THE BITCOIN BLOCKCHAIN AS FINANCIAL MARKET INFRASTRUCTURE: A CONSIDERATION OF OPERATIONAL RISK

*Angela Walch**

New York University Journal of Legislation & Public Policy
Vol. 18, Issue 4, 2015, Forthcoming

Contents

INTRODUCTION

> "We have elected to put our money and faith in a mathematical framework that is free of politics and human error . . . ."[1]
>
> "If no-one owns it, how can I trust it? . . .
> In short, if you trust mathematics, you can trust Bitcoin."[2]
>
> "There are places where authority is required: No one should want Congress's laws on a wiki. Or instructions for administering medication. Or the flight plan of a commercial airliner."[3]
>
> "The faith that technology can redeem all of our sins and fix all of our problems is the ultimate hubris."[4]
>
> "Working on Bitcoin's core code is really scary, actually, because if you wreck something, you can break this huge $8 billion project. . . . And that's happened. We have broken it in the past."[5]

* * *

Since 2012, almost $930 million of venture capital has been invested in virtual currency companies,[6] with over $450 million invested in 2015

---

* Assistant Professor, St. Mary's University School of Law. J.D., Harvard Law School, 2002. A.B., Harvard College, 1998. I would like to thank Michael Ariens, Shawn Bayern, Catherine Martin Christopher, Reuben Grinberg, Colin Marks, Eric Posner, Todd Senulis, Jonathan Zittrain, Paul Finkelman, the editors of the *New York University Journal of Legislation & Public Policy*, participants at the "Inside Bitcoins NYC" conference from July 2013, participants in the 2014 Arizona State University Legal Scholars Conference, participants at the 2015 Harvard Law School Institute of Global Law and Policy mini-conference on Monetary Design in Global Perspective, and students in my Law of Money seminars for helpful comments, explanations, and insights. I would also like to thank my research assistants Tapash Agarwal, Sarah Scheidt, and Andrew Stephens.

[1] Nathaniel Popper & Peter Lattman, *Never Mind Facebook; Winklevoss Twins Rule in Digital Money*, N.Y. TIMES, April 11, 2013, at A3 (statement of Tyler Winklevoss).

[2] *Frequently Asked Questions*, MULTIBIT, https://multibit.org/faq.html (last visited Oct. 21, 2015). Multibit is a Bitcoin wallet. Companies that store Bitcoin users' private keys (essentially passwords), which enable them to transfer their bitcoins, are known as "wallet" companies.

[3] LAWRENCE LESSIG, REMIX: MAKING ART AND COMMERCE THRIVE IN THE HYBRID ECONOMY 85 (2008).

[4] SIVA VAIDHYANATHAN, THE GOOGLIZATION OF EVERYTHING 77 (2011).

[5] Leah McGrath Goodman, *The Face Behind Bitcoin*, NEWSWEEK, Mar. 14, 2014, at 21 (quoting Gavin Andresen, core developer of the Bitcoin software code).

[6] *See Bitcoin Venture Capital*, COINDESK, http://www.coindesk.com/bitcoin-venture-

alone.[7] In the past 18 months, a former Chairman of the Securities and Exchange Commission,[8] a former Treasury Secretary and chief economic advisor of President Obama,[9] a former chair of the Federal Deposit Insurance Corporation (FDIC),[10] and a former CEO of the Depository Trust and Clearing Corporation (DTCC)[11] have become advisors to or board members of virtual currency companies. Richard Branson has thrown an exclusive invitation-only "blockchain" summit on his private island,[12] and elite universities like Stanford and MIT are offering courses on virtual currencies.[13]

"Blockchain"[14] is the buzzword of the moment in financial circles, with a debate raging over whether private (permissioned) blockchains or public

---

capital/ (last visited Oct. 22, 2015).

[7] *See id.*

[8] *See Arthur Levitt Advises Bitcoin Companies: BitPay and Vaurum*, BUSINESSWIRE (Oct. 28, 2014), http://www.businesswire.com/news/home/20141028005244/en/Arthur-Levitt-Advises-Bitcoin-Companies-BitPay-Vaurum#.Vgye8ctViko (reporting that Arthur Levitt, former chairman of the Securities and Exchange Commission, will serve as an advisor to BitPay (a Bitcoin payment processor) and Vaurum (a Bitcoin exchange)).

[9] *See* Michael Casey, *Bitcoin Startup 21 Unveils Product Plan: Embeddable Mining Chips*, DOW JONES INST. NEWS (May 18, 2015) (reporting that Lawrence Summers, former Secretary of the Treasury, has joined the advisory board of 21 Inc., a Bitcoin company seeking to produce an "embedded mining chip"); Yessi Bello Perez, *Xapo Adds Former Visa and Citibank Execs to Board of Advisors*, COINDESK (May 26, 2015), http://www.coindesk.com/bitcoin-is-exempt-from-vat-says-european-court-of-justice/ (reporting that Summers had been appointed to the board of advisors of Xapo, a Bitcoin services provider, along with the founder of Visa and the former CEO of Citibank).

[10] *See* Nathaniel Popper, *ItBit Bitcoin Exchange Gets Banking License in New York, A First in U.S.*, N.Y. TIMES, May 8, 2015, at B5 (reporting that Sheila Bair, former chairwoman of the Federal Deposit Insurance Corporation had been appointed a board member of ItBit, a Bitcoin exchange).

[11] Yessi Bello Perez, *Ripple Appoints DTCC's Former CEO as Advisor*, COINDESK (June 1, 2015), http://www.coindesk.com/ripple-appoints-dtccs-former-ceo-as-advisor/ (reporting that Donald Donahue, former CEO of the Depository Trust & Clearing Corporation (DTCC), "the main clearinghouse for US securities and derivatives," became an advisor to Ripple Labs, a digital currency company).

[12] *See* BLOCKCHAIN SUMMIT, http://www.blockchainsummit.io/ (providing information on the May 25–28, 2015 Blockchain Summit held on Necker Island).

[13] *See* Danielle Meegan, *The New Virtual Currency Trend: Going Back to School!*, DIGITAL MONEY CORP. (Sept. 15, 2015), http://www.digitalmoneycorp.com/blog/the-new-virtual-currency-trend-going-back-to-school/ (reporting that universities such as MIT, Stanford, NYU, Princeton, and Duke offer courses on virtual currencies).

[14] "Blockchain" is the word for the common ledger, or list, that is maintained by virtual currencies. In Part I, I provide an overview of how Bitcoin and its blockchain operate.

(permissionless) blockchains are more desirable for financial structures.[15] Some businesses are building their own private blockchains, while others are building on top of the Bitcoin blockchain.[16] In this paper, I consider the implications of building financial market infrastructure[17]—such as payment, settlement, or clearing systems—on top of the Bitcoin blockchain. I do this

[15] Private (permissioned) blockchains are common ledgers shared amongst a known group of parties with only certain parties having the ability, or permission, to make changes to the ledger. Public (permissionless) blockchains like Bitcoin's are publicly available common ledgers that allow anyone who runs the Bitcoin software to participate in making changes to the ledger. *See* BITFURY GROUP & JEFF GARZIK, PUBLIC VERSUS PRIVATE BLOCKCHAINS: PART I: PERMISSIONED BLOCKCHAINS (2015), http://bitfury.com/content/4-white-papers-research/public-vs-private-pt1-1.pdf) (presenting explanation of permissioned and permissionless blockchains, and arguments for and against each type, focusing on the Bitcoin blockchain as "the most commercially successful and secure permissionless blockchain"); BITFURY GROUP & JEFF GARZIK, PUBLIC VERSUS PRIVATE BLOCKCHAINS: PART II: PERMISSIONLESS BLOCKCHAINS (2015), (same); Ian Allison, *Nick Szabo: If banks want benefits of blockchains they must go permissionless*, INT'L BUS. TIMES (Sept. 8, 2015), http://www.ibtimes.co.uk/nick-szabo-if-banks-want-benefits-blockchains-they-must-go-permissionless-1518874 (reporting an interview with cryptography and cyber expert, Nick Szabo, who argued that permissionless blockchains offer true innovation while permissioned blockchains keep existing problems with financial infrastructures); Giulio Prisco, *Blythe Masters And Wall Street Opt For 'Permissioned' Non-Bitcoin Blockchains*, BITCOIN MAG. (Sept. 2, 2015), https://bitcoinmagazine.com/articles/blythe-masters-wall-street-opt-permissioned-non-bitcoin-blockchains-1441227797 (reporting that permissioned blockchains are attractive to companies because they offer "a completely known universe of transaction processors").

[16] *See* Prisco, *supra* note 15 (reporting that many financial institutions are working to create private blockchains rather than rely on the Bitcoin blockchain); Andrew Robinson & Matthew Leising, *Blythe Masters Tells Banks: The Blockchain Changes Everything*, BLOOMBERG (Aug. 31, 2015), http://www.bloomberg.com/news/features/2015-09-01/blythe-masters-tells-banks-the-blockchain-changes-everything (noting that Nasdaq is using the Bitcoin blockchain to trial certain share issuances and transfers).

[17] Although Bitcoin is not now functioning as financial market infrastructure, in this paper I consider the implications of the Bitcoin blockchain potentially *supporting* financial market infrastructure. I therefore use the Federal Reserve's definition of "financial market infrastructures," which is consistent with the definition used globally, throughout this paper. *See Supervision and Oversight of Financial Market Infrastructures*, FED. RESERVE (Sept. 2, 2009), http://www.federalreserve.gov/paymentsystems/over_about.htm. The Federal Reserve defines "financial market infrastructures" as "multilateral systems among participating financial institutions, including the system operator, used for the purposes of clearing, settling, or recording payments, securities, derivatives, or other financial transactions. *Id.* FMIs include payment systems, central securities depositories, securities settlement systems, central counterparties, and trade repositories." Federal Reserve Policy on Payment System Risk, 79 Fed. Reg. 67,326, 67,333 (Nov. 12, 2014) [hereinafter Fed Policy on Payment System Risk]. *See also* COMM. ON PAYMENT & SETTLEMENT SYS. & TECH. COMM. INT'L ORG. SEC. COMM'NS, PRINCIPLES FOR FINANCIAL MARKET INFRASTRUCTURES (2012), www.bis.org/cpmi/publ/d101a.pdf [hereinafter *PFMI*] (upon which the Federal Reserve's definition of financial market infrastructure is based).

from an operational risk perspective, examining how Bitcoin's most fundamental features—its status as decentralized, open-source software—pose important risks to its stability as potential financial market infrastructure.

In Parts I and II of the paper, I provide needed context for the reader. Part I provides a brief overview of the key features of Bitcoin and its blockchain that are relevant to my argument. Part II discusses how Bitcoin and blockchain technology are poised to disrupt financial market infrastructures, why the uninterrupted operation of these systems is so vital, and how global financial regulators address operational risks[18] in existing financial market infrastructures.

Part III provides the meat of my argument. In this Part, I lay out the operational risks of Bitcoin that concern me, including the inherent vulnerabilities of software, the governance problems that arise from Bitcoin's decentralized, open-source status, and the expertise problems that stem from having software developers control potential financial market infrastructure through their code development. After explaining each risk, I demonstrate how each threatens the Bitcoin blockchain's reliability as potential financial market infrastructure.

In Part IV, I provide possible reasons why these operational risks have not received as much regulatory or academic attention as the "use" risks of Bitcoin.[19]

I conclude the paper with recommendations that policy-makers, regulators, and the business community explicitly factor these risks into their evaluation of the Bitcoin blockchain (and that of other virtual

[18] In the Fed Policy on Payment System Risk, the Federal Reserve defines "operational risk" as "the risk that deficiencies in information systems or internal processes, human errors, management failures, or disruptions from external events will result in the reduction, deterioration, or breakdown of services provided by the FMI. Furthermore, operational risk also includes physical threats, such as natural disasters and terrorist attacks, and information security threats, such as cyberattacks. Further, deficiencies in information systems or internal processes include errors or delays in processing, system outages, insufficient capacity, fraud, data loss, and leakage." Fed Policy on Payment System Risk, *supra* note 17, at 5. The Policy notes that this definition of operational risk is "consistent with [that] presented in the PFMI." *Id.* I use this definition throughout this paper.

[19] I consider the "use" risks of Bitcoin to be those risks that arise from how it may be used, such as crimes that can be committed with it (like money laundering and online sales of illegal goods and services), how it should be taxed, how people who handle it on behalf of others (e.g., exchanges and wallet companies) should be regulated, etc.

currencies) as potential financial market infrastructure. I also briefly outline the larger questions that my analysis raises about the use of open-source software in other critical infrastructures.

Before jumping in, it may be helpful to clarify what I am *not* doing in this paper. In considering the operational risks of Bitcoin in connection with its blockchain's suitability as financial market infrastructure, I am not defending existing financial market infrastructures as flawless, or even necessarily better than the Bitcoin blockchain.[20] For instance, this paper is not intended to be a defense of the costly and slow existing payment systems. It may be that after a weighing of risks and benefits, financial systems that run on the Bitcoin blockchain (or that of other decentralized virtual currencies) are more desirable than certain existing financial market infrastructures. However, I want to be sure that we are adequately considering Bitcoin's operational risks (primarily stemming from technology and governance issues) in performing the cost-benefit analysis, and below, I seek to flesh out those risks.

My primary goal in this paper is to ensure that the cost-benefit analysis performed in determining whether to replace existing financial market infrastructure with systems built on top of the Bitcoin blockchain is as fulsome as possible—explicitly accounting for operational risks. Infrastructure's most essential trait is *reliability*, and thus evaluating the reliability of potentially new infrastructure must be done with great care.

I. BITCOIN AND ITS BLOCKCHAIN

Bitcoin is peer-to-peer[21] open-source[22] software that operates to create and maintain a distributed public ledger.[23] This public ledger is known as

[20] Existing financial market infrastructures are known to be costly and inefficient. *See* Robinson & Leising, *supra* note 16 (describing the "opaque and clunky back-office processes" that slow financial transactions).

[21] Peer-to-peer software is distinctive in that a central computer server does not run it. Rather, the software operates over the connections that individual computers make with one another. For an overview of peer-to-peer software, see Detlef Schoder, Kai Fischbach & Christian Schmitt, *Core Concepts in Peer-to-Peer Networking*, *in* PEER TO PEER COMPUTING: THE EVOLUTION OF A DISRUPTIVE TECHNOLOGY 1–27 (Ramesh Subramanian & Brian D. Goodman eds., 2005).

[22] For a sustained discussion of open-source software, see *infra* Part III.C.

[23] *See* ANDREAS M. ANTONOPOULOS, MASTERING BITCOIN: UNLOCKING DIGITAL CRYPTOCURRENCIES 18 (2014). Mr. Antonopoulos is a well-respected figure in the Bitcoin community and has taught university courses on digital currencies. I have chosen to cite his December 2014 book on Bitcoin for many of the basics of Bitcoin's operation because he is an identifiable, seemingly credible person, while the website that purports to be "behind"

the "blockchain,"[24] and it is analogous to a database that shows all changes made since its creation. The Bitcoin blockchain is maintained by a network of computers (referred to as "miners") that solves complex mathematical equations as part of verifying changes made to the ledger.[25] Crucially, the network of computers running the Bitcoin software and maintaining the blockchain is *decentralized*, with no central authority that controls it.[26] Because there are no permissions required to join the network of computers that run the Bitcoin software and help to maintain the blockchain, the Bitcoin blockchain is said to be public, or "permissionless," distinguishing it from private, or "permissioned," blockchains that are being developed by financial and technology companies.[27]

Major players in the financial industry have seized on the technology that maintains the blockchain (or common ledger) as a significant innovation.[28] It is seen as a way to achieve a reliable shared list without having a central party to maintain it.[29]

Importantly, the computer network that runs the Bitcoin software is not the only part of Bitcoin that is decentralized. The software development process is as well, meaning that there is no central entity that is officially charged with maintaining or fixing the software.[30] In fact, the actual creator of the Bitcoin software remains a mystery; an unknown software coder or group of coders known by the pseudonym "Satoshi Nakamoto" introduced it to the world in 2009.[31]

Bitcoin (bitcoin.org) does not come from a unified, identifiable source. *See About bitcoin.org: Who owns bitcoin.org?*, BITCOIN.ORG, https://bitcoin.org/en/about-us (last visited Oct. 21, 2015) ("Bitcoin.org was originally registered and owned by Bitcoin's first two developers, Satoshi Nakamoto and Martti Malmi. When Nakamoto left the project, he gave ownership of the domain to additional people, separate from the Bitcoin developers, to spread responsibility and prevent any one person or group from easily gaining control over the Bitcoin project. . . . Bitcoin.org is not Bitcoin's official website. Just like nobody owns the email technology, nobody owns the Bitcoin network. *As such, nobody can speak with authority in the name of Bitcoin.*") (emphasis added).

[24] *See* ANTONOPOULOS, *supra* note 23, at 176–77.

[25] *Id.* at 173–74.

[26] *See id.* at 1.

[27] *See supra* notes 15–16 and accompanying text.

[28] *See, e.g.*, Nathaniel Popper, *Wall Street Takes a Keen Interest in Bitcoin's Latest Technology; Bitcoin's blockchain tech is being examined to see if it can be used to create a new way of transacting online*, IRISH TIMES, Sept. 14, 2015, (Finance), at 5 (reporting on the interest in blockchain technology by numerous major banks across the globe).

[29] *See id.*; Robinson & Leising, *supra* note 16; THE ECONOMIST, *The great chain of being sure about things*, Oct. 31, 2015, 21.

[30] *See* ANTONOPOULOS, *supra* note 23, at 1.

[31] *See id.* at 3–4.

The Bitcoin software has evolved significantly since its initial release,[32] and changes to the software have come about through the efforts of a mix of volunteer and paid programmers, who determine what changes should be made through "informal processes that depend on rough notions of consensus and that are subject to no fixed legal or organizational structure."[33] As will be discussed at length in this paper, Bitcoin software maintenance and development is spearheaded by a team of around five "core developers,"[34] who release periodic new versions of the software,[35] and who have certain privileges that other coders do not, such as the ability to send emergency messages to all nodes,[36] and to make decisions about what changes are included in a new release of the Bitcoin software.[37]

Although this paper focuses on the Bitcoin blockchain because that is the current topic of public conversation, Bitcoin was initially seen as a possible alternative currency and is often referred to as a virtual currency,

[32] *See* Goodman, *supra* note 5, at 23 (quoting Gavin Andresen, head developer of the Bitcoin software code, as stating that the developers "have rewritten roughly 70 percent of the code since inception").

[33] Shawn Bayern, *Of Bitcoins, Independently Wealthy Software, and the Zero-Member LLC*, 108 NW. U. L. REV. ONLINE 257, 259 (2014).

[34] The core developers listed on the Bitcoin software development website are Wladimir J. van der Laan, Gavin Andresen, Jeff Garzik, Gregory Maxwell, and Pieter Wuille. *Bitcoin Development*, BITCOIN.ORG, https://bitcoin.org/en/development (last visited Nov. 14, 2015).

[35] *See, e.g.*, Joon Ian Wong, *Bitcoin Core 0.10 Gives Developers Simplified Access to Network Consensus*, COINDESK (Feb. 17, 2015), http://www.coindesk.com/bitcoin-core-0-10-gives-developers-simplified-access-network-concensus/ (reporting on the Feb. 16, 2015 release of core Bitcoin software by the core developers).

[36] The emergency message power "allow[s] the core developer team to notify all bitcoin users of a serious problem in the bitcoin network, such as a critical bug that require[s] user action." ANTONOPOULOS, *supra* note 23, at 157. Alerts have "only been used a handful of times, most notably in early 2013 when a critical database bug caused a multiblock fork to occur in the bitcoin blockchain." *Id.* The password that allows the sending of the network-wide emergency messages is held only "by a few select members of the core development team." *Id.*; *see also* ARTHUR GERVAIS ET AL., IS BITCOIN A DECENTRALIZED CURRENCY? (2014), http://eprint.iacr.org/2013/829.pdf (arguing that giving the emergency alert power only to the core developers "gives these entities privileged powers to reach out to users and urge them to adopt a given Bitcoin release").

[37] *See* Tom Simonite, *The Man Who Really Built Bitcoin*, MIT TECH. REV., (Aug. 15, 2014), http://www.technologyreview.com/featuredstory/527051/the-man-who-really-built-bitcoin/ (describing how only the core developers have the power to "change the code behind Bitcoin and merge in proposals from other volunteers"); *see also* GERVAIS ET AL., *supra* note 36, at 6 ("This [software development process] limits the impact that users have, irrespective of their computing power, to affect the development of the official Bitcoin [software].").

digital currency, or cryptocurrency.[38] There have been prior attempts to create virtual currency, or digital money,[39] but Bitcoin is the most successful thus far.[40] In the context of Bitcoin as a virtual currency, the currency unit is described as a "bitcoin."[41] A "bitcoin" is actually only an entry within the blockchain, marking a party's right to spend a certain amount of bitcoins.[42] There is no actual file or other tangible "thing" that comprises a bitcoin—it is just a representation of ownership within the blockchain.[43] When a bitcoin is transferred to another party, all the computers that run the Bitcoin software (referred to as "nodes") work together to verify that the party seeking to transfer that bitcoin has not already transferred it to someone else.[44] This prevents double-spending of a bitcoin by its owner.[45]

---

[38] Regulators have sought in recent years to create a definition of "virtual currency." In 2012, the European Central Bank (ECB) defined "virtual currency" as "a type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community." EUROPEAN CENT. BANK, VIRTUAL CURRENCY SCHEMES 5 (2012) [hereinafter 2012 ECB PAPER], http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf. In 2015, the ECB revised its definition of "virtual currency" to "a digital representation of value, not issued by a central bank, credit institution or e-money institution, which, in some circumstances, can be used as an alternative to money." EUROPEAN CENT. BANK, VIRTUAL CURRENCY SCHEMES: A FURTHER ANALYSIS 25 (2015) [hereinafter 2015 ECB PAPER], http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf. The U.S. Department of Treasury has defined "virtual currency" as "a medium of exchange that operates like a currency in some environments, but does not have all the attributes of real currency." DEP'T OF TREASURY FIN. CRIMES ENF'T NETWORK, GUIDANCE FIN-2013-G0001, APPLICATION OF FINCENS'S REGULATIONS TO PERSONS ADMINISTERING, EXCHANGING, OR USING VIRTUAL CURRENCIES 1 (2013). The U.S. Government Accountability Office (GAO) defines "virtual currency" as "a digital representation of value that is not government-issued legal tender." *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-14-496, VIRTUAL CURRENCIES: EMERGING REGULATORY, LAW ENFORCEMENT, AND CONSUMER PROTECTION CHALLENGES 4 (2014).

[39] *See* Reuben Grinberg, *Bitcoin: An Innovative Alternative Digital Currency*, 4 HASTINGS SCI. & TECH. L.J. 159, 168–74 (2012) (providing a historical overview of prior forms of digital or virtual currencies).

[40] *See* 2015 ECB PAPER, *supra* note 38, at 6–7.

[41] A convention has developed to distinguish between (a) references to the Bitcoin software and network and (b) references to individual bitcoins that comprise the units of the currency. Lower case "bitcoins" refer to the individual units of the currency; upper case "Bitcoin" refers generally to the phenomenon of Bitcoin, the software, its protocol, or the Bitcoin network. *See Vocabulary*, BITCOIN.ORG, https://bitcoin.org/en/vocabulary.

[42] *See* 2015 ECB PAPER, *supra* note 38, at 13 ("[U]sers do not hold units of the currency in decentralised [virtual currencies]. They actually hold keys which give access to a certain account balance, which is stored in the blockchain.").

[43] *See id.*

[44] *See* ANTONOPOULOS, *supra* note 23, at 109–11.

[45] *See id.*

As of this writing, there are nearly fifteen million bitcoins in circulation;[46] the software caps the total number of bitcoins ever to be created at twenty-one million.[47] New bitcoins are created through the blockchain verification process, with the first computer to solve the equations that verify transactions compensated with a specified number of newly created bitcoins.[48] This compensation incentivizes parties to participate in the Bitcoin network and ensures that the blockchain is maintained. By design, the pace of mining bitcoins becomes slower and slower, as over time the difficulty of the equations to be solved by the miners increases while the number of bitcoins awarded for solving equations decreases.[49] Although individuals started out as the initial miners of bitcoins, as mining began to be seen as lucrative, an arms race of sorts developed to generate bitcoins the fastest.[50] This has culminated in extremely high-powered and expensive computer equipment, coupled with vast amounts of electricity, being needed to mine bitcoins. As a result, mining is now almost exclusively dominated by businesses devoted to mining and mining consortiums (known as "pools").[51]

For my purposes, what is most important about Bitcoin is that many people believe that its blockchain innovation can disrupt important systems within our society, including systems that comprise our financial market infrastructures.[52] In Part II, I discuss this possible disruption and how global financial regulators address operational risk in existing financial market infrastructures. Note that a detailed understanding of the Bitcoin software is

---

[46] *Total Bitcoins in Circulation*, BLOCKCHAIN.INFO, https://blockchain.info/charts/total-bitcoins (last visited Oct. 22, 2015).

[47] *See* ANTONOPOULOS, *supra* note 23, at 2.

[48] *Id.* at 173.

[49] *See id.* at 195–96.

[50] *See id.* at 204–06. For an analysis of Bitcoin mining practices, see generally NICOLAS T. COURTOIS, MAREK GRAJEK & RAHUL NAIK, THE FUNDAMENTAL INCERTITUDES OF BITCOIN MINING (2014), http://arxiv.org/pdf/1310.7935v3.pdf.

[51] *See* ANTONOPOULOS, *supra* note 23, at 207–10.

[52] *See, e.g.*, ACCENTURE, BLOCKCHAIN IN THE INVESTMENT BANK 5 (2015), http://fsblog.accenture.com/capital-markets/wp-content/uploads/sites/2/2015/06/CM_ATS_POV_Blockchain_in_the_Investment_Bank-web.pdf ("Accenture believes that, although the potential of the technology is only just emerging, Blockchains will become the critical backbone of the future capital markets infrastructure."); Laura Shin, *Money's New Operating System*, FORBES, Sept. 28, 2015, at 100 (reporting on the ways that blockchains may alter existing financial and recordkeeping practices); Robinson & Leising, *supra* note 16 (reporting claims that blockchains will be as transformative as the Internet towards financial systems).

unnecessary to follow the arguments made in this paper[53]; rather, the most basic attributes of Bitcoin are my focus: its status as *open-source, decentralized software* that purports to displace financial market infrastructures.

II. DISRUPTING EXISTING FINANCIAL MARKET INFRASTRUCTURES

As discussed above, the proponents of Bitcoin and other virtual currencies seek to replace existing financial market infrastructures. In this Part, I discuss this potential disruption, the significance of financial market infrastructure, and how global financial regulators address operational risk in existing financial market infrastructures.

A. Virtual Currency as Disruptor

The name of the game with virtual currency is disruption. Proponents of Bitcoin and blockchain technology speak of the quadrillion dollar markets they seek to displace.[54]

In the early days of Bitcoin, the buzz was primarily about how Bitcoin could serve as an actual currency that displaced the fiat currencies issued by governments.[55] When the economy of Cyprus collapsed in 2013, the price of Bitcoin spiked as many depositors in Cypriot banks bought bitcoins to avoid having government currency that could be frozen or seized by the government.[56] Many of the early users of Bitcoin were motivated by the idea of the creation of money moving from the hands of government to the

[53] For a more substantial technical description of Bitcoin, see generally ANTONOPOULOS, *supra* note 23 (providing a useful overview of how Bitcoin works by a prominent Bitcoin proponent and directed primarily at software coders). For cultural analyses of the phenomenon, see generally NATHANIEL POPPER, DIGITAL GOLD: BITCOIN AND THE INSIDE STORY OF THE MISFITS AND MILLIONAIRES TRYING TO REINVENT MONEY (2015) (providing a history of Bitcoin and the people involved with it); PAUL VIGNA & MICHAEL J. CASEY, THE AGE OF CRYPTOCURRENCY: HOW BITCOIN AND DIGITAL MONEY ARE CHALLENGING THE GLOBAL ECONOMIC ORDER (2015) (providing an overview of Bitcoin along with the risks and opportunities it presents).

[54] *See* Consensus Conference Agenda, "A $1.6 Quadrillion Opportunity: Securities Settlement and Clearing", Sept. 10, 2015 http://10times.com/consensus-newyork (describing a blockchain conference sponsored by prominent virtual currency news site CoinDesk in which one of the panels discussed the opportunity for blockchain technology to disrupt the $1.6 quadrillion securities settlement and clearing market).

[55] *See, e.g.*, David Yermack, *Is Bitcoin a Real Currency? An Economic Appraisal* 7–8 (Nat'l Bureau of Econ. Research, Working Paper No. 19747, 2014).

[56] *See* Emma Rowley, *Russians Turn to Bitcoin After Cyprus Crisis*, SUNDAY TELEGRAPH, Apr. 7, 2013 (Business), at 5 (reporting speculation that Bitcoin's price increase was related to the Cyprus banking crisis).

hands of individuals.[57]

In the intervening years, many economists and finance scholars have critiqued Bitcoin's capacity to serve as money. They have noted that Bitcoin fails to perform the three basic functions of money (to serve as a unit of account, a store of value, and a medium of exchange) due to the extreme swings in its value and the limited number of parties that will accept it.[58] Others have pointed to flaws in the monetary policy that is embedded in Bitcoin's structure, such as the hardwired limit on the number of Bitcoins that may ever be created.[59] It seems that many have moved on from the idea that Bitcoin will be a viable currency that competes with government-issued currencies.[60]

More recently, the conversation about virtual currencies has shifted to a focus on the possible transformative applications of the blockchain—the common ledger that is verified through a decentralized computer network rather than by a single central party.[61] Prominent actors such as Andrew

[57] *See, e.g.*, Grinberg, *supra* note 39, at 172–74 (describing the attraction that Bitcoin holds for "gold bugs"); Yermack, *supra* note 55, at 7–8 (describing the libertarian interest in Bitcoin "due to its lack of connection to any government").

[58] *See, e.g.*, 2015 ECB PAPER, *supra* note 38, at 23–25 (noting that virtual currencies like Bitcoin are not money or currency from an economic or legal perspective); STEPHANIE LO & J. CHRISTINA WANG, FED. RESERVE BANK OF BOS., BITCOIN AS MONEY? 3–11 (2014), https://www.bostonfed.org/economic/current-policy-perspectives/2014/cpp1404.pdf (concluding that Bitcoin does not perform money's functions as a medium of exchange, unit of account, or store of value); Yermack, *supra* note 55 (concluding that Bitcoin does not satisfy the standard definition of a currency because it does not perform money's functions as a medium of exchange, store of value, and unit of account); THE GOLDMAN SACHS GRP., ALL ABOUT BITCOIN 6 (2014), http://www.paymentlawadvisor.com/files/2014/01/GoldmanSachs-Bit-Coin.pdf (concluding that "bitcoin[] and other digital currencies[] currently lie somewhere on the boundaries between currency, commodity and financial asset").

[59] *See, e.g.*, Paul Krugman, *Golden Cyberfetters*, N.Y. TIMES: THE CONSCIENCE OF A LIBERAL (Sept. 7, 2011), http://krugman.blogs.nytimes.com/2011/09/07/golden-cyberfetters/ (noting that Bitcoin is prone to deflation due to the limits on its quantity); *Yermack*, supra note 55, at 17 (arguing that Bitcoin is prone to deflation due to cap on the number of bitcoins to be created); Daniel Reber & Simon Feurstein, *Bitcoins: Hype or Real Alternative*, *in* INTERNET ECONOMICS VIII 90 (Burkhard Stiller et al. eds., 2014) (noting that Bitcoin is subject to deflation in the long-run).

[60] *See Blockchain's Whirlwind Month—So Far*, PYMNTS.COM (Oct. 16, 2015), http://www.pymnts.com/in-depth/2015/blockchains-whirlwind-month-so-far/ (noting the shift in focus toward the potential of Bitcoin's blockchain technology rather than as a currency).

[61] For recent feature articles on the blockchain in prominent financial publications, see, e.g., Shin, *supra* note 52; Robinson & Leising, *supra* note 16; THE ECONOMIST, *supra* note 29; Jane Wild et. al., *Technology: Banks Seek the Key to the Blockchain*, Nov. 1, 2015, FIN.

Haldane, Chief Economist of the Bank of England, and the Financial Stability Oversight Council have noted that Bitcoin and other virtual currencies may have promise as payment systems.[62] Others point to its ability to disrupt other aspects of the financial system.[63] Most of the largest financial institutions now have substantial teams of people devoted to investigating ways that blockchain technology could improve their businesses.[64] And titans of the finance and business world, from Larry Summers to Marc Andreessen, are rushing to become involved in virtual currencies.[65] Rather than being seen as a way to rebel against government-controlled currency, or a way to commit crime via the Internet, virtual currencies are now being viewed by regulators and financial industry stalwarts as a significant innovation for the financial system that could save time, cut costs, and create jobs.[66]

B. Regulatory Treatment of Existing Financial Market Infrastructures

This all sounds great. Don't we want to save time, cut costs, and create jobs every time there is an opportunity to do so? Isn't this a no-brainer?

TIMES.

[62] *See, e.g.*, Speech by Andrew Haldane, Chief Economist of the Bank of England, at Portadown Chamber of Commerce, Northern Ireland, *How Low Can You Go?*, Sept. 18, 2015 (noting, in a speech about money and monetary policy, that "the distributed payment technology embodied in Bitcoin has real potential") (available at http://www.bankofengland.co.uk/publications/Documents/speeches/2015/speech840.pdf); FIN. STABILITY OVERSIGHT COUNCIL, 2015 ANNUAL REPORT 114, http://www.treasury.gov/initiatives/fsoc/studies-reports/Documents/2015%20FSOC%20Annual%20Report.pdf ("[T]he potential applications and uses of the peer-to-peer network for transferring value in the payment and financial service industry warrant continued monitoring."); Robleh Ali et al., *Innovations in payment technologies and the emergence of digital currencies*, 54 BANK ENGLAND Q. BULL. 262, 266 (2014) (evaluating the promise that digital currencies hold for payment systems).

[63] *See generally, e.g.*, Shin, *supra* note 52; Robinson & Leising, *supra* note 16; THE ECONOMIST *supra* note 29; Wild, *supra* note 61.

[64] *See* Wild, *supra* note 61 (describing the initiatives at major banks to investigate how the blockchain could be used to improve the financial services industry).

[65] *See supra* note 9 (describing Lawrence Summers' involvement with virtual currency companies; Marc Andreessen, Opinion *Why Bitcoin Matters*, N.Y. TIMES (Jan. 21, 2014), http://dealbook.nytimes.com/2014/01/21/why-bitcoin-matters/?pagewanted=all (comparing Bitcoin to the Internet in terms of its revolutionary potential).

[66] For such claims by the financial industry, *see, e.g.*, THE ECONOMIST, *supra* note 29, at 24 (noting claims by Santander, a bank, that distributed ledgers could save the banking industry $20 billion a year by 2022); Wild, *supra* note 61; Shin, *supra* note 52 ; Robinson & Leising, *supra* note 16.

It *is* good news that there is a new technology that could positively transform these areas. There are profuse criticisms of existing financial market infrastructures. Existing systems are faulted for their ancient and creaky technology, the slow speed at which payments are processed across borders or transactions are settled, and the high fees charged to move money around the world.[67] These systems feel obsolete in a world that is used to sending photos, videos, and other information via the swipe of a smart-phone. The centralization and concentration of risk in large clearinghouses or settlement systems is also troubling to many.[68]

Little surprise, then, that potential transformations in these areas are heralded as a big deal. But in all the excitement over this technological boon, we must keep in mind the enormous importance of reliable financial market infrastructure, and ensure that replacements to existing financial market infrastructures can be counted on. In the following paragraphs, I describe how global financial regulators treat existing financial market infrastructures. This discussion is not intended to be an in-depth treatise on the global regulation of financial market infrastructures, but rather a high-level overview. My goal here is to highlight the important role financial market infrastructures are acknowledged to play in global financial stability, buttressing my argument that the operational risks of Bitcoin are relevant in evaluating its quality as potential financial market infrastructure.

First, what is "financial market infrastructure" and why is it of concern to global financial regulators? The Federal Reserve, consistent with standards set by the G20 and Financial Stability Board,[69] defines "financial

---

[67] *See* Shin, *supra* note 52; Robinson & Leising, *supra* note 16.

[68] *See generally, e.g.*, Felix B. Chang, *The Systemic Risk Paradox: Banks and Clearinghouses Under Regulation*, 2014 COLUM. BUS. L. REV. 747 (2014); Sean J. Griffith, *Governing Systemic Risk: Towards a Governance Structure for Derivatives Clearinghouses*, 61 EMORY L.J. 1153 (2012); Jeremy C. Kress, *Credit Default Swaps, Clearinghouses, and Systemic Risk: Why Centralized Counterparties Must Have Access to Central Bank Liquidity*, 48 HARV. J. ON LEGIS. 49 (2011); Kristin N. Johnson, *Clearinghouse Governance: Moving Beyond Cosmetic Reform*, 77 BROOK. L. REV. 681 (2012).

[69] Guido Ferrarini and Paolo Saguato, *Regulating Financial Market Infrastructures*, *in* OXFORD HANDBOOK ON FINANCIAL REGULATION (2015) 2 (describing the "supranational" approach to regulating financial market infrastructures, with "international regulatory guidelines adopted by the G20 and then developed by the Financial Stability Board"). "The Group of Twenty (G20) is the premier forum for its members' international economic cooperation and decision-making. Its membership comprises 19 countries plus the European Union." https://g20.org/about-g20/. The Financial Stability Board (FSB) is "an international body that monitors and makes recommendations about the global financial

market infrastructures" (or FMIs) as "multilateral systems among participating financial institutions, including the system operator, used for the purposes of clearing, settling, or recording payments, securities, derivatives, or other financial transactions. FMIs include payment systems, central securities depositories, securities settlement systems, central counterparties, and trade repositories."[70] These types of systems act as the networks, or the "plumbing systems," through which money and other forms of value flow in our modern economy.[71]

As the Federal Reserve notes, "Financial market infrastructures . . . are critical components of the nation's financial system . . . . The safety and efficiency of these systems may affect the safety and soundness of U.S. financial institutions, and in many cases, are vital to the financial stability of the United States."[72] In adopting standards for financial market infrastructures, the Federal Reserve's "objective is to foster the safety and efficiency of payment, clearing, settlement, and recording systems and to promote financial stability, more broadly."[73]

The consequences of failure in a system that serves as financial market infrastructure are severe, with "a failure [possibly] lead[ing] ultimately to a disruption in the financial markets more broadly and undermin[ing] public confidence in the nation's financial system."[74] Further, the interconnectedness and interdependence inherent among financial market infrastructures mean that they can function as "transmission channel[s] of systemic risk."[75] The 2008 Financial Crisis made everyone aware of just how easily risk can be transmitted through our financial system, and financial market infrastructures provide the pathways for that transmission.

Although the Federal Reserve policies described above note how critical financial market infrastructure is to the stability of the *U.S.* financial

---

system…The FSB promotes international financial stability; it does so by coordinating national financial authorities and international standard-setting bodies as they work toward developing strong regulatory, supervisory and other financial sector policies. …The FSB, working through its members, seeks to strengthen financial systems and increase the stability of international financial markets. The policies developed in the pursuit of this agenda are implemented by jurisdictions and national authorities." http://www.financialstabilityboard.org/about/.

[70] *Fed Policy on Payment System Risk*, *supra* note 17, at 3.

[71] *Id.* at 6.

[72] *Id.* at 3.

[73] *Id.*

[74] *Id.* at 5.

[75] *Id.*

system, it is clear that they are also crucial to global financial stability, given the international character of our financial system today.[76] With the renewed emphasis on financial stability since the 2008 Financial Crisis, "governments and regulators of the leading economies" worked together to reach an "international consensus" on "key guiding principles" and "more detailed guidelines" to support the stability of financial market infrastructures,[77] with many countries basing their policies on the April 2012 *Principles for Financial Market Infrastructures (PFMI)* report by the Committee on Payment and Settlement Systems (CPSS) and Technical Committee of the International Organization of Securities Commissions (OPSCO).[78]

The international guidelines for financial market infrastructures seek to mitigate risks to the structures to help maintain their stability.. According to the *Federal Reserve Policy on Payment System Risk*, "the basic risks in payment, clearing, settlement, and recording systems may include credit risk, liquidity risk, operational risk, and legal risk."[79] The international *PFMI* adds systemic risk, general business risk, and custody and investment risks to that list.[80] This paper focuses on *operational risk*, which the Federal Reserve defines as:

> the risk that deficiencies in information systems or internal processes, human errors, management failures, or disruptions from external events will result in the reduction, deterioration, or breakdown of services provided by the [financial market infrastructure] . . . . Operational risk also includes physical threats, such as natural disasters and terrorist attacks, and information security threats, such as cyberattacks. Further, deficiencies in information systems or internal processes include errors or delays in processing, system outages, insufficient capacity, fraud, data loss, and leakage.[81]

Global financial regulators have identified a number of principles to help financial market infrastructures lessen their risks. Particularly relevant

[76] *See* Ferrarini & Saguato, *supra* note 69, at 2.
[77] *Id*. at 4.
[78] *See PFMI*, *supra* note 17.
[79] *Fed Policy on Payment System Risk*, *supra* note 17, at 4.
[80] *See PFMI*, supra note 17, at 18–20.[81] *Fed Policy on Payment System Risk*, *supra* note 17, at 5, 5 n.8.
[81] *Fed Policy on Payment System Risk*, *supra* note 17, at 5, 5 n.8.

to my analysis are those dealing with operational risks spawned by governance structures and technology. From the *PFMI*, these include:

> *Principle 2: Governance:* An FMI should have governance arrangements that are clear and transparent, promote the safety and efficiency of the FMI, and support the stability of the broader financial system, other relevant public interest considerations, and the objectives of relevant stakeholders.
>
> *Principle 3: Framework for the comprehensive management of risks:* An FMI should have a sound risk-management framework for comprehensively managing legal, credit, liquidity, operational, and other risks. . . .
>
> *Principle 17: Operational risk:* An FMI should identify the plausible sources of operational risk, both internal and external, and mitigate their impact through the use of appropriate systems, policies, procedures, and controls. Systems should be designed to have a high degree of security and operational reliability and should have adequate, scalable capacity. Business continuity management should aim for timely recovery of operations and fulfilment of the FMI's obligations, including in the event of a wide-scale or major disruption."[82]

As I discuss in Part III below, these risk mitigation principles are problematic for Bitcoin and likely for other decentralized virtual currencies. In Part III, I lay out the operational risks of Bitcoin in relation to its blockchain's potential role as financial market infrastructure. As I will discuss, Bitcoin's most fundamental features generate important operational risks whose mitigation would require, in some cases, an abandonment of the core premises of the virtual currency. Most notably, the governance and risk management standards for financial market infrastructures seem impossible in a system premised on decentralization, which only exacerbates the technology risks involved.

Of course, it is currently inappropriate to categorize the Bitcoin blockchain as financial market infrastructure because of its limited use and the relatively small values that are moved across its network. Systems don't become "financial market infrastructure" in regulators' eyes until they reach a certain scale. For instance, the Federal Reserve's *Policy on Payment System Risk* applies only to payment systems of a certain scale—those that "expect to settle a daily aggregate gross value of U.S. dollar-denominated

[82] *PFMI*, *supra* note 17, at 3.

transactions exceeding $5 billion on any day during the next 12 months."[83] Obviously, the Bitcoin blockchain supports exchange values that are nowhere close to that size at the moment;[84] however, blockchain proponents are targeting replacing precisely the systems that comprise existing financial market infrastructures,[85] so a discussion of how regulators treat existing financial market infrastructures is worthwhile. It is clearly better to consider the operational risks generated by Bitcoin's fundamental structures *now* rather than waiting until we are widely *relying* on the Bitcoin blockchain as infrastructure, and *then* realizing that its fundamental structures make it unreliable. With that goal in mind, in the next Part, I describe key operational risks that undermine the Bitcoin blockchain's reliability as potential financial market infrastructure.

III. BITCOIN'S OPERATIONAL RISKS AND ITS POTENTIAL AS FINANCIAL MARKET INFRASTRUCTURE

Given that blockchain technology is being discussed as a potential disruptor of certain financial market infrastructures, the reliability of the technology is paramount. Therefore, in this Part, I explicate important risks to Bitcoin's operation—particularly focusing on the technology and governance risks that are generated by Bitcoin's most basic features.

These structural features are:

1) its status as software;

2) its decentralized structure;

3) its open-source software development process; and

4) its expertise problem.[86]

---

[83] *Fed Policy on Payment System Risk*, *supra* note 17, at 6.

[84] *See* Wild, *supra* note 61 ("On an average day more than 120,000 transactions are added to bitcoin's blockchain, representing about $75m exchanged").

[85] *See supra* notes 61-66 and accompanying discussion.

[86] There are certainly other risks that threaten Bitcoin's ongoing operation. *See generally* MARIAM KIRAN & MIKE STANNETT, NEMODE, BITCOIN RISK ANALYSIS (2014), http://www.nemode.ac.uk/wp-content/uploads/2015/02/2015-Bit-Coin-risk-analysis.pdf (considering, among other risks: technology risks including reliance of the Bitcoin system on the availability of high-powered mining computers only produced by a few companies worldwide; the possibility of malware affecting the Bitcoin code; miners taking advantage of software errors to increase their rewards; the vulnerability of miners to attacks; the concentration of miners making their exposure to natural disasters relevant to the network operating); GARETH W. PETERS ET AL., OPENING DISCUSSION ON BANKING SECTOR RISK

In the Subparts that follow, I examine the operational risks created by each of these core features, and then discuss how these risks undermine the Bitcoin blockchain's reliability as financial market infrastructure.[87]

A. Bitcoin as Software

At its most basic level, Bitcoin is software, and living in a computer-driven, digital world has made all of us intimately familiar with the problems endemic to software. To list but a few that are readily perceived by non-techies like myself:

1) software always has bugs;

2) software is vulnerable to attack;

3) software is ever-changing through new releases; and

4) few people understand how software works.

In this Subpart, I discuss each of these weaknesses of software, and explain why that weakness is problematic for the Bitcoin blockchain's function as financial market infrastructure.

1. Software always has bugs

According to computer experts, "software today remains, in many ways, far less reliable and more prone to bugs than in the past."[88] It is

---

EXPOSURES AND VULNERABILITIES FROM VIRTUAL CURRENCIES: AN OPERATIONAL RISK PERSPECTIVE 20–23, 28–30 (2014), http://arxiv.org/pdf/1409.1451.pdf (examining how the operational risks of virtual currencies, including, among others, the risks of an organized attack on the system, transaction malleability, and double-spending, reliance on IT of mining network, and software problems, could impact the banking sector). In this paper, I focus on the risks I consider most urgent. I also do not mean to suggest that these risks are unfamiliar to regulators, academics, the media, or to members of the Bitcoin community. I do believe that they are worth explicitly considering, though, in the context of the Bitcoin blockchain's function as potential financial market infrastructure.

[87] I do not attempt to state the likelihood that a particular risk will lead to the Bitcoin network's collapse, although that would be a valuable area of further research. I consider each risk to have potentially catastrophic consequences for Bitcoin if it materializes. Thus, I am satisfied that even if the risk has a very low chance of coming to fruition it should still be relevant in making decisions about Bitcoin.

[88] Derek E. Bambauer, *Ghost in the Network*, 162 U. PA. L. REV. 1011, 1022 (2014) (citations omitted) (arguing for regulation tailored towards improving cyber-security through mitigation of harms rather than elimination of threat).

widely acknowledged that there is no such thing as flawless software; there are always errors or "bugs" that negatively affect the performance of the software or make it vulnerable to attacks by hackers.[89] This has been a problem since computers were created, and even with our amazing and rapid improvements in technology, software—like the humans who create it—remains inherently imperfect.[90]

Errors in software may be introduced in many different ways, including the programmer's lack of understanding or expertise in the programming language or the software structure or goals; the incompatibility of different releases of software; sloppiness, carelessness, or rushing on the part of the programmer; poorly coordinated collaboration; lack of big-picture oversight; miscommunications between programmers; and any other number of situations that cause people to create imperfect products.[91]

As an example, the "catastrophic" Heartbleed bug that was discovered in OpenSSL in April 2014[92] came about through a coding error that a contributor to the open-source software "unfortunately . . . missed" when he submitted it to the core developers for the project.[93] The core developer who reviewed the suggested code to determine whether to accept it into the next release version of the software "apparently also didn't notice" the error, "so the error made its way from the development branch

[89] I discuss software's vulnerability to attacks in relation to Bitcoin in Part III.A.2 *infra*.

[90] *See* Bambauer, *supra* note 92, at 1021 ("Software is . . . structurally prone to failure, despite significant efforts to remediate it. . . . Eliminating bugs completely is simply impossible.").

[91] For a discussion of how people dynamics and skills are determinative of the quality of software, see generally ROBERT GLASS, FACTS AND FALLACIES ABOUT SOFTWARE ENGINEERING (2003).

[92] Open SSL is an open-source software that provides part of the fundamental security structure of the Internet, and the Heartbleed bug made private information, such as passwords, credit card data and other personal information, from supposedly secure transactions available to hackers. Computer security experts deemed it "catastrophic." *See* Brian X. Chen, *Q. and A. on Heartbleed: A Flaw Missed by the Masses*, N.Y. TIMES: BITS (Apr. 9, 2014, 2:26 PM), http://bits.blogs.nytimes.com/2014/04/09/qa-on-heartbleed-a-flaw-missed-by-the-masses/?_r=0.

[93] Ben Grubb, *Man who introduced serious 'Heartbleed' security flaw denies he inserted it deliberately*, SYDNEY MORNING HERALD (Apr. 11, 2014), http://www.smh.com.au/it-pro/security-it/man-who-introduced-serious-heartbleed-security-flaw-denies-he-inserted-it-deliberately-20140410-zqtal.html (quoting Robin Seggelmann, author of the code containing the Heartbleed bug).

into the released version."[94] The developer who wrote the buggy code said the error was "quite trivial," but the impact was "severe."[95] Indeed, the impact was so severe that the U.S. Department of Homeland Security issued a public security alert about Heartbleed,[96] and a group of leading technology companies immediately created an initiative to jointly fund the development of open-source software that, like Open SSL, is a critical part of the Internet's security infrastructure.[97] This initiative was immediately put to work when the even more damaging Shellshock bug—lurking for twenty-two years—was discovered in September 2014 in Bash software, another open-source project that forms a key part of the Internet infrastructure.[98]

Unsurprisingly, the Bitcoin code is known to have errors that cause glitches in its operations.[99] The Bitcoin software development website

---

[94] *Id.*

[95] *Id.*

[96] *See, e.g.*, Larry Zelvin, Dir. of the Nat'l Cybersec. & Communic'ns Integration Ctr., *Reaction on "Heartbleed": Working Together to Mitigate Cybersecurity Vulnerabilities*, DEP'T HOMELAND SEC. BLOG (Apr. 11, 2014, 7:52 AM), http://www.dhs.gov/blog/2014/04/11/reaction-%E2%80%9Cheartbleed%E2%80%9D-working-together-mitigate-cybersecurity-vulnerabilities-0 (providing information on Heartbleed, the government's response, and steps for the public to take to protect itself).

[97] *The Linux Foundation's Core Infrastructure Initiative Announces New Backers, First Projects to Receive Support and Advisory Board Members*, LINUX FOUND. (May 29, 2014, 4:56 AM), http://www.linuxfoundation.org/news-media/announcements/2014/05/core-infrastructure-initiative-announces-new-backers (describing the private initiative, funded by large companies including Facebook, Google, HP and others, to fund development of open-source software that "support[s] critical infrastructure"); *see also* Nicole Perlroth, *A Contradiction at the Heart of the Web*, N.Y. TIMES, Apr. 19, 2014, at B1 (discussing how the underfunding of Open SSL software development contributed to developers creating and failing to identify the Heartbleed bug).

[98] *See* Perlroth, *supra* note 97, at B1 (reporting on Shellshock, a "particularly alarming software bug that could be used to take control of hundreds of millions of machines around the world, potentially including Macintosh computers and smartphones that use the Android operating system" that was discovered in Bash, "a free piece of [open-source] software that is now built into more than 70 percent of the machines that connect to the Internet").

[99] *See Issues List*, GITHUB, https://github.com/bitcoin/bitcoin/labels/Bug, (last visited Oct. 22, 2015) (showing that in the Bitcoin software development repository there are 79 unresolved bugs while 427 reported bugs have been resolved); *see also* Rainer Böhme et al., *Bitcoin: Economics, Technology, and Governance*, 29 J. ECON PERS. 213, 228 (2015), http://ssrn.com/abstract=2495572 ("[T]he Bitcoin platform faces operational risks through potential vulnerabilities in the protocol design . . . ."); Vasilis Kostakis & Chris Giotitsas, *The (A)Political Economy of Bitcoin*, TRIPLEC: COMM., CAPITALISM & CRITIQUE (2014), http://www.triple-c.at/index.php/tripleC/article/view/606/578 (noting that "[b]eing still in development it is yet unknown how many bugs are hidden in the [Bitcoin] code").

includes a list of bugs that have already been identified and need fixes,[100] and there are instructions for software developers to send encrypted descriptions of critical bugs they discover to the Bitcoin core developers.[101] As the list of known bugs implies, the core software is always being rewritten to resolve these issues. Further, a 2014 study performed by a Bitcoin advocacy organization entitled *Removing Impediments to Bitcoin's Success: A Risk Management Study* (the "Risk Management Study") identified the existence of a significant bug in either the Bitcoin protocol or code as a "low-likelihood, high consequence threat" to Bitcoin (although it concluded that continued operation of the code is the most appropriate way to discover and remedy any existing bugs).[102] Finally, even the primary core developer for Bitcoin has acknowledged his fears of an undiscovered catastrophic bug lurking in the code.[103]

Why this is a problem for Bitcoin as financial market infrastructure

Technology risk is not new to our financial market infrastructures, as they already rely on software to operate in most cases. So, Bitcoin may be no riskier than other financial market infrastructures in this regard. A valuable avenue for further research would be some specific empirical comparisons between the software for particular financial market infrastructures and Bitcoin.

It is important not to assume that just because Bitcoin is newer, it is necessarily less buggy. It is even more important to consider how Bitcoin's governance structures, or lack thereof, help to magnify its technology risks,

---

[100] *Issues List*, *supra* note 99.

[101] The instructions provide:

> If you find a vulnerability related to Bitcoin, non-critical vulnerabilities can be emailed in English to any of the core developers or sent to the private bitcoin-security mailing list listed above. An example of a non-critical vulnerability would be an expensive-to-carry-out denial of service attack. Critical vulnerabilities that are too sensitive for unencrypted email should be sent to one or more of the core developers, encrypted with their PGP key(s).

Contribute Bug Reports, BITCOIN.ORG, https://bitcoin.org/en/bitcoin-core/contribute/issues (last visited Oct. 6, 2015).

[102] THE BITCOIN FOUND., REMOVING IMPEDIMENTS TO BITCOIN'S SUCCESS: A RISK MANAGEMENT STUDY 20–21 (2014), https://bitcoinfoundation.org/wp-content/uploads/2014/07/Bitcoin-Risk-Management-Study-Spring-2014.pdf [hereinafter RISK MANAGEMENT STUDY].

[103] *See* Simonite, *supra* note 37.

as I discuss in Parts III.B and III.C below

2. Software is vulnerable to attack

As we all know, hacking is already an omnipresent threat to modern software and is only increasing. There are daily reports of significant and damaging security breaches and data thefts that result from computer hackers exploiting errors in software.[104] Although there are ongoing efforts to resist hacking, it is a rare person who will argue that any software is completely invulnerable to hacking. As the Financial Security Oversight Council noted in its 2015 Annual Report, "recent cyber attacks have heightened concerns about the potential of an even more destructive incident that could significantly disrupt the workings of the financial system."[105]

Thus, the security of the Bitcoin software and network are of fundamental importance in evaluating the Bitcoin blockchain as potential financial market infrastructure. It is important here to distinguish between (a) vulnerabilities of the Bitcoin software and network and (b) vulnerabilities of companies that service those who participate in the Bitcoin network. The Bitcoin ecosystem now contains numerous intermediaries, such as exchanges, wallet companies, and payment processors, which hold bitcoins as part of their business models.[106] Many of these intermediaries have been hacked in attempts to steal the bitcoins they hold.[107] Importantly, though, attacks on intermediaries in the Bitcoin

[104] *See, e.g.*, Brian X. Chen, *Apple Says It Will Add New iCloud Security Measures After Celebrity Hack*, N.Y. TIMES: BITS (Sept. 4, 2014, 11:32 PM), http://bits.blogs.nytimes.com/2014/09/04/apple-says-it-will-add-new-security-measures-after-celebrity-hack/ ("Apple said on Thursday that it would strengthen its security measures after a recent episode where hackers broke into the Apple accounts of a number of celebrities, stole their nude photos and leaked them on the Internet."); David E. Sanger & Nicole Perlroth, *Bank Hackers Steal Millions via Malware*, N. Y. TIMES, Feb. 15, 2015, at A1 (reporting the Feb. 2015 discovery that "more than 100 banks and other financial institutions in 30 nations" were robbed by a team of hackers in what may be "one of the largest bank thefts ever"); Robin Sidel, *Home Depot's 56 Million Card Breach Bigger than Target's*, WALL STREET J. (Sept. 18, 2014, 5:43 PM), http://www.wsj.com/articles/home-depot-breach-bigger-than-targets-1411073571 (describing the security breaches at Home Depot, Target, and other merchants).

[105] FIN. STABILITY OVERSIGHT COUNCIL, *supra* note 61, at 3.

[106] Examples of Bitcoin exchanges include Coinbase, BitStamp, ItBit, and OKCoin. Examples of Bitcoin wallet companies include Circle, Armory, DarkWallet, and Blockchain. Examples of Bitcoin payment processors include BitPay and Coin.co.

[107] *See, e.g.*, Richard Boase, *Hackers steal $1.2 Million of bitcoins from Inputs.io, a*

ecosystem are not attacks on the Bitcoin software and network itself. While an attack on an intermediary (such as an individual exchange) only affects the particular bitcoins being handled or held by that exchange,[108] an attack on the Bitcoin software or network could have the much more severe consequence of simultaneously halting the exchange of *all* bitcoins. Attacks on the Bitcoin software or network are therefore a systemic operational risk to the Bitcoin blockchain as financial market infrastructure.

Bitcoin proponents argue that the Bitcoin software and network have extremely strong security features that make it difficult if not impossible for Bitcoin to be attacked.[109] For instance, the decentralized structure of the network makes it impossible to ensure that all nodes within the Bitcoin network could necessarily be reached simultaneously in an attack (unless, of course, one of the core developers were forced by an attacker to send an emergency message to all nodes that allowed a network-wide attack through the adoption of malicious code).[110] Further, proponents explain that it is extremely difficult if not impossible to tamper with the blockchain and that older parts of the blockchain (those reflecting Bitcoin transactions that occurred in the past) become more and more immutable and robust over time.[111]

---

supposedly secure wallet service, COINDESK, (Nov. 7, 2013), http://www.coindesk.com/hackers-steal-bitcoins-inputs-io-wallet-service/ (reporting on theft of bitcoins from wallet service); Stan Higgins, *BTER Claims $1.75 Million in Bitcoin Stolen in Cold Wallet Hack*, COINDESK, (Feb. 15, 2015), http://www.coindesk.com/bter-bitcoin-stolen-cold-wallet-hack/ (reporting on alleged hack of China Bitcoin exchange BTER, with $1.75 million in bitcoins stolen); Ahmed Murad, *Hackers breach bitcoin exchange; Customers advised not to make deposits at virtual currency's leading European bourse*, FIN. TIMES, Jan. 7, 2015, at 13 (reporting on hack of U.K. Bitcoin exchange BitStamp, with theft of 19,000 bitcoins worth about $5 million).

[108] Of course, an attack on a major exchange or other significant actor in the Bitcoin ecosystem could affect the value of all bitcoins by causing the public to lose faith in Bitcoin, as was the case when Mt. Gox reported losing $450 million worth of bitcoins during its collapse in February 2014. *See* Murad, *supra* note 102. A leading Bitcoin price index showed that the price of a bitcoin fell from around $800 on Feb. 6, 2014 to around $700 on Feb. 7, 2014 as Mt. Gox paused withdrawals prior to its collapse. *See Bitcoin Price Index Chart*, COINDESK, http://www.coindesk.com/price/ (last visited Oct. 25, 2015).

[109] *See, e.g.*, ANTONOPOULOS, *supra* note 23, at 211, 213; CAMPBELL R. HARVEY, BITCOIN MYTHS AND FACTS 5 (2014), http://ssrn.com/abstract=2479670 ("Bitcoin is probably the most secure form of transaction in the history of the world. . . . [T]o break into the blockchain, you would need an enormous amount of computing power.").

[110] *See* ANTONOPOULOS, *supra* note 23, at 157, 211.

[111] *See Id.* at 211; HARVEY, *supra* note 109, at 5. *But see* Simon Barber et al., *Bitter to Better: How to Make Bitcoin a Better Currency*, *in* 7397 FINANCIAL CRYPTOGRAPHY (FC 2012), LECTURE NOTES IN COMPUTER SCIENCE 399, 404–06 (2012), https://crypto.stanford.edu/~xb/fc12/bitcoin.pdf. In this computer science paper. The authors describe the increasing and "very real" risk of a "history-revision" attack that could rewrite the Bitcoin blockchain, replacing real transactions with made-up ones. The authors

Yet, there are widely acknowledged vulnerabilities to which Bitcoin is susceptible that malicious actors could exploit to disrupt Bitcoin's operation. The most prominent threat is known as the "51% Attack."[112] This type of attack would come from parties who control at least 51% of the computing power[113] that the Bitcoin system uses to validate transactions and create the blockchain (or transaction ledger).[114] Although this type of attack was largely theoretical in the early days of Bitcoin because the miners who validated Bitcoin transactions were mostly individuals, it is possible today given the growth of large "mining pools" that control significant portions of the Bitcoin computing power (and hence, have enough "votes" to control which transactions are validated and what shows up on the blockchain).[115]

The effects of such an attack could be to revise recently settled transactions on the blockchain and to prevent current and future transactions from being completed.[116] Given that Bitcoin's primary benefit is the reliability of the blockchain, any ability to tamper with it or to manipulate its creation is highly damaging to the reliability of the system, and thereby to its credibility as financial market infrastructure. The attacker could also "double-spend" its own previously spent bitcoins—in effect, committing theft.[117]

While theft could be one motivation for orchestrating such an attack,

---

propose solving this problem by automating the creation of authoritative copies of the blockchain, creating "checkpoints." *Id.* The authors note that the Bitcoin core developers already do create "checkpoints" of the blockchain that they push out with new software releases, but argue that putting the creation of checkpoints in the hands of the developers makes them unreliable. *Id.*

[112] *See, e.g.*, ANTONOPOULOS, *supra* note 23, at 211; JOSHUA A. KROLL ET AL., THE ECONOMICS OF BITCOIN MINING, OR BITCOIN IN THE PRESENCE OF ADVERSARIES 11–12 (2013), http://www.econinfosec.org/archive/weis2013/papers/KrollDaveyFeltenWEIS2013.pdf; Barber, *supra* note 111.

[113] Such an attack on the blockchain could succeed even with less than a 51% share of the computing power, with claims that as little as 30% of the computing power could succeed in this type of attack. *See* ANTONOPOULOS, *supra* note 23, at 212; ITTAY EYAL & EMIN GUN SIRER, MAJORITY IS NOT ENOUGH: BITCOIN MINING IS VULNERABLE (2013), http://arxiv.org/pdf/1311.0243.pdf (demonstrating in a controversial computer science paper that "selfish miners" of any portion of ownership could collude to control the Bitcoin network).

[114] *See* ANTONOPOULOS, *supra* note 23, at 211–12.

[115] *Id.*

[116] *Id.*

[117] *Id.*

another motivation could simply be to bring down Bitcoin, particularly if it becomes more widely used.[118] To obtain the requisite computing power would require "enormous investment," but such an attack "could conceivably be launched by a well-funded, most likely state-sponsored, attacker."[119]

Bitcoin proponents have argued that a 51% attack is highly unlikely for several reasons. First, the attack would be extremely expensive to conduct because obtaining the needed computing power would cost so much.[120] Second, after spending all the money to accumulate all the computing power, it would be against the attacker's financial interest to destroy the system in which it had invested so much.[121] And third, the 51% threshold has already been hit by certain mining pools, and they have not yet performed such an attack.[122]

Unfortunately, none of these reasons provide comfort that a 51% attack is impossible. Certain individuals and industries with great wealth could decide that it was in their interest to invest enough to destroy the credibility of Bitcoin. For instance, there has been much public discussion about how Bitcoin and other virtual currencies threaten the current model of financial services,[123] a trillion dollar industry.[124] States could also decide that it was

---

[118] *Id.* at 212–13.

[119] *Id.* at 213.

[120] *Id.*; HARVEY, *supra* note 109, at 5–6.

[121] *See* KROLL, *supra* note 112, at 12–13 ("[A] 51% . . . attack [by a mining cartel] is unlikely to generate enough reward within the Bitcoin economy to be worthwhile to the attacker."); *see also* Daniel Cawrey, *Are 51% Attacks a Real Threat to Bitcoin?*, COINDESK (June 20, 2014), http://www.coindesk.com/51-attacks-real-threat-bitcoin/ (stating that miners, "whose profits depend largely on the price of bitcoin being high . . . [have] no real incentive to attack the network").

[122] *See* Jon Matonis, Exec. Dir. of the Bitcoin Found., *The Bitcoin Mining Arms Race: GHash.io and the 51% Issue*, COINDESK (July 17, 2014), http://www.coindesk.com/bitcoin-mining-detente-ghash-io-51-issue/ (arguing that tensions have eased about the threat of a mining pool executing a 51% attack after a July 9, 2014 meeting of miners in London resulted in the GHash.io mining pool pledging to "do all it can to limit its share of the total bitcoin network to 39.99%").

[123] *See* Aaron Timms, *Big Banks are Confident in the Face of the Bitcoin Threat*, INSTITUTIONAL INV. (Oct. 10, 2014), http://www.institutionalinvestor.com/inside-edge/3389462/Big-Banks-Are-Confident-in-the-Face-of-the-Bitcoin-Threat.html#.VQSCj47F8nU (discussing banking industry's response to claims that Bitcoin could "unbundle the banks" and "reimplement the entire financial system as a distributed system as opposed to a centralized system"). This threat may have changed now that the financial industry seems to be embracing blockchain technology as a whole, so may no longer have an incentive to destroy Bitcoin. However, destroying Bitcoin could demonstrate that the permissioned blockchains being developed by the financial industry

in their best interest to destroy Bitcoin and be willing to devote enough resources to complete such an attack.[125] If Bitcoin became more widely-used, or if its blockchain began to serve as the backbone of significant financial infrastructures, there would be plenty of states (e.g., North Korea) or terrorist actors (e.g., ISIS) who would have both the incentives and resources to attempt this type of attack. Moreover, the fact that those parties who have held the relevant threshold of computing power have not used it to harm Bitcoin in the past, does not mean that will always be the case. Finally, the more widely known and used Bitcoin becomes and the greater a role it plays as financial market infrastructure, the more attractive a target it becomes for those with an interest in destroying it.

While the 51% attack is the most widely acknowledged threat to Bitcoin's operation, distributed denial of service (DDOS) attacks could also disrupt the operation of the Bitcoin network, and therefore its blockchain. For example, in early March 2015, there was a wave of DDOS attacks against at least five Bitcoin mining pools, including one of the larger pools, GHash.Io.[126] With GHash.Io, the attack resulted in the pool being unable to mine bitcoins for hours at a time.[127] DDOS attacks against miners in the Bitcoin network have been a recurrent problem since 2011.[128] Given that

---

are superior to Bitcoin and allow the financial industry to maintain control over financial market infrastructures.

[124] *See The Financial Services Industry in the United States*, U.S. DEPT. OF COMMERCE, http://selectusa.commerce.gov/industry-snapshots/financial-services-industry-united-states (last visited Mar. 8, 2015) ("In 2012, finance and insurance represented 7.9 percent (or $1.24 trillion) of U.S. gross domestic product.").

[125] *See* KROLL, *supra* note 112, at 13 (arguing that "governments are the most plausible source" of a 51% attack on Bitcoin from outside the Bitcoin network).

[126] *See* Stan Higgins, *Bitcoin Mining Pools Targeted In Wave Of DDOS Attacks*, COINDESK (Mar. 12, 2015), http://www.coindesk.com/bitcoin-mining-pools-ddos-attacks/ (reporting that mining pools AntPool, BW.com, NiceHash, CKPool and GHash.io were hit by DDOS attacks, with hackers demanding ransoms to end the attack).

[127] *See* Julia McGovern, *Official Statement on the Last Week's DDoS-attack against GHash.IO Mining Pool*, CEX.IO BLOG (Mar. 13, 2015), http://blog.cex.io/news/official-statement-on-the-ddos-attack-against-ghash-io-mining-pool-13355 (reporting on the GHash.IO mining pool on a DDoS attack it suffered the week of Mar. 7, 2015 that prevented miners from mining for 6 hours, with the hacker demanding five to ten bitcoins to end the attack).

[128] *See* Benjamin Johnson et al., *Game-Theoretic Analysis of DDoS Attacks Against Bitcoin Mining Pools*, 8438 FIN. CRYPTOGRAPHY & DATA SECURITY 72, 73 (2014) (evaluating the incentives miners have to inflict DDOS attacks on one another); Marie Vasek et al., *Empirical Analysis of Denial-of-Service Attacks in the Bitcoin Ecosystem*, 8438 FIN. CRYPTOGRAPHY & DATA SECURITY 57, 68 (2014) (estimating 142 DDOS attacks on the Bitcoin ecosystem between May 2011 and Oct. 2013, with thirty-eight percent of those attacks on mining pools, and noting that "over 60% of large mining pools have been

the mining process is actually the process that verifies bitcoin transactions and makes additions to the shared ledger, a simultaneous attack against many or all miners could compromise the Bitcoin network. As the Bitcoin mining industry continues to consolidate,[129] this threat becomes greater, as there are fewer targets that hackers must hit to achieve a network-wide outage.

Additional vulnerabilities of the Bitcoin software and protocol could emerge through improvements in mathematical cryptanalysis or through quantum computing.[130] This means that the cryptography that underlies Bitcoin could become less impenetrable (and thus more vulnerable) due to advances in our knowledge of mathematics, or that the computers that work to solve the algorithms in Bitcoin could become so much more powerful that the algorithms can be too easily solved.

There is also the problem identified by Donald Rumsfeld in regards to weapons of mass destruction in Iraq that applies to all forms of risk assessment:

> [A]s we know, there are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns—the ones we don't know we don't know. And if one looks throughout the history of our country and other free countries, it is the latter category that tend to be the difficult ones.[131]

There is simply no way to identify Bitcoin's "unknown unknowns"—the flaws that parties might be able to exploit (to their benefit and/or Bitcoin's detriment) in the future. The devastating Heartbleed bug, hidden in plain sight in the OpenSSL code, is a reminder of how software vulnerabilities can lurk undetected, a risk of which Bitcoin's own core developers are well

---

DDoSed, compared to just 17% of small ones").

[129] *See* Nermin Hajdarbegovic, *Acquisitions and Partnerships Fuel Bitcoin Mining Sector Expansion*, COINDESK (Aug. 25, 2014), http://www.coindesk.com/acquisitions-partnerships-fuel-bitcoin-mining-sector-expansion/ (reporting on recent, rapid consolidation in the Bitcoin mining industry).

[130] Email from Shawn Bayern, Larry and Joyce Beltz Professor of Torts at Fla. State Univ. Coll. of Law, to author (Jan. 20, 2015, 11:33pm) (on file with author). *See also* Böhme et al., *supra* note 99, at 228 ("[T]he Bitcoin platform faces systemic operational risks through . . . breakthroughs in cryptanalysis.").

[131] Donald H. Rumsfeld, Secretary of Defense, Department of Defense News Briefing (Feb. 12, 2002), http://archive.defense.gov/Transcripts/Transcript.aspx?TranscriptID=2636 (transcript).

aware.[132]

Why this is a problem for Bitcoin as financial market infrastructure

Clearly, Bitcoin shares its vulnerability to hacking with existing digital financial market infrastructure, so perhaps does not pose a *greater* technology failure risk than they do, and may even be more resilient. However, though many have suggested it is highly resistant to hacking, it is important to remember that it is not *invulnerable*.

Bitcoin's susceptibility to a 51% attack creates a new type of technology risk, however, which appears difficult to overcome with its existing design. As noted above, if the Bitcoin blockchain were to become more widely used, perhaps as the architecture of a large payment system, it would be an extremely tempting target for an attack by a terrorist group, as its failure would be a devastating event to all who rely on that infrastructure. Indeed, the recent cyberattack on Sony Corporation—possibly by North Korea[133]—should give us pause in creating such a high-consequence target that determined attackers could bring down. While it is true that the Bitcoin system is small now, if more of our financial systems begin to rely on it, this risk will become more significant.

3. Software is ever-changing through new releases

Software is always on the move. Rather than being a static creation, during the period that software remains in use, it is generally changing as different versions or "releases" of the software are issued by software developers. New versions of software are created to fix bugs or to introduce new features and may be incompatible with earlier versions of the software. For example, the release notes for the tenth version of the Bitcoin software, released by the core developers in February 2015, state that it is incompatible with prior versions of the software.[134]

---

[132] *See* Simonite, *supra* note 37.

[133] *See* David E. Sanger & Martin Fackler, *Tracking the Cyberattack on Sony to North Koreans*, N.Y. TIMES (Jan. 19, 2015), http://www.nytimes.com/2015/01/19/world/asia/nsa-tapped-into-north-korean-networks-before-sony-attack-officials-say.html (reporting on President Obama's statement that North Korea was responsible for the November through December 2014 cyberattack on Sony Pictures and that the United States would retaliate).

[134] *See* Wong, *supra* note 35; *Upgrading and Downgrading: Downgrading Warning*, GITHUB, https://github.com/bitcoin/bitcoin/blob/0.10/doc/release-notes.md (last visited Mar. 13, 2015) (stating that "the block files and databases are not backwards-compatible

New versions of the Bitcoin code have already caused serious problems for the Bitcoin network. There has been uneven updating to newer versions of software by the computers that operate the Bitcoin network (the "nodes" and "miners"), and this has resulted in potentially catastrophic consequences.

For instance, in March 2013, Bitcoin experienced a "hard fork" in the software, meaning that two separate blockchains (or transaction histories) were being simultaneously developed by computers within the Bitcoin network.[135] The fork was "due to nodes using two different versions of the bitcoin protocol"[136] and meant that there were effectively two ledgers being kept for Bitcoin transactions. This throws the entire system into chaos because Bitcoin's core principle is that the common ledger is reliable and true. Although the network recovered from this fork due to the collaboration of the core software developers and certain mining pools (as discussed in Part III.B), this demonstrates the system-wide risks posed by uneven updating of new releases of software.

Perhaps even more significant is the epic struggle between versions of the Bitcoin core software that is ongoing as of this writing. Referred to as the "block size debate," this dispute amongst the Bitcoin core (and other) developers deals with how much memory files within the blockchain should consume.[137] Viewed as a matter that must be addressed in order for Bitcoin to operate smoothly on a larger scale (i.e., to accommodate more changes to the blockchain as would need to be the case if other financial market infrastructures utilized it), the matter has come to a head, with various versions of the Bitcoin code proposed by different factions of developers.[138] With Bitcoin, adopting a new software release also means agreeing to the policy choices embedded in the code, and this dispute threatens to split the network—which could ultimately lead to separate "forked" blockchains.[139]

---

with pre-0.10 versions of Bitcoin Core or other software").

[135] *See 11/12 March 2013 Chain Fork Information*, BITCOIN.ORG (Mar. 11, 2013) http://bitcoin.org/en/alert/2013-03-11-chain-fork.

[136] FRANÇOIS R. VELDE, FED. RES. BANK CHI., BITCOIN: A PRIMER 3 (2013), https://www.chicagofed.org/publications/chicago-fed-letter/2013/december-317.

[137] *See* Grace Caffyn, *What is the Bitcoin Block Size Debate and Why Does It Matter?*, CoinDesk (Aug. 21, 2015), http://www.coindesk.com/what-is-the-bitcoin-block-size-debate-and-why-does-it-matter/.

[138] *See id.*

[139] *See* Arvind Narayan & Andrew Miller, *Bitcoin faces a crossroads, needs an effective decision-making process*, FREEDOM TO TINKER (May 11, 2015), https://freedom-to-tinker.com/blog/randomwalker/bitcoin-faces-a-crossroads-needs-an-effective-decision-

As will be discussed in Parts III.B and III.C, new releases cannot be forced on anyone in the network, and require adoption by a majority of the computing power in the network to take effect.[140]

Why this is a problem for Bitcoin as financial market infrastructure

The evolving nature of software through new releases may be a bigger problem for decentralized Bitcoin than it is for more centralized financial market infrastructures. Since controversial new releases of Bitcoin software may be unevenly adopted, there would seem to be potential for periodic forks in the network when consensus cannot be found amidst the parties in the network. This undermines the reliability of the Bitcoin blockchain, as has already been demonstrated in the March 2013 fork.

In a centralized financial market infrastructure, however, or even in "permissioned blockchains," new releases of software can likely be implemented more easily, since adopting the new version can be mandated on participants, perhaps through the contract that allows participation in the permissioned blockchain.

4. Few people understand how software works

The final operational risk associated with Bitcoin's status as software that I will discuss is the fact that, as with all software, only a small percentage of the population understands how software works. Software coders have a particular expertise that makes the quality of their code, and even the basic functions it performs, opaque to people who are not experts in the relevant software language. The recent admission by Volkswagen that its software made the emissions of its vehicles appear lower than they actually were demonstrates clearly the power of software coders and the inability of non-coders to perceive problems or even illegal actions enabled by the code.[141] Software coding is truly an area in which knowledge (of code) is power.

---

making-process/ (noting that the proposed versions of the Bitcoin software to address the block size problem reflect policy choices and affect different Bitcoin users differently).

[140] *See id.*

[141] *See* Jim Dwyer, *Volkswagen's Diesel Fraud Makes Critic of Secret Code a Prophet*, N.Y. TIMES (Sept. 22, 2015), http://www.nytimes.com/2015/09/23/nyregion/volkswagens-diesel-fraud-makes-critic-of-secret-code-a-prophet.html?_r=0 (describing the dangers of secret software code and arguing that it should be inspected).

a. Why this is a problem for Bitcoin as financial-market infrastructure

It is true that most people do not understand how existing financial market infrastructures work, any more than they understand how software works. Perhaps we already have an overly complex system that either no one or only a very select group of experts understands, and there is no way that virtual currencies make an already bad situation worse.

Yet, for the moment at least, virtual currency's complexity and the software and network knowledge required to truly understand it means that there is an even more limited number of people who understand it (assuming that anyone actually does).[142] This is because having a sophisticated understanding of Bitcoin or other virtual currencies requires extensive knowledge in multiple fields, likely including software coding, networks, cybersecurity, economics, payment systems, money, financial and economic history, finance, and surely many more. This is not to say that there aren't some amazing people who have mastered this array of fields, but that it is surely a very select group.

The fact that only a very limited portion of the population truly understands how Bitcoin operates gives rise to systemic operational risks. This is because it requires the population to put extreme amounts of trust in the skill and integrity of the people making decisions about the Bitcoin code and network. The larger the system becomes, with more "blockchain" companies using the Bitcoin network to accomplish their tasks,[143] the more pressure that is put on this small group of experts to make desirable policy choices[144] that they implement accurately and safely into the code. We should proceed with caution in building complex, opaque systems that carry out tasks of significant systemic importance.[145]

---

[142] *Cf.* LO & WANG, *supra* note 58, at 7 (noting that "anecdotally, the typical [Bitcoin] user tends to be well versed in internet applications and even programming"); 2012 ECB PAPER, *supra* note 38, at 27 (noting the complexity of Bitcoin and the "high-risk situation" created by the fact that users of it may not understand how it works).

[143] *See* Shin, *supra* note 52.

[144] Of course, the desirability of a particular policy choice for Bitcoin (Should there be transaction fees? Should the limit on total bitcoins be increased? What should the block size be?) will vary depending on which constituency is being asked.

[145] The open source nature of the Bitcoin code does mitigate this risk as it allows other coders to evaluate the code. This contrasts with the proprietary nature of the Volkswagen code, which was unavailable to regulators or the public for scrutiny. *See* Dwyer, *supra* note 141. However, there is still a barrier between the expertise of the coders and the expertise

Something so difficult for non-experts to understand is difficult for regulators to address, as the world learned to its chagrin with the opaque credit-default swaps, shadow banking practices, and mortgage-backed securities that led us into the 2008 Financial Crisis.[146] Letting subject matter experts (in the case of finance, the "quants,"[147] and in the case of Bitcoin, the software developers) tell regulators—"trust us, it works"—is highly problematic from a risk-management perspective, particularly when we are talking about potential financial market infrastructure, and when more and more influential people and businesses are pushing virtual currencies forward and proclaiming them likely to be as transformative as the Internet.[148]

* * *

As demonstrated in this Part, the inescapable involvement of software in the ongoing operation and maintenance of the Bitcoin blockchain creates significant operational risks that must be considered if Bitcoin functions as financial market infrastructure.

B. Bitcoin's Decentralized Structure

Bitcoin is described almost universally as a "decentralized peer-to-peer" currency. This means that Bitcoin does not operate from a single server or central computer, but instead, "means, practically speaking, that

---

of financiers and regulators—bridging the knowledge and communications gap between these groups is difficult and can lead to unexpected risks.

[146] For a treatment of how the reliance on complicated financial structures and algorithms helped to create the 2008 Financial Crisis, see SCOTT PATTERSON, THE QUANTS: HOW A NEW BREED OF MATH WHIZZES CONQUERED WALL STREET AND NEARLY DESTROYED IT (2010).

[147] *Id*.

[148] *See, e.g.*, Andreessen, *supra* note 65 ((comparing Bitcoin to the Internet in terms of its revolutionary potential); Tom Braithwaite & Ben McLannahan, *Master Joins Cryptocurrency Start-Up*, FIN. TIMES (Mar. 10, 2015), http://www.ft.com/cms/s/0/e29808a8-c744-11e4-9e34-00144feab7de.html#axzz3nQl8hY6t (reporting that Blythe Masters, who formerly was "instrumental in developing the credit default swaps market [at J.P. Morgan]" in the 1990's has become CEO of Digital Asset Holdings, a trading platform for "big banks and asset managers" built on the Bitcoin blockchain); Kristin Broughton, *Former SEC Chairman Levitt to Advise Bitcoin Firms*, 179 AMER. BANKER 167 (Oct. 29, 2014) (reporting that former SEC Chairman Arthur Levitt is advising Bitcoin companies BitPay and Vaurum); Matthew Heller, *Veteran Bank Exec Joins Bitcoin Startup as CFO*, CFO.COM, http://ww2.cfo.com/people/2014/12/veteran-bank-exec-joins-bitcoin-startup-cfo/ (Dec. 12, 2014) (reporting that Paul Camp, "former head of JP Morgan Chase's global transaction services business, has become the latest executive to migrate from traditional banking and finance to the digital currency industry, joining startup Circle Internet Financial as CFO").

the entire system is made up of versions of the software that end-users download and run on their personal computers."[149] This structure echoes other well-known peer-to-peer software programs such as BitTorrent or Grokster. Indeed Bitcoin's decentralization is described by the Bitcoin Foundation as "[a] key characteristic of Bitcoin and a source of its strength."[150]

Bitcoin's decentralized structure means that "there is a meaningful sense in which nobody is in charge of Bitcoin."[151] Bitcoin does not have an official organization or party that operates it. Instead, there is a sort of "unofficial" group of core software developers who maintain the code, including implementing fixes to flaws and introducing new features.[152] However, there is no single legal entity for which this group of software developers works in performing their maintenance of the Bitcoin software code, and these developers have no official responsibility to Bitcoin to perform their work to a certain standard or even to continue their work at all.

This setup creates a systemic operational risk for Bitcoin, as Bitcoin's ongoing operation is threatened by the fact that:

i) there is no entity or person that assumes responsibility for the performance of Bitcoin;

[149] Bayern, *supra* note 33, at 1488.

[150] RISK MANAGEMENT STUDY, *supra* note 102, at 2.

[151] Bayern, *supra* note 33, at 1489. *But see* GERVAIS, *supra* note 36, at 54 (concluding that due to centralized mining and software development, "Bitcoin isn't a truly decentralized system as it is deployed and implemented today"); KROLL, *supra* note 112, at 18 (noting that "[T]he lead developers of the open source [Bitcoin] software have become a de facto rules governance body for the Bitcoin economy"); BEN LAURIE, DECENTRALISED CURRENCIES ARE PROBABLY IMPOSSIBLE (BUT LET'S AT LEAST MAKE THEM EFFICIENT) 4 (2011), http://www.links.org/files/decentralised-currencies.pdf ("If Bitcoin is, indeed, using a known consensus group, then it has, after all, a central authority (that consensus group), and is not, therefore, a decentralised currency."); Grinberg, *supra* note 39, at 175 n.71 ("This development team constitutes the de facto central bank of Bitcoin.").

[152] Bayern, *supra* note 33, at 1491 (noting that "Bitcoin does not operate in as rigorously decentralized a manner as Nakamoto originally designed it" and that "the developers of the Bitcoin client have the ongoing capacity to change the Bitcoin protocol in minor but incompatible ways, actively managing the community of Bitcoin users to make sure that the Bitcoin network upgrades in ways they have determined.") (citations omitted). *See also* Danny Bradbury, *Why Bitcoin's Core Developers Want Multiple Versions*, COINDESK (Oct. 19, 2014), http://www.coindesk.com/bitcoins-core-developers-want-multiple-versions/ (describing the exclusive powers that the core developers have to make changes to the Bitcoin code).

ii) no one is in charge;

iii) it is impossible to tell who the voice of the group is; and

iv) there is no defined group that comprises Bitcoin or its management– just an amorphous, ever-shifting cluster of people who come and go within the group as they please.

Because of this decentralized structure, there is *no one* who is responsible for keeping the Bitcoin software operational. This means that even if there is a crucial repair that is needed to prevent complete collapse of the software, no one in particular would be *required* to perform the repair. Since no one is "responsible" for the code, even those core developers who have been voluntarily working to maintain Bitcoin may decide not to help in a moment of crisis, perhaps deeming their continued involvement to be personally risky.[153] It is true that in prior moments of crisis, such as the March 2013 blockchain fork discussed below, the Bitcoin core developers worked to resolve the crisis,[154] but that does not prove that they may necessarily be relied upon to do so in the future.

In addition, decision-making may be slower than it needs to be to resolve an operational crisis, due to the fact that no one is in charge of Bitcoin. As there is no defined power or accountability structure, no one has to listen to anyone else's ideas about how to resolve a crisis. There are no definitively appointed decision-makers. This is different than having no one at all responsible for keeping the software operational; this risk is that even if people decide to take on responsibility for resolving a problem with the Bitcoin software or protocol, their authority to do so, and their resulting ability to implement their solution, is in question. This means that anyone with a suggested resolution to a crisis may merely propose a solution, but it may take too long to achieve buy-in from other members of the Bitcoin community to successfully implement the solution in an emergency situation. We see this type of argument commonly made in debates over the limits of the executive power of the President of the United States, who may need to act quickly in a crisis without waiting for specific authority from Congress.[155]

---

[153] Of course, analogous to employees and their stock options, coders who own substantial numbers of bitcoins have a financial incentive to keep the code operational in order to preserve their own wealth. Whether this is a sufficient incentive is an open question. I am grateful to Andrew Stephens for this insight.

[154] *See infra* notes 161-164 and accompanying text.

[155] *See generally* ERIC POSNER & ADRIAN VERMEULE, THE EXECUTIVE UNBOUND: AFTER THE MADISONIAN REPUBLIC (2011) (arguing a strong presidency is necessary in the

The inability to obtain buy-in to a change in the Bitcoin protocol or software may also be a problem in non-crisis situations, when the core developers feel that a certain change to the Bitcoin protocol or software is in society's best interest (e.g., if they decided that the cap on the number of total bitcoins needed to be changed). Because changes to the Bitcoin software are ultimately made through the adoption of the new software by users, some users could hold out, preventing needed changes. This may be a real problem with Bitcoin particularly, as many of its users believe strongly in the decentralization premise, and may be unwilling to agree to fundamental changes to Bitcoin—even if such changes would be beneficial to society. (Interestingly, during the publication cycle of this paper, this situation began to play out in real time through the block size debate described in Part III.A.3 above, which has manifested in a split in the core developers on the trajectory of Bitcoin, unresolved as of this writing).[156]

Decentralization also threatens Bitcoin's continued operation because it means that no one has the authority to speak as "the voice" of Bitcoin.[157] In a decentralized organization, with no rights or rules, there is no way to determine what is in the "best interests" of Bitcoin. Although certain people have assumed the role of "the voice" of Bitcoin already, they have not done so with authority to represent the interests of all owners of bitcoins. For instance, both the core developers of the Bitcoin software and representatives of an organization called "The Bitcoin Foundation"[158] have met with many government regulators to explain and advocate for certain treatments of Bitcoin,[159] but none of these people have any official authority

---

modern world as the executive is often called upon to act quickly in a world of far more complexity than that of the Framers); Saikrishna Bangalore Prakash, *The Imbecilic Executive*, 99 VA. L. REV. 1361 (2013) (arguing that despite arguments to the contrary the Constitution limits the President's ability to act unilaterally even in times of emergency).

[156] *See supra* notes 137-139 and accompanying text.

[157] *See About bitcoin.org: Who owns bitcoin.org?*, *supra* note 23 ("[N]obody can speak with authority in the name of Bitcoin.").

[158] The Bitcoin Foundation was created in July 2012 to advocate for the success of Bitcoin. *See Transparency*, BITCOIN FOUND., https://bitcoinfoundation.org/transparency/. Since then, there has been much debate in the Bitcoin community over the role of the Bitcoin Foundation, and in the fall of 2014, the Foundation limited its mission to supporting the development of the Bitcoin core software. *See Everybody Pivots*, BITCOIN FOUND. (Nov. 19, 2014), https://bitcoinfoundation.org/bitcoin/everybody-pivots/ (describing the evolving goals of The Bitcoin Foundation, from "public policy, education and outreach, [and] core development" originally to its current "focus on funding the ongoing core development" of Bitcoin).

[159] *See* Brian Fung, *Inside the Bitcoin advocates' closed-door meeting with federal regulators*, WASHINGTON POST (Aug. 27, 2013), http://www.washingtonpost.com/blogs/the-switch/wp/2013/08/27/inside-the-bitcoin-

to represent Bitcoin or its community. Yet, these people have in many ways stepped up to become the "voice" of Bitcoin because regulators have sought to be educated about it, and had to talk to *somebody*.[160] Bitcoin's decentralized structure means that there cannot be an official voice of the organization, which is highly problematic in a world that needs to understand Bitcoin in order to evaluate its risks and benefits.

Decentralization also means that the people who comprise the Bitcoin community are always in flux. Nodes may freely enter and exit the Bitcoin peer-to-peer system, meaning that the composition of the group is difficult to pin down. This makes it even more difficult to determine who has authority to speak on behalf of Bitcoin, to determine what is best for Bitcoin and its users, or to make and implement decisions in the case of a crisis.

Operational crises are not merely far-fetched what-if scenarios. Bitcoin has already experienced several software malfunctions that could have caused its collapse if not remedied by a coordinated effort of Bitcoin software developers and miners. For example, as discussed earlier, the March 2013 "hard fork" resulted in two separate forms of the blockchain being created by computers within the Bitcoin network, when the system's entire value is premised on the existence of a single, authoritative blockchain.[161] The developers realized that the fork had been caused by computers within the network using different versions of the Bitcoin protocol."[162] Bitcoin's much-vaunted "decentralization" was revealed to be incomplete, as the core developers were able to contact and persuade enough Bitcoin mining pools to take action to ensure that one ledger (as recommended by the core developers) survived and the second ledger did not.[163] This revealed that certain people within the Bitcoin community have

---

advocates-closed-door-meeting-with-federal-regulators/ (reporting on the meeting between members of the Bitcoin Foundation and representatives from the U.S. Justice Department, Federal Bureau of Investigation, Department of Homeland Security, Internal Revenue Service, Secret Service and the Financial Crimes and Enforcement Division (FinCEN) of the Treasury Department); Simonite, *supra* note 37.

[160] *See Everybody Pivots*, *supra* note 158 ("In the beginning, the foundation did it all—public policy, education and outreach, core development—*primarily because there was no one else to do it*.") (emphasis added).

[161] *See 11/12 March 2013 Chain Fork Information*, *supra* note 135.

[162] VELDE, *supra* note 136, at 3.

[163] *See* Gavin Andresen, *March 2013 Chain Fork Post-Mortem*, GITHUB: BITCOIN IMPROVEMENT PROPOSALS (Mar. 20, 2013), https://github.com/bitcoin/bips/blob/master/bip-0050.mediawiki (stating that "[miners] Marek Palatinus and Michael Marsee quickly downgraded their nodes to restore a pre-0.8 chain as canonical, despite the fact that this caused them to sacrifice significant amounts of

power to make certain decisions that affect the operations of Bitcoin as a currency. Yet the parties who made these decisions were not selected through any official process (such as voting), and were in no way accountable for the outcomes of their actions. While a potential crisis was averted in the instance of the March 2013 hard fork, this does not guarantee that a decentralized structure will enable successful crisis management in the future.[164]

So, Bitcoin currently operates in a rather contradictory way—it is decentralized in some ways but not in others. The parties who act as the central authority within Bitcoin acknowledge their power in certain situations, but not in others; because there is no "official" power structure, it is not possible to hold those in power accountable for their actions. This ambiguous status is troubling in many ways.

Why this is a problem for Bitcoin as financial- market infrastructure:

Bitcoin's decentralized structure is particularly problematic given the potential of the Bitcoin blockchain to serve as financial market infrastructure. A decentralized structure creates the risks that *no one* will even attempt to ensure that Bitcoin works; that even if someone does step up to help, he or she has no official authority or ability to implement suggested fixes; that the crisis management process may be slowed because of the lack of authority or responsibility; and that it will be difficult to tell who should be involved in the process because the Bitcoin community is so fluid.

With existing centralized financial market infrastructure, it is at least clear who has the responsibility to manage and repair it, and it is possible to impose risk management obligations on *someone*. Indeed, global financial regulators set standards for "financial market infrastructure" that are targeted at the defined entities who own and operate them. As made painfully clear with the Heartbleed bug and as commentators have noted in

---

money and they were the ones running the bug-free version"); *see also* GERVAIS, *supra* note 36, at 57 (describing the resolution of the blockchain fork and stating that the manner of resolution was "at odds with Bitcoin's claim that it's a decentralized system and that the majority of the computing power regulates its decisions").

[164] Resolving the March 2013 fork required groups that held a significant percentage of the computing power used to mine Bitcoins to agree to support a particular version of the blockchain. *See* Andresen, *supra* note 163. This meant they had to act altruistically rather than in their own best interest and "sacrifice significant amounts of money." *Id.* Such altruistic acts cannot be presumed in the future.

other contexts, when no one has direct responsibility to perform a task, it may very well go unperformed, as people tend to assume that someone else will handle it.[165] Maintaining the functionality of financial market infrastructure is hugely important, and having no one specifically tasked with the responsibility for achieving this for Bitcoin is a significant risk.

C. Bitcoin as Open-Source Software

Bitcoin's status as open-source software also creates systemic operational risks that generate instability. I will first provide a brief explanation of what open-source software is, then move to explain the risks this structure raises for Bitcoin. This discussion is not intended to resolve the ongoing and impassioned debate on the merits of open-source software generally[166] but merely to acknowledge that its use does create operational risks for Bitcoin, particularly in the context of the Bitcoin blockchain's role as potential financial market infrastructure.

Open-source software is software that makes its "source code" (i.e., its human language instruction manual) freely available to the world.[167] Software that is open-source is made available to users through a license agreement that gives the user permission to alter the source code.[168] Open-source software is contrasted against "proprietary software," which is issued under a license agreement that forbids the licensee from making any changes to the software.[169] Software that is purchased from companies like Microsoft or Adobe is generally proprietary software.

The method of developing and maintaining open-source software is one of its defining attributes, and distinguishes it most sharply from

---

[165] *See* Perlroth, *supra* note 97 (quoting Columbia University computer science professor Steven. M. Bellovin as saying of the Heartbleed bug: "This bug was introduced two years ago, and yet nobody took the time to notice it. . . . Everybody's job is not anybody's job"); *see also* Andrew Meneely et al., *An Empirical Investigation of Socio-technical Code Review Metrics and Security Vulnerabilities*, 2014 PROC. 6TH INT'L WORKSHOP ON SOC. SOFTWARE ENGINEERING 37, http://dl.acm.org/citation.cfm?doid=2661685.2661687 (evaluating "Linus' Law" empirically and noting the negative impact of the "Bystander Effect" in the discovery of security vulnerabilities in open-source software).

[166] For an overview of the debate, see generally FADI P. DEEK & JAMES A. MCHUGH, OPEN SOURCE: TECHNOLOGY & POLICY (2008).

[167] *See id.* at 1.

[168] *See id.*

[169] *Id.*

proprietary software. Open-source software is developed in a collaborative, open way.[170] When the full source code is posted publicly for all to see, software developers take the initiative to craft improvements to the software, such as new features or fixes to problems.[171] They propose their changes publicly, and the code evolves over time.[172] Crucially, open-source software developers are usually not paid for their work; rather, it is generally done in developers' spare time and is viewed as an altruistic or reputation-enhancing activity.[173]

Open-source software is viewed by some as having many benefits over proprietary software. The collaborative ethos of the software creation process in open-source software is celebrated. Many state that open-source software is less vulnerable and more resilient than proprietary software, because the development of the software is transparent, and since more eyes are looking for bugs, more bugs will be noticed and fixed.[174] But, even open-source software is widely acknowledged to be plagued with bugs, as a developer for Mozilla (a prominent open-source software that runs the web browser Firefox) stated in 2005 that "everyday, almost 300 bugs appear . . . far too much for only the Mozilla programmers to handle."[175] Indeed, as discussed in Part IV.A.1 of this paper, it is widely understood within the Bitcoin developer community (though not discussed much in the mainstream press) that there are ongoing problems with the Bitcoin code that require fixes.[176]

---

[170] *See id.* at 162.

[171] *See id.* at 5.

[172] *See id.* at 163.

[173] *See id.* at 162–63.

[174] *See id.* at 5, 59–60. As famously stated by Eric Raymond in the seminal *The Cathedral and the Bazaar*, Linus' law [is that] "given enough eyeballs, all bugs are shallow" or "[g]iven a large enough beta-tester and co-developer base, almost every problem will be characterized quickly and the fix will be obvious to someone." Eric Steven Raymond, *Release Early, Release Often*, THE CATHEDRAL & THE BAZAAR (2000), http://www.catb.org/~esr/writings/cathedral-bazaar/cathedral-bazaar/ar01s04.html. *But see* GLASS, supra note 91 (arguing that there is no evidence that, once past a threshold small number of developers, more developers will either identify or resolve more software bugs). The recent Heartbleed and Shellshock bugs also tend to undermine Raymond's claim that all bugs will be found quickly in open-source software. *See supra* notes 92–98 and accompanying text.

[175] CLAIRE LE GOUES ET AL., THE CASE FOR SOFTWARE EVOLUTION 205 (2010), http://www.cs.cmu.edu/~clegoues/docs/legoues-foser10.pdf (citations omitted) (paper presented at the 18th FSE/SDP Workshop of the Future of Software Eng'g Res.).

[176] *See supra* notes 99-103 and accompanying text. Additionally, the Bitcoin Foundation has assessed the likelihood of certain threats to its software. On a scale of one to seven, the Foundation assesses the likelihood that "significant" bugs lurk in the Bitcoin protocol at around 4 and the likelihood that "significant" bugs lurk in the software code at

Leaving aside any debate over whether Bitcoin's open-source nature makes it less buggy or whether open-source is better than proprietary software generally, the open-source character of the development of Bitcoin's software and protocol creates important systemic operational risks for the Bitcoin blockchain. These include (1) the risk that no one will properly maintain the code because no one has the actual *responsibility* to do so; (2) the risk that conflicts of interest may shape the management of the Bitcoin code (and therefore financial market infrastructure itself); and (3) the risk that consensus on changes may be unachievable, leading to splits (or "forks") in the network. I will discuss each of these risks in turn.

Bitcoin's status as open-source software means that everyone interested *may* participate in the continued development and maintenance of the software, but, crucially, that no one *must* do so. This echoes some of the risks raised by Bitcoin's decentralized structure. As stated in Part III.B above, if no one *must* do it, there is no guarantee that it will be done, or that it will be done well. We see some of the tensions created by Bitcoin's open-source nature beginning to play out already, as the volunteer nature of the code maintenance and development is buckling under the weight of managing an ever-more important project (its importance increasing with its more widespread use, higher valuation, and the huge investments being made in the ecosystem surrounding it). For example, over the past year and during the publication cycle of this paper, the compensation of the team of core developers has shifted dramatically, accompanied by much debate.[177]

Moreover, the open-source nature of Bitcoin software development means that important repairs to the code are delayed because, until very recently, no one has had a full-time job—with full-time pay—to service the

---

more than 4.5. RISK MANAGEMENT STUDY, *supra* note 102, at 8.

[177] *See Bitcoin raises its profile but investors demand more: Impatient backers want virtual currency to grow into viable payment network*, IRISH TIMES, Aug. 4, 2014, (Finance), at 4 (describing the debate within the Bitcoin community about how to fund the development of the core software); *Is funding a development team really that difficult?*, BITCOIN FORUM (June 27, 2014, 2:13 PM), https://bitcointalk.org/index.php?topic=667926.0 (debating the need to provide additional funding for development of the Bitcoin software and the appropriate source of the funds); Nermin Hajdarbegovic, *Mike Hearn: Underfunding is Leaving Bitcoin Development in Crisis*, COINDESK (June 25, 2014), http://www.coindesk.com/mike-hearn-underfunding-leaving-bitcoin-development-crisis/ (describing a leading Bitcoin software developer's concerns that "the core bitcoin system is radically underfunded and underdeveloped from where it needs to be").

code.[178] Indeed, both the core developers and high profile investors in companies providing Bitcoin-related products or services have raised alarms that the code development structure has delayed important necessary repairs to the Bitcoin code.[179] If core developers are not paid for their efforts on Bitcoin, they must have other sources of income. Thus, until recently, Bitcoin code maintenance and development has been only a hobby for these people to pursue in their spare time. Since they have had to fit code maintenance in before or after their real jobs, it is not surprising that crucial changes to the Bitcoin software have been slow.[180] Professional investors like the venture capitalists that have been piling in to Bitcoin over the last two years[181] are not used to having to wait for fixes to business problems—paying the party who can fix the problem to do it well and quickly is how professional business people operate. The maverick structure of Bitcoin software development has therefore been frustrating for the professional

[178] *See Strengthening the Core*, BITCOIN FOUND. BLOG (Nov. 20, 2014), https://blog.bitcoinfoundation.org/strengthening-the-core/ (describing how the compensation of the core developers has evolved over time).

[179] *See* Danny Bradbury, *Gavin Andresen to Bitcoin Companies: Support Open Source*, COINDESK (Feb. 21, 2014), http://www.coindesk.com/gavin-andresen-bitcoin-companies-support-open-source/ (reporting that Bitcoin core developer Gavin Andresen wrote to Bitcoin companies urging them to assist the core developers in developing, reviewing, and testing the code rather than treating the code like a purchased product); Hajdarbegovic, *supra* note 181 (reporting a software developer's concerns that "because developers are not incentivised [through pay] . . . they simply don't tend to tackle the big problems and little progress is being made"); Kadhim Shubber, *Jeremy Allaire: Bitcoin Developers Need to 'Step Up'*, COINDESK (July 2, 2014), http://www.coindesk.com/circle-ceo-jeremy-allaire-issues-challenge-bitcoins-core-developers/ (reporting that CEO of Bitcoin wallet company Circle calls for changes in the software development process to support the huge industry being built on top of the code).

[180] As core developer Gavin Andresen wrote in a blog post on Bitcoin software development:

> People are busy. They have lives, families, careers and hobbies outside of Bitcoin. It's unrealistic to put expectations of a full-time employee onto a volunteer. As more and more people come to rely on this protocol and businesses build products and services powered by Bitcoin, it becomes increasingly more important to have a dedicated team doing the painstaking work it requires.

Bitcoin Foundation, *Welcome Sergio Lerner!*, BITCOIN FOUND. BLOG (Dec. 5, 2014), https://blog.bitcoinfoundation.org/welcome-sergio-lerner/ [hereinafter *Welcome Sergio Lerner*].

[181] *State of Bitcoin 2015: Ecosystem Grows Despite Price Decline*, COINDESK (Jan. 7, 2015), http://www.coindesk.com/state-bitcoin-2015-ecosystem-grows-despite-price-decline/ (reporting that venture capital investment in Bitcoin-related companies totaled $433 million from 2012 to the end of 2014).

moneyed interests that have entered the Bitcoin ecosystem.[182]

These problems with adequate maintenance of the code due to its open-source status have spurred searches for fixes that, in turn, create other problems. Businesses and advocacy organizations within the Bitcoin ecosystem have recognized that the Bitcoin code needs more time and attention from the core developers, so they have started to pay the core developers for their work on Bitcoin. Over the course of Bitcoin's existence, the compensation of the core developers has evolved from no compensation, to compensation by private businesses within the Bitcoin ecosystem, to compensation by non-profit digital currency advocacy groups. As of this writing, several of Bitcoin's core developers are based in the Massachusetts Institute of Technology's Digital Currency Initiative, and are compensated by MIT.[183] It is unclear who is paying the remaining core developers (if anyone), but in the past, some of the core developers were paid by the non-profit Bitcoin Foundation, while others were full-time employees of Bitcoin-focused businesses. [184] For instance, from May 2013 to December 2014, core developer Jeff Garzik was a full-time employee of BitPay, a prominent business that facilitates businesses' acceptance of bitcoin payments.[185]

This compensation of the core developers may be necessary to adequately maintain the code, but it raises clear conflicts of interest. If a developer is paid by a particular business to do work on a communal, public project like Bitcoin, the developer has a strong incentive (i.e., a paycheck) to prioritize his employer's interests over the interests of the Bitcoin community as a whole. One could imagine a scenario in which a developer's employer had a different interest than other Bitcoin owners; the developer may choose to further his or her employer's interest over other

[182] *See* Shubber, *supra* note 183.

[183] *See* Brian Forde, *Welcome to the MIT Media Lab, Gavin, Wlad, and Cory*, MIT MEDIA LAB (April 22, 2015), https://medium.com/mit-media-lab-digital-currency-initiative/welcome-to-the-mit-media-lab-gavin-wlad-and-cory-977ae418c084 (reporting that Gavin Andresen, Wladimir van der Laan, and Cory Fields, "three of the leading developers of the Bitcoin core project," have accepted positions at the Digital Currency Initiative).

[184] *See Strengthening the Core*, *supra* note 182 (stating that three Bitcoin software developers are paid by the Bitcoin Foundation, one developer is paid by private company BitPay, and two developers are paid by private company Blockstream); *Welcome Sergio Lerner*, *supra* note 184 (stating that the Bitcoin Foundation has hired Sergio Lerner as a new developer to focus on security testing of the Bitcoin code).

[185] *See* Elizabeth Ploshay, *BitPay Hires Jeff Garzik*, BITCOIN MAG. (May 15, 2013), http://bitcoinmagazine.com/4515/bitpay-hires-jeff-garzik/. According to Mr. Garzik's LinkedIn page, he worked for Bitpay until December 2014. *See infra* note 194.

Bitcoin owners, with no official accountability to anyone. This plays out not just through changes made to the Bitcoin software code but also in the ways that the core developers interact with regulators, businesses, and media, as the core developers have been sought out as the "voices" of Bitcoin.[186] The messages that the core developers convey to outside parties may benefit or harm some bitcoin owners more than others. A quick skim of the Bitcoin internet forums reveals that bitcoin owners have different ideas about what is beneficial for the currency,[187] and the conflicts of interest carried by the core developers may certainly impact their behaviors and decisions regarding Bitcoin.

Finally, the mode of open-source software development means that consensus to proposed changes to the code may be difficult to achieve. As of this writing, this problem is playing out through a heated debate over the appropriate "block size."[188] A technical point (how much computer memory a "block" should consume) that has real implications on the costs and power dynamics of the network,[189] this debate is emblematic of the important policy choices embedded in every change to the software—whether they seem purely technical or not. The core developers have split into different factions on this point, and the debate threatens to similarly split the network,[190] raising questions about the value of the "bitcoins" embedded in each surviving network and how financial market infrastructure or a business ecosystem balanced on top of a severed series of networks would operate. Even if the block size debate is resolved without a "fork," there are infinite other serious technical (and therefore policy) issues that could fracture the network, making this a significant operational risk.

---

[186] *See supra* notes 157–60 and accompanying text.

[187] *See, e.g.*, *Topic: How Could Bitcoin Evolve?*, BITCOIN FORUM (Oct. 3, 2014, 6:52:59 PM), https://bitcointalk.org/index.php?topic=809588.0 (debating ending proof of work (Pow) as part of Bitcoin mining, among other matters); *Topic: The Problem of Centralized Develpoment ("core devs") in Bitcoin*, BITCOIN FORUM (Oct. 22, 2014, 5:42 PM), https://bitcointalk.org/index.php?topic=831540.0 (debating whether the Bitcoin core developers should simply implement the wishes of the Bitcoin community as expressed through votes or should also make policy decisions that they implement in the code).

[188] *See supra* note 137-139 and accompanying text.

[189] This debate has money and power implications, because the size of a block determines how much memory a computer has to devote to storing copies of the blockchain, or ledger. The system creates its "distributed trust" through multiple copies of the blockchain spread throughout the network. Computer memory costs money; money determines who is able to afford to participate in the network. The more money it costs to participate, the fewer "nodes" or "miners" there will be in the network (or the more concentrated mining pools become), meaning the network can become more and more centralized as it becomes cost-prohibitive to participate.

[190] *See* Caffyn, *supra* note 137.

Why this is a problem for Bitcoin as financial market infrastructure:

While problems like inadequate code maintenance, conflicts of interest among code developers, or failure to obtain consensus to software changes may not be of great significance in a typical open-source software project, such as one that creates a web browser (like Firefox) or a computer operating system (like Linux), they are of grave importance in software whose functioning undergirds financial market infrastructure. Financial market infrastructures such as money and payment systems act in many ways as public goods,[191] making the risk of failure due to an overlooked software glitch, conflicts of interest with a private employer, and a fractured network due to failed consensus on a software change highly problematic. The operation of financial market infrastructures is critical to financial stability, hence their strict regulation, which includes both governance and risk-management requirements.[192] Leaving fixes to financial market infrastructure to be remedied by a hobbyist who has no accountability (other than reputation) to do the repair correctly or in a timely manner, or who may be incentivized by a paycheck to act on behalf of his or her private employer rather in the interests of the public, is a high-risk way to operate these vital structures.

Both sides of the coin (sorry) are problematic here: either Bitcoin adheres to traditional open-source decentralized practices of maintaining the software through purely volunteer contributions, resulting in inadequate code maintenance and higher risk of software problems or it tries to do better software maintenance by having private parties compensate core developers for their work, introducing conflicts of interest into the mix. Either scenario is worrisome if the Bitcoin blockchain serves as financial market infrastructure. In spite of the "open" nature of open-source software, its development methods, coupled with the decentralized structure of Bitcoin, create significant operational risks.

D. Bitcoin's Expertise Problem

The final operational risk that I will discuss in this paper is what I term the "expertise problem." This is the risk that springs from people with

[191] Ferrarini & Saguato, *supra* note 69, at 20 ("In particular, policy makers stressed the importance of public regulation in modeling prudential and corporate governance standards for FMIs, given the 'public' nature of their services.").

[192] *See supra* Part II.B.

predominantly technical (computer or software) expertise operating and controlling an item that has, in recent history at least, been maintained and controlled by parties who at least purport to have some education and expertise related to money or finance.[193]

Software coders, who make the decisions about what the Bitcoin software will look like and what functions the system will have, are not necessarily financial systems experts. The known backgrounds of the core team of developers are in computer science and software development, not in economics, finance, financial systems, or monetary policy.[194] Examples of decisions that have been made by the software developers (including the original developer, Satoshi Nakamoto) include: having a cap on the number of Bitcoins that may ultimately be issued; having Bitcoins be divisible into a certain number of smaller chunks; reflecting all transactions on a common ledger that is distributed amongst Bitcoin nodes; the trajectory of Bitcoin; and how Bitcoin should interact with government regulators. There are no doubt countless others. All of these decisions impact viability and success of the Bitcoin blockchain as financial market infrastructure, and all have been made by software developers rather than financial systems experts.

---

[193] Eric Posner referred to this expertise problem in his piece for *New Republic* in December 2013:

> In response to those who have argued that bitcoin is inherently deflationary because the supply does not grow as rapidly as the global economy—which encourages hoarding of money rather than its use for investment—one commentator pointed out that the "bitcoin community" can increase the supply of bitcoins through majority rule by jointly reprogramming the underlying software, which is publicly accessible. But if this is true, it means that bitcoin is controlled by a central bank after all, albeit one whose boardroom holds millions of people. The money supply is determined by votes cast by people who know nothing about monetary economics and little about the economic conditions that justify modification of it. So on what basis would they decide to increase the supply of the currency, and by how much?

Eric A. Posner, *Bitcoin's Bandwagon Has Never Been More Crowded*, NEW REPUBLIC (Dec. 3, 2013), http://www.newrepublic.com/article/115801/bernankes-bitcoin-comments-signal-growing-acceptance; *see also* Yermack, *supra* note 55, at 5 (noting that "macroeconomic policy decisions [about Bitcoin could end up] controlled by an online discussion forum or blog rather than by an expert agency such as the Federal Reserve").

[194] For profiles on core developers, see Gavin Andresen, LINKEDIN, https://www.linkedin.com/in/gavin-andresen-6987971 (last visited Nov. 9, 2015); Jeff Garzik, https://www.linkedin.com/in/jeffgarzik LINKEDIN, (last visited Nov. 9, 2015); Pieter Wuille, LINKEDIN, https://www.linkedin.com/in/pieterwuille (last visited Nov. 9, 2015). Neither Gregory Maxwell nor Wladimir J. van der Laan appear to have a LinkenIn profile or other publicly available profiles. *See also* Simonite, *supra* note 37 (describing Gavin Andresen's background in computer science and software development).

Why this is a problem for Bitcoin as financial market infrastructure

If a crisis related to Bitcoin's operation or value should arise, there are no financial systems or payments experts who would *necessarily* be involved in reacting to the crisis. The computer experts would be the primary first responders, and would rely on their own backgrounds to determine the appropriate response. This is what happened with the March 2013 fork in the Bitcoin blockchain, when the core developers coordinated a response to resolve the matter.[195] This is not to say that experts in one field cannot succeed in another (indeed, I seek to point out some problems with Bitcoin itself from a non-expert's perspective) but that with something as important as financial market infrastructure, it seems to make sense to have people with an in-depth understanding of the world financial and monetary systems as a whole, involved in making decisions about how it operates. To pretend that with Bitcoin, *no one* makes these decisions or that the computer coders who manage Bitcoin are not making policy choices with critical implications is both false and dangerous.

The creation of financial systems infrastructure by non-experts, as is the case with Bitcoin and other virtual currencies, aligns with the trend of production by non-experts that is widely recognized and discussed in Internet and media circles.[196] Bitcoin represents an extension of this trend of decentralized amateurs seizing control of the creation of a product from centralized sources deemed to have power and expertise.[197] While this movement of amateur creation has generated amazing creative content, and is laudable in many ways, there are certain products or things that pose risks that demand they be produced or managed by those with relevant expertise or authority. As even Lawrence Lessig, an avid supporter of open-source

[195] *See supra* notes 161–64 and accompanying text.

[196] *See generally* YOCHAI BENKLER, THE WEALTH OF NETWORKS: HOW SOCIAL PRODUCTION TRANSFORMS MARKETS AND FREEDOM (2006) (discussing the social benefits of peer production versus centralized production); LESSIG, *supra* note 3 (discussing the cultural shift towards nonprofessionals contributing creatively to information development and the economic structure). This trend is best demonstrated by the widespread creation of media content by individuals as opposed to more centralized sources. Professor Lawrence Lessig has referred to this as a transition from a primarily "Read Only" world to one which is also "Read-Write", where the masses do not just consume (or "read") content, but actively create (or "write") it themselves. *Id.* at 84–85. Rather than content coming solely from record labels, movie studios, or mainstream newspapers, it comes from individually made recordings that people post on YouTube, websites, or blogs.

[197] *See* VIGNA & CASEY, *supra* note 53, at 276–78 for a description of the trend towards amateur control of traditionally centralized product and service markets.

software and the peer production movement, has acknowledged, "There are places where authority is required: No one should want Congress's laws on a wiki. Or instructions for administering medication. Or the flight plan of a commercial airliner."[198]

Financial market infrastructure, with its important social functions, is one of these places. Just as certain areas like flight plans and medication dosages require *authority* to rely upon, given the dire consequences of errors in these matters, so too do these areas require *expertise*. Functioning financial market infrastructure benefits everyone who uses it, and users of a particular payment system or central clearinghouse are crippled if it stops working. A high level of expertise in money, finance, financial systems, and economics, rather than just the technical or mechanical processes that operate the infrastructure, is essential in those running the system, given the important policy choices that the Bitcoin developers are making through their code.

* * *

As Part III has demonstrated, the Bitcoin blockchain is subject to significant operational risks, primarily related to its technology and governances issues, which impact its reliability as financial market infrastructure.

V. WHY AREN'T WE TALKING MORE ABOUT BITCOIN'S OPERATIONAL RISKS?

The operational risks of Bitcoin have not gone unnoticed, but they have received far less attention than the harms that might be caused by Bitcoin's use. Thus far, regulators have primarily focused their attentions on categorizing Bitcoin under existing laws, identifying and halting the harms that Bitcoin's use can facilitate (e.g., the operation of illicit online marketplaces like Silk Road or money laundering), and regulating the businesses that operate the Bitcoin ecosystem, such as exchanges and wallet companies.[199] Only relatively recently have regulators and scholars begun to talk more about the operational risks of Bitcoin in their public writings. For example, within the last eighteen months, the European Central Bank

[198] LESSIG, *supra* note 3, at 84–85.

[199] For a regularly updated compilation of regulatory actions on virtual currencies, see *Virtual Currency Regulation Resources*, DAVIS POLK, http://bitcoin-reg.com/ (highlighting actions by the Internal Revenue Service, Commodity Futures & Trading Commission, Securities and Exchange Commission, FINCEN, and other money transmission and consumer protection regulators) (last visited Oct. 23, 2015).

and the European Banking Authority wrote about the technology and governance risks associated with virtual currencies.[200] Two recent computer science papers have also opened a more in-depth analysis of Bitcoin's operational risks.[201] In general, however, while there have been references and short discussions related to Bitcoin's operational risks in academic or U.S. regulatory writings, these are few compared to the extensive writings on Bitcoin's "use" risks.[202]

In general, regulators' consideration of Bitcoin has focused on questions like, "What bad things does Bitcoin allow people to do?" and "How does Bitcoin fit under existing law?" without fully resolving questions like, "What is it?" and "How is it made to work reliably?" In this Part, I seek here to take a step back to ensure that we are fully cognizant of and comfortable with our management of the more fundamental operational risks of Bitcoin in considering its blockchain as potential financial market

[200] In February 2015, the European Central Bank noted that Bitcoin's open-source software development process means that "no single entity [is] responsible for preventing or resolving [major] incidents." 2015 ECB PAPER, *supra* note 38, at 20. It noted that "[l]ike any highly IT and network-dependent mechanism, [virtual currencies] are specifically subject to operational risks. These include a wide spectrum of risks, ranging from technical failures to hacking, without obligations to mitigate these risks as is the case for financial institutions and payment systems. Those failures or hacking attacks can occur at individual level (loss or theft of private cryptographic keys or user credentials) or on a wider scale (disruption to, or hacking of, the technical infrastructure of the key actors)." *Id.* at 22; *see also* EUROPEAN BANKING AUTH., EBA OPINION ON 'VIRTUAL CURRENCIES' 38 (2014), https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf (identifying operational risks of virtual currencies, such as the fact that the software operating the currency can be changed, "accidently introduc[ing] errors or being done without "good faith"; "the operator of a virtual currency may lack adequate and secure IT infrastructure and governance arrangements . . . or [fail to] act with sufficient integrity" (speaking of a centralized virtual currency); "lack of corporate capacity and governance: lack of skills, expertise, systems, controls, organizational structure and governance exercised by market participants").

[201] *See* KIRAN & STANNETT, *supra* note 86; PETERS ET AL., *supra* note 86.

[202] *See, e.g.*, VELDE, *supra* note 136, at 3 (hinting at operational risks of Bitcoin in its discussion of blockchain forks, continued maintenance of the code by "a small set of programmers," and "incentives to hijack" Bitcoin); Grinberg, *supra* note 39, at 175–76, 179–81 (providing a brief discussion of "potential technology failures" of Bitcoin, including failure of anonymity associated with the currency, theft of bitcoins from users, and DDOS attacks on the Bitcoin system and noting that the developers of the Bitcoin software may make changes to it that could undermine confidence in the currency); Reber & Feurstein, *supra* note 59, at 91–92 (noting in passing that Bitcoin is subject to "operational risk, the risk that arises through the reliance on the functioning of the Bitcoin network"). Interestingly, the Bitcoin Foundation, a Bitcoin advocacy organization, published a lengthy list of threats to Bitcoin's success, including operational risks. *See* RISK MANAGEMENT STUDY, *supra* note 102, at 1, 2, 6–19.

infrastructure.[203]

There are a number of possible reasons why the operational risks of Bitcoin have received less attention from regulators or commentators. These reasons may include:

a) Bitcoin and other virtual currencies have been viewed as too insignificant or outside the mainstream to warrant concern with the robustness of their ongoing operation;

b) Bitcoin's operational risks are viewed as too obvious, minor, or boring to merit extended discussion;

c) Bitcoin is seen, or at least described, by many of its proponents as a perfect, organic product, rather than a product created and managed by humans;

d) regulators and society in general have grown comfortable with computer software playing an integral role in our lives, and even with the sharing or open-source models of creating and maintaining the software;

e) "techno-fundamentalism"; and

f) a belief that innovation is inherently positive and we must give innovation the chance to demonstrate its full benefits before condemning or shutting down innovative practices.

I will take each of these possible reasons in turn and discuss why they are insufficient reasons to gloss over Bitcoin's operational risks.

A. Bitcoin Is Too Small to Matter

Bitcoin has been dismissed by many as irrelevant, with its circle of

[203] Sarah Jane Hughes and Stephen T. Middlebrook hint at these issues:

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

Sarah Jane Hughes & Stephen T. Middlebrook, *Regulating Cryptocurrencies in the United States: Current Issues and Future Directions*, 40 WM. MITCHELL L. REV. 813, 839 (2014).

use limited to a relatively small group of people. Writings by regulators have also perceived its narrow use, noting how the number of daily Bitcoin transactions pales in comparison with the number of daily non-cash transactions.[204]

Based largely on this limited use, certain regulators concluded that Bitcoin did not pose a risk of harm to the larger economy. If Bitcoin is used by only a few people, the argument goes, then only those few will be hurt if it fails, so why worry about whether Bitcoin works properly or not?[205]

For a while, this was a reasonable position to take, but I argue that the moment for dismissing Bitcoin as a fad has passed. Too many well-known, credible people are singing its praises and investing huge sums of money to build the Bitcoin and other virtual currency ecosystems.[206] Moreover, in the fall of 2012, when the European Central Bank (ECB) provided the initial global regulatory guidance on Bitcoin, there were only around 10,000 users of Bitcoin.[207] By contrast, in early November 2015, the *Financial Times* reported that more than 120,000 transactions are added to the Bitcoin blockchain every day."[208]

Bitcoin therefore represents a much greater threat than it did previously, and for this reason regulators need to more explicitly factor Bitcoin's operational risks into their evaluation of Bitcoin.[209]

---

[204] *See* 2015 ECB PAPER, *supra* note 38, at 16–17.

[205] *See, e.g.*, 2012 ECB PAPER, *supra* note 38, at 6, 7 (noting that virtual currencies "cannot jeopardise financial stability, owing to their limited connection with the real economy, their low volume traded and a lack of wide user acceptance" and that "[o]wing to the small size of virtual currency schemes, these risks do not affect anyone other than users of the schemes").

[206] *See supra* notes 6-13 and accompanying text.

[207] *See* 2012 ECB PAPER, *supra* note 38, at 25.

[208] Wild, *supra* note 61. Of course, as the ECB has noted, his number is still miniscule compared to the "274 million non-cash retail payment transactions per day for the EU only." 2015 ECB PAPER, *supra* note 38, at 17.

[209] In 2012, the ECB noted that it would have to continue to reevaluate the risk posed by virtual currencies. 2012 ECB PAPER, *supra* note 38, at 7 ("[The risk] assessment could change if usage increases significantly, for example if it were boosted by innovations which are currently being developed or offered. As a consequence, it is recommended that developments are regularly examined in order to reassess the risks."). In its 2015 report, the ECB noted that "As in 2012, again because of their small size, [virtual currencies] do not pose a threat to payment system stability." 2015 ECB PAPER, *supra* note 38, at 27. However, it noted that this could change depending on how integrated mainstream financial players become with virtual currencies and whether there is "a significant increase in users and the volume of transactions" in virtual currencies. *Id.* Further, the ECB acknowledged that virtual currencies "do have the potential to have an impact on monetary

B. Bitcoin's Operational Risks are Obvious, Minor, or Boring

It is obvious that Bitcoin is decentralized, open-source software. It is also obvious that it is operated by people other than celebrated financial systems experts. These facts about Bitcoin are prominently displayed in virtually all descriptions of it, from the website www.bitcoin.org that seeks to educate the public on Bitcoin[210] to the White Paper written by Satoshi Nakamoto[211] to the Bitcoin Foundation's website and materials.[212] These attributes of Bitcoin are not secrets, so perhaps everyone discussing Bitcoin's risks is already factoring them into their own risk analysis without the need to belabor them.

But, sometimes it is worth stepping back and more deeply considering the fundamental attributes of something when assessing its risks. When the securitization of subprime mortgages was in full swing during the mid-2000s, it would have been helpful if more people creating and purchasing mortgage-backed securities had considered that a basic attribute of a subprime mortgage was that it was issued at a subprime interest rate *because the borrower was a significant credit risk*—and that that inherent risk needed to be factored into both the rating and pricing of the aggregated mortgage-backed security. Just because the risk that many mortgages would be defaulted on simultaneously seemed low, the high consequences of it were discounted. It is just these types of risks—low likelihood, high consequence ones—that Nassim Nicholas Taleb argued that we tend to inappropriately discount in the seminal *Black Swan*[213] and that I seek to ensure we are not doing now with our evaluation of Bitcoin and other virtual currencies.

C. Bitcoin is Organic and Untainted by Human Hands.

> "We have elected to put our money and faith in a mathematical framework that is free of politics and human error . . . ."[214]

---

policy and price stability, financial stability and the smooth operation of payment systems." *Id.* at 29.

[210] BITCOIN PROJECT, http://www.bitcoin.org (last visited Oct. 25, 2015).

[211] Nakamoto, *supra* note 26.

[212] BITCOIN FOUND., https://bitcoinfoundation.org/ (last visited Mar. 12, 2015).

[213] *See generally* NASSIM N. TALEB, THE BLACK SWAN: THE IMPACT OF THE HIGHLY IMPROBABLE (2d ed. 2010).

[214] Popper & Lattman, *supra* note 1, at A3. The cited statement was made by Tyler Winklevoss.

> "If no-one owns it, how can I trust it? . . .
> In short, if you trust mathematics, you can trust Bitcoin."[215]

These statements have been put out into the world by proponents of Bitcoin, and they suggest to those who receive them that Bitcoin is somehow flawless and perfect—more of an elegant math theorem that follows the laws of science or nature rather than an invention of man. According to Tyler Winklevoss, a prominent Bitcoin supporter, Bitcoin is "a mathematical framework that is free of politics and human error."[216]

This type of messaging suggests that no person is responsible for Bitcoin itself—for the software's fundamental attributes (e.g., its limit on the total number of bitcoins that may be generated; how bitcoins are produced; making the software open-source and peer-to-peer, etc.) gives the impression that Bitcoin, like a math equation or a naturally occurring phenomenon like a flower, just *is*. Humans, with all of their foibles and flaws, did not make and do not make decisions about Bitcoin's fundamentals—Bitcoin operates because it is just math.

Perhaps these types of statements are meant to be taken with a grain of salt, or perhaps they stem from enthusiasm about Bitcoin by its proponents, but they are fundamentally inaccurate and potentially dangerous messages. Ordinary people created and maintain Bitcoin, and those facts make Bitcoin subject to human error—witness the long list of bugs that the Bitcoin developers themselves post publicly.[217] Bitcoin is subject to politics as much as any other human endeavor—witness the debates over its future in the Bitcoin message boards,[218] the important role the core developers play in determining its future,[219] and the potential conflicts of interests raised by the core developers' sources of income.[220] Witness the power struggle ongoing between the grownup, moneyed interests coming into the Bitcoin ecosystem through venture capital investments, and the early adopters who were/are interested in Bitcoin as a cool computer project or a realization of the dreams of Austrian economics.[221] Bitcoin is inescapably a *people* project, and, like all such

---

[215] MULTIBIT, *supra* note 2.
[216] Popper & Lattman, *supra* note 1, at A3.
[217] *See generally Issues List*, *supra* note 94.
[218] *See generally* BITCOIN FORUM, https://bitcointalk.org (last visited Oct. 25, 2015).
[219] *See supra* notes 32-37, 161-64, 177-190 and accompanying text.
[220] *See supra* notes 183-87 and accompanying text.
[221] *See* Velde, *supra* note 136 at 3–4 (noting that "much of the interest in Bitcoin" is inspired by the ideas of Friedrich Hayek of the Austrian School of Economics).

projects, is flawed in certain ways.

D. We are Comfortable with Software and Technology

Another reason why these operational risks may be discounted is that we as a society have become comfortable with the large role that software or other digital products play in our lives, and we have even become comfortable with open collaboration or open source software models. If we are comfortable with software running our phones, photos, security systems, cars, and so many other fundamental pieces of our lives, why should we care if a new type of software is used to run our financial market infrastructures? Aren't all of them electronic already?

This may be a natural response in today's hyper-digital world, but we must remember that Bitcoin is not just any old software, and financial market infrastructure is systemically important in a special way. As discussed in Part III, Bitcoin's governance risks only exacerbate its technology risks, meaning that we must be extremely careful of the weight we expect the Bitcoin blockchain to bear. Systemically important financial market infrastructures may well be too heavy to run on top of the Bitcoin network.

E. "Techno-fundamentalism"

"Techno-fundamentalism," a term coined by cultural historian Siva Vaidhanathan, may also explain why Bitcoin's operational risks have received less attention from regulators and academics. "Techno-fundamentalism" refers to a "blind faith in technology," which Vaidhanathan used to describe the ethos of Google. He notes that:

> "The particular kind of hubris that energizes Google is the notion that you can always invent something to solve the problem that the last invention created. That's techno-fundamentalism. . . . Techno-fundamentalism assumes not only the means and will to triumph over adversity through gadgets and schemes but also the sense that invention is the best of all possible methods of confronting problems."[222]

In describing Google, Vaidhanathan wrote:

> "Google works so well, so simply, and so fast that it inspires

[222] *Id.* at 76.

> trust and faith in its users. As the science fiction writer Arthur C. Clarke famously wrote, "Any sufficiently advanced technology is indistinguishable from magic." And of course trust in magic, or suspension of disbelief, is a central part of the process of embracing the deific. That's why so much of what we say and write about the experience of Google sounds vaguely religious."[223]

Techno-fundamentalism also seems to be related to overlooking the human element in technology:

> "[A]t its root is the black box of technological design. Although consumers and citizens are invited to be dazzled by the interface, the results, and the convenience of a technology, they are rarely invited in to see how it works. Because we cannot see inside the box, it's difficult to appreciate the craft, skills, risk, and brilliance of devices as common as an iPod or a continuously variable transmission in an automobile."[224]

Vaidhanathan's concept of techno-fundamentalism seems an apt description of much of the exuberance and passion we have seen Bitcoin proponents use to describe it, as well as the tendency to ignore the very human problems involved in governing the software code. The message that a techno-fundamentalist might have about financial market infrastructure is that all of its problems can finally be solved through the use of technology and math—virtual currencies such as Bitcoin represent that solution. From the Winklevoss twins, to venture capitalists, to the Bitcoin entrepreneurs who crowd the Bitcoin conferences and meetups now held around the globe, Bitcoin proponents are confident that Bitcoin represents a transformative and positive step forward in the evolution of financial systems.[225] It is the plodding Luddites (and the killjoy academics) like

---

[223] *Id.* at 53 (citations omitted).

[224] *Id.* at 52.

[225] *See, e.g.*, *Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currency: Hearing Before the S. Comm. on Homeland Sec. and Governmental Affairs*, 113th Cong. 5 (available at www.hsgac.senate.gov/download/?id=4cd1ff12-312d-429f-aa41-1d77034ec5a8) (2013) (statement of Patrick Murck, General Counsel, Bitcoin Foundation) ("[W]e believe Bitcoin holds out a number of powerfully beneficial social and economic outcomes, including global financial inclusion, enhanced personal liberty and dignity, improved financial privacy, and a stable money supply for people in countries where monetary instability may threaten prosperity and even peace."); Jerry Brito & Andrea Castillo, BITCOIN: A PRIMER FOR POLICY-MAKERS (2d ed. 2013) (identifying Bitcoin benefits as "lower transaction costs," "potential to combat poverty and oppression," and "stimulus for financial innovation"); Andreessen, *supra* note 65; Popper & Lattman,

myself who are left to sound the notes of caution as the technology moves forward.

F. Let a Thousand Virtual Currencies Bloom

The final reason I'll discuss for why we might not be addressing the operational risks of Bitcoin is a belief that innovations need to be encouraged and allowed to flourish rather than being shut down. This is different than the worship of technology that defines "techno-fundamentalism" and seems to be afoot with regulators' treatment of Bitcoin. Indeed, Janet Yellen, Chair of the Board of Governors of the Federal Reserve System, recently noted that:

> The costs and benefits of developing new statutes or regulations related to digital currencies should be weighed carefully. New regulation, such as the creation of special licenses for digital currency providers, may work to strengthen the soundness of virtual currency schemes and increase public trust in the products, as some may refrain from investing in or using digital currencies due to a perceived legal uncertainty and/or lack of consumer protection. On the other hand, new regulation would need to be flexible enough to address effectively the evolving nature of digital currency systems and technology *while not stifling innovation*.[226]

A separate presentation on virtual currencies given by an economist of the Boston Federal Reserve stated that "[the l]ongstanding Federal Reserve position on virtual currency [was that] . . . regulators should be careful not to inhibit experimentation and growth of innovative payment technologies."[227]

U.S. regulators have been wary of reflexively outlawing Bitcoin and other virtual currencies.[228] There have been numerous warnings given by

---

supra note 1 .

[226] Letter from Janet Yellen, Chair, Fed. Reserve Sys., to Congressman Mick Mulvany (Sept, 4, 2015) (emphasis added) (responding to a question regarding whether she thinks new regulations are needed for Bitcoin and other virtual currencies).

[227] OZ SHY ET AL., FED. RESERVE BANK BOS., CAN ECASH & VIRTUAL CURRENCY COMPETE WITH OTHER ELECTRONIC PAYMENTS? 12 (2014).

[228] *See* CONFERENCE OF STATE BANK SUPERVISORS, CSBS POLICY ON STATE VIRTUAL CURRENCY REGULATION 1 (2014) ("State regulators recognize the public interest in allowing [virtual currency] technologies to develop in a purposeful manner, providing clarity and certainty for implementation, and ensuring the stability of the larger financial marketplace.").

Bitcoin proponents that Bitcoin has created and will create many, many jobs, and that the United States stands to drive these jobs abroad if it over-regulates virtual currency.[229] Regulators appear to be heeding these warnings and to be working to understand virtual currencies before they regulate.[230] Indeed, a bill was filed in Congress in December 2014 that would ban U.S. states and municipalities from regulating cryptocurrencies for a period of time to allow them to develop.[231]

This is generally a laudable position to take, as regulators certainly do not want to be accused of constricting innovation and job growth. However, this guiding principle should not blind them to important structural risks embedded in new technologies, particularly when these new technologies are attracting significant investment and attention from prominent business and policy leaders.

CONCLUSION

New technologies like Bitcoin always challenge our existing ways of thinking. What do we do with innovations that fundamentally alter key aspects of the way we live? Do we let them grow and see what benefits come of them, or do we try to anticipate their strengths and weaknesses and steer development to protect ourselves?

Financial market infrastructures form the circulatory system of our modern economies, and their failures can threaten financial stability. We should therefore scrutinize innovations that radically reshape these structures to make sure we are comfortable that they are robust enough to last. It is true, of course, that our current financial market infrastructures are fragile or flawed in their own ways. But, we should not overlook important operational risks as we glimpse opportunities to improve upon existing structures.

---

[229] *See* JERRY BRITO & ANDREA CASTILLO, BITCOIN: A PRIMER FOR POLICYMAKERS (2d ed. 2013), http://coincenter.org/2013/08/bitcoin-primer-policymakers/; Andreessen, *supra* note 65; Nikolei M. Kaplanov, *Nerdy Money: Bitcoin, The Private Digital Currency, and the Case Against its Regulation*, 25 LOY. CONSUMER L. REV. 111, 171 (2012) ("Allowing bitcoin to operate unfettered by substantial regulation allows it to contribute towards job creation, economic growth, and opportunity.").

[230] The Senate Hearings on Virtual Currencies, the meetings of multiple Federal Agencies with representatives of the Bitcoin community, and the creation of various task forces to monitor virtual currencies demonstrate regulators' efforts to learn about virtual currencies.

[231] Cryptocurrency Protocol Protection and Moratorium Act, H.R. 5777, 113th Cong. (2014).

In this paper, I have sought to illuminate important technology and governance risks that could impact Bitcoin's ongoing operation and therefore the operation of any financial market infrastructure that uses its blockchain. The amalgamation of Bitcoin's vulnerability to bugs, attacks, and uneven adoption of new releases, coupled with the governance problems that stem from its decentralized, open-source nature, must factor into the analysis of whether the Bitcoin blockchain is reliable. From my perspective, this package of risks, taken as a whole, makes Bitcoin too unreliable to support financial market infrastructure.

Given that significant resources are being devoted to Bitcoin and its surrounding ecosystem, as well as financial market infrastructures that will rely on it, it is vital to evaluate these risks now, to avoid building important structures on shaky foundations. While the harms that a Bitcoin blockchain failure would cause right now are relatively limited (particularly in comparison to what a collapse of an existing major payment system or clearing house would cause), the more structures that come to rely on the Bitcoin blockchain, the greater the global harms (and the waste of resources) will be.

Further, the analysis in this paper is relevant to the existing debate on whether open-source software, with its historically uncompensated and unaccountable software development process, is suitable for other types of critical public-focused infrastructures or practices, such as electronic voting, emergency management, national security, air traffic control, or weapons systems. If the open-source development process is problematic for Bitcoin in its role as financial market infrastructure because of the lack of accountability and conflicts of interest that can arise with the compensation of coders, then it may be similarly problematic for other critical public infrastructures. This is an area for further research.

We have watched before as massive structures in the financial industry were built on faulty foundations, and have all paid the price when those structures inevitably collapsed.[232] Let us hope that we have learned the lesson to attend to embedded risks as we are shaping new structures now.

[232] *See* PATTERSON, *supra* note 150.