

BLOCKCHAIN DEVELOPMENT AND FIDUCIARY DUTY

Raina S. Haque, Rodrigo Seira Silva-Herzog, Brent A. Plummer, and Nelson M. Rosario*

INTRODUCTION	139
I. THE GENERAL OPERATIONS AND INCENTIVES OF OPEN SOURCE PRODUCTION	146
II. BLOCKCHAIN GOVERNANCE AND PROTOCOL DEVELOPMENT	151
III. PROTOCOL DEVELOPERS IN MOMENTS OF CRISIS	167
IV. THE IMPROPER FIT OF CORPORATE FIDUCIARY	173
V. EFFECTS OF IMPUTING FIDUCIARY DUTIES ON PROTOCOL DEVELOPERS	183
CONCLUSION: TOWARDS A BETTER UNDERSTANDING OF PUBLIC BLOCKCHAIN NETWORK GOVERNANCE FOR APPROPRIATE LIABILITY FRAMEWORKS	186

INTRODUCTION

In 2018, Bitcoin’s value dropped a whopping 70%.¹ The number of crypto-related litigation proceedings tripled by the end of the year,² leading to the birth of crypto litigation as a practice area. An alphabet soup of federal agencies—IRS, SEC, CFTC, CFPB, FinCen, CFPB, and FTC—

* Haque is a Professor of Practice in Emerging Technologies at Wake Forest University School of Law. Seira Silva-Herzog is a practicing lawyer at Cooley LLP. Plummer is a third-year law student at Wake Forest University School of Law. Rosario is an adjunct professor at Chicago-Kent School of Law. We thank Professors Andrew Verstein, Christine Coughlin, Ron Wright, Marie Amelie George, and Russell Gold, and Wake Forest Law students Josephine Fina and Brooke Driver, and the Wake Forest University School of Law Works-in-Progress workshop for their generous review and comments, and Professor Mary Susan Lucas for her timely research assistance.

¹ See BITCOIN, COINMARKETCAP, <https://coinmarketcap.com/currencies/bitcoin/#charts> (last visited Feb. 17, 2019).

² See Mark Emem, *Buyer’s Remorse? Cryptocurrency Lawsuits Have Tripled Since 2017*, CCN (Sept. 16, 2018), <https://www.ccn.com/buyers-remorse-cryptocurrency-lawsuits-have-tripled-since-2017>.

created groups to research and investigate blockchain³ and cryptoasset-based ventures (“cryptoventures”).⁴ Charges of fraud and criminality resulted from the spate of state and federal government investigations launched since 2017.⁵

By enabling new modes of human interaction, technological advancements catalyze the evolution of existing regulatory frameworks and spur the reassessment of regulatory tools and approaches. The rapidity at which computer technology evolves outpaces the rate at which much legislation, rulemaking, and law can be codified. Our economy is increasingly structured not only by traditional fiduciary actors, but also by software systems.⁶ Through software systems, assets are able to permeate markets rapidly and at a greater scale.⁷ Rightfully, scholars and regulatory officials reexamine liability frameworks for software developers.⁸ The advent of blockchain technologies dramatically demonstrates the challenge of scrutinizing an interconnected software system. Blockchain technologies emerged extra-institutionally.⁹ These technologies enable a wide array of never-before possible peer-to-peer interactions. Blockchain-based transactions bypass regulatory control.¹⁰

We have explored the governance role of blockchain developers for the two most prominent¹¹ public¹² blockchain communities and networks. With

³ There are, in fact, many blockchains; we focus on two prominent ones in this Article. *See* PRIMAVERA DE FILIPPI & AARON WRIGHT, *BLOCKCHAIN AND THE LAW: THE RULE OF CODE 21*, 31 (2018).

⁴ *See* Stefan Stankovic, *US Cryptocurrency Regulation: Policies, Regimes & More*, UNBLOCK (July 13, 2018), <https://unblock.net/us-cryptocurrency-regulation/#h3>.

⁵ *See* Jean Eaglesham et al., *Crypto Craze Drew Them In; Fraud, in Many Cases, Emptied Their Pockets: SEC and State Regulators Have Brought More Than 90 Crypto Cases over the Past Two Years, but Tracing Funds Is Hard Because of the Elusive Nature of the Currency*, WALL ST. J. (Dec. 26, 2018), <https://www.wsj.com/articles/crypto-craze-drew-them-in-fraud-in-many-cases-emptied-their-pockets-11545820200>.

⁶ *See generally* John Daley, *Insecure Software Is Eating the World: Promoting Cybersecurity in an Age of Ubiquitous Software-Embedded Systems*, 19 STAN. TECH. L. REV. 533 (2016).

⁷ DE FILIPPI & WRIGHT, *supra* note 3, at 61.

⁸ *See generally* Gregory Scopino, *Preparing Financial Regulation for the Second Machine Age: The Need for Oversight of Digital Intermediaries in the Futures Markets*, 439 COLUMBUS BUS. L. REV. 112 (2015). *See also* Epicenter, *Podcast #253 Angela C. Walch: The Case for Treating Developers as Fiduciaries in Public Blockchains*, YOUTUBE (Sep. 19, 2018), <https://youtu.be/qvkiymH0i1U>.

⁹ *See* Daniel Araya, *The Challenges of Cryptocurrency Regulation*, THE REGULATORY REVIEW (Oct. 9, 2018), <https://www.theregreview.org/2018/10/09/araya-challenges-cryptocurrency-regulation>.

¹⁰ DE FILIPPI & WRIGHT, *supra* note 3, at 45 (“By using a blockchain, parties can transfer digital currencies or other valuable assets without the need to rely on a centralized clearinghouse or trusted authority.”).

¹¹ The two most prominent public blockchain systems are Bitcoin and Ethereum per number of detectable nodes. As of February 12, 2019, the Bitcoin network contained 10,601 nodes. *See Global Bitcoin Nodes Distribution*, BITNODES (Feb. 12, 2019), <https://bitnodes.earn.com>.

respect to the incentives and operations of prominent public blockchains, the role played by core developers in the governance of these networks does not exhibit the structural dynamics that warrant the imposition of fiduciary obligations for the benefit of cryptoasset holders. These developers are structurally unable to make decisions to foist changes upon the participants of a network.

The evolution of software systems outpaces the rate at which legal scholarship can timely examine the operational dynamics of software development. Such dynamics should be integral to an analysis of the appropriate liability framework for software developers.¹³ Blockchain technologies use state-of-the-art encryption technology for automated validation of transaction data.¹⁴ Many blockchain networks that are open to the public use a gamified incentive scheme to further validate the history of transactions and maintain conformity in the data recorded across the distributed ledgers.¹⁵ Despite its uncanny birth,¹⁶ or maybe even because of it, blockchain technology has been adopted world-wide.¹⁷

Many of the traditional gatekeepers of certain highly regulated activities, such as early stage venture financing and cross-border money transmission, have called for regulation and scrutiny of blockchain ecosystems.¹⁸ Financial and prudential regulators are called on to perform a

As of February 12, 2019, the Ethereum network contained 7,591 nodes. *See Ethereum Node Tracker*, ETHERSCAN (Feb. 12, 2019), <https://etherscan.io/nodetracker#>.

¹² A public blockchain is permissionless, which means that the network allows for anyone to join the network and pursue “permissionless innovation” without the permission of a central authority or the permission of the other network participants so long as the “application is compatible with the established protocol and consensus rules.” *See* Christian Catalini & Joshua S. Gans, *Some Simple Economics of the Blockchain* 16 (Nat’l Bureau of Econ. Research, Working Paper No. 22952, 2018).

¹³ *See* Tamar Frankel, *Fiduciary Law*, 71 CALIF. L. REV. 795, 806-08 (1983) (positing that the judicial use of “mechanical analogies” in analyzing possible fiduciary relationships “result[s] in rules that are confusing and inappropriate.”).

¹⁴ *Id.* at 22.

¹⁵ Christian Catalini & Joshua S. Gans, *Some Simple Economics of the Blockchain* 1 (Nat’l Bureau of Econ. Research, Working Paper No. 22952, 2018).

¹⁶ As opposed to prior related technologies such as the Internet, blockchain technology was not born of traditional research and development institutions such as private industry, universities, the military, or public-private partnerships; it was born of online fora and public discourse, and catalyzed by a pseudonymous actor or actors.

¹⁷ *See* Arjun Kharpal, *Beyond Bitcoin: How the World Is Experimenting with the Blockchain*, CNBC (Aug. 29, 2018), <https://www.cnbc.com/2018/08/29/bitcoin-world-is-experimenting-with-blockchain.html>.

¹⁸ In a recent speech, CFTC Commissioner Brian Quintenz phrased the resulting issue succinctly: “How can our regulatory apparatus, built to register and oversee intermediaries, adequately police our markets and set standards for a disintermediated market?” *See* Brian Quintenz, CFTC Comm’r, *Remarks of Commissioner Brian Quintenz at the 38th Annual GITECH Technology Week Conference* (Oct. 16, 2018) (transcript available at <https://www.cftc.gov/PressRoom/SpeechesTestimony/opaquintenz16>).

tough balancing act. To begin with, they must sift through the explosion of information and misinformation on the Internet to gain baseline knowledge about the technology. They must then, on the one hand, remain vigilant and guard against potential fraud, consumer harm, and systemic risk. On the other hand, they must ensure that their stakeholders are able to benefit from the value created by new technological developments and that the markets they oversee remain competitive.

Determining where this innovative technology fits into legal frameworks is more than a hypothetical exercise for courts, regulators, and legislatures. Since the Bitcoin network launched in 2009, there have been a variety of cases that have grappled with the advent of blockchain technologies enabling disintermediated transactions that are pseudonymous and cross-jurisdictional.¹⁹

Cryptocurrency's use as a tool for money laundering schemes is one such regulatory concern. As an example, *US v. Ulbricht* concerned the arrest and eventual conviction of Ross Ulbricht for, among other things, maintaining an auction website where individuals could purchase illegal items with bitcoin.²⁰ Ulbricht was charged with money laundering in connection with the sales of items on his website "The Silk Road."²¹ His counsel argued that he could not be charged with money laundering because transactions in bitcoin were not financial transactions as defined by 18 U.S.C. § 1956.²²

Whether or not cryptocurrency is within the purview of money transmitter laws is an issue for every state. For example, *US v. Faiella* examined whether facilitating bitcoin transactions on behalf of customers constituted operating a money service business necessitating a money transmission license.²³ Defendants Robert Faiella and Charlie Shrem were charged with operating an unlicensed money transmission business.²⁴ The defendants argued that they were improperly charged, because bitcoin did not qualify as money under 18 U.S.C. § 1960.²⁵

¹⁹ See, e.g., Securities and Exchange Commission v. PlexCorps, et al., No. 17-cv-07007 (E.D.N.Y. Dec. 1, 2017).

²⁰ See *United States v. Ulbricht*, 31 F. Supp. 3d 540 (S.D.N.Y. 2014); see also *United States v. Ulbricht*, 858 F.3d 71 (2d Cir. 2017); see also THE DAO REPORT OF INVESTIGATION PURSUANT TO SECTION 21(A) OF THE SECURITIES EXCHANGE ACT OF 1934: THE DAO (2017).

²¹ See *United States v. Ulbricht*, 31 F. Supp. 3d 540 (S.D.N.Y. 2014).

²² In denying the defendant's motion the court stated, "the only value for Bitcoin lies in its ability to pay for things—it is digital and has no earthly form; it cannot be put on a shelf and looked at or collected in a nice display case. Its form is digital—bits and bytes that together constitute something of value." *United States v. Ulbricht*, 31 F. Supp. 3d 540, 570 (S.D.N.Y. 2014).

²³ See *United States v. Faiella*, 39 F. Supp. 3d 544, 545-47 (S.D.N.Y. 2014).

²⁴ See *id.* at 545.

²⁵ The court in dismissing the claim stated that "[f]irst, 'money' in ordinary parlance means 'something generally accepted as a medium of exchange, a measure of value, or a means of

Even well-settled securities laws have been reexamined due to the advent of blockchain technologies and the cryptographic tokens they enable. In 2017, the Securities and Exchange Commission issued what is colloquially known as “The DAO Report.”²⁶ In the report, the SEC discussed the results of their investigation into “whether The DAO, an unincorporated organization; Slock.it UG (“Slock.it”), a German corporation; Slock.it’s co-founders; and intermediaries may have violated the federal securities laws” by issuing cryptographic tokens.²⁷ As explained in the report, the DAO “is one example of a Decentralized Autonomous Organization, which is a term used to describe a ‘virtual’ organization embodied in computer code and executed on a distributed ledger or blockchain.”²⁸ The DAO sold tokens, “TheDAO tokens,” to investors who would then vote on projects to allocate funds to.²⁹ As such, in The DAO Report the SEC analyzed whether this initial coin offering, or “ICO,” of TheDAO tokens constituted an illegal securities offering.³⁰

One ICO offering typical of the wild west nature of this technology space included two high-profile celebrity endorsements from a rapper and a boxer, respectively.³¹ In *SEC v. Sharma*, the SEC charged the two cofounders of a company, CentraTech, Inc., that claimed to offer a “crypto debit card,” and touted non-existent relationships with Visa and MasterCard, with securities fraud.³²

payment.” Additionally, the court noted that “the text of Section 1960 refers not simply to ‘money,’ but to ‘funds.’” In particular, Section 1960 defines “money transmitting” as “transferring funds on behalf of the public by any and all means.” As such, the court concluded “Bitcoin clearly qualifies as ‘money’ or ‘funds’ under these plain meaning definitions. Bitcoin can be easily purchased in exchange for ordinary currency, acts as a denominator of value, and is used to conduct financial transactions.” *See id.*

²⁶ See THE DAO REPORT OF INVESTIGATION PURSUANT TO SECTION 21(A) OF THE SECURITIES EXCHANGE ACT OF 1934: THE DAO (2017).

²⁷ The SEC concluded that they did violate federal securities law, but the SEC decided not to pursue any enforcement action against the creators of the DAO. *Id.*

²⁸ *See id.*

²⁹ *See id.*

³⁰ The SEC’s first bullet point in its argument makes clear that the SEC believes its rules apply to even so-called decentralized organizations: “Foundational Principles of the Securities Laws Apply to Virtual Organizations or Capital Raising Entities Making Use of Distributed Ledger Technology.” The SEC emphasized that “[i]n analyzing whether something is a security, ‘form should be disregarded for substance,’ *Tcherepnin v. Knight*, 389 U.S. 332, 336 (1967), ‘and the emphasis should be on economic realities underlying a transaction, and not on the name appended thereto.’ *United Housing Found.*, 421 U.S. at 849.” *See id.*

³¹ See Securities and Exchange Commission v. Sharma, 1:18-cv-02909 (S.D.N.Y. April 4, 2018).

³² *See id.*

In addition to the attention from regulators, state legislatures issue legislation dictating the treatment of public blockchain networks.³³ For example, on September 28, 2018, the California State Assembly approved an update to their laws to include a definition of “blockchain,” as “a mathematically secured, chronological, and decentralized ledger or database”; whereas, the State of Vermont defines blockchain as “a cryptographically secured, chronological, and decentralized consensus ledger or consensus database maintained via Internet, peer-to-peer network, or other interaction.”³⁴ In 2018 alone, there were thirty-six different blockchain-related pieces of legislation introduced in state legislatures around the country.³⁵ These competing, and sometimes conflicting, approaches to this new technology speak to the interest in these platforms, and the need for clarity on how these new platforms should be treated by the law.

It may be tempting, when facing a wildfire of developments resulting from this emerging technology, to advocate for a fiduciary obligation on all blockchain developers. Subsequent to a major exploitation of the token-transferring code used by The DAO, which split the prominent Ethereum blockchain community into two and resulted in token value volatility, some scholarship³⁶ promoted views one scholar summarized by the title of her article—“Call Blockchain Developers What they Are: Fiduciaries.”³⁷ In the Twitter universe, there was a related attempt to create a hashtag movement: #codersasfiduciaries.³⁸ The thrust of the argument presented is that public blockchain developers have open-ended control of cryptoassets that belong to others.³⁹

³³ See Matthew E. Kohen & Justin S. Wales, *State Regulations on Virtual Currency and Blockchain Technologies*, CARLTON FIELDS (Jan. 9, 2019).

³⁴ VT. STAT. ANN. tit. 12, § 1913(a)(1) (West 2018).

³⁵ See Heather Morton, *Blockchain State Legislation*, NATIONAL CONFERENCE OF STATE LEGISLATURES (July 10, 2018), <http://www.ncsl.org/research/financial-services-and-commerce/the-fundamentals-of-risk-management-and-insurance-viewed-through-the-lens-of-emerging-technology-webinar.aspx> (last visited Feb. 11, 2019).

³⁶ See Philipp Hacker et al., *Regulating Blockchain: Techno-Social and Legal Challenges - An Introduction*, forthcoming in *REGULATING BLOCKCHAIN: TECHNO-SOCIAL AND LEGAL CHALLENGES* (Philipp Hacker, Ioannis Lianos, Georgios Dimitropoulos & Stefan Eich eds., Oxford Univ. Press, 2019).

³⁷ See Angela Walch, *Call Blockchain Developers What They Are: Fiduciaries*, AMERICAN BANKER (Aug. 9, 2016), <https://www.americanbanker.com/opinion/call-blockchain-developers-what-they-are-fiduciaries>.

³⁸ See #codersasfiduciaries, TWITTER, <https://twitter.com/search?q=%23codersasfiduciaries&src=tyah> (last visited Feb. 17, 2019).

³⁹ See Angela Walch, *Call Blockchain Developers What They Are: Fiduciaries*, AMERICAN BANKER (Aug. 9, 2016), <https://www.americanbanker.com/opinion/call-blockchain-developers-what-they-are-fiduciaries> (stating, “With millions of dollars of other people’s money on the line, these were enormous decisions for this small group of [core developers] to

These calls for the imposition of the fiduciary standard to be applied to “coders”⁴⁰ lack discernment of the many distinct operational roles and structural incentives of public blockchain developers. There is a long-held doctrine that careful deliberation is needed before a finding of fiduciary duty⁴¹—we agree. It is critical that regulators apply a legal framework that reflects the way an economy works, and the economic incentives⁴² and structural roles of the agents involved.⁴³ Scholars who have studied technological revolutions have noted that a critical step in devising the social and regulatory paradigm that will allow a society to benefit from the full potential of a new technology is to fight the reflex to force age-old legal concepts from prior technoeconomic paradigms onto new economic models.⁴⁴

This article addresses the forgoing issue in four parts. In Part I, we discuss the operations of open source, decentralized development to better understand these developers’ functions and how cryptocurrencies are used to build blockchain networks. In Part II, we discuss the different developers

make. This exercise of power makes them look an awful lot like fiduciaries of ether holders, and maybe even of investors in the DAO.”).

⁴⁰ In modern software development, “coders” connote even the most replaceable workers of software development; they may be least trained and skilled and have no authority to guide software design. Software developers and engineers, however, have specialized knowledge of the underlying software application and more authority about the design of the software. *See* Isaac Lyman, *Choosing A Job Title (For People Who Code): Are you a coder, programmer, developer, engineer, architect or something else?*, MEDIUM (Apr. 19, 2017), <https://medium.com/@isaaclyman/choosing-a-job-title-for-people-who-code-316a7673a83c>.

⁴¹ *See* Deborah A. DeMott, *Beyond Metaphor: An Analysis of Fiduciary Obligation*, 1988 DUKE L.J. 879, 924-25 (“Fiduciary obligation has a number of characteristics that classify it among the law’s most exotic species...The considerable variety of relationships in which parties are bound by fiduciary obligation further complicates the analysis. Determining whether fiduciary obligation applies in a particular context and what requirements inhere in the imposition of fiduciary obligation demands recognition of this situation-specificity. Although...careful analysis can resolve many questions about fiduciary obligation, the difficulty of that undertaking should not be underestimated.”).

⁴² An incentive is something that makes people act in a particular way. As we shall explore in the context of public blockchain networks, incentives may be used to achieve common gains by aligning parties with different motivations and degrees of knowledge. *See* Sinclair Davidson et al., *Economics of Blockchain* (Mar. 8, 2016), <https://ssrn.com/abstract=2744751> or <http://dx.doi.org/10.2139/ssrn.2744751>.

⁴³ As recently stated in a blog post by Bill Gates, “lawmakers need to adjust their economic policymaking to reflect these new realities.” Bill Gates, *Not Enough People Are Paying Attention to This Economic Trend*, GATES NOTES: THE BLOG OF BILL GATES (Aug. 14, 2018), <https://www.gatesnotes.com/Books/Capitalism-Without-Capital>.

⁴⁴ *See* CARLOTA PEREZ, *TECHNOLOGICAL REVOLUTIONS AND FINANCIAL CAPITAL: THE DYNAMICS OF BUBBLES AND GOLDEN AGES* 145 (2002) (arguing that “[a]n adequate set of institutions is needed to complement, shape and guide the transformations that take place in the economic sphere [due to technological revolutions]. Yet, it cannot be a blissful return to what worked in the previous paradigm; it must be the complex design of what will work with the new one.”).

involved in creating blockchain and blockchain-based systems and the governance structure under which they operate. We examine moments of crisis in blockchain communities that illustrate this governance in Part III. In Part IV, we emphasize the distinction between blockchain protocol developers and directors and officers of a corporation. We conclude our analysis by briefly exposing the effects of imputing fiduciary obligations on protocol developers.

I. THE GENERAL OPERATIONS AND INCENTIVES OF OPEN SOURCE PRODUCTION

To understand blockchain development operations, an understanding of open source production is critical.

a. Blockchain traces its roots to open source software development

Bitcoin and the public blockchain networks that followed from it have several innovative features, but their process of development, the method through which they came into being and are evolving, traces its roots to the open source production system that grew out of the early days of the Internet and the free software movement.⁴⁵ The term “open source”⁴⁶ refers to software that is freely distributed in source code⁴⁷ form and evolves through a process that “involves software developers at many different locations and organizations sharing code to develop and refine software applications.”⁴⁸ In

⁴⁵ For example, the code of the main clients of Bitcoin, Ethereum, and Hyperledger, as well as portions of the clients of Enterprise Ethereum and Corda, all consist of open source code. See DE FILIPPI & WRIGHT, *supra* note 3, at 21, 28; see also Martin Valenta & Philipp Sandner, *Comparison of Ethereum, Hyperledger Fabric, and Corda*, 2017 FSBC WORKING PAPER. Further, according to Chris Dixon, “the cryptocurrency movement is the spiritual heir to previous open computing movements, including the open source software movement led most visibly by Linux, and the open information movement led most visibly by Wikipedia.” Chris Dixon, *Crypto tokens: A breakthrough in open network design*, MEDIUM (June 1, 2017), <https://medium.com/@cdixon/crypto-tokens-a-breakthrough-in-open-network-design-e600975be2ef>.

⁴⁶ The Open Source Initiative manages a comprehensive definition of open source software that may be found at <http://opensource.org/docs/osd>.

⁴⁷ The Linux Information Project defines “source code” as “the version of software as it is originally written (i.e., typed into a computer) by a human in plain text (i.e., human readable alphanumeric characters).” See *Source Code Definition*, THE LINUX INFORMATION PROJECT (Feb. 14, 2006), http://www.linfo.org/source_code.html.

⁴⁸ Jean Tirole & Josh Lerner, *The Simple Economics of Open Source* 1-4 (2000 HBS FIN. WORKING PAPER NO. 00-059) (In recounting the early days of the Internet, Tirole and Lerner note that “many of the key aspects of the computer operating systems and the Internet were developed in academic settings such as Berkeley and MIT during the 1960s and 1970s, as well as in central corporate research facilities where researchers had a great deal of autonomy

contrast, “proprietary” code refers to code that is distributed in object code⁴⁹ form only and where the source code is protected as a trade secret.

As we shall explore more in depth in Section II (c), anyone is free to suggest a change to the code of an open source software application,⁵⁰ but only those developers with “commit access”⁵¹ to the code repository have the power to incorporate a change into the code repository. Commit access does not enable the protocol developers who wield it the power to force code changes on other network participants; network participants must act to download code changes.⁵²

b. Production through voluntary contributions of independent actors

A main principle of open source production is that development work is undertaken by independent volunteers who decide on their own account to collaborate with others in an iterative fashion.⁵³ As compared to software development in a traditional technology firm, which is undertaken by employees who are instructed by managers to work on specific parts of a project, developers contributing to open source production systems work on projects that interest them if and when they want to contribute.⁵⁴ While developers in open source production systems do organize into

(such as Bell Labs and Xerox’s Palo Alto Research Center). In these years, the sharing by programmers in different organizations of basic operating code of computer programs—the source code—was commonplace.” The archetypal example of open source software development is Linux, the first version of which was released by Linus Torvalds in 1991 and eventually grew to amass many thousands of contributions and went on to become the operating system of choice for many of the world’s leading tech companies today.)

⁴⁹ “Object code” is the “output of a compiler [a specialized computer program that reads and translates source code into object code] after it processes source code.” An object code “is usually a machine code, also called a machine language, which can be understood directly by a specific type of CPU (central processing unit).” See *Object Code Definition*, THE LINUX INFORMATION PROJECT (Aug. 7, 2005), http://www.linfo.org/object_code.html.

⁵⁰ See *The Open Source Definition*, OPEN SOURCE INITIATIVE, <https://opensource.org/docs/osd> (last modified Mar. 22, 2007) (mandating that open source software “must allow modifications and derived work.”).

⁵¹ To have “commit access” means having “the right to make changes to the copy of the code that will be used for the project’s next official release.” See KARL FOGEL, *PRODUCING OPEN SOURCE SOFTWARE* 28 (2nd ed. 2017).

⁵² See ARVIND NARAYANAN ET AL., *BITCOIN AND CRYPTOCURRENCY TECHNOLOGIES: A COMPREHENSIVE INTRODUCTION* 171 (2016) (explaining that the protocol developers with commit access “can urge the community [the blockchain participants] on, but they don’t have formal power to force people to follow them if they take the system in a technical direction that the community doesn’t like.”).

⁵³ See Bilgin Ibryam, *How Blockchain Will Influence Open Source*, OPENSOURCE.COM (Aug. 2, 2018), <https://opensource.com/article/18/8/open-source-tokenomics>.

⁵⁴ See Jos Poortvliet, *6 Reasons Open Source is Good for Business*, OPENSOURCE.COM (Oct. 13, 2017), <https://opensource.com/article/17/10/6-reasons-choose-open-source-software>.

communities, often around specific projects, interests or ideologies, these structures generally lack any formal hierarchy or power parity that characterizes software development firms.⁵⁵

c. Open access to code and ability to “fork”

In an open source production system, anyone can suggest a code change to the community. Anyone is also allowed to modify the existing code and try to build her own community to support a revised version of the code (a concept generally referred to as “forking,” which is discussed in more detail in Section II (c) below).

To accomplish the goal of being free and public available, open source projects publish their source code in online repositories and license it under a spectrum of free and open source (“FOSS”) licenses.⁵⁶ These licenses recognize open collaboration as the driver of production and require the commitment to making any iteration of the code freely available to the public for future use or modification.⁵⁷

d. Building cryptoeconomic institutions with cryptocurrencies

The Bitcoin project allowed for the newfound ability to transfer value over a peer-to-peer network and validate such transfers using a gamified incentive scheme that uses bitcoin, a cryptocurrency.⁵⁸ Bitcoin’s most significant contribution to open source development may stem from the Bitcoin network’s ability to solve the “double spend problem,”⁵⁹ which had hampered all previous attempts to launch a peer-to-peer virtual currency system.⁶⁰ Satoshi’s solution was to design an architecturally and politically decentralized payment transfer system that relies on a gamified verification scheme to be tamper-evident.⁶¹ By running the appropriate hardware and

⁵⁵ See Section II below for a further discussion of the governance structures of public blockchain networks.

⁵⁶ See generally Joshua Krumholz et al., *Blockchain and Intellectual Property: A Case Study*, in *BLOCKCHAIN & CRYPTOCURRENCY REGULATION 2019* (Josias N. Dewey ed., 1st ed. 2018). See also Brooke Driver, Comment, *Risky Business: A Proposal to Limit Liability for Developers of Open Source Software*, 8 *WAKE FOREST J. L. & POL’Y* 1 (2019).

⁵⁷ See *id.*

⁵⁸ See Satoshi Nakamoto, *Bitcoin: A Peer-To-Peer Electronic Cash System* (Oct. 31, 2018), <https://bitcoin.org/bitcoin.pdf>.

⁵⁹ The “double spend” problem is a flaw in digital currency systems where one participant with “a piece of data representing a unit of virtual cash” sends that piece of data to two or more people thereby double spending the same virtual cash. The recipients of the virtual cash have no way of knowing the money they received has been sent elsewhere. See NARAYANAN ET AL., *supra* note 52, at XIV.

⁶⁰ DE FILIPPI & WRIGHT, *supra* note 3, at 18-20.

⁶¹ *Id.* at 20-26.

software and connecting to the Internet, anyone can participate in this system to transact with anyone else.⁶² Furthermore, anyone can use her computer to participate in the system's protocol for validating the record of transfer.⁶³ This protocol is known as a Proof-of-Work ("PoW") consensus mechanism, and participants in it are known as "miners."⁶⁴

It is the PoW consensus mechanism that gamifies participation in the validation scheme.⁶⁵ Miners who are successful at proposing a batch of validated transactions that other network participants accept as valid are awarded in bitcoin.⁶⁶ This is the only way in which bitcoin can be generated.⁶⁷ The protocol for mining purposefully includes an energy-expensive routine; this routine deters malicious miners from tampering with the blockchain's history, making it computationally expensive to do so.⁶⁸ A miner has to pay (in energy) to play, so to speak.

The result is the ability of a network of computers, known as nodes, to support bitcoin transfers.⁶⁹ These nodes can be owned and operated by any entity, thus the network is decentralized.⁷⁰ Because of the protocol that runs the software applications on these nodes and governs the gamified validation scheme, Bitcoin is unable to be copied and is limited in number.⁷¹ Each of these nodes has a localized copy of the Bitcoin blockchain.⁷²

The Bitcoin network's introduction of bitcoin, or a blockchain network's native cryptocurrency⁷³ generally, provides a new "mechanism

⁶² *Id.* at 20-22.

⁶³ *Id.* at 22-24.

⁶⁴ See Nakamoto, *supra* note 58.

⁶⁵ See NARAYANAN ET AL. *supra* note 52, at 38-45.

⁶⁶ See *id.*

⁶⁷ Similar to how miners of physical-world resources are ones that bring such resources into the world, the efforts of Bitcoin miners are what generates Bitcoin for virtual payment. See *id.*

⁶⁸ DE FILIPPI & WRIGHT, *supra* note 3, at 25 (stating that "because the Bitcoin blockchain operates via consensus, a would-be attacker or group of attackers would need to rewrite the transaction history of the Bitcoin blockchain at a pace that is faster than the majority of honest [miners] supporting the network.").

⁶⁹ See NARAYANAN ET AL., *supra* note 52, at 66-69.

⁷⁰ See *id.* at 28-29 (explaining that "anybody can run a Bitcoin node, and the entry to barrier is fairly low").

⁷¹ See DE FILIPPI & WRIGHT, *supra* note 3, at 26 ("By combining the proof of work consensus algorithm and the block reward incentivization scheme, Nakamoto developed a scheme capable of solving the double spending problem by building a decentralized system that could limit the supply of bitcoin and process transactions without the need for a central clearinghouse.").

⁷² *Id.*

⁷³ In this article, we refer to all assets generated by or on a blockchain network as "cryptoassets." We use the term "cryptocurrency" to refer to cryptoassets that are generated by the blockchain network's validation scheme. We use the term "token" to connote assets created by the operations of smart contracts. Generally, there are different opinions about whether cryptocurrencies are a type of cryptographic token or a different species from

design”⁷⁴ tool to develop more complex incentive systems on top of open source networks. Using cryptocurrency, networks can now be designed in a way that economically incentivizes participants with different preferences and information to act collaboratively to maintain the value of the network.⁷⁵ Native cryptocurrencies work as an incentive for network participants by motivating holders to grow the network and drive demand for the cryptocurrency, therefore leading to an appreciation in the cryptocurrency’s market price.⁷⁶ Ownership of cryptocurrency is the economic incentive that keeps developers, miners, and other network participants to work to maintain the integrity of a blockchain network that uses the PoW consensus mechanism.⁷⁷

In this sense, cryptocurrencies enable the transformational aspect of public blockchain networks—the ability to create and execute rule-systems that result in new organizational and institutional forms of economic governance and “enable bespoke socio-economic coordination.”⁷⁸ The stability of public blockchain networks, a subspecies of distributed ledger systems, is a result of gamification.⁷⁹ “A blockchain is in this sense a new species of rule-system for economic coordination: so, alongside firms,

cryptographic tokens, or whether tokens are a subspecies of cryptocurrency. *See* ANDREAS M. ANTONOPOULOS & GAVIN WOOD, *MASTERING ETHEREUM: BUILDING SMART CONTRACTS AND DAPPS* (2019) (arguing that cryptocurrency is a type of token). *But see Crypto Token*, INVESTOPEDIA, <https://www.investopedia.com/terms/c/crypto-token.asp> (last updated Apr. 3, 2018) (stating that tokens are a type of cryptocurrency).

⁷⁴ “Mechanism design is the sub-field of microeconomics and game theory that considers how to implement good system-wide solutions to problems that involve multiple self-interested agents, each with private information about their preferences.” DAVID CHRISTOPHER PARKES, *ITERATIVE COMBINATORIAL AUCTIONS: ACHIEVING ECONOMIC AND COMPUTATIONAL EFFICIENCY* 23 (2001). In other words, “Mechanism design is the art of designing the rules of a game to achieve a specific desired outcome. While game theory takes the rules of a game as given and helps us determine outcomes based on them and the strategic interaction of players, mechanism design uses the framework of game theory with incomplete information and asks about the consequences of different rules and chooses the game structure rather than inheriting one.” Eden Dhaliwal et al., *Token Ecosystem Creation*, OUTLIER VENTURES 46 (Oct. 25, 2018), <https://outlierventures.io/wp-content/uploads/2018/10/Token-Ecosystem-Creation-Outlier-Ventures-PDF.pdf>.

⁷⁵ *See* DE FILIPPI & WRIGHT, *supra* note 3, at 25-26.

⁷⁶ *See id.*

⁷⁷ Chris Dixon highlights how cryptocurrencies are also effective tools to finance the launch of networks and enable network participants to overcome the “bootstrap problem” by introducing a tradable asset with that “add financial utility when application utility is low.” Chris Dixon, *Crypto Tokens: A Breakthrough in Open Network Design*, MEDIUM (June 1, 2017), <https://medium.com/@cdixon/crypto-tokens-a-breakthrough-in-open-network-design-e600975be2ef>. This novel financing model raises interesting securities laws issues which are outside of the scope of this Article.

⁷⁸ Davidson et al., *supra* note 42, at 6-7.

⁷⁹ *See* DE FILIPPI & WRIGHT, *supra* note 3, at 25-26.

markets, clubs, commons, and governments we now also have blockchains.”⁸⁰

II. BLOCKCHAIN GOVERNANCE AND PROTOCOL DEVELOPMENT

In the first section we uncovered some of the underlying dynamics present in open source production and public blockchain development. This section examines the influence protocol developers have on changes to public blockchain software applications. We do this by: (a) recognizing that public blockchain networks, like any organization, necessarily develop governance structures; (b) clarifying whom “protocol developers” refers to and analyzing the general role and motivation of the different types of protocol developers; and (c) providing an overview of how changes to the Bitcoin Core and Ethereum software applications are implemented in practice.

a. “Decentralized” does not mean “structureless”

When we refer to open source production and public blockchain networks, and in particular their governance, we do not assume that by virtue of being “decentralized”⁸¹ they are anarchic systems. We subscribe to the view that “[s]tructurelessness is organizationally impossible” and that “[a]ny group of people of whatever nature that comes together for any length of time for any purpose will inevitably structure itself in some fashion.”⁸² Therefore, a study of dynamics necessitates the differentiation of participants in a network.

b. The function and incentives of protocol developers in public blockchain networks

i. Defining “protocol developer”

In the context of open source software production, the term “developer” may generally refer to various unrelated individuals who play fundamentally different roles over time.⁸³ When talking about public

⁸⁰ Davidson et al., *supra* note 42, at 6-7.

⁸¹ For a detailed discussion of decentralization, see Vitalik Buterin, *The Meaning of Decentralization*, MEDIUM (Feb. 6, 2017), <https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274>.

⁸² Jo Freeman, *The Tyranny of Structurelessness*, JOFREEMAN.COM, <https://www.jofreeman.com/joreen/tyranny.htm> (May 1970).

⁸³ See Dirk Riehle, *How Open Source is Changing the Software Developer’s Career*, IEEE COMP. VOL. 48, no. 5, 51-57 (May 2015).

blockchain networks, it is first important to distinguish between developers contributing to the software application supporting the network (whom we have been referring to as “protocol developers”) from the developers building decentralized applications by coding and deploying program specific code known as “smart contracts”⁸⁴ onto public blockchain networks (whom we shall refer to as “smart contract developers”).

Our use of the term “protocol developer” is admittedly a loose one, given that it refers to individuals playing a range of roles, all of whom contribute in some fashion to maintaining a software application. One role is the “catalyst” developer, who provides the impetus for the launch of a decentralized open source project,⁸⁵ and as we shall see, subsequently recedes from the networks’ governance.⁸⁶ Another role is played by the developers who voluntarily contribute their efforts collaboratively and iteratively to an existing open source project.⁸⁷ Before analyzing these two roles more in depth, we should note that open source projects are often structured so that certain protocol developers have “commit access,” such access allowing them to incorporate changes into the public repository.⁸⁸ Further, while traditionally open source developers are unpaid volunteers, certain protocol developers are employed by businesses or foundations associated with the open source project to which they are contributing.⁸⁹

ii. Catalyst developers and network effects

While public blockchain networks can exhibit decentralizing tendencies⁹⁰ over time,⁹¹ out of necessity they begin with a sponsor, which

⁸⁴ Nick Szabo first described “smart contracts” in the late 1990s. See Nick Szabo, *Formalizing and Securing Relationships on Public Networks*, FIRST MONDAY (Sept. 1, 1997), <https://ojsphi.org/ojs/index.php/fm/article/view/548/469>. For our purposes, we define “smart contracts” as “a computer program (or executable computer code) that alters an account’s balance or status.”

⁸⁵ Jean Tirole & Josh Lerner, *The Simple Economics of Open Source* (2000 HBS FIN. WORKING PAPER No. 00-059).

⁸⁶ *Id.*

⁸⁷ *Id.*

⁸⁸ *Id.*

⁸⁹ For example, several of the Bitcoin Core developers are employed by the company Blockstream.

⁹⁰ See *Canaccord Report: Bitcoin Mining Becoming Less Centralized*, THE BITCOIN MAG (Feb. 6, 2019), <https://thebitcoinmag.com/canaccord-report-bitcoin-mining-becoming-less-centralized/3397> (stating that control of the Bitcoin network is becoming less concentrated over time).

⁹¹ SEC Director of Corporation Finance William Hinman acknowledged this potential in his description of the Ethereum network, leading him to conclude that current sales of Ether are not sales of securities. See William Hinman, *Digital Assets Transactions: When Howey Met Gary (Plastic)*, SEC (June 14, 2018), <https://www.sec.gov/news/speech/speech-hinman-061418>.

tends to be a centralized group or even a single individual. In fact, open source projects often share similar genesis stories associated with an individual who becomes frustrated by a circumstance, takes it upon herself to address the issue, and invites others to help along the way.

Agents responsible for beginning decentralized organizations (including open source projects such as Linux, Apache, Wikipedia, Craigslist, and even Alcoholics Anonymous) are referred to as “catalysts.”⁹² Catalysts play a dynamic role in the development of decentralized organizations, being critically important at the beginning, but incrementally stepping back and allowing others to make decisions as the project grows and matures, eventually ceding control.⁹³

The role of a catalyst developers is evident when looking at the Bitcoin and Ethereum networks. With the backdrop of the world financial crisis, “Satoshi Nakamoto” famously published the Bitcoin whitepaper in October 31, 2008 and soon after coded the very first Bitcoin software application,⁹⁴ releasing it in January 2009. She/he/they⁹⁵ interacted on web forums for a short time thereafter, before disappearing into oblivion without ever after being successfully identified. Satoshi’s ability to define the general architecture of the Bitcoin project, coalesce a community around Bitcoin and later disappear, makes Satoshi an archetypal catalyst developer.⁹⁶

Catalyst developers create the anchor point for network effects.⁹⁷ Decentralized open source projects and public blockchain networks, such as

⁹² See ORI BRAFMAN & ROD A. BECKSTROM, *THE STARFISH AND THE SPIDER: THE UNSTOPPABLE POWER OF LEADERLESS ORGANIZATIONS* (2008).

⁹³ Brafman and Beckstrom provide additional context describing catalysts arguing that “[i]n open organizations, a catalyst is the person who initiates a circle (a decentralized group with norms) and then fades away into the background... In letting go of the leadership role, the catalyst transfers ownership and responsibility to the circle... Once the catalyst leaves, however, his or her presence is still felt. The catalyst is an inspirational figure who spurs other to actions.” *Id.* at 92-93. In their seminal study of open source economics, Jean Tirole and Josh Lerner provide a similar account of the role of catalyst developers in the development of open source software projects noting that, “although the leader is often at the origin a user who attempts to solve a particular program, the leader over time performs less and less programming.” Josh Lerner & Jean Tirole, *The Simple Economics of Open Source* 21 (Nat’l Bureau of Econ. Research, Working Paper No. 7600, 2000).

⁹⁴ This client was later renamed “Bitcoin Core.” See *Bitcoin Core Version 0.9.0* released Mar. 19, 2014, <https://bitcoin.org/en/release/v0.9.0#rebranding-to-bitcoin-core> (last accessed Feb. 18, 2019).

⁹⁵ “The true identity of this person, or even group of people, is a well-kept secret.” See PAUL VIGNA & MICHAEL J. CASEY, *THE AGE OF CRYPTOCURRENCY: HOW BITCOIN AND DIGITAL MONEY ARE CHALLENGING THE GLOBAL ECONOMIC ORDER* 41 (2015).

⁹⁶ See Mike Orcutt, *Ethereum Founder Vitalik Buterin Says His Creation Can’t Succeed Unless He Takes a Step Back*, MIT TECHNOLOGY REVIEW (Nov. 1, 2018), <https://www.technologyreview.com/s/612372/ethereums-founder-vitalik-buterin-says-his-creation-cant-succeed-unless-he-takes-a-step/amp>.

⁹⁷ The archetypal example used to explain network effects is the invention of the telephone systems. At the point where there was one telephone in the world, the telephone network as a

the Bitcoin and Ethereum networks, exhibit strong positive network effects, which means that the more users who flock to the network, the more the value of the network increases for other users.⁹⁸ Therefore, in order for a public blockchain or other open source project to be successful and exhibit the value creation associated with network effects, the catalyst who launched the project will need to attract more participants to join the network and contribute their efforts. Incentivizing contributions from other developers is not an easy task and requires, at a minimum, that the catalyst developer (i) establish trust in the fundamentals of the project and her role in its governance, and (ii) provide opportunities for developers to build something that is seen as valuable and interesting by them and others in the community.⁹⁹

iii. *The incentives of developers contributing to open source projects*

Analyzing the issue from a different point of view, one may ask: what motivates skilled protocol developers to contribute to an existing open source project? Developers are generally highly technical workers who have the potential to be lucratively compensated for their work by modern technology firms.¹⁰⁰ Yet, by contributing to open source projects such as the Bitcoin or Ethereum project, developers are generally not directly

whole did not provide a very valuable service. However, each additional telephone that is connected to the network would add to the overall value. See Antonio Regalado, *The Economics of the Internet of Things*, MIT TECHNOLOGY REVIEW, (May 20, 2014), <https://www.technologyreview.com/s/527361/the-economics-of-the-internet-of-things>.

⁹⁸ See Christian Catalini & Joshua S. Gans, *Some Simple Economics of the Blockchain A-2* (Nat'l Bureau of Econ. Research, Working Paper No. 22952, 2018) (stating, "in proof-of-work systems, a blockchain is only as secure as the amount of computing power dedicated to mining it. This generates economies of scale and a positive feedback loop between network effects and security: as more participants use a cryptocurrency, its value increases, which in turn attracts more miners (due to higher rewards), ultimately increasing the security of the shared ledger.").

⁹⁹ According to Tirole and Lerner, the leader of an open source project "must (a) provide a vision, (b) make sure that the overall project is divided into much smaller and well-defined tasks ("modules") that individuals can tackle independently from other tasks, (c) attract other programmers, and last but not least, (d) 'keep the project together' (prevent it from forking or being abandoned)." Josh Lerner & Jean Tirole, *The Simple Economics of Open Source* 21 (Nat'l Bureau of Econ. Research, Working Paper No. 7600, 2000).

¹⁰⁰ According to the U.S. Bureau of Labor Statistics, the median yearly salary for software developers in 2017 was \$103,560. See *Occupational Outlook Handbook: Software Developers*, U.S. BUREAU OF LABOR STATISTICS (Apr. 13, 2018), <https://www.bls.gov/ooh/computer-and-information-technology/software-developers.htm#tab-1>.

remunerated and unlikely to get anything of direct value¹⁰¹ from their contributions unless the project ends up a success.¹⁰²

Nonetheless, developers contribute to open source projects in droves. Bitcoin was launched in 2009, and a decentralized group of developers has maintained the “Bitcoin Core” software application,¹⁰³ which as of February 2019 had over 18,000 revisions (or “commits”) implemented by over 570 individual contributors.¹⁰⁴ The Go-Ethereum software application has over 10,500 implemented by almost 400 contributors.¹⁰⁵ Let us examine this phenomenon.

1. *Social and psychological incentives*

The academic literature finds that contributors to the earliest open source software projects were motivated by the medium- to long-term social and psychological impact of their work, as opposed to motivation through short-term economic payoff.¹⁰⁶ Studies that focus on the open source economies that evolved with the invention of the Internet described developers’ motivations as “career concerns” and “ego gratification,” which is essentially reputational value they gained from being seen as a significant contributor to a successful open source project.¹⁰⁷ Open source economies exhibited stronger “signaling incentives,” which motivated developers to provide value to their community in hopes of being able to accrue reputational benefits from successful contributions down the line.¹⁰⁸

In addition, contributors to open source projects are often animated by an ideology which influences their decision-making over design and architectural choices. For example, the open source software movement was

¹⁰¹ As noted earlier in Section I (d) *infra* and discussed further in Section I (b) *supra*, this dynamic changes with Bitcoin’s introduction of cryptocurrency.

¹⁰² Developers’ contributions to an open source project are a sunk cost in the sense that, if the project is not successful, there is little developers will be able to take away from their contributions that has immediate value.

¹⁰³ In addition to the Bitcoin Core software application, there are 22 other software applications that can run on the Bitcoin network.

¹⁰⁴ See *bitcoin/bitcoin*, GITHUB, <https://github.com/bitcoin/bitcoin> (last visited Feb. 17, 2019).

¹⁰⁵ See *ethereum/go-ethereum*, GITHUB, <https://github.com/ethereum/go-ethereum> (last visited Feb. 17, 2019).

¹⁰⁶ LERNER & TIROLE, *supra* note 99, at 14, 24.

¹⁰⁷ *Id.* at 14.

¹⁰⁸ Tirole and Lerner argued that signaling incentives were relatively stronger (i) the more visible the performance to the relevant audience; (ii) the higher the impact of effort on performance, and (iii) the more informative the performance about talent. They noted how open source projects publicized the contributions of developers, increasing the signaling power of such efforts, by going through considerable efforts to make the nature of their decision-making process transparent, and giving credit to the authors is essential in the open source context. *Id.* at 24.

closely associated with the free and open source software (“FOSS”) ideology.¹⁰⁹ Similarly, the emergence of Bitcoin and other public blockchain networks is associated with the “cypherpunk” ideology, which was in part a reaction to the perceived shortcomings of the international financial system and a lack of privacy in modern societies.¹¹⁰

2. Economic incentives through native cryptocurrencies

While the developers contributing to the earliest open source software projects were mostly motivated by social and psychological factors,¹¹¹ the Bitcoin project inaugurated a new paradigm of open source production by introducing cryptocurrencies and gamification into open source economies. As noted in Section I (d), native cryptocurrencies provide a new mechanism design tool that could be used to influence the actions of network participants. For example, catalyst developers can come to acquire the cryptocurrencies by means of a pre-mined allocation. Contributing developers can also now be directly remunerated for their contributions with the native cryptocurrency. By owning the native cryptocurrency, these developers will be directly economically incentivized to attract more users to the network and drive demand for the native cryptocurrency, thereby leading to the appreciation of cryptocurrency’s value. Taken together with the long-term social and psychological drivers, including reputational gains and ideological motives, native cryptocurrency can be used to align the incentives of developers with other network participants towards a common goal.

c. How changes to software applications are made and the role of developers in implementing those changes in the network

This section seeks to describe the process through which changes to a software application of a public blockchain network are made. More importantly, it examines the role of protocol developers in the process of updating a software application and implementing it on the network.

¹⁰⁹ See Brooke Driver, Comment, *Risky Business: A Proposal to Limit Liability for Developers of Open Source Software*, 8 WAKE FOREST J. L. & POL’Y 1, 1 (2019).

¹¹⁰ “Therefore, privacy in an open society requires anonymous transaction systems.” Eric Hughes, *A Cypherpunk’s Manifesto*, ACTIVISM.NET (Mar. 9, 1993), <https://www.activism.net/cypherpunk/manifesto.html>.

¹¹¹ See LERNER & TIROLE, *supra* note 99.

i. Changes to a public blockchain's software application come from the political consensus of network participants

Public blockchain networks do not function in reliance on one single “code base,” but rather can support a range of software applications so long as they all conform to the consensus rules¹¹² of the network.¹¹³ In this sense, while Bitcoin Core is the original and most important software application on the Bitcoin network, it does not represent the totality of the network, nor does it have a monopoly over the consensus rules or the direction of development of the network.¹¹⁴ Similarly, Go-Ethereum is a popular software application for interacting with the Ethereum network,¹¹⁵ but it is not the only one. As we argue, the consensus rules and development direction of public blockchain networks are defined by the choices made by the economically significant¹¹⁶ network participants as to which software application to run.¹¹⁷

Public blockchain networks vary significantly in their architecture and design. Using the Bitcoin and Ethereum protocols as examples, the direct participants of the network (the “formal participants”) are (1) the network users (e.g., cryptocurrency holders) and (2) the network nodes (both miners and other nodes that run the software application). There are multiple other interested parties with influence over public blockchain governance (the “indirect participants”), including (3) developers (both protocol developers and others such as smart contract developers) and also (4) businesses that service the blockchain network and provide the related infrastructure

¹¹² DE FILIPPI & WRIGHT, *supra* note 3, at 40, 42-43 (“Consensus mechanisms [or consensus rules] make it possible for a distributed network of peers to record information to a blockchain, in an orderly manner, without the need to rely on any centralized operator or middleman.” Public blockchain consensus rules often include proof of work consensus mechanisms and incentivization structures.).

¹¹³ Networks maintain a set of consensus rules that they require of all blocks for compatibility. When users ultimately disagree about the sets of consensus rules to enforce, the result is a chain split. *Id.* at 24.

¹¹⁴ “The Bitcoin Core software project cannot change what software users are running and the users are a lot more independent minded than many people think, in our view.” *Competing with Bitcoin Core*, BITMEX RESEARCH (Oct. 15, 2018), <https://blog.bitmex.com/bitcoin-cores-competition>.

¹¹⁵ ETHEREUM HOMESTEAD, <http://ethdocs.org/en/latest/ethereum-clients/go-ethereum> (last visited Feb. 18, 2019).

¹¹⁶ Economically significant network participants are those with greater hashpower (or hash rate). Hashpower is the length of time (how fast) it takes a miner to solve the hash puzzle measured in billions of hashes per second. *See Hashrate*, UNBLOCK, <https://unblock.net/glossary/hashrate> (last visited Feb. 17, 2019).

¹¹⁷ “[Consensus] rules are defined by the clients economically significant users currently run.” *Id.*

(including equipment manufacturers and exchanges).¹¹⁸ In addition to the formal and indirect participants outlined above, public blockchain networks develop large communities composed of a diverse ecosystem. These ecosystems include many additional participants, including unaffiliated individuals willing to trade valuable services or assets for the native cryptocurrencies of the blockchain network or cryptographic tokens resulting from smart contracts that run on the network.

ii. *A multi-level coordination model of public blockchain governance*

Changes to a public blockchain network that affect the fundamental consensus rules of the protocol are rare, and when they do happen they occur as the result of informal coordination between the various participants through a complex multi-level political process.¹¹⁹

Vitalik Buterin, the catalyst for the Ethereum Network, provides a helpful framework for understanding public blockchain network governance and the role of developers in it. He describes blockchain network governance using a multi-layered “coordination model.”¹²⁰ At a fundamental—“Layer 1”—level, every formal participant has the ability to “run whatever software [application] they want in their capacity as a user, miner, participant, validator or whatever other kind of agent a blockchain protocol allows them to be.”¹²¹ As mentioned before, the bottom layer provides formal network participants with ultimate decision-making authority regarding what software application to run or whether to update the software application with new versions that exist. Due to the strong positive network effects experienced by public blockchain networks, the decision of each of the formal participants is influenced by their perception of other formal network participants’ likely choices. The informal participants coordinate the formal participants’ decision making. The native cryptocurrency of the network aligns the incentives of the network participants; participants all have a stake in maintaining or increasing the value of the native cryptocurrency.

As Vitalik Buterin conceptualizes it, operating above layer 1 are “coordination institutions” which “create focal points around how and when

¹¹⁸ Jeffery Atik, *Hard Forks on the Bitcoin Blockchain: Reversible Exit, Continuing Voice*, 1 STAN. J. BLOCKCHAIN L. & POL. 25 (2018).

¹¹⁹ “Blockchains are governed, and blockchain governance outcomes will be driven by the politics of participants in the public blockchain space.” Vlad Zamfir, *Blockchain Governance 101*, MEDIUM (Sept. 29, 2018), https://medium.com/@Vlad_Zamfir/blockchain-governance-101-eea5201d7992.

¹²⁰ Vitalik Buterin, *Notes on Blockchain Governance* (Dec. 17, 2017) <https://vitalik.ca/general/2017/12/17/voting.html>.

¹²¹ *Id.*

individuals should act in order to better coordinate behavior.”¹²² These coordinating institutions use their structural ability to signal preferences and steer the formal participants of a network towards collective decision-making.¹²³

In this context, protocol developers play a dual role in that they both (1) provide the “choices” for every formal participant to act on by maintaining and revising versions of a software application,¹²⁴ and (2) play the role of a coordinating institution in advocating for a change. Critically, protocol developers lack the ability to force software changes and updates on other network participants.

There are thus recursive value dependencies that bind the network participants: the value of the cryptocurrency is dependent upon the volume of transactions that use it, the volume of transactions is dependent upon the stability and reputation of the network, the stability of the network is dependent upon the miners that participate in the validation scheme, the validation schemes are provided by the protocol developers, the protocol developers are incentivized by the value of the native cryptocurrency they may hold (and the social and psychological factors discussed above), the miners are incentivized by the value of the cryptocurrency they may gain by participating in the validation scheme. Thus, native cryptocurrency is an integral driver in the PoW mechanism design.¹²⁵

iii. Lifecycle of a Bitcoin software application update

Updates to a public blockchain’s software application (including Bitcoin Core) can be proposed by anyone.¹²⁶ In the case of Bitcoin Core, small code enhancements or patches (which neither require standardization between projects nor relation to the network’s consensus rules) can be

¹²² *Id.* For example, BIP 9 was introduced to serve as a signaling mechanism for the Bitcoin protocol, enabling miners to indicate that they are prepared to implement a change by including information in the header of each block they mine.

¹²³ Vitalik provides a useful illustration describing coordination institutions “as putting up green or red flags in the air saying ‘go’ or ‘stop,’ with an established culture that everyone watches these flags and (usually) does what they say.” *Id.*

¹²⁴ “Most node operators don’t want to write much software, and it’s a technical challenge for anyone to independently write compatible implementations of any consensus protocol even if they have a specification. As a result, node operators rely on software repositories (usually hosted on Microsoft/GitHub servers) to provide them with the software they choose to run.” Zamfir, *supra* note 119.

¹²⁵ That is not to say that price manipulation is not a concern for cryptocurrencies. See Andrew Verstein, *Crypto Assets and Insider Trading Law’s Domain*, IOWA L. REV. (forthcoming 2019), <https://ssrn.com/abstract=3339551>; Paul Vigna & Alexander Osipovich, *Bots are Manipulating Price of Bitcoin in ‘Wild West of Crypto,’* WALL ST. J., Oct. 2, 2018, <https://www.wsj.com/articles/the-bots-manipulating-bitcoins-price-1538481600>.

¹²⁶ “Bitcoin is free software and any developer can contribute to the project.” *Bitcoin Development*, BITCOIN CORE, <https://bitcoin.org/en/development#code-review>.

suggested by opening an “issue” or responding to one of the open “pull requests” on the GitHub page, available publicly at <https://github.com/bitcoin/bitcoin>.¹²⁷

Major changes to the Bitcoin Core software application are suggested through Bitcoin Improvement Proposals (“BIPs”).¹²⁸ Each BIP is proposed by an individual—referred to as a “champion”—who drafts the proposal in the required style and format¹²⁹ and initiates discussions on Internet forums. Most importantly, once the BIP has been drafted, the champion must leverage her prestige and persuade others to support her idea.¹³⁰

The BIP submission process is broken up into several stages. During the first informal stage, a champion presents a BIP in draft form to the Bitcoin community, including by sharing the idea with the Bitcoin development mailing list.¹³¹ This public draft of the BIP is intensely studied, debated, tested and refined by the community, enabling the BIP’s champion to flesh out the draft and address any initial concerns.

Once a BIP has been “socialized” with the community and is properly formatted, it may be submitted to the publicly available Bitcoin GitHub repository as a “pull request,” which is analogous to a request for change.¹³² At this point, an editor (the “BIP Editor”)¹³³ will decide whether to accept the pull request to the Bitcoin Core BIP repository. While the BIP Editor has the nominal power to reject a BIP at this stage, the risk of censorship is ameliorated in practice because all GitHub pull requests are publicly available online.¹³⁴ Bitcoin Core’s policy calls for a liberal standard of BIP

¹²⁷ Available at <https://github.com/bitcoin/bitcoin>.

¹²⁸ Amir Taaki submitted the first-ever BIP, BIP 1, in August 19, 2011, where he laid out the original BIP workflow. BIP 1 was subsequently replaced by BIP 2 submitted by Luke Dashjr in February 3, 2016. According to BIP 2, “A BIP is a design document providing information to the Bitcoin community, or describing a new feature for Bitcoin or its processes or environment. The BIP should provide a concise technical specification of the feature and a rationale for the feature.” BIP 1 is available at <https://github.com/bitcoin/bips/blob/master/bip-0001.mediawiki>; BIP 2 is available at <https://github.com/bitcoin/bips/blob/master/bip-0002.mediawiki>.

¹²⁹ BIP 2 requires that all BIPs contain the following parts: (i) Preamble - Headers containing metadata about the BIP; (ii) Abstract - A short (~200 word) description of the technical issue being addressed; (iii) Copyright - The BIP must be explicitly licensed under acceptable FOSS license; (iv) Specification - Description of the syntax and semantics of any new features; (v) Motivation - Explanation of why the existing protocol is inadequate to address the problem that the BIP solves; (vi) Rationale - Description of what motivated the design; (vii) Backwards compatibility - Description of any backwards incompatibilities; and (viii) Reference implementation - Test code.

¹³⁰ See *id.* See also *supra* note 128.

¹³¹ See *bitcoin-dev - Bitcoin Protocol Discussion*, LINUX FOUNDATION, <https://lists.linuxfoundation.org/mailman/listinfo/bitcoin-dev> (last visited Feb. 18, 2019).

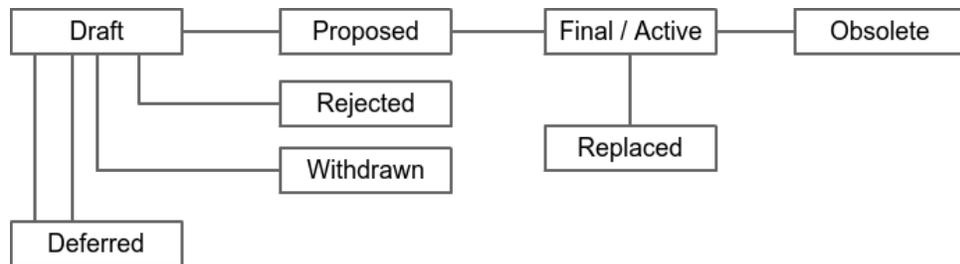
¹³² The repository is located at <https://github.com/bitcoin/bips>.

¹³³ The current Bitcoin Core BIP Editor is Luke Dashjr, who can be contacted at luke_bipeditor@dashjr.org.

¹³⁴ The GitHub pull requests are publicly available at <https://developer.github.com/v3/pulls>.

acceptance that focuses on formatting and technical requirements over a normative judgment of the BIP.¹³⁵ Moreover, a developer who has her BIP censored by the Bitcoin Core BIP Editor may implement her desired change by “soft forking” the Bitcoin Core code and launching her own software application on the Bitcoin network or resorting to a “hard fork” that splits the network. “Forking” is described in Section II (c) below.

Once a BIP has been accepted and merged into the Bitcoin Core repository, the BIP Editor will assign the BIP a number,¹³⁶ label it according to its formal type,¹³⁷ and give the BIP the status of “Draft.” From Draft status, the BIP can progress according to the flowchart laid out below, with “Active” referring to a BIP that has been implemented¹³⁸:



¹³⁵ BIP 2 states “*The BIP editor will not unreasonably reject a BIP*. Reasons for rejecting BIPs include duplication of effort, disregard for formatting rules, being too unfocused or too broad, being technically unsound, not providing proper motivation or addressing backwards compatibility, or not in keeping with the Bitcoin philosophy.” (*emphasis added*). See instructions in Bitcoin Core’s GitHub page stating that “People wishing to submit BIPs, first should propose their idea or document to the bitcoin-dev@lists.linuxfoundation.org mailing list. After discussion, please open a PR. After copy-editing and acceptance, it will be published here. *We are fairly liberal with approving BIPs, and try not to be too involved in decision making on behalf of the community*. The exception is in very rare cases of dispute resolution when a decision is contentious and cannot be agreed upon. In those cases, the conservative option will always be preferred. Having a BIP here does not make it a formally accepted standard until its status becomes Final or Active.” Available at <https://github.com/bitcoin/bips> (*emphasis added*).

¹³⁶ Champions do not number the BIPs they propose when submitting them to the Git repository, but instead give the BIP a descriptive name. The BIP Editor assigns each BIP a number based on a predetermined classification system based on the layer of the Bitcoin protocol which the BIP modifies, with lower-number layers involving more intricate interoperability requirements. See BIP 123, <https://github.com/bitcoin/bips/blob/master/bip-0123.mediawiki>.

¹³⁷ There are three kinds of BIPs: (i) “Standard Track BIPs” which describe any change that affects most or all Bitcoin implementations, such as a change to the network protocol and are the type of BIP with which we are concerned in this paper; (ii) “Informational BIPs” which describe a Bitcoin design issue, or provide general guidelines or information to the community; and (iii) “Process BIPs” which describe a process surrounding Bitcoin, or proposes a change to a process. See BIP 2, *supra* note 135.

¹³⁸ *Id.*

A champion can change the status of a BIP from Draft → Withdrawn or Deferred. However, a BIP's path from Draft → Proposed → Active (but not yet Final or implemented on the Bitcoin network) requires buy-in from the Bitcoin Core developer “technocracy.” This entails the BIP achieving a “rough consensus”¹³⁹ amongst active developers on the mailing list.¹⁴⁰

For a BIP to get from Draft status to Final status (meaning implemented on the Bitcoin network) it must be adopted by the formal participants of the Bitcoin network, which we have seen play a separate role from that of the protocol developers. This is a key point. Protocol developers do not formally “touch” the blockchain; they can only propose changes to a certain software application. Implementation of any changes to a public blockchain network, such as a BIP, requires the consensus of the formal participants, which are influenced by the indirect participants in a multi-layered coordination-model.

There are two paths that a BIP can take to go from Final → Final status and be implemented on the Bitcoin network.

1. *Soft forks*

Certain BIPs propose a “tightening” of the consensus rules of the Bitcoin protocol (i.e., the ruleset is narrowed, disallowing new blocks that previously would have been valid) and thus require only a “soft fork” to be implemented. These types of modifications are said to be “backwards compatible” because full nodes (other than miners) are not required to upgrade to the implementing software application to maintain consensus in the network (given that full nodes running the old, non-implementing software application will still be able to accept new blocks generated by the miners running the new implementing software application). As such, implementing a soft fork BIP requires only adoption of the miners, usually through a supermajority “vote” of 95% of active hashpower.¹⁴¹

To facilitate reaching consensus amongst miners, procedures such as a Miner Activated Soft Fork (“MASF”) have been devised that allow miners to signal their support for a particular BIP by including messages or “flags” in the headers of the blocks they successfully mine. As miners raise flags over time, a group position emerges. MASFs therefore function “as a kind

¹³⁹ A “rough consensus” is reached when a proposed BIP has been “open to discussion on the development mailing list for at least one month, and no person maintains any unaddressed substantiated objections to it. Addressed or obstructive objections may be ignored / overruled by general agreement that they have been sufficiently addressed, but clear reasoning much be given in such circumstances.” *Id.*

¹⁴⁰ *Id.*

¹⁴¹ See, e.g., Jimmy Song, *Why the UASF Segwit Scenario is Hopelessly Naïve*, MEDIUM (Apr. 18, 2017), <https://medium.com/@jimmysong/why-the-uasf-segwit-scenario-is-hopelessly-naive-70338711bc3c>.

of pre-election polling, gauging sentiment and promoting the formation of a common understanding of what will come to pass.”¹⁴²

Miners truly “vote” on whether to implement a BIP by choosing whether to apply their computational power to mine on the network that implements the software application. Given the positive network effects of public blockchain networks, when deciding whether to mine to validate the implementing or non-implementing software application, miners must anticipate which version of the software application the broader community will coalesce around. Scholars have therefore argued that “[a] miner’s ‘vote’ is better understood as its prediction of the collective stance of the broader miner community than as an expression of the voting miner’s individual preference.”¹⁴³

The “economic majority,” a term referring to a combination of network users and other indirect participants such as wallets and exchanges, exerts indirect influence over the adoption of soft forks. Mining is a for-profit industry in which profits are determined in large part by the cost of computational power to mine in relation to the value of the cryptocurrency being mined. Therefore, a key factor in a miner’s decision framework (i.e., which version of the software application to run and which history to adopt) is the effect that a certain proposed code change will have on the value of the cryptocurrency. The value of the cryptocurrency is in turn determined by those willing to offer things of value in exchange for the underlying cryptocurrency (be it goods, services, fiat currencies, or other cryptoassets). Therefore, while soft forks can be normatively implemented without direct user participation, given the profit-motive of miners, the economic majority’s preferences are ultimately reflected in a miners’ decision-making framework.

As an example, the economic majority can employ coordination procedures, such as a User Activated Soft Fork (a “UASF”), to exert leverage over the miners in the context of a potential soft fork.¹⁴⁴ As implemented in connection with BIP 16, the USAF entitled full nodes and other informal participants to signal support for a “flag day” upon which all participating full nodes would be committed to upgrade to a new software application and reject blocks produced by miners running the old non-implementing software application. In connection with BIP 148, the contentious SegWit update which was the centerpiece of Bitcoin Core’s project to enable increase the volume of transactions batched, the UASF only required a certain threshold of users to signal for approval given that a

¹⁴² Atik, *supra* note 118, at 30-31 (noting that MASFs have been used to successfully activate multiple soft forks in the past, including BIP 65 and BIP 112. However, it led to issues with BIP 66 when hashpower indicated most miners had upgraded when in fact they had not).

¹⁴³ *Id.* at 28.

¹⁴⁴ See BIP 148 implementing SegWit; BIP 16 implementing Pay-to-Script-Hash.

substantial percentage of the network had already upgraded to the implementing software application. While miners are still required to implement a “User Activated” Soft Fork, the mechanism works as a signaling strategy to influence miners’ decisions to implement a BIP out of fear of losing the block rewards by building on a minority chain.¹⁴⁵

2. *Hard forks*

Network participants can also exert influence over a public blockchain’s governance through “hard forks.” As opposed to soft forks, hard forks implement code changes that “loosen” the consensus rules of a blockchain’s protocol (i.e., the ruleset becomes broader, allowing for previously disallowed blocks to be treated as valid). Hard forks are therefore not backwards compatible, in the sense that full nodes which do not upgrade to the new implementing software application (or simply implement a software application with different consensus rules and create a new chain) will not accept blocks created by miners running the upgraded software application. While soft forks can be implemented by miners only, the implementation of hard forks requires every formal participant to choose to upgrade to the new implementing software application. Hard forks therefore represent a “permanent divergence from the previous version of the Blockchain.”¹⁴⁶

Critically, a “hard fork” serves as the ever-present escape valve accessible to any network user or informal participant who finds available software applications disagreeable.¹⁴⁷ It effectively allows any individual to copy the current publicly-available source code of a certain public blockchain’s software application, modify it to reflect a new ruleset, re-release it to the public and coalesce a community around the revised protocol.¹⁴⁸ In this way, hard forks ensure “the community as a whole can never be forced to adopt undesirable changes to Bitcoin.”¹⁴⁹ For example,

¹⁴⁵ See, e.g., Jimmy Song, *Bitcoin, UASF and Skin in the Game*, MEDIUM (May 29, 2017), <https://medium.com/@jimmysong/bitcoin-uasf-and-skin-in-the-game-7695031c5689>.

¹⁴⁶ See Andrew Tar, *UASF vs. UAHF, Explained*, COINTELEGRAPH (July 19, 2017), <https://cointelegraph.com/explained/uasf-vs-uahf-explained>. See also DE FILIPPI & WRIGHT, *supra* note 3, at 24.

¹⁴⁷ See Alphonse Pace, *Chain Splits and Resolutions*, MEDIUM (Mar. 7, 2017), <https://medium.com/@alpalpalp/chain-splits-and-resolutions-d3398bddf4ab>.

¹⁴⁸ “[A] portion of the community that questions the legitimacy of a governance decision can make a copy of the blockchain network (and corresponding software repositories) and maintain a ‘fork’ of the blockchain outside of the governance of the original chain.” See Zamfir, *supra* note 119. For example, Nakamoto’s original code has now been forked over 22,000 times, per <https://github.com/bitcoin/bitcoin>.

¹⁴⁹ See Alex Galea, *Bitcoin Development: Who Can Change the Core Protocol?*, MEDIUM

should a bad actor or group take the Bitcoin Core software application in a poor direction, the broader community would have the ability to reverse the undesired change or make new modifications and launch a new project.¹⁵⁰

While copying a publicly available software application might seem simple in theory, hard forks have limitations and are costly in practice.¹⁵¹ By potentially splitting a community in two, hard forks threaten the value creation and efficiencies derived from network effects. Further, hard forks can result in contentious disputes over which of the post-fork chains get to use the pre-fork trademark.¹⁵² However costly in terms of compromising network effects, hard forks provide an “exit” option to formal participants of a public blockchain that ensures they will not have “crammed down” a version of the code they do not support.

Hard forks thus provide a viable avenue to minimize risks of undue influence on the code by third parties.¹⁵³ Formal participants are able to “vote with their feet.”¹⁵⁴

(Mar. 30, 2018), <https://medium.com/@galea/bitcoin-development-who-can-change-the-core-protocol-478b8ac5fe43>.

¹⁵⁰ “Therefore, concerns about the Bitcoin Core software repository becoming deleted, hacked or hijacked should be far less of an issue than many people think. If this happens it will not affect clients users are already running and if further upgrades or improvements are needed, one can simply switch to a different repository or many different repositories, without worrying about any coordination problem or other risks.” See *Competing with Bitcoin Core*, BITMEX (Oct. 15, 2018), <https://blog.bitmex.com/bitcoin-cores-competition>.

¹⁵¹ A recent study noted “that forked assets consistently underperform their parents [which] runs contrary to the commonly articulated belief that value can easily be forked as users readily switch between networks.” See BlockChannel, *A Brief Study of Cryptonetwork Forks*, MEDIUM

(Sept. 24, 2018), <https://medium.com/blockchannel/a-brief-study-of-cryptonetwork-forks-1377791d0354>. Vlad Zamfir described this as the “power law rule [which] means that even though it is very possible to fork, there will only ever be a small number of forks that are ultimately successful enough to be considered a ‘major blockchain.’ As a result, the blockchain governance regimes of a small number of major blockchains will determine governance outcomes for the entire blockchain space.” See Zamfir, *supra* note 119.

¹⁵² See Ciaran Murray, *Are Public Blockchain Systems Money Services Business In Disguise*, RULES OF THE GAME (Oct. 12, 2017), <http://rulesofthegame.blog/2017/10/12/are-public-blockchain-systems-money-services-businesses-in-disguise>. See also Zamfir, *supra* note 119.

¹⁵³ Scholars have dismissed the significance of hard forks by analogizing them to the ability of a public shareholder to exit their investment by selling her shares, arguing that this ability to “exit” does not negate the fiduciary duties owed to the holder by public company directors. See Angela Walch, *In Code(rs) We Trust: Software Developers as Fiduciaries in Public Blockchains* 12 (July 19, 2018),

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3203198. (“Much is made of token-holders ‘right to exit’ via the forking process or selling the token, but the ability to exit should not be relevant to the fiduciary analysis; shareholders of publicly-registered stock can always exit by selling the stock, yet are still owed fiduciary duties by officers and directors of the company.”). These views assume that blockchain developers have open control and the ability to bind network participants to software application changes. As we argue in Section IV (b), the analogy of cryptocurrency holders to shareholders does not hold up given that

d. Lifecycle of an Ethereum Update

Similar to Bitcoin, the Ethereum community employs an improvement process. That process involves the creation of an Ethereum Improvement Proposal (“EIP”) that is a “design document providing information to the Ethereum community, describing a proposed new feature or its processes or environment.”¹⁵⁵ More specifically, as detailed on the Ethereum GitHub website, EIPs “describe standards for the Ethereum platform, including core protocol specifications, client APIs, and contract standards.”¹⁵⁶ As with Bitcoin, anyone can submit EIPs that may or may not be accepted by the community.¹⁵⁷

There is an inherent distinction between Ethereum and Bitcoin that should be understood; this distinction informs the identification of different types of blockchain developers.¹⁵⁸ Bitcoin’s protocol supports few payment-transfer functions; its protocol would have to change to support more complex functionality that is associated with general computing.¹⁵⁹ The Ethereum blockchain supports the development of general computing programs (called smart contracts, as discussed previously) by anyone,¹⁶⁰ and the creation and accessibility of such programs do not require an EIP; any smart contract developer can create such accessible programs on the Ethereum blockchain without any action or oversight by a protocol developer.¹⁶¹ In this way, Ethereum can be thought of as a platform that enables programming projects orchestrated by organizations other than the Enterprise Ethereum Alliance, Ethereum’s catalyst sponsor. Among these projects were those that created tokens for the purposes of raising capital for ventures (called initial coin offerings [“ICOs”] or token sales).¹⁶² Protocol developers’ commits do not generate or destroy the cryptoasset tokens that are the center of ICO litigation. Smart contract developers create those

public company directors are able to *bind* shareholders, while protocol developers cannot bind cryptocurrency holders.

¹⁵⁴ Verstein, *supra* note 125.

¹⁵⁵ See ANTONOPOULOS, *supra* note 73, at xxvii.

¹⁵⁶ See *EIPs*, GITHUB (Aug. 7, 2018),

<https://github.com/ethereum/EIPs/blob/master/README.md> (last accessed February 18, 2019).

¹⁵⁷ *Id.*

¹⁵⁸ Shaanan Cohney et al., *Coin-Operated Capitalism*, 119 COLUM. L. REV. 591 (2019).

¹⁵⁹ *Id.*

¹⁶⁰ *Id.*

¹⁶¹ DE FILIPPI & WRIGHT, *supra* note 3, at 28. See also ANTONOPOULOS & WOOD, *supra* note 73.

¹⁶² See Cohney et al., *supra* note 158.

tokens through the creation of smart contracts that they deploy on the network directly.¹⁶³

III. PROTOCOL DEVELOPERS IN MOMENTS OF CRISIS

The capitalization of blockchain cryptoassets was over twelve billion USD¹⁶⁴ and has increased by billions since.¹⁶⁵ Along with the rise of cryptoassets having real market value is an increase in crises resulting from hacks and exploits of token exchanges and smart contracts, leading to losses of over one billion USD to date.¹⁶⁶ These hacks and exploits are often the result of bugs in the software code.

a. The Ethereum Hard Fork

The decision to fork or not fork is one taken by network participants during moments of crisis.¹⁶⁷ At least two major exploits have touched the history of the Ethereum network. These compromises provide a lens into the operations of developers and whether the actions taken by protocol developers warrant the safeguards provided by the corporate fiduciary duty.

As mentioned in the introduction, The DAO, an unincorporated organization run by the founders of Slock.it UG,¹⁶⁸ is a German corporation that works on IoT infrastructure.¹⁶⁹ Theda project ran on the Ethereum blockchain through the actions of smart contract developers. The project had the “objective of operating as a for-profit entity that would create and hold a corpus of assets through the sale of DAO tokens to investors, which assets would then be used to fund ‘projects.’”¹⁷⁰ After \$150 million worth of tokens were sold, a flaw in the smart contract code was exploited, resulting in the theft¹⁷¹ of about \$50 million worth of tokens in the summer months of 2016.¹⁷²

¹⁶³ See *id.* at 13.

¹⁶⁴ See Simone Porru et al., *Blockchain-oriented Software Engineering: Challenges and New Directions* (2017), https://www.researchgate.net/publication/313844963_Blockchain-oriented_Software_Engineering_Challenges_and_New_Directions.

¹⁶⁵ Cohny et al., *supra* note 158, at 14.

¹⁶⁶ See Porru et al., *supra* note 164 (summarizing that these attacks and exploits have resulted in over 1 billion USD losses).

¹⁶⁷ DE FILIPPI & WRIGHT, *supra* note 3, at 24 (“At times, forks occur as a result of a network split, possibly due to a network attack...At other times, forks occur...because of an actual refusal to adopt the technical changes embodied in a new codebase.”).

¹⁶⁸ THE DAO REPORT OF INVESTIGATION PURSUANT TO SECTION 21(A) OF THE SECURITIES EXCHANGE ACT OF 1934: THE DAO 1 (2017).

¹⁶⁹ *Id.*

¹⁷⁰ *Id.*

¹⁷¹ There is debate over whether the DAO Exploiter violated any laws. See Drew Hinkes, *A Legal Analysis of the DAO Exploit and Possible Investor Rights*, BITCOIN MAGAZINE (June

Arguably, participants in The DAO network were put on notice that the smart contract code superseded any representations or warranties. The purchasers of The DAO token were put on notice of this Term on The DAO website:

The terms of The DAO Creation are set forth in the smart contract code existing on the Ethereum blockchain at 0xbb9bc244d798123fde783fcc1c72d3bb8c1894. Nothing in this explanation of terms or in any other document or communication may modify or add any additional obligations or guarantees beyond those set forth in The DAO's code. Any and all explanatory terms or descriptions are merely offered for educational purposes and do not supersede or modify the express terms of The DAO's code set forth on the blockchain; to the extent you believe there to be any conflict or discrepancy between the descriptions offered here and the functionality of The DAO's code at 0xbb9bc244d798123fde783fcc1c72d3bb8c1894, The DAO's code controls and sets forth all terms of The DAO Creation.¹⁷³

This is only one of many disclosures that the DAO put out. Another statement published by The DAO reads:

The DAO's smart contract code governs the Creation of DAO tokens and supersede any public statements about The DAO's Creation made by third parties or individuals associated with The DAO, past, present and future. The software code currently available at <https://github.com/slockit/dao> is the sole source for the terms under which DAO tokens may be created.¹⁷⁴

Risks

The Creation of DAO tokens carries with it significant risk. Prior to Creating DAO tokens, carefully consider the exemplary and non-exhaustive list of risks set forth below

21, 2016), <https://bitcoinmagazine.com/articles/a-legal-analysis-of-the-dao-exploit-and-possible-investor-rights-1466524659>.

¹⁷² See THE DAO REPORT, *supra* note 168.

¹⁷³ Adam J. Kolber, *Not-So-Smart Blockchain Contracts and Artificial Responsibility*, 21 STAN. TECH. L. REV. 198, 200 (2018).

¹⁷⁴ Drew Hinkes, *A Legal Analysis of the DAO Exploit and Possible Investor Rights*, NASDAQ (June 21, 2016), <https://www.nasdaq.com/article/a-legal-analysis-of-the-dao-exploit-and-possible-investor-rights-cm638561>.

and, to the extent necessary, consult a lawyer, accountant, and/or tax professionals prior to Creating DAO tokens.

1. Risk of Security Weaknesses in The DAO's Software

The DAO concept is both experimental in nature and unproven. There is a risk that, as an open source project, any contributor to The DAO's software could introduce weaknesses or bugs into the DAO software, causing the loss of DAO tokens or ETH in one or more or even all of the DAO Token Holder's accounts.

2. Risk of Weakness in the DAO underlying blockchain, and/or Ethereum Network

The DAO software is itself based on an unproven platform: the Ethereum blockchain. There is a risk that, as an open source project, any contributor to the Ethereum blockchain could introduce weaknesses or bugs into the Ethereum software, causing the loss of DAO tokens or ETH in one or more or even all of the DAO Token Holder's accounts.

3. Risk of unforeseen attack vectors

The field of Digital Cryptography is very new and for this reason, there is a risk of unforeseen attack both in terms of the underlying cryptographic protocol that back the functioning of the DAO as well as 'game theory' related vectors which have not been documented to date. Both these vectors represent a risk that could lead the loss of DAO tokens or ETH in one or more or even all of the DAO Token Holder's accounts.¹⁷⁵

The DAO appeared to admit that its platform was in an experimental state and explained risks. In so doing, it can be inferred that The DAO wanted to shift liability away from itself and its smart contract developers through, in so many words, caveat emptor.

This preemptive shift in liability does not mean that the smart contract developers were totally careless programmers; among the several safeguards smart contract developers built into The DAO smart contract was a withdrawal latency of twenty-eight days.¹⁷⁶ This window of time proved to be critical; it was used by the Ethereum protocol developers to organize the Ethereum community to decide what to do while the attacker could not

¹⁷⁵ *Id.*

¹⁷⁶ ANTONOPOULOS & WOOD, *supra* note 73, at 327.

exchange stolen DAO tokens for ether, the native cryptocurrency of the Ethereum ecosystem.¹⁷⁷

A soft fork of the system was considered by Ethereum protocol developers and nearly reached execution stage,¹⁷⁸ but ultimately the soft fork plans were abandoned because there was a denial of service exploit in the soft fork.¹⁷⁹ The Ethereum developers had about twenty-two days left before the attacker would be able to convert DAO tokens into ether.¹⁸⁰ The Ethereum protocol developers, facing a closing window in which to fully resolve the effects of the theft, concluded that a hard fork would be the best option.¹⁸¹

Even then, with this conclusion that a hard fork was the best option, the protocol developers decided to create a software application allowing network participants (Layer 1 of Buterin's conceptual model) to decide whether or not to enable the fork.¹⁸² Whether or not the default should be for a client to opt-in (for the hard fork) or opt-out (against the hard fork) was debated.¹⁸³ Ultimately, a vote was opened on carbonvote.com,¹⁸⁴ where users could vote based on their ether supply. Of the 80% of the ether supply that voted,¹⁸⁵ 80% voted for opting-out to be the default. Thus, the decision to have the opt-out of the fork as the default was finalized.¹⁸⁶ Five days later, Ethereum implemented a hard fork that resulted in two Ethereum networks: one with a state change that essentially returned the value of DAO tokens, which is the modern day Ethereum; and the other that continued with the effects of the attack in its blockchain history, Ethereum Classic.¹⁸⁷

The present-day Ethereum gained a majority of the mining power, but Ethereum Classic had a sizeable community of 10% of the mining power and value.¹⁸⁸ All Ethereum users who held ether at the time of the fork had funds on both blockchains (ETH for Ethereum and ETC for Ethereum Classic), and soon the exchange Poloniex listed ETC.¹⁸⁹

¹⁷⁷ *Id.* at 327.

¹⁷⁸ See Felix Lange, *Security Alert - DoS Vulnerability in the Soft Fork*, ETHEREUM BLOG (June 28, 2016), <https://blog.ethereum.org/2016/06/28/security-alert-dos-vulnerability-in-the-soft-fork>.

¹⁷⁹ ANTONOPOULOS & WOOD, *supra* note 73, at 327.

¹⁸⁰ *Id.* at 327-328.

¹⁸¹ *Id.*

¹⁸² *Id.*

¹⁸³ *Id.*

¹⁸⁴ *Id.* This website is still used by the Ethereum community to vote on software update proposals. See <http://carbonvote.com>.

¹⁸⁵ Only 5.5% of the total supply voted in this one-day window. ANTONOPOULOS & WOOD, *supra* note 73, at 328.

¹⁸⁶ ANTONOPOULOS & WOOD, *supra* note 73, at 327-29.

¹⁸⁷ *Id.* at 327-330.

¹⁸⁸ *Id.* at 328.

¹⁸⁹ *Id.*

This incident illustrates a number of different aspects about the Ethereum protocol developers. Assuming *arguendo* that the protocol developers had an agenda to cram down a hard fork so that history of The DAO exploit was universally erased, it was not successful; the Ethereum Classic community retained the history of the exploit, and that blockchain and community exist to this day.¹⁹⁰ Second, even when committing the code to hard-fork, the hard fork was effectuated by Layer 1 formal participants adopting the software update of the hard fork.¹⁹¹

In January 2019, recent to the time of this writing, the Ethereum Classic blockchain network detected a 51% attack on the network, in which one entity controlled the majority (at least 50%) of the mining computational power and altered the transaction history of that blockchain.¹⁹² As discussed above, the Ethereum Classic blockchain network is the result of the minority mining community that chose to not adopt a hard fork to mitigate the effects of The DAO exploit.¹⁹³ It is possible that this network's vulnerability is a result of the mining power that left it for the present-day Ethereum network.¹⁹⁴ The hard fork resulted in a near reset of network effects for the Ethereum Classic community.¹⁹⁵ This illustrates that hard forking can impair the robustness, and therefore security, of the resulting blockchain networks. However, the miners did vote with their feet,¹⁹⁶ and the protocol developers did not and could not force the fork on anyone.¹⁹⁷

There are notably poor blockchain smart contract development practices,¹⁹⁸ like the lack of adequate testing to prevent The DAO smart contract code exploit,¹⁹⁹ and there are compelling reasons why a disclaimer attempting to negate representations should not shield public smart contract

¹⁹⁰ *Id.* at 330.

¹⁹¹ *Id.*

¹⁹² Jose Antonio Lanz, *Hacker Responsible for 51% Attack Against Ethereum Classic Returns Part of the Stolen Funds*, EWN (Jan. 13, 2019), <https://ethereumworldnews.com/hacker-51-percent-attack-ethereum-classic-returns-funds>. Interestingly, the value taken as a result of the 51% attack was returned.

¹⁹³ ANTONOPOULOS & WOOD, *supra* note 73.

¹⁹⁴ Michael J. Casey, *The Ethereum Classic Attacker Has Sent a Bigger Message*, COINDESK (Jan. 14, 2019), <https://www.coindesk.com/the-ethereum-classic-attacker-has-sent-a-bigger-message>.

¹⁹⁵ *Id.*

¹⁹⁶ Verstein, *supra* note 125.

¹⁹⁷ ANTONOPOULOS & WOOD, *supra* note 73.

¹⁹⁸ Giuseppe Destefanis, et al., *Smart Contracts Vulnerabilities: A Call for Blockchain Software Engineering?*, BLOCKCHAIN ORIENTED SOFTWARE ENGINEERING (IWBOSE) 2018 INTERNATIONAL WORKSHOP 19-25 (2018) (stating “[t]he feeling of many software engineers about such huge interest in Blockchain technologies and, in particular, on the many software projects rapidly born and quickly developed around the various Blockchain implementations or application, is that of unruly and hurried software development.”).

¹⁹⁹ *See* Kolber, *supra* note 173.

development organizations from any culpability or liability.²⁰⁰ However, these failures should not and need not be imputed to all blockchain developers alike; as The DAO hard fork events show, the *protocol developers* helped remedy the situation caused by the exploitation of the smart contract developer's code. The protocol developers helped to coordinate and execute the will of the cryptocurrency holders with utmost consideration and under the constraints of little time. They also did not cram down changes on the community, but rather created the remedy-implementing software option for members who wanted to support a blockchain history that did not recognize the theft.²⁰¹

b. The Bitcoin Core secret update

Developing, maintaining, and understanding blockchain systems are complex tasks that run the risk of errors being made and bugs being introduced into the codebase for the blockchain systems.²⁰² Recently, a secret update was applied to the most popular Bitcoin client software, Bitcoin Core, to fix a bug that would have allowed a miner to artificially inflate the supply of bitcoin.²⁰³

Through the Bitcoin Core bug reporting system, an anonymous individual reported a bug which enabled a distributed denial of service

²⁰⁰ Brian Quintenz, commissioner of the CFTC, stated a hypothetical about an event contracts run through smart contracts on a blockchain network and discussed which party could be accountable for such an activity. He concluded that the smart contract developers were most appropriate, stating, "I think the appropriate question is whether these code developers could reasonably foresee, at the time they created the code, that it would likely be used by U.S. persons in a manner violative of CFTC regulations. In this particular hypothetical, the code was specifically designed to enable the precise type of activity regulated by the CFTC, and no effort was made to preclude its availability to U.S. persons. Under these facts, I think a strong case could be made that the code developers aided and abetted violations of CFTC regulations. As such, the CFTC could prosecute those individuals for wrongdoing." *Remarks of Commissioner Brian Quintenz at the 38th Annual GITEX Technology Week Conference*, CFTC (Oct. 16, 2018), <https://www.cftc.gov/PressRoom/SpeechesTestimony/opaquintenz16>.

²⁰¹ Protocol developers can be smart contract developers as well, but they often are not. When creating liability frameworks to apply categorically, it makes sense to distinguish the hats involved, if/when the same person is wearing more than one.

²⁰² For a general discussion of the difficulties inherent in blockchain development posed by the lack of clarity surrounding the technology, see RAND Europe, *Understanding the landscape of Distributed Ledger Technologies/Blockchain: Challenges, opportunities, and the prospects for standards*, 13, https://www.rand.org/content/dam/rand/pubs/research_reports/RR2200/RR2223/RAND_RR2223.pdf.

²⁰³ Alyssa Hertig, *The Latest Bitcoin Bug Was So Bad, Developers Kept Its Full Details a Secret*, COINDESK (Sept. 24, 2018), <https://www.coindesk.com/the-latest-bitcoin-bug-was-so-bad-developers-kept-its-full-details-a-secret>.

attack on the Bitcoin Core client.²⁰⁴ In analyzing the reported bug, a second bug was discovered that would have enabled a miner to artificially inflate the supply of Bitcoin.²⁰⁵ This second bug was kept secret by the Bitcoin Core developers until a patch for both bugs was published to the community.²⁰⁶ Later, an individual independently discovered the second bug, and consequently the Bitcoin Core team published their recounting of the bug and the associated timeline.²⁰⁷

The Bitcoin Core developers keeping the bug secret raises the question of what safeguards should exist from developers exploiting that information to the detriment of network participants, and what recourse, if any, network participants should have against the developers. A user of the blockchain system could bring a claim of unfair trade practices alleging fraud against the developers that kept the bug secret, particularly, under Section 5 of the Federal Trade Commission Act.²⁰⁸ Additionally, or alternatively, a potential claim of insider trading could be brought against any developers trading on non-public information.²⁰⁹ Andrew Verstein notes that “crypto assets are subject to at least enough of the insider trading jurisprudence to allow federal prosecutors to bring successful criminal actions.”²¹⁰

A framework similar to safe harbor provisions for data breach reporting may be the most appropriate model for a path forward. Under such a framework, developers may have a grace period to disclose the existence of bugs, and assuming they do not trade on the information to the detriment of network participants, they may not be held liable for keeping the bug secret.²¹¹

IV. THE IMPROPER FIT OF CORPORATE FIDUCIARY

Scholarship on the law of fiduciary duties starts with an admission to the effect that the law is “messy,”²¹² and that the fiduciary concept itself is “elusive.”²¹³ Courts use “ad hoc” approaches²¹⁴ to “examine whether the

²⁰⁴ *CVE-2018-1744 Full Disclosure*, <https://bitcoincore.org/en/2018/09/20/notice> (last visited April 18, 2019).

²⁰⁵ *Id.*

²⁰⁶ *Id.*

²⁰⁷ *Id.*

²⁰⁸ Section 5(a) of the Federal Trade Commission Act (FTC Act) (15 USC §45).

²⁰⁹ *See, e.g.*, Verstein, *supra* note 125.

²¹⁰ *Id.*

²¹¹ *See, e.g.*, the recently passed Ohio statute concerning Safe Harbor at <https://www.legislature.ohio.gov/legislation/legislation-summary?id=GA132-SB-220.a>.

²¹² D. Gordon Smith, *The Critical Resource Theory of Fiduciary Duty*, 55 VAND. L. REV. 1399, 1400 (2002).

²¹³ Deborah A. DeMott, *Beyond Metaphor: An Analysis of Fiduciary Obligation*, 1988 DUKE L. J. 879, 915 (1988).

²¹⁴ Smith, *supra* note 212, at 1400.

relationship involved in the litigation is sufficiently like those in the paradigm cases to support an extension of the obligation to that relationship.”²¹⁵ Critics state that this “jurisprudence of analogy”²¹⁶ has led to applying the fiduciary principle “to disparate fact situations”²¹⁷ that exacerbates the “confusion and uncertainty,”²¹⁸ and that “analogies frequently do not result in appropriate rules.”²¹⁹

We recognize the importance of fiduciary obligations as a tool to “give a judge a framework for crafting a hypothetical bargain.”²²⁰ We agree with the law and economics view that fiduciary duties are appropriate for “reducing agency costs associated with the separation of ownership and control.”²²¹ We also acknowledge that, however problematic, the use of analogies is a logical *starting* point for understanding social changes. Yet for technologies that emerge extra-institutionally, we must be prepared to examine distinctions, however onerous the task of technical comprehension, before shoehorning a duty so high as a fiduciary duty.

At least one scholar suggests that because “developers look a lot like officers or directors of a corporation,” having analogous fiduciary duties is fitting.²²² This line of reasoning follows from the view of “[cryptoassets] as shares of stock in a corporation.”²²³ The cumulative effect of reasoning based on a string of analogies underscores the risks of jurisprudence that is supported by analogizing a series of “disparate fact situations.”²²⁴

a. Corporate fiduciary duty

We put aside the growing body of scholarship that decries the corporate fiduciary obligation as a “myth,”²²⁵ and begin to deconstruct the succession of analogies by studying fiduciary duty generally. Arguing from a law and economics point of view, Robert Sitkoff states:

²¹⁵ DeMott, *supra* note 213, at 879.

²¹⁶ *Id.* at 915.

²¹⁷ Reed C. McBride, *City of Hope v. Genentech: Keeping Fiduciary Duties Where They Belong*, 24 BERKELEY TECH. L. J. 179 (2009).

²¹⁸ J.C. SHEPARD, LAW OF FIDUCIARIES 7 (1981).

²¹⁹ Frankel, *supra* note 13.

²²⁰ Kelli A. Alces, *Debunking the Corporate Fiduciary Myth*, 35 J. CORP. L. 239, 244 (2009).

²²¹ See Larry E. Ribstein, *Fencing Fiduciary Duties*, 91 BOS. UNIV. L. REV. 899, 902 (2010).

²²² Walch, *supra* note 153.

²²³ *Id.*

²²⁴ Deborah A. DeMott, *Beyond Metaphor: An Analysis of Fiduciary Obligation*, 1988 DUKE L. J. 879, 915 (1988).

²²⁵ See Kelli A. Alces, *Debunking the Corporate Fiduciary Myth*, 35 J. CORP. L. 239 (2009). See also Stephen Mark Bainbridge, *Much Ado About Little? Directors' Fiduciary Duties in the Vicinity of Insolvency*, J. BUS. TECH. L. (forthcoming, UCLA SCHOOL OF LAW, LAW-ECON RESEARCH PAPER No. 05-26).

[b]y delegating a task to an agent, the principal benefits from specialist service... But these benefits come at the cost of being made vulnerable to abuse if the agent is given discretion the exercise of which cannot easily be observed or verified. In such circumstances, the agent may be tempted to favor the agent's interests when they diverge from those of the principal. The losses and other inefficiencies resulting from this misalignment of interests are called *agency costs*.²²⁶

Through the imposition of fiduciary duties, “[t]he agent is induced to act in the best interests of the principal by the threat of after-the-fact liability for failure to have done so. Deterrence in this sense means *ex post* settling up with the principal for any breach of the agent's *ex ante* fiduciary duties.”²²⁷ “When market forces can or do adequately constrain agency costs,” however, “the relationship in question is no longer properly regarded as a fiduciary.”²²⁸

Fiduciary obligations are applied to relationships where one party (the “beneficiary”) is structurally vulnerable to abuses of power and agency problems due to its reliance on a second party (the “fiduciary”) to act on its behalf in an *unobservable* and *discretionary* manner.²²⁹ Fiduciary obligations are standards that enable courts to provide a remedy when “the protective mechanisms outside of fiduciary law cannot adequately eliminate the risk.”²³⁰ Therefore, if one party (the potential beneficiary) can protect itself from abuse of power through alternative methods, such as observing the other party (the potential fiduciary) or by recourse to other legal regimes, there is no need for the application of fiduciary law.²³¹

From the point of view of legal institutional design, fiduciary obligations are a *deterrence tool* to address the structural and inherent risk exhibited in certain types of relationships. Under this regulatory approach, the fiduciary is enabled to act on behalf of the beneficiary and exercise discretion in unobservable ways, but the beneficiary is subsequently

²²⁶ Robert H. Sitkoff, *An Economic Theory of Fiduciary Law*, in PHILOSOPHICAL FOUNDATIONS OF FIDUCIARY LAW 199 (Andrew Gold & Paul Miller eds., 2014).

²²⁷ *Id.*

²²⁸ See Alces, *supra* note 220, at 240. See also Robert Cooter & Bradley J. Freedman, *The Fiduciary Relationship: Its Economic Character and Legal Consequences*, 66 N.Y.U. L. REV. 1045, 1067 (1991) (pointing out that fiduciary relationships give way to market exchange when contracts provide the proper incentives); Frank H. Easterbrook & Daniel R. Fischel, *Contract and Fiduciary Duty*, 36 J. L. & ECON. 425 (1993).

²²⁹ See, e.g., G. Tullock, *The Welfare Costs of Tariffs, Monopolies and Theft*, WESTERN ECON. J. 5:3 224-232 (1967). See also Douglas G. Baird & M. Todd Henderson, *Other People's Money*, 60 STAN. L. REV. 1309, 1322 (2008).

²³⁰ Frankel, *supra* note 13, at 808.

²³¹ *Id.* at 811.

provided with the means to scrutinize whether the fiduciary's actions were undertaken in the beneficiary's best interests and with adequate skill.²³²

Therefore, fiduciary obligations are a judicial deterrence tool designed to work by influencing the fiduciary's internal cost-benefit analysis of engaging in self-serving behavior through the threat of litigation (e.g., a corporate director is less likely to engage in a self-dealing transaction if under a model of rational self-interest, she believes that as a result of such self-dealing behavior she will face a lawsuit for breach of fiduciary duties that will cost her more than what she is able to gain through her actions).

Traditionally, corporate fiduciary duty arises from the view that corporate officers and directors owe fiduciary duties because they are managing the assets of the owner-shareholders in a trustee-like manner.²³³ Under applicable state corporate law, the stockholders of a corporation have the sole power to elect directors.²³⁴ Generally, shareholders select specific directors to serve on a company's board due to their expertise in a particular area or connections in a certain industry, which the shareholders hope will benefit them by resulting in improved prospects for their company.²³⁵ Upon being elected by the stockholders of a corporation, directors are empowered to be the ultimate managers of the "business and affairs of the corporation."²³⁶ This power is codified in Section 141(a) of the DGCL²³⁷ and by similar statutes in other states.²³⁸

When stockholders invest in a certain company, they entrust their capital to the corporation's directors, who function as the shareholder's agents. Given the deference directors receive under the business judgment rule, directors are legally empowered to make decisions on behalf of stockholders, and in certain circumstances can do so even against the express wishes of the latter.²³⁹ Courts therefore impose fiduciary duties on

²³² Sitkoff, *supra* note 226, at 201.

²³³ Frankel, *supra* note 13, at 805. *But see, e.g.*, Margaret M. Blair & Lynn A. Stout, *A Team Production Theory of Corporate Law*, 85 VA. L. REV. 247, 299 (1999) (positing that directors owe the duties to the corporation as a whole).

²³⁴ DEL. CODE ANN. tit. 8, § 211 (West 2019).

²³⁵ DEL. CODE ANN. tit. 8, § 141 (e) (2008) fully protects corporate officers and directors from liability for relying in good faith upon the records of the corporation and upon such information, opinions, reports or statements presented to the corporation by any of the corporation's officers or employees, or committees of the board of directors, or by any other person as to matters the member reasonably believes are within such other person's professional or expert competence and who has been selected with reasonable care by or on behalf of the corporation.

²³⁶ *Aronson v. Lewis*, 473 A.2d 805, 811 (Del. 1984), overruled on other grounds by *Brehm v. Eisner*, 746 A.2d 244, 253-54 (Del. 2000).

²³⁷ DEL. CODE ANN. tit. 8, § 141(a) (West 2019).

²³⁸ *See, e.g.*, Model Business Corporation Act.

²³⁹ Baird and Henderson point out that directors can make a number of decisions that particular shareholder interests oppose, and that actually harm shareholders for the benefit of other investors. Including the decision to file bankruptcy, note the ability of directors to

directors requiring them to protect the interests of the corporation and to act in the stockholders' best interests.²⁴⁰

b. Where the analogy between protocol developers and corporate directors fails

Protocol developers are distinct from corporate directors in several ways. Protocol developers cannot be said to act as the legal agent of any other network participant, individually or collectively. Protocol developers' voluntary, collaborative and iterative contributions take place in the context of open source production, making their contributions inherently different from the actions undertaken by a fiduciary during her representation of the beneficiary as delineated by an agreed-upon and pre-existing agency relationship. To begin with, there is no expectation between the cryptocurrency holder and the protocol developers of the latter having a legal agent role.²⁴¹ Protocol developers do not make representations of a trustee-like fiduciary position.

Protocol developers lack the ability to bind any other network participants to software application changes, and no other network participant has the power to direct or control the voluntary actions of protocol developers. We have seen how implementation of any change to a particular software application takes place through a multi-level political process and requires consent of formal participants to a public blockchain network. The actions of protocol developers do not deprive any other network participant of their ability to act in their own self-interest, since

structure a merger so as to remove the shareholder's right to vote on it, and the provision of appraisal rights to compensate shareholders who were forced to give up their shares against their will. Baird & Henderson, *supra* note 229.

²⁴⁰ See, e.g., *Arnold v. Soc'y for Sav. Bancorp, Inc.*, 678 A.2d 533, 539 (Del. 1996). The board generally owes fiduciary duties to the preferred and common stockholders equally. However, if the interests of the preferred and common stockholders diverge, the board owes its fiduciary duties exclusively to the common stockholders. *In re Trados Inc. S'holder Litig.*, 2009 WL 2225958 (Del. Ch. July 24, 2009). Under certain state constituency statutes, the board of directors is empowered to consider the interests of constituencies other than the stockholders, including employees, customers, suppliers, and creditors. The DGCL contains no such provision. In the event the corporation is insolvent, directors continue to owe fiduciary duties to the corporation, but in certain jurisdictions the corporation's creditors can replace the stockholders as the primary beneficiaries of those duties. However, when the Delaware Supreme Court addressed this issue, it found that creditors of a corporation have no right to assert direct claims against directors for breach of fiduciary duty. *N. Am. Catholic Educ. Programming Found. Inc. v. Gheewalla*, 930 A.2d 92 (Del. 2007).

²⁴¹ Frankel highlights the need for the "fiduciary" to accept the position and responsibilities by noting that "[t]he fiduciary is free to enter or refrain from entering the relation, and cannot be forced to serve without his consent," and arguing further that "[a] person may agree or refuse to serve as a fiduciary out of purely selfish reasons. On this point, fiduciary law is as individualistic as contract." Frankel, *supra* note 13, at 820, 830.

every participant is free to run whichever version of the software application for the public blockchains. These actors can independently audit the proposed revisions and evaluate their choices. A protocol developers' ability to influence the welfare of the cryptocurrency holder (i.e., the value of the cryptocurrency) is therefore limited to proposing and advocating for a solution that may or may not be subsequently adopted by the community.

A fundamental characteristic of fiduciary relationships is the entrustor's delegation of power or property to the fiduciary, which is necessary for the latter to achieve her goal. For example, we have discussed how shareholders cede ownership and control over the assets of a corporation to the directors and corporate officers.²⁴²

In contrast, there is no action that takes place between a protocol developer and a cryptoasset holder or any other network participant that could be adequately characterized as a delegation of property or power. There is no agency agreement delegating power between protocol developers and other network participants, nor means for the network participants to exercise formal power or control over the protocol developers. Further, the ability of protocol developers to act is not dependent or enabled by a specific action taken by any cryptocurrency holder.

The attenuated relationship between a public blockchain protocol developer and a cryptocurrency holder is established on the basis of two separate actions: (a) a protocol developer's decision to contribute code to a particular software application and (b) another's decision to participate in the public blockchain network by acquiring cryptoassets or operating a node. Neither of these actions alone, nor their combination, constitute a delegation of power or property by a cryptocurrency holder or the acceptance of such power or authority of the cryptocurrency holder by a given protocol developer.

The decision of an individual to acquire cryptocurrency cannot be interpreted as a delegation of property or power to a protocol developer given that, because of that action, protocol developers are neither directly gaining control over property nor gaining the ability to bind the cryptoasset holder to any decision. Critically, the purchase of cryptocurrencies should not be confused with the purchase of public company equity securities, given that public company directors can legally bind the shareholders' rights and interests, even against their will. For example, the board of directors of a public company may rebuff a merger offer that would result in a

²⁴² "Conventional wisdom holds that corporate officers and directors owe fiduciary duties because they are managing the assets of others, and to the extent the firm's shareholders are the owners of the company, it is those shareholders' assets that officers and directors are managing." Kelli Alces Williams, *Debunking The Corporate Fiduciary Myth*, 35 J. CORP. L. 239, 245 n. 25 (2009).

shareholder receiving a significant premium for her shares.²⁴³ In contrast, protocol developers have no such ability to bind other network participants.

One may argue the potential effect that updates to a certain software application proposed by protocol developers may have on the value of the cryptocurrency demonstrates a delegation of property from the cryptoasset holders to the protocol developer, which could be the basis of a fiduciary relationship. However, the cryptocurrency's potential diminution does not reflect the existence of a fiduciary relationship because it is due to the reaction of the economic majority to a development adopted through a multi-level political process.

c. Protocol developers do not pose the same risks of traditional fiduciaries

We have shown in the prior section how the relationship between protocol developers and other participants in public blockchain networks does not share structural similarities to the relationship between a fiduciary and beneficiary. In this sub-section, we show that protocol developers do not pose the dangers that fiduciary obligations are meant to deter, namely abuse of power or agency costs.

i. Protocol developers' motivations align with those of the network participants

Fiduciaries are usually empowered to act with discretion and bind the beneficiary, resulting in the risk that they will act in self-serving ways to the detriment of the beneficiary. In addition, the risks posed by fiduciary relationships are often heightened by the inherent inability of the beneficiary to monitor the fiduciary's performance of her services. For example, shareholders are entitled to only certain information about the actions of the board, and while the beneficiary can monitor the fiduciary, this monitoring is limited to achieve a public policy goal.²⁴⁴ Fiduciary duties are therefore applied to ameliorate the information asymmetries arising from the beneficiary's limited ability to monitor a fiduciary who could possibly exploit her.

In contrast, a protocol developer's actions are radically more transparent and do not exhibit the same information asymmetries as

²⁴³ See, e.g., Bernard S. Sharfman, *The Importance of the Business Judgment Rule*, 14 N.Y.U. J. L. & BUS. 27 (2017).

²⁴⁴ A fundamental principle in corporate law known as the business judgment rule confers upon the public company director discretion to take certain actions without soliciting input from shareholders. This is done in the belief that the directors are in the best position to make the decisions for the company.

traditional fiduciary relationships. An open source software application is, by definition, readily accessible to the public through an online repository. Moreover, updates made to a certain software application, through BIPs and EIPs, are heavily discussed and analyzed by the community both in technical and general terms. “Anyone who stumbles upon the thick Twitter, Reddit and Medium chatter addressing Bitcoin reform or reads the Bitcoin-related GitHub postings can readily monitor activity in the Bitcoin developer community.”²⁴⁵ Given that a significant part of the impetus for protocol developer contributions to public blockchain networks is the reputational value gained from being associated to important contributions to the project, these projects also make contributions highly visible and attributable to specific protocol developers.²⁴⁶

While many cryptocurrency holders are not sufficiently knowledgeable to understand the technical details of projects or revisions, a vibrant ecosystem of participants has developed with the technical knowledge and economic incentives to take a “deep dive” into the technicalities of projects and signal preferences to formal network participants and the market generally. We explored in Section II (c) how certain institutions play a coordinating role with formal participants in the network and by the same process provide synthesized information to the broader market through their statements and actions.

ii. Protocol developers are structurally unable to act selfishly to the detriment of other network participants

We have noted that protocol developers contributing to a certain software application are traditionally not directly remunerated for their efforts by other participants in the network, and as such, the impetus for their contributions can be attributed to (a) long-term reputational value from contributing to important projects and (b) economic value from the potential price appreciation of cryptocurrencies they may hold. Given that protocol developers are incentivized by reputational gains from their contributions to a successful project and by economic gains from the value appreciation of cryptocurrency due to network effects, a protocol developer’s ability to benefit from her contribution to a certain software application is directly linked to the success and growth of the related network. Given the incentive alignment between protocol developers and other network participants, the

²⁴⁵ Atik, *supra* note 118.

²⁴⁶ The list of all contributors to the Bitcoin Core software application is accessible at <https://bitcoin.org/en/development#bitcoin-core-contributors>.

need to impose fiduciary duties is obviated.²⁴⁷ This context is disparate from that of traditional fiduciary relationships that provide the fiduciary with the ability and incentive to act selfishly to extract short-term value to the detriment of the beneficiary.

The DAO exploit exemplifies the above point. As discussed earlier, the Ethereum protocol developers took care to poll holders of Ether to determine if they preferred a default in the software application of forking or not forking; these developers were under no obligation to conduct such a poll to direct the design the hard fork software. However, the protocol developers' interests are to increase the value of the network, and the value of the network is reflected by a community's willingness to transact on it and participate in its validation scheme. Thus, the protocol developers wanted to know the wishes of the community to design the software application in accordance with those wishes; doing so salvaged the network's value for what is the modern-day Ethereum network.

The community that did not want the hard fork did not vanish were free to keep on to the blockchain history and protocol that they wanted. That Ethereum Classic community continues to this day. Assuming *arguendo* that protocol developers wanted all network participants to "convert" to adopt the hard fork, the protocol developers failed; they were unable to foist their decisions onto this community.

Corporate boards and directors have much more coercive power—for example, they are able to bind the corporation against the will of shareholders. Protocol developers simply lack the authoritative power that warrant the imposition of fiduciary obligations.

iii. The structural dynamics and incentive structures of public blockchain network governance ameliorates the risks that protocol developers will act carelessly

Blockchain technology is still in its nascent stage and is highly experimental. As a result, errors in the code of software applications occur and can be expected to continue.²⁴⁸ However, given the motivations of protocol developers and the multi-party political process governing changes

²⁴⁷ Frankel argues that "[w]hen the fiduciary's interests coincide with those of the entrustor, the entrustor is partially protected because as the fiduciary acts in his own interest he will automatically act in the interest of the entrustor." Frankel, *supra* note 13.

²⁴⁸ For example, in September 2018, a new bug was discovered in the Bitcoin Core software application that could have been potentially been exploited to shut down the network or create additional bitcoins. See Jimmy Song, *Bitcoin Core Bug CVE-2018-17144: An Analysis*, MEDIUM (Sept. 27, 2018), <https://hackernoon.com/bitcoin-core-bug-cve-2018-17144-an-analysis-f80d9d373362>.

to the network, the risks that protocol developers will act carelessly and harm other network participants is much lower than in the context of traditional fiduciaries. Protocol developers are directly incentivized to produce the highest quality code given that they are staking their reputations on it and are economically incentivized to do so. Further, public blockchain networks have developed processes and standards for auditing code, such as BIPs and EIPs. Not only is each update scrutinized by arguably the most capable protocol developers in the system, but they are also analyzed and tested by other network participants who have significant economic interest and technical capabilities to audit the code before implementing it.²⁴⁹ Open source production's track record of innovation in highly technical areas is a testament itself to the quality of work produced by this development paradigm.²⁵⁰

- c. There are alternative methods to regulate protocol developers which negate the need to extend fiduciary duties

Fiduciary obligations are imposed in the absence of other alternative means of redress. As noted by Frankel, “[i]f the entrustor can protect himself from abuse of power, there is no need for the intervention of fiduciary law.”²⁵¹ The imposition of fiduciary duties on protocol developers is therefore inadequate given the existence of alternative mechanisms to control protocol developers and other participants in public blockchain networks.

There are existing legal frameworks that are much better suited for dealing with the risks potentially posed by protocol developers and other participants in public blockchain networks, including the imposition of commodity and securities laws at the federal and state level, money transmission and payments law at the federal and state level, as well as general consumer protection, anti-fraud and criminal regulations. While an in-depth discussion of the relative benefits of each regulatory framework is outside of the scope of this Article, courts and policymakers have a wide array of tools they can use to protect the interest of participants in public blockchain networks, several of which reflect the realities of the techno-economic paradigm more closely than would the imposition of fiduciary duties.

²⁴⁹ Scholars studying open source production systems have commented on the efficiencies of the “parallel debugging” enabled when code is freely accessible to the public.

²⁵⁰ Those innovations are discussed in Section V (c).

²⁵¹ Frankel, *supra* note 13, at 811. *See also* Kelli Alces Williams, *Debunking The Corporate Fiduciary Myth*, 35 J. CORP. L. 239, 243 n. 20 (2009) (“Where a duty or relationship need not be fiduciary because the relationship is adequately governed by non-fiduciary mechanisms, it is not ‘fiduciary’ at all.”).

V. EFFECTS OF IMPUTING FIDUCIARY DUTIES ON PROTOCOL DEVELOPERS

Imputing fiduciary obligations to public blockchain protocol developers ignores the design mechanisms in place that curb the risk of wanton decision making by the protocol developers. It is instructive to analyze how designating protocol developers as fiduciaries would affect the judicial process and open source production systems. Once we consider the potential implications of regulating protocol developers as fiduciaries, the impracticability and undesirability of adopting such a position becomes clear.

a. Impractical for courts

At its mildest, labeling protocol developers as fiduciaries would present courts with the challenge of forcing the static concepts of “fiduciary” and “beneficiary” onto a highly dynamic context of public blockchain network governance.

i. Assessing which protocol developers owe fiduciary duties

A protocol developer may contribute one minor line of code that is utterly essential to network functionality. Another may constantly contribute a high volume of lines over a long period of time, but still be a functionary whose work is wholly non-essential and could easily be replaced by others. Alternatively, a “contributor” may not even write actual code at all but instead make a conceptual suggestion that is critical, or simply review other’s code and discover an important bug. Given the different types of activities that individual protocol developers engage in, it would be untenable to suggest that every single protocol developer who makes any contribution, no matter how small or irrelevant, to a public blockchain network is a *de facto* fiduciary.

At the same time, given the highly dynamic, collaborative and iterative nature of public blockchain development, there is simply no alternative way to define which protocol developers rise to a status warranting the label of fiduciary. Those who argue that fiduciary duties should apply to developers are aware of this definitional issue and resort to either referring to a laundry list of different terminologies²⁵² or relying on conclusory definitions.²⁵³

²⁵² A proponent of the view that coders should be regulated as fiduciaries references variations of the term “developers,” including “*core developers*” (e.g., pg. 6), “*prominent developers*” (pg. 6), “*software developers*” (pg. 7 in context of BTC fork), “*key developers*” (pg. 7 in context of BTC fork), “*Ethereum developers*” (pg. 8 in context of ETH fork),

The temporary influence held by certain protocol developers is derived from the reputations they established through the quality and frequency of their contributions and from the value of the particular contribution at stake. Moreover, the fact that a particular protocol developer can wield influence over a software application at a certain moment does not mean that she will continue to exercise that influence, and critically it does not mean that she is able to bind any other participants in the network. Therefore, it would be functionally impossible for courts to provide a static definition that delineates with clarity which protocol developers are “influential enough” to warrant the imposition of fiduciary obligations. Importantly, without the ability to delineate which developers are fiduciaries, protocol developers themselves will be unable to take the necessary steps to protect themselves.

One might argue that those protocol developers with “commit access” to the code repository of a particular software application should be identified as fiduciaries. However, this would entail a misunderstanding of the power dynamics in public blockchain governance, given that protocol developers exhibit a range of influence not defined exclusively or even particularly by this access. Moreover, “commit access” to a specific software application, such as Bitcoin Core, does not entail control over a network which we have noted can support different software applications. Separately, applying fiduciary obligations to individuals with commit access is also likely to be an ineffective regulatory approach, given the potential for technological work-around that could provide developers with anonymity.

ii. The risk of strike suits

Fiduciary obligations are a deterrence mechanism that provide legal recourse to parties who are structurally susceptible to abuses of power.²⁵⁴

“dominant developers” (pg. 8 in context of ETH fork), “small number of developers” (pg. 8 in context of ETH fork) and “certain developers.” Walch, *supra* note 153.

²⁵³ Walch defines “developers” as “those making decisions about the policy choices to be embedded in the code, how to best technically manifest those choices, and then actually crafting and reviewing the code to achieve those policy and technical choices,” noting that [w]ithin this group of contributors, importantly, not all participants are equal. For instance, in open-source software projects like public blockchains, a team of “core developers” or “maintainers” generally leads the software development process. This means that although this group of people may not be united under the roof of an entity structure, they function as leaders and decision-makers for the code.” *Id.* at 5. However, we have seen how no developer has the power to make decisions about the consensus rules and development of a network, but rather how those decisions are made by the formal network participants and economic majority.

²⁵⁴ Frankel, *supra* note 13, at 809 (stating “function and the delegation of power pose a basic problem: while the fiduciary must be entrusted with power in order to perform his function, his possession of the power creates a risk that he will misuse it and injure the entrustor. The fiduciary cannot effectively benefit the entrustor without a delegation of power, but at the

The imposition of fiduciary obligations on public blockchain protocol developers would allow, under the most extreme position, any member of the public holding cryptocurrencies at large to file a lawsuit in their local court and have a judge determine whether, in proposing a certain code update to a software application, a protocol developer owed a duty of loyalty or duty of care to the allegedly aggrieved party and whether either duty was violated. Imposing the fiduciary standard on protocol developers for the benefit of cryptoasset holders would grant the public at large, or even a subset of blockchain network participants, the ability to file under a cause of action for breach of a heightened duty, creating the potential for strike suits that would be piled on to an already overwhelmed court system.²⁵⁵

b. Create motive for subverting the mechanism design of a public blockchain

Corporate fiduciaries are often paid handsomely for the risk they take on as fiduciaries, and these benefits incentivize them to keep corporate matters under their scrutiny and control. Protocol developers, as we have discussed, are not directly compensated and volunteer to create software applications that allow users to participate in the blockchain network—a network that relies upon decentralization of participation for its stability. Imputing fiduciary obligations to protocol developers may cause the protocol developers to take more authority over the network and subvert the purpose of public blockchains. The purpose of public blockchains is to allow for open transacting. For example, a protocol developer, knowing that she would be held to such a high standard for any cryptocurrency owner, may decide to create barriers for network participation entry so that she has less risk by swaying network participation. Under such a high standard, she may also design consensus rules that favor transactions and miners that she desires to lower her liability risk. Imputing fiduciary obligations would threaten the decentralized ecosystem of public blockchains.

c. Chill open source innovation

Importantly, the imposition of fiduciary duties on protocol developers and the risk of liability that determination entails could potentially end the viability of open source production. Open source production has emerged in recent decades as a startling paradigm of human interaction that has enabled

same time, it is difficult or impossible to eliminate the fiduciary's ability to use the power for another purpose to the detriment of the entrustor.”).

²⁵⁵ Fed. Prac. & Proc. Civ. § 1296, Chapter 4, 5A (4th ed.) (discussing that the particularity standard for pleadings helps prevent strike suits).

innovative new models of social organization and is increasingly responsible for producing more of the world's information.

Open source production has an impressive track record of technological innovation, made more remarkable by how modern economic theory is largely unable to explain its accomplishments. Writing in 2017 of the success of Apache, the open source web server software, Yochai Benkler stated, “[a]ny economist who would have predicted in 1996 that a group of developers working on webserver software, using no formal managerial hierarchy and relying on a copyright license that gave no one exclusive proprietary control over the products of the collaboration would beat Microsoft in a market that was core to Microsoft’s Internet strategy would have been laughed out of the room. And yet Apache beat Microsoft Server over the past twenty years, and its fastest growing competitor is Nginx, another FOSS project.”²⁵⁶

If we study its track record, we see how open source production—as a human coordination mechanism—has enabled remarkable technological innovations and is today responsible for an increasing amount of the information production in the world. Some of these technological innovations include: Apache, Linux (the preferred operating system for programmers), Wikipedia (the killer of Encarta), as well as today’s public blockchain networks.²⁵⁷

Contributions to open source production systems are voluntary and partially animated by social and psychological factors. In the event these contributors were made potentially liable to the public at large based on newly expanded and untested fiduciary standards, they would be likely to reconsider contributing to such projects, resulting in them ceasing to do so, or continuing in covert or non-public ways. If the risk of liability derived from the imposition of fiduciary obligations changes the incentive mechanism of public blockchain networks, open source production risks grinding to a halt.

CONCLUSION: TOWARDS A BETTER UNDERSTANDING OF PUBLIC BLOCKCHAIN NETWORK GOVERNANCE FOR APPROPRIATE LIABILITY FRAMEWORKS

We have argued that public blockchain protocol developers do not function as corporate fiduciaries, and further that labeling protocol

²⁵⁶ Yochai Benkler, *Peer Production, the Commons, and the Future of the Firm*, 15 STRATEGIC ORG. 264 (2017), <http://nrs.harvard.edu/urn-3:HUL.InstRepos:37078633>.

²⁵⁷ “[P]roponents of open source software state that the structure fosters the creation of vibrant—and valuable—developer communities, and leads to a common set of well tested, transparent, interoperable software modules upon which the developer community can standardize.” Krumholz et al., *supra* note 56.

developers as fiduciaries would be impractical and have other negative effects including potentially destroying the open source production model.

However, we have also readily acknowledged that public blockchain networks necessarily develop governance structures (however latent or dynamic) and that in some circumstances, protocol developers can exercise an influential role in the implementation of changes to certain software applications. As such, it is important to focus on better understanding the role that all participants in public blockchain networks play in their governance, and that the community of developers contributes to achieving this understanding.²⁵⁸ It is important to study the incentive mechanisms that guide those in these roles. In addition, we acknowledge the critical role of regulators in protecting the public and policing the markets, including by holding accountable developers who design and launch malicious and unsafe smart contracts and other software applications.²⁵⁹ However, for the reasons stated above, we find the argument for extending fiduciary duties to protocol developers for the prominent blockchain networks we have focused on to be both untenable and undesirable at this point.

In addition to the various regulatory frameworks currently available and those that may be designed to specifically reflect this techno-economic paradigm, an alternative and promising method to regulate the behavior of protocol developers and other participants in public blockchain networks is through the imposition of “on-chain” governance protocols.²⁶⁰ By means of these blockchain-based consensus mechanisms, formal participants of a network may be able to decide which code updates are implemented according to a pre-existing ruleset. Blockchains are at their core a “foundational technology for new forms of governance for making rule-

²⁵⁸ For example, the Bitcoin Core developers should consider clarifying who in particular has commit access to the Bitcoin Core repository.

²⁵⁹ For example, CFTC Commissioner Quintenz argued that while neither public blockchain developers contributing protocol-level changes, nor miners, nor users should be generally held responsible for unlawful activity on potentially occurring on public blockchain networks, developers working on specific smart contracts (“Smart Contract Developers”) may be held legally responsible if they can “reasonably foresee” that their smart contracts will be used illegally. *Remarks of Commissioner Brian Quintenz at the 38th Annual GITEX Technology Week Conference*, CTFC (Oct. 16, 2018), <https://www.cftc.gov/PressRoom/SpeechesTestimony/opaquintenz16>. Recent enforcement actions against smart contract developers include the cease and desist settlement announced by the SEC on November 8, 2018 against the operator of a digital asset exchange on the basis of operating an unregistered securities exchange. Available at <https://www.sec.gov/news/press-release/2018-258>. In addition, an Arkansas court recently sentenced a software developer to 33 months in prison for aiding and abetting computer intrusions by selling malware to individuals who used the malware to steal sensitive information. Available at <https://www.justice.gov/opa/pr/arkansas-man-sentenced-prison-developing-and-distributing-prolific-malware>.

²⁶⁰ Such as the ones proposed by the Tezos and Decred projects.

governed economic orders.²⁶¹ Therefore, the technology itself may provide means to regulate the actions of the relevant participants. In contrast, the imposition of fiduciary duties on protocol developers risks the “corporate capture” of blockchain governance whereby experimentation with new human institutional arrangements is foregone in place of adopting a corporate governance structure.²⁶²

²⁶¹ Sinclair Davidson et al., *Disrupting Governance: The New Institutional Economics of Distributed Ledger Technology* 1, 3 (2016), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2811995.

²⁶² Zamfir, *supra* note 119.