund (ETF).[246] Gambling sites are reported, such as Satoshi Dice, "which allow punters to gamble in a weird, automated fashion."[247] Jared Ho reports that during early 2014 "Overstock.com announced that it would begin accepting bitcoins as payment for consumer purchases. The company's announcement makes Overstock.com the first major US online retailer to accept bitcoins, albeit via a third-party payment processor."[248] Bitcoin ATM machines are available in Canada, London,[249] Seattle, Washington and Austin, Texas as of early 2014.[250]

Verifications (2012), *available at* http://bitslog.files.wordpress.com/2012/04/mave1.pdf ; Written Testimony of Barry E. Silbert,Founder & CEO, Second Market & Founder, Bitcoin Investment Trust, to the New York State Department of Financial Services, Hearings on the Regulation of Virtual Currencies (Jan. 28, 2014) (*available at* http://www.dfs.ny.gov/about/hearings/vc_01282014/silbert.pdf).

[246] *See* Christopher Condon, *Winkelvosses' Lawyer in Talks With SEC Over Bitcoin ETF,* BLOOMBERG (Feb. 2, 2014, 6:09 PM), http://www.bloomberg.com/news/2014-01-30/winklevosses-lawyer-in-talks-with-sec-over-bitcoin-etf.htm; *see also* Winkelvoss Bitcoin Trust, Registration Statement (Form S-1, Amend. 1) (Oct. 8, 2013), *available at* http://www.sec.gov/Archives/edgar/data/1579346/000119312513393903/d562329ds1a.htm.

[247] Ford, *supra* note 148, at 81.

[248] Jared Ho, *Are User Identification Networks the Future of Commercial Bitcoin Transactions?,* FREEDOM TO TINKER (Feb. 13, 2014), https://freedom-to-tinker.com/blog/jaredho/are-user-identification-networks-the-future-of-commercial-bitcoin-transactions/.

[249] *See* Matthew Sparkes, *UK's First Bitcoin Cash Machine Launches in Shoreditch,* THE TELEGRAPH (Mar. 7, 2014, 12:45 PM), http://www.telegraph.co.uk/technology/10682842/UKs-first-Bitcoin-cash-machine-launches-in-Shoreditch.html.

[250] *See* Saroj Kar, *Seattle and Austin Get the Crown of First US Cities to Pioneer Bitcoin ATMs*, SILICONANGLE (Feb. 24, 2014), http://siliconangle.com/blog/2014/02/24/seattle-and-austin-get-the-crown-of-first-us-cities-to-pioneer-bitcoin-atms/.

M. A Threat to International Currency Stability?

[83] To examine how Bitcoin might pose a threat to international currency stability, let us briefly examine the role of the International Monetary Fund ("IMF"). Rebuilding international economies proved to be a major task at the end of World War II. As a specialized agency of the United Nations, the IMF is charged with tasks of (1) overseeing the international monetary system to ensure exchange rate stability, and (2) to encourage members to eliminate exchange restrictions that discourage free trade.[251] Nicholas Plassaras observes that the IMF "is the international institution tasked with coordinating the international foreign currency exchange. It sets minimum standards for what member nations can do to their individual currencies, in order to preserve global economic stability."[252] Plassaras poses the following threat scenario

> Because Bitcoin is not formally backed by a country's government, it is not bound by the IMF's guidelines. As a result, Bitcoin poses a serious threat to the economic stability of the foreign currency exchange if it continues to grow in both value and usage. Any other digital currency that entered widespread use would pose similar problems. Because private digital currencies like Bitcoin fall outside the IMF's legal framework, the IMF is unable to obtain those currencies directly. As a result, the IMF is limited in what it can do to intervene in the event that a private digital currency like Bitcoin is used to attack the value of a conventional currency through what is known as a "speculative attack." A speculative attack occurs when an investor wishes to take advantage of a "weak currency," a

[251] *See About the IMF: History: Cooperation and Reconstruction (1944-71)*, INTERNATIONAL MONETARY FUND, http://www.imf.org/external/about/histcoop.htm (last visited May 13, 2014).

[252] Plassaras, *supra* note 139, at 380.

> currency that has depreciated in value relative to other currencies. If left unchecked, a successful attack can push a weak currency's value even lower, resulting in a destabilization of the international foreign currency exchange. If Bitcoin becomes an important currency in international commerce, its use in speculative attacks could cause serious economic harms unless the IMF develops a way to counter them.[253]

[84] Plassaras contends that the problem may, with time, become an ever greater threat to world order, in that

> [T]he longer the IMF takes to bring Bitcoin within its control, the more difficult controlling Bitcoin will become. Bitcoins are generated through computer software which is programmed to halt the production of new Bitcoins by approximately 2025. Once Bitcoins can no longer be generated, their supply becomes finite and their value can be expected to increase. As their value increases, so does the expense that the IMF has to incur in order to obtain them. Because having a supply of Bitcoins is necessary to effectively counter a speculative attack, the sooner the IMF can acquire a supply of Bitcoins, the cheaper counteracting such an attack will be.[254]

V. LIBERTY RESERVE

[85] On May 20, 2013, a sealed indictment was returned by a grand jury in the Southern District of New York charging Defendants Liberty Reserve S.A., Arthur Budovsky, Vladimir Kats, Ahmed Yassine Abdelghani, Allan Esteban Hidalgo Jimenez, Azzeddine El Amine, Mark

[253] *Id.* at 380-81.

[254] *Id.* at 381.

Marmilev, and Maxim Chukharev with (1) conspiracy to commit money laundering,[255] conspiracy to operate an unlicensed money transmitting business,[256] and operation of an unlicensed money transmitting business.[257] The Indictment seeks the forfeiture of property involved in the money laundering conspiracy or the unlicensed money transmitting business offenses consisting of: funds held in 45 accounts located in Australia, Costa Rica, China, Cypress, Hong Kong, Latvia, Morocco, Russia, Spain, and the United States, and Internet domain names: Libertyreserve.com, Exchangezone.com, Swiftexchanger.com, Moneycentralmarket.com, Asianagold.com, and Eurogoldcash.com.[258]

A. E-Gold (2006)

[86] The founding of Liberty Reserve allegedly dates back to defendants Budovsky and Kats' prior failed attempt at running Gold Age, Inc., a third-party digital exchange service called "e-Gold," reportedly the most popular digital currency operation at the time.[259] Assistant Attorney General Raman reports that establishing an account only required a valid e-mail address, thus providing international transactions that were highly anonymous.[260] Accordingly, "e-Gold became a popular payment method for sellers of child pornography, operators of investment scams, and perpetrators of credit card and identity fraud. At its peak, e-Gold reportedly moved over $6 million each day for more than 2.5 million

[255] *See* 18 U.S.C. §1956(h) (2012).

[256] 18 U.S.C. §371 (2012).

[257] 18 U.S.C. §§1960, 1962 (2012).

[258] *See* Indictment at ¶¶ 14, 16, United States v. Liberty Reserve, 13 Crim. 368 (S.D.N.Y. May 20, 2013) (*available at* https://archive.org/stream/704540-liberty-reserve-indictment/704540-liberty-reserve-indictment_djvu.txt).

[259] *Id.* at ¶ 11 (The Founding of Liberty Reserve).

[260] Raman, *supra* note 8.

accounts. In 2008, e-Gold and the three individuals pleaded guilty."[261] The complaint reports that "in December 2006, Budosvky and Kats were convicted in New York State of operating 'Gold Age, Inc.' as an unlicensed money transmitting business. At or about the same time, E-Gold [sic] and several of its principals were charged with various offenses including money laundering."[262] The complaint further alleges that following his criminal conviction, defendant Arthur Budovsky "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. Accordingly, Budovsky immigrated to Costa Rica, where in 2006, he and Ahmed Yassine Abdelghani, . . . the defendant, had incorporated Liberty Reserve."[263]

B. How Liberty Reserve Works

[87] The indictment reveals that

> [T]o use Liberty reserve's digital currency, commonly referred to as 'LR,' a user first was required to open an account through the Liberty Reserve website. In registering, the user was required to provide basic identifying information, such as name, address, and date of birth. However, unlike traditional banks or legitimate online payments processors, Liberty Reserve did not require users to validate their identity information, such as by providing official identification documents or a credit card. Accounts could therefore be opened easily using fictitious or anonymous identities.

[261] *Id.*

[262] Indictment *supra* note 258 at ¶ 11 (The Founding of Liberty Reserve).

[263] *Id.* at ¶ 12.

Once a user established an account with Liberty reserve, the user could then conduct transactions with other Liberty Reserve users. That is, the user could receive transfers of 'LR' from other user's accounts, and transfer LR from his own account to other users – including any 'merchants' that accepted LR as payment. Liberty reserve charged a one-percent fee every time a user transferred LR to another user through the Liberty Reserve system. In addition, for an additional 'privacy fee' of 75 cents per transaction, a user could hide his own Liberty Reserve account number when transferring funds, effectively making the transfer completely untraceable, even within Liberty reserve's already opaque system.

To add an additional layer of anonymity, Liberty Reserve did not permit users to fund their accounts by transferring money to Liberty Reserve directly, such as by issuing a credit card payment or wire transfer to Liberty Reserve. Nor could Liberty Reserve users withdraw funds from their accounts directly, such as through an ATM withdrawal. Instead, Liberty Reserve users were required to make any deposits or withdrawals through the use of third-party 'exchangers,' thus enabling Liberty Reserve to avoiding collecting any information about its users through banking transactions or other activity that would leave a centralized financial paper trail.

Liberty Reserve's 'exchangers' were third-party entities that maintained direct financial relationships with Liberty Reserve, buying and selling LR in bulk from Liberty Reserve in exchange for mainstream currency. The exchangers in turn bought and sold this LR in smaller transactions with end users in exchange for mainstream currency. Thus, in order to fund a Liberty Reserve account, a user was required to transmit mainstream currency in some fashion (through a money remitter, for example) to an

> exchanger. Upon receiving the user's payment, the exchanger credited the user's Liberty Reserve account with a corresponding amount of LR, by transferring LR from the exchanger's Liberty Reserve account to the user's account. Similarly, if a Liberty Reserve user wished to withdraw funds from his account, the user was required to transfer LR from his account, and the exchanger then made arrangements to provide the user a corresponding amount of mainstream currency.
>
> The Liberty Reserve website recommended a number of 'pre-approved' exchangers. These exchangers tended to be unlicensed money transmitting businesses operating without significant governmental oversight or regulation, concentrated in Malaysia, Russia, Nigeria, and Vietnam. The exchangers charged transaction fees for their services, typically amounting to five percent or more of the funds being exchanged. Such fees were much higher than those charged by mainstream banks or payment processors for comparable money transfers.[264]

C. Criminal Activity

[88] The indictment contends that

> Liberty Reserve's system was designed so that criminals could affect financial transactions under multiple layers of anonymity and thereby avoid apprehension by law enforcement. Not surprisingly, Liberty Reserve was in fact used extensively for illegal purposes, functioning in effect as the bank of choice for the criminal underworld. Liberty Reserve users routinely established accounts under false names – including such blatantly criminal monikers as

[264] *Id.* at ¶¶ 14-18 (The Criminal Design of Liberty Reserve).

> 'Russia Hackers' and 'Hacker Account.' Believing themselves to be protected by this anonymity, Liberty Reserve users then engaged in criminal transactions with an impunity that would have been impossible in the legitimate financial system.
>
> To further enable the use of Liberty reserve for criminal activity, its website offered a 'shopping cart interface' that 'merchant' websites could use to accept LR currency as a form of payment. The 'merchants' who accepted LR currency were overwhelmingly criminal in nature. They included, for example: traffickers of stolen credit card data and personal identity information; peddlers of various types of online Ponzi and get-rich-quick schemes; computer hackers for hire; unregulated gambling enterprises; and underground drug-dealing websites.
>
> In addition to being used to process payments for illegal goods and services online, Liberty Reserve was also used by cyber-criminal associates. Liberty Reserve was used by credit-card theft and computer-hacking rings operating in countries around the world, including Vietnam, Nigeria, Hong Kong, China, and the United States, to distribute proceeds of these conspiracies among the members involved.[265]

[89] Jennifer Shasky Calvery, FinCEN Director, states "Liberty Reserve operated as an online… money transfer system . . . deliberately designed to avoid regulatory scrutiny and tailored its services to illicit actors looking to launder their ill-gotten gains . . . [a] $6 billion money laundering operation."[266] Acting Assistant U.S. Attorney General Raman

[265] *Id.* at ¶¶ 19-21 (The Criminal Use of Liberty Reserve).

[266] Calvery, *supra* note 94, at 11, 6.

contends that the Liberty Reserve case demonstrates the DOJ's determination "to pursue purported major money laundering facilitators, even those who hide offshore."[267] Because of the action taken by the DOJ, Raman states that "the site was shuttered and effectively put out of business, and seven defendants were charged. One is in custody in the United States, one has entered a guilty plea, three others, including the lead defendant Budovsky, are pending extradition," and two others are at large.[268]

VI. SILK ROAD

[90] Between January 2011 and arrest of its entrepreneur during October, 2013, Silk Road operated as an intermediary, much like eBay or CraigsList, by providing buyers and sellers with a transaction infrastructure platform. However, unlike eBay or CraigsList, Silk Road is dedicated to providing a high level of anonymity between buyers, sellers and third parties who might desire to learn the details of these transactions. Silk Road is just one of several *anonymous networks* that have recently become possible with the advent of relatively easy-to-use browser interfaces, such as the "Tor browser bundle."[269]

A. How Silk Road Works

[91] In their letter addressed to Attorney General Eric Holder and the DEA, U.S. Senators Manchin and Schumer write that

[267] Raman, *supra* note 8.

[268] *Id.*

[269] Nicholas Christin, *Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace* 2 (In Proceedings of the 22nd International World Wide Web Conference (WWW'13), 213 Rio de Janeiro, Brazil (May 2013), Working Paper No. CMU-CyLab-12-018), *available at* http://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab12018.pdf (internal quotations omitted).

> By utilizing the anonymizing network TOR, Silk Road ensures that users' tracks on the site are hidden. The only method of payment for these illegal purchases is an untraceable peer-to-peer currency known as Bitcoins. After purchasing Bitcoins through an exchange, a user can create an account on Silk Road and start purchasing illegal drugs from individuals around the world and have them delivered to their homes within days.[270]

[92] Sites dealing primarily in illicit goods and services such as Black Market Reloaded and The Silk Road "use Bitcoins because they can be exchanged and accumulated like cash without any third party recording [these] transactions . . . unlike PayPal or other ways of sending money online, [Bitcoins] are untraceable since they do not require a particular identity to be attached to them."[271] Dorit Ron and Adi Shamir report that "Silk Road also used a so-called "tumbler" which, as the site explained, 'sent all payments through a complex, semi-random series of dummy transactions making it nearly impossible to link your payment with any coins leaving the site.'"[272]

[93] The indictment announced on February 4, 2014 in Manhattan federal court of Ross William Ulbricht, a/k/a "Dread Pirate Roberts," a/k/a "Silk Road", states that

---

[270] Letter from U.S. Senators Joe Manchin and Charles E. Schumer to Eric Holder, U.S. Attorney General and Michele Leonhart, Administrator, Drug Enforcement Administration (*available at* http://manchin.senate.gov/public/index.cfm/press-releases?ID=284ae54a-acf1-4258-belc-7aceelf7e8b3).

[271] Bauman, *supra* note 42, at 17.

[272] Dorit Ron & Adi Shamir, *How Did Dread Pirate Roberts Acquire and Protect His Bitcoin Wealth?*, Proceedings of the 18th International Conference on Financial Cryptography and Data Security, 2 (Barbados, 2014), *available at* http://cryptome.org/2013/11/bitcoin-pirate-nakamoto.pdf.

> ULBRICHT sought to anonymize transactions on Silk Road in two principal ways. First, ULBRICHT operated Silk Road on what is known as "The Onion Router," or "Tor" network, a special network of computers on the Internet, distributed around the world, designed to conceal the true IP addresses of the computers on the network and thereby the identities of the networks' users. Second, ULBRICHT designed Silk Road to include a Bitcoin-based payment system that served to facilitate the illegal commerce conducted on the site, including by concealing the identities and locations of the users transmitting and receiving funds through the site.[273]

B. Criminal Activity

[94] Nicholas Christin reports that "these anonymous online markets very often specialize in 'black market' goods, such as pornography, weapons or narcotics."[274] U.S. Senator Joe Manchin urged during June 2011 that the Drug Enforcement Agency and U.S. Attorney General "immediately shut down an anonymous online black market for drugs, including prescription drugs, cocaine, LSD and heroin."[275] Making specific reference to Silk Road, the Senator's press release observes that "[t]he illicit network . . . allows users anywhere in the country to purchase illicit drugs using untraceable currency and have them shipped to their

[273] Press Release, United States Attorney's Office for the Southern District of New York, Manhattan U.S. Attorney Announces The Indictment of Ross Ulbricht, The Creator and Owner of The "Silk Road" Website (Feb. 4, 2014) (*available at* http://www.justice.gov/usao/nys/pressreleases/February14/RossUlbrichtIndictmentPR.php).

[274] Christin, *supra note* 269, at 2.

[275] Press Release, U.S. Senator Joe Manchin, Manchin Urges Federal Law Enforcement to Shut Down Online Black Market for Illegal Drugs (June 6, 2011) (*available at* http://www.manchin.senate.gov/public/index.cfm/press-releases?ID=284ae54a-acf1-4258-be1c-7acee1f7e8b3).

homes via the United States Postal Service."[276] The October 25, 2013 complaint and civil forfeiture action filed in Manhattan federal court allege that Ross William Ulbricht had owned and operated, since about January 2011, an "underground website known as Silk Road, which emerged as the most sophisticated and extensive criminal marketplace on the internet."[277] This complaint further alleges that Silk Road "served as a sprawling black-market bazaar where unlawful goods and services, including illegal drugs of virtually every variety, were bought and sold regularly by the site's users . . . [and] was used by several thousand drug dealers and other unlawful vendors to distribute hundreds of kilograms of illegal drugs" during its approximately 2 ½-year operating life.[278] The Manhattan U.S. Attorney described Silk Road as "a hidden website designed to enable its users to buy and sell illegal drugs and other unlawful goods and services anonymously and beyond the reach of law enforcement."[279] Moreover,

> In addition to the civil action, a criminal complaint against ULBRICHT was filed in Manhattan federal court charging him with one count of narcotics conspiracy, one count of conspiracy to commit computer hacking, and one count of money laundering conspiracy. ULBRICHT was arrested in San Francisco, California, on October 1, 2013 . . . .

[276] *Id.*

[277] Press Release, FBI & U.S. Attorney's Office for the Southern District of New York, Manhattan U.S. Attorney Announces Seizure of Additional $28 Million Worth of Bitcoins Belonging to Ross William Ulbricht, Alleged Owner and Operator of 'Silk Road' Website (Oct. 25, 2013) (*available at* http://www.fbi.gov/newyork/press-releases/2013/manhattan-u.s.-attorney-announces-seizure-of-additional-28-million-worth-of-bitcoins-belonging-to-ross-william-ulbricht-alleged-owner-and-operator-of-silk-road-website).

[278] *Id.*

[279] *Id.*

> ULBRICHT has also been charged in a separate indictment pending in federal court in Baltimore, Maryland.[280]

[95] According to the February 4, 2014 indictment and other information and documents previously filed in Manhattan federal court:

> ULBRICHT deliberately operated Silk Road as an online criminal marketplace intended to enable its users to buy and sell drugs and other illegal goods and services anonymously and outside the reach of law enforcement . . .
>
> The vast majority of items for sale on Silk Road were illegal drugs, which were openly advertised as such on the site. As of September 23, 2013, Silk Road had nearly 13,000 listings for controlled substances, listed under such categories as "Cannabis," "Dissociatives," "Ecstasy," "Intoxicants," "Opioids," "Precursors," "Prescription," "Psychedelics," and "Stimulants." From November 2011 to September 2013, law enforcement agents made more than 100 individual undercover purchases of controlled substances from Silk Road vendors. These purchases included heroin, cocaine, ecstasy, and LSD, among other illegal drugs, and were filled by vendors believed to be located in more than ten different countries, including the United States, Germany, the Netherlands, Canada, the United Kingdom, Spain, Ireland, Italy, Austria and France.
>
> In addition to illegal narcotics, other illicit goods and services were openly bought and sold on Silk Road as well. For example, as of September 23, 2013, there were: 159 listings under the category "Services," most of which offered computer-hacking services, such as a listing by a vendor offering to hack into social networking accounts of

[280] *Id.*

> the customer's choosing; 801 listings under the category "Digital goods," including malicious software, hacked accounts at various online services, and pirated media content; and 169 listings under the category "Forgeries," including offers to produce fake driver's licenses, passports, Social Security cards, utility bills, credit card statements, car insurance records, and other forms of false identification documents.
>
> Using the online moniker "Dread Pirate Roberts," or "DPR," ULBRICHT controlled and oversaw every aspect of Silk Road, and managed a small staff of paid, online administrators who assisted with the day-to-day operation of the site. Through his ownership and operation of Silk Road, ULBRICHT reaped commissions worth tens of millions of dollars generated from the illicit sales conducted through the site. ULBRICHT also demonstrated a willingness to use violence to protect his criminal enterprise and the anonymity of its users. ULBRICHT even solicited six murders-for-hire in connection with operating the site, although there is no evidence these murders were actually carried out.[281]

C. Use of Bitcoin

[96] The FBI and U.S. Attorney's Office for the Southern District of New York announced on October 25, 2013 that "[a]long with a prior seizure of approximately 29,655 Bitcoins, federal law enforcement agents have now seized a total of approximately 173,991 Bitcoins in connection with the Silk Road case . . . worth over $33.6 million."[282] Just a few weeks later, as of November 15, 2013, the value of these 173,991 Bitcoins

[281] United States Attorney's Office, *supra* note 273.

[282] FBI & U.S. Attorney's Office, *supra* note 277.

doubled to more than $70 million.[283] This seizure arises as a result of "a civil action previously filed . . . on September 30, 2013, seeking the forfeiture of all assets of Silk Road, including its website and all of its Bitcoins because those assets allegedly were used to facilitate money laundering and constitute property involved in money laundering."[284]

[97] On January 16, 2014, the U.S. Attorney for the Southern District of New York announced the forfeiture of approximately 29,655 Bitcoins (worth approximately $28 million) and the forfeiture of the Silk Road hidden website.[285] Just ten days later, the unsealing of charges were announced "against ROBERT M. FAIELLA, a/k/a/ 'BTCKing,' an underground Bitcoin exchanger, and CHARLIE SHREM, the Chief Executive Officer and Compliance Officer of a Bitcoin exchange company, for engaging in a scheme to sell over $1 million in Bitcoins to users of 'Silk Road.'"[286] Allegations in the Criminal Complaint revealed:

> From about December 2011 to October 2013, FAIELLA ran an underground Bitcoin exchange on the Silk Road website, a website that served as a sprawling and anonymous black market bazaar where illegal drugs of virtually every variety were bought and sold regularly by the site's users. Operating under the username "BTCKing," FAIELLA sold Bitcoins − the only form of payment

[283] Raman, *supra* note 8.

[284] FBI & U.S. Attorney's Office, *supra* note 277.

[285] Press Release, United States Attorney's Office for the Southern District of New York, Manhattan U.S. Attorney Announces Forfeiture Of $28 Million Worth Of Bitcoins Belonging To Silk Road (Jan. 16, 2014), http://www.justice.gov/usao/nys/pressreleases/January14/SilkRoadForfeiture.php.

[286] Press Release, United States Attorney's Office for the Southern District of New York, Manhattan U.S. Attorney Announces Charges Against Bitcoin Exchangers, Including CEO Of Bitcoin Exchange Company, For Scheme To Sell And Launder Over $1 Million In Bitcoins Related To Silk Road Drug Trafficking (Jan. 27, 2014), http://www.justice.gov/usao/nys/pressreleases/January14/SchremFaiellaChargesPR.php.

> accepted on Silk Road − to users seeking to buy illegal drugs on the site. Upon receiving orders for Bitcoins from Silk Road users, he filled the orders through a company based in New York, New York (the "Company"). The Company was designed to enable customers to exchange cash for Bitcoins anonymously, that is, without providing any personal identifying information, and it charged a fee for its service. FAIELLA obtained Bitcoins with the Company's assistance, and then sold the Bitcoins to Silk Road users at a markup.
>
> SHREM is the Chief Executive Officer of the Company, and from about August 2011 until about July 2013, when the Company ceased operating, he was also its Compliance Officer, in charge of ensuring the Company's compliance with federal and other anti-money laundering ("AML") laws. SHREM is also the Vice Chairman of a foundation dedicated to promoting the Bitcoin virtual currency system.
>
> SHREM, who personally bought drugs on Silk Road, was fully aware that Silk Road was a drug-trafficking website, and through his communications with FAIELLA, SHREM also knew that FAIELLA was operating a Bitcoin exchange service for Silk Road users. Nevertheless, SHREM knowingly facilitated FAIELLA's business with the Company in order to maintain FAIELLA's business as a lucrative source of Company revenue. SHREM knowingly allowed FAIELLA to use the Company's services to buy Bitcoins for his Silk Road customers; personally processed FAIELLA's orders; gave FAIELLA discounts on his high-volume transactions; failed to file a single suspicious activity report with the United States Treasury Department about FAIELLA's illicit activity, as he was otherwise required to do in his role as the Company's Compliance Officer; and deliberately helped FAIELLA circumvent the Company's AML restrictions, even though it was

> SHREM's job to enforce them and even though the Company had registered with the Treasury Department as a money services business.
>
> Working together, SHREM and FAIELLA exchanged over $1 million in cash for Bitcoins for the benefit of Silk Road users, so that the users could, in turn, make illegal purchases on Silk Road.
>
> In late 2012, when the Company stopped accepting cash payments, FAIELLA ceased doing business with the Company and temporarily shut down his illegal Bitcoin exchange service on Silk Road. FAIELLA resumed operating on Silk Road in April 2013 without the Company's assistance, and continued to exchange tens of thousands of dollars a week in Bitcoins until the Silk Road website was shut down by law enforcement in October 2013.[287]

[98] From analysis performed on available Bitcoin data compared with FBI disclosures, Dorit Ron and Adi Shamir contend that the FBI has yet to recover all the Bitcoins earned by the Dread Pirate Roberts (Ross William Ulbricht):

> [T]here is a huge variability in the amount he earned which we are aware of, which is inconsistent with the reasonable assumption that the total volume of business carried out on Silk Road was increasing at a roughly constant rate. In particular, the months of May, June and September 2013 are completely missing from this list. Assuming that DPR continued to receive at least some commissions from Silk Road during these months, it seems likely that he was simply using a different computer during these periods,

[287] *Id.*

> which the FBI had not found or was unable to penetrate. In addition, it is evident that about a third of the bitcoins in these accounts, were moved out prior to his arrest. As it is believed that the Silk Road marketplace generated sales revenue of more than 9.5 million bitcoins with an average commission rate of 6.67%, we can conclude that he received about 633,000 BTCs in commissions. Consequently, the amounts seized by the FBI represent only about 22% of these commissions, while the amounts that we have identified . . . seem to represent about a third.[288]

VII. DEMISE OF MT. GOX

[99] Mt. Gox, once the dominant online marketplace for the purchase and sale of Bitcoin, apparently failed on February 25, 2014, leaving many investors who held Bitcoin stranded.[289] The Mt. Gox website was replaced with a letter addressed to its customers from Mark Karpeles which read: "I would like to use this opportunity to reassure everyone that I am still in Japan, and working very hard with the support of different parties to find a solution to our recent issues."[290] A companion note under the signature of the "MtGox Team" states, "In light of recent news reports and the potential repercussions on MtGox's operations and the market, a decision was taken to close all transactions for the time being in order to protect the site and our users. We will be closely monitoring the situation and will

[288] Ron & Shamir, *supra* note 272, at 11.

[289] *See generally* Robin Sidel, Michael J. Casey & Eleanor Warnock, *Shutdown of Mt. Gox Rattles Bitcoin Market*, WALL ST. J. (Feb. 26, 2014, 1:21 PM), http://online.wsj.com/news/articles/SB10001424052702304834704579404101502619422 (discussing the shutdown of Mt. Gox).

[290] Mark Karpeles, *Dear MtGox Customers*, (Feb. 26, 2014), *available at* https://www.mtgox.com; The Associated Press, *Bitcoin Exchange, Mt. Gox, CEO Mark Karpeles still in Japan*, CBC NEWS (last updated Feb. 27, 2014, 1:53 AM), http://www.cbc.ca/news/technology/bitcoin-exchange-mt-gox-ceo-mark-karpeles-still-in-japan-1.2553126.

react accordingly."[291] During 2009, Mt. Gox began operations "as an exchange for trading cards tied to a popular online game called Magic: The Gathering. It soon shifted its focus to Bitcoin . . . ."[292] Although perhaps too early to know the complete reasons for Mt. Gox's failure, press accounts mention "accusations that as much as 6 percent of the Bitcoins in circulation were now missing − worth more than $300 million at current exchange rates."[293] Another news source states that "Mt. Gox lost almost 750,000 bitcoins in a long − running theft . . . valued at about $400 million at current prices."[294] In an astonishing price recovery, Tuesday evening [Feb. 24, 2014] the price of a Bitcoin stood around $525, not far from where it was when the Mt. Gox news emerged Monday night.[295] Less than a year earlier, Tokyo-based Mt. Gox was reported to handle 80% of all trading activity in Bitcoin and is reported to have said that "as the bitcoin market continues to evolve and expand, [Mt. Gox] must adjust to new regulatory and compliance demands."[296]

[291] Mark Wilson, *Bitcoin exchange Mt. Gox is offline 'in light of recent news reports'*, BETANEWS.COM, http://betanews.com/2014/02/25/bitcoin-exchange-mt-gox-is-offline-in-light-of-recent-news-reports/ (last visited May 18, 2014).

[292] Sidel, Casey & Warnock, *supra* note 289.

[293] Rachel Abrams & Nathaniel Popper, *Trading Site Failure Stirs Ire and Hope For Bitcoin*, N.Y. TIMES (Feb. 25, 2014, 9:16 PM), http://dealbook.nytimes.com/2014/02/25/trading-site-failure-stirs-ire-and-hope-for-bitcoin/?_php=true&_type=blogs&_r=0.

[294] Sidel, Casey & Warnock, *supra* note 289.

[295] *Id.*

[296] Jeffrey Sparshott, *Bitcoin Exchange Bolsters User Verification*, WALL ST. J. (May 30, 2013, 9:52 PM), http://online.wsj.com/news/articles/SB10001424127887324866904578515552017379238 ; *see generally* Tyler Moore & Nicholas Christin, *Beware the Middleman: Empirical Analysis of Bitcoin-Exchange Risk*, In FINANCIAL CRYPTOGRAPHY & DATA SECURITY, v 7859, Lecture Notes in Computer Science, 25 Springer, (Apr. 2013), *available at* http://lyle.smu.edu/~tylerm/fc13.pdf (examining investor risk of track record of 40 Bitcoin exchanges established during prior three years and finding that 18 of these had closed).

VIII. BITCOIN AFTER LIBERTY RESERVE AND SILK ROAD

[100] Concerns that have been voiced during recent years have reached new prominence since the Liberty Reserve indictment. Reuben Grinberg observes that "although the Bitcoin economy is flourishing, users are anxious about Bitcoin's legal status and the possibility of a government crackdown. Some point to Bitcoin's ability, like all digital and anonymous currencies, to facilitate money laundering, tax evasion, and trade in illegal drugs and child pornography."[297] Catherine Martin Christopher contends 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."[298]

[101] In discussing the "perplexities" of virtual currencies, FinCEN Director, Jennifer Shasky Calvery, notes the importance, "potential," and

[297] Grinberg, *supra* note 234, (citing epii, Comment on *How long until governments outlaw bitcoin usage?*, BITCOIN FORUM (Mar. 29, 2011 8:40:41 AM), http://bitcointalk.org/index.php?topic=5110.msg74627#msg74627 ("I think that illegalization is Bitcoin's most likely mode of failure.")); *see*, *e.g.*, *id.* n. 7 ("Considering how quickly services like Silk Road [an anonymous marketplace for illegal drugs] have sprung up, and the fact that the demographic of people who seem most interested in Bitcoin at this point tends to overlap with the demographic of likely tax evaders, I am afraid that this illegalization might just be a matter of time."); *see also,* Derek A. Dion, Note, *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, 167 (2013) (discussing the legal principles that can be potentially leveraged to regulate Bitcoin).

[298] Catherine Martin Christopher, *Whack-a-Mole: Why Prosecuting Digital Currency Exchanges Won't Stop Online Laundering,* LEWIS & CLARK L. REV., 1 (forthcoming 2013), *available at* http://ssrn.com/abstract=2312787; *see generally* Paul H. Farmer, Note, *Speculative Tech: The Bitcoin Legal Quagmire & the Need for Legal Innovation*, 9 J. BUS. & TECH. L. 85 (2014), *available at* http://digitalcommons.law.umaryland.edu/jbtl/vol9/iss1/6.

great "promise" of advances offered to our economy by virtual currencies.[299] Director Calvery states

> The innovations we are seeing within the financial services industry are a benefit to commerce on many levels. From providing services to the unbanked, to the development of new financial products, the virtual economy holds great promise . . . [the] challenge to our great innovators [will be to] extend your focus to devising creative solutions for preventing the abuse of virtual currencies by criminals, such as those who would exploit children.[300]

[102] Our discussion of the future of virtual currencies should consider the views of François Velde who states

> I'm not quite sure why there is so much attention paid to the use of Bitcoin to settle legal transactions − cash has been used for those purposes forever. If anything, a virtual currency like Bitcoin provides traceability − if you have access to a criminal's hard drive, and therefore to his wallet information, you could prove in court that certain payments were made.[301]

A. Future Regulatory Dialogue: Legal Interoperability

[103] The debate regarding open access and internet governance has been ongoing for many years.[302] Jonathan Zittrain observes that

[299] Calvery, *supra* note 94, at 4.

[300] *Id.*

[301] E-mail from François R. Velde, Senior Economist, Federal Reserve Bank of Chicago, to author (Feb. 11, 2014, 14:23 CST) (on file with author).

[302] *See generally* Mark A. Lemley & Lawrence Lessig, *The End of End-to-End: Preserving the Architecture of the Internet in the Broadband Era*, 48 UCLA L. REV. 925,

> Cyberlaw's challenge ought to be to find ways of regulating − though not necessarily through direct state action − which code can and cannot be readily disseminated and run upon the generative grid of Internet and PCs, lest consumer sentiment and preexisting regulatory pressures prematurely and tragically terminate the grand experiment that is the Internet today.[303]

[104] Urs Gasser and John G. Palfrey have broadly defined the term *legal interoperability* as "the working-together among legal norms, either within a given legal system of a nation state (e.g. federal and state legislation) or across jurisdictions or nations."[304] Their core belief is found in the argument "that policy-makers in the digital age should not only aim for higher levels of technical and related layers of interoperability, but should by default also seek to increase legal and, eventually, policy interoperability, particularly as we move towards multi-level governance systems."[305] Thus, I will extend their argument to

929-930 (2001); Lawrence B. Solum & Minn Chung, *The Layers Principle: Internet Architecture and the Law* (U. San Diego Pub. Law Research, Working Paper No. 55, 2003), *available at* http://ssrn.com/abstract=416263; Laura DeNardis, *The Emerging Field of Internet Governance*, Yale Information Society Project Working Paper Series (2010), *available at* http://ssrn.com/abstract=1678343.

[303] Jonathan Zittrain, *The Generative Internet*, 119 HARV. L. REV. 1974, 1979 (2006).

[304] Urs Gasser & John G. Palfrey, Jr., *Fostering Innovation and Trade in the Global Information Society: The Different Facets and Roles of Interoperability*, Berkman Ctr. Res. Pub. No. 2012-20, 8 (Dec. 12, 2012), *available at* http://ssrn.com/abstract=2192647.

[305] *Id.* at 9 (citing L. Hooghe & G. Marks, *Unraveling the Central State, But How? Types of Multi-Level Governance*, 97 AM. POL. SCI. REV. 233, 236-239 (2003) (Gasser & Palfrey propose 'to include interoperability as an additional design principle for both Type I and Type II multi-governance systems as a means to address the respective coordination problems')); *see also* Urs Gasser & John G. Palfrey, Jr. & Matthew B. Becker, *Mapping Cloud Interoperability in the Globalized Economy: Theory and Observation from Practice*, Berkman Ctr. Res. Pub. No. 2012-19, (June 1, 2012), *available at* http://ssrn.com/abstract=2192641.

contend that by optimizing the international governance of virtual currency, this legal interoperability should "enable the flow of goods, services, and information across legal systems."[306] Gasser and Palfrey offer at least three reasons why focusing on attaining *legal interoperability* should prove beneficial

> 1. Legal interoperability is a mechanism that reduces the costs associated with cross-jurisdictional business transactions;
>
> 2. Anecdotal evidence suggests that legal interoperability, at least in the ICT [information and communication technology] space with its unique characteristics, drives innovation, competition, trade, and economic growth;
>
> 3. "[I]ncreased levels of best-practice-oriented legal interoperability may also foster fundamental values and rights, such as information privacy and freedom of expression."[307]

[105] Gasser and Palfrey are quick to point out that their concept of *legal interoperability* does not necessarily require "new international law or the establishment of international organizations. Which approach should be pursued in the context of a given governance issue − like . . . cloud computing . . . depends on an in-depth analysis of the various

[306] Gasser & Palfrey, *supra* note 304 (citing H. Burkert, 'The Information Law Approach: An Exemplification,' in U. Gasser (ed.), *Information Quality Regulation: Foundations, Perspectives and Applications* (Baden-Baden: Nomos, 2004), 75-90)) (On the information law approach more generally; observing, 'A particularly interesting subset of legal interoperability issues is interoperability among legal norms aimed at regulating information. Such an information law approach to interoperability, which would have to differentiate among the different types and contexts of information still needs to be developed . . .)).

[307] Gasser & Palfrey, *supra* note 304, at 9.

technological, market, and legal factors . . . ."[308] Grinberg predicts that U.S. federal and state regulations will need to clarify how Bitcoin fits regarding: "registration with state or federal regulators; know your customer (KYC), anti-money laundering (AML) and counter-terrorist financing; capital requirements; consumer protection standards; disclosure requirements; security standards; entering into derivatives on cryptocurrencies; taxation; and risk management and counterparty due diligence standards."[309] Zittrain writes

> Precisely because the future is uncertain, those who care about openness and the innovation that today's Internet and PC facilitate should not sacrifice the good to the perfect − or the future to the present − by seeking simply to maintain a tenuous technological status quo in the face of inexorable pressure to change. Rather, we should establish the principles that will blunt the most unappealing features of a more locked-down technological future while acknowledging that unprecedented and, too many who work with information technology, genuinely unthinkable boundaries could likely become the rules from which we must negotiate exceptions.[310]

[308] *Id.* at 10; *see also* Nikolei M. Kaplanov, *Nerdy Money: Bitcoin, The Private Digital Currency, And The Case Against Its Regulation*, 25 LOY. CONSUMER L. REV. 111, 114 (2012).

[309] Reuben Grinberg, *Davis Polk Discusses The Failure of Mt. Gox and Other Recent Bitcoin Catastrophes: Why Banks Should Care,* THE CLS BLUE SKY BLOG (Columbia Law School's Blog on Corporations and the Capital Market) (Mar. 13, 2014), *available at* http://clsbluesky.law.columbia.edu/2014/03/13/davis-polk-discusses-the-failure-of-mt-gox-and-other-recent-bitcoin-catastrophes-why-banks-should-care/.

[310] Zittrain, *supra* note 303, at 1977-78.

B. Implications for Further Research

[106] The list of important research questions remaining to be more fully explored include: whether virtual currency is easier to steal than physical currency, how vulnerable are virtual currencies to counterfeiting, does Bitcoin maintain first-mover advantage or is it vulnerable to other virtual currencies, will depository "bank-like" financial service entities develop to accept deposits and make loans denominated in virtual currencies, are Bitcoin exchanges vulnerable to breaches from cyber attack; under what conditions are virtual currencies able to remain anonymous, is physical currency really less efficient for illegal activities than Bitcoin, and whether virtual currencies or Bitcoin alone becomes significant enough to threaten the effectiveness of central bank monetary policy and global currency markets?[311] Ed Felten raises the questions of: when a miner who is "controlling more than 33.3% of mining power but less than 50%, is there still an equilibrium in which all miners are honest? . . . [and] is [there] an equilibrium that can actually occur in which the Bitcoin economy can no longer function?"[312]

[107] Economist Robert J. Shiller states that "Bitcoin's future is very much in doubt . . . I believe that electronic forms of money could give us better pricing, contracting and risk management."[313] Moreover,

[311] *See* Allen, *supra* note 18. This list draws heavily from questions raised by the U.S. Federal Reserve at a meeting held on June 14, 2013 at the World Bank and attended by officials of the European Central Bank, International Centre for Missing & Exploited Children (ICMEC), International Monetary Fund, U.S. Department of Treasury's Office on Terrorist Financing and Financial Crimes, and others.

[312] Ed Felten, *Game Theory and Bitcoin,* FREEDOM TO TINKER (Nov. 11, 2013), https://freedom-to-tinker.com/blog/felten/game-theory-and-bitcoin/.

[313] Robert J. Shiller, *In Search of a Stable Electronic Currency,* N.Y. TIMES (Mar. 1, 2014), http://www.nytimes.com/2014/03/02/business/in-search-of-a-stable-electronic-currency.html.

> Bitcoin has been a bubble. But the legacy of the Bitcoin experience should be that we move toward a system of stable economic units of measurement − a system empowered by sophisticated mechanisms of electronic payment.[314]

IX. CONCLUSION

[108] Virtual currencies have quickly become a reality, gaining significant traction in a very short period of time, and are evolving rapidly. Innovation in the pace of development of new currencies and technologies continues to create ongoing challenges for responsible users of technology and regulators alike. Virtual currencies, due primarily to its anonymous characteristic, have been linked to numerous types of crimes, including facilitating marketplaces for: assassins; attacks on businesses; child exploitation (including pornography); corporate espionage; counterfeit currencies; drugs; fake IDs and passports; high yield investment schemes; sexual exploitation; stolen credit cards and credit card numbers; and weapons. While technological advances create great opportunities to improve the health, living conditions, and general wellbeing of mankind; new technologies also create great challenges for nation states.

[314] *Id.*