2019

In Code(rs) We Trust: Software Developers as Fiduciaries in Public Blockchains

Angela Walch
St. Mary's University School of LAw, awalch@stmarytx.edu

3

In Code(rs) We Trust

Software Developers as Fiduciaries in Public Blockchains

*Angela Walch**

I. Introduction

> 'Those who are not expert developers or computer scientists who have invested a great deal of time in learning the design principles and codebase of a blockchain must place a great deal of faith in the expert developer community.'[1]

'A computer operates only in accordance with the information and directions supplied by its human programmers. If the computer does not think like a man, it is man's fault.'[2]

A decade into Bitcoin's existence, governance questions around it and other public blockchains abound. Do these 'decentralized' structures even have governance? If so, what does it look like? Who has power, and how is it channelled or constrained? Are power structures implicit or explicit? How can we improve upon the ad hoc governance structures of early blockchains? Is 'on-chain governance,' like that proposed by Tezos and others, the path forward?

In August 2016, in the aftermath of the DAO theft and resulting Ethereum hard fork, I argued in *American Banker* that the core developers and significant miners of public blockchains function as fiduciaries of those who rely on these systems and should, therefore, be accountable as such.[3] The DAO episode provided a gripping real-world demonstration that certain people within nominally decentralized public blockchains were making decisions about other people's money and resources, yet this power was largely unacknowledged, undefined, and unaccountable.

In this chapter, I explore in greater depth my claim that certain developers of public blockchains act as fiduciaries,[4] as events since the DAO continue to point to the exercise of power within these systems without corresponding accountability.[5] With the peer-to-peer

* This paper was selected for presentation at the 2nd International Workshop—P2P Financial Systems 2016 at UCL on 8 September 2016. I would like to thank Samir Parikh, Aaron Wright, Patrick Murck, Ajit Tripathi, Tim Pastoor, Andrew Miller, Vlad Zamfir, Philipp Hacker, Drew Hinkes, Stephen Palley, Tim Swanson, Ciaran Murray, participants at the 2015 Southeastern Association of Law Schools Annual Conference New Scholars Program, the 2017 Blockchain and the Constitution of a New Financial Order: Legal and Political Challenges Conference at UCL, faculty workshops at Thurgood Marshall School of Law at Texas Southern University and Texas A&M Law School, the P2P Financial Systems 2016 Workshop, and the active crypto Twitterverse for helpful feedback and insights.

[1] Nick Szabo, 'Money, Blockchains, and Social Scalability' (*Unenumerated*, 9 February 2017) https://unenumerated.blogspot.com/2017/02/money-blockchains-and-social-scalability.html.

[2] *State Farm Mutual Auto Ins. v. Bockhorst*, 453 F 2d 533, 537 (10th Cir. 1972).

[3] Angela Walch, 'Call Blockchain Developers What They Are: Fiduciaries' (2016) *American Banker*, https://www.americanbanker.com/opinion/call-blockchain-developers-what-they-are-fiduciaries.

[4] In this chapter, 'developers' is used as shorthand for those involved in making decisions about the software that operates public blockchains. This group may include people who write software code, make decisions about policies that should be reflected in software code, review software code, etc. The term excludes miners and other nodes in the network that run the software.

[5] The governance of 'private' or 'permissioned' blockchains deserves its own careful scrutiny but is beyond the scope of this chapter. Private (i.e. permissioned) blockchains are data structures with a known and trusted group of transaction processors. 'Public' (i.e. 'permission-less') blockchains, like Bitcoin and Ethereum, are data structures for which anyone can become a transaction processor simply by running the applicable software.

computer network that operates these data structures through the running of software code, governance occurs through the software development and transaction verification processes. This chapter focuses on the software development process and compares the role of dominant software developers to a general definition of a fiduciary, finding many likenesses between the two. Recognizing that significant experimentation in governance is ongoing with public blockchains, I provide an initial outline of the core issues and questions raised by the fiduciary categorization.[6]

The age-old fiduciary concept may initially seem a poor fit for cutting-edge public blockchains, which are celebrated for enabling human coordination without the need to trust in a central party.[7] Indeed, the adjective 'trust*less*' is still regularly applied to these systems.[8] By contrast, the fiduciary concept is based fully on trust, one party entrusting another to make decisions on her behalf. Applying the fiduciary construct to public blockchains thus emphasizes that—even in public blockchains—we have not escaped the need to trust in other humans. Though some in the public blockchain space describe these systems as 'trust-minimized',[9] I see them as 'trust-shifting'; the need to trust in others has simply moved from its traditional place (e.g. the officers and directors of a *bona fide* corporation), leaving us to discern where it has landed. In these systems that operate money, smart contracts, and potentially many other critical human practices, people continue to lead and make important decisions on behalf of others; we just have to name them and decide how to treat them.

Understanding public blockchain governance is not merely an academic matter. Accurately describing the roles that various parties play in the governance of blockchain systems has implications for many different legal analyses related to these systems. A single important example is the application of securities laws to public blockchain systems.[10] If we do not press past a superficial description of public blockchain systems as 'decentralized', then we do not perceive the important decision makers within these systems, who wield significant power throughout the life of the blockchain.

In a broader sense, blockchain technology is being lauded as transformative for every human practice that uses recordkeeping (so, all of them). If blockchain technology achieves even a small portion of its projected potential, then it may soon undergird many critical infrastructures within our societies, ranging from property records, to payment and voting systems. And, if blockchain technology ends up enabling our most fundamental social infrastructures, then the governance processes for creating, maintaining, and altering the technology deserve careful scrutiny, as these processes will affect the resilience of the technology as well as any infrastructure that comes to rely on it.[11]

[6] In addition to developers, there are other parties who play important roles in a public blockchain system, including miners (transaction processors), nodes (those that do not actually process transactions), users, and exchanges (businesses that exchange one cryptocurrency for another cryptocurrency or a traditional sovereign currency like the US dollar). See, e.g., Jatinder Singh and Johan David Michels, 'Blockchain as a Service: Providers and Trust' (2017) Queen Mary, University of London, School of Law Legal Studies Research Paper No. 269/2017, https://ssrn.com/abstract=3091223. I plan to analyse the governance roles of these parties in later papers.

[7] Primavera De Filippi and Aaron Wright, *Blockchain and the Law: The Rule of Code* (Harvard University Press 2018), 2–3.

[8] ibid., 26.

[9] NickSzabo, 'The Dawn of Trustworthy Computing' (*Unenumerated*, 11 December 2014), http://unenumerated.blogspot.com/2014/12/the-dawn-of-trustworthy-computing.html.

[10] Securities regulators around the world are evaluating how the tokens of blockchain systems fit into existing securities laws, with a number of prosecutions stemming from the initial coin offering mania that struck the cryptocurrency world in 2017. On 14 June 2018, a representative of the US Securities and Exchange Commission stated that it was unlikely that Bitcoin or Ethereum were securities due to their decentralized status because 'purchasers would no longer reasonably expect a person or group to carry out essential managerial or entrepreneurial efforts.' Speech by William Hinman, 'Digital Asset Transactions: When Howey Met Gary (Plastic)' (14 June 2018) Speech, https://www.sec.gov/news/speech/speech-hinman-061418.

[11] Angela Walch, 'The Bitcoin Blockchain as Financial Market Infrastructure: A Consideration of Operational Risk' (2015) 18 *New York University Journal of Legislation and Public Policy*, 83, considers the operational risks created by informal governance processes in Bitcoin and their implications for its suitability as financial market infrastructure. Angela Walch, 'Open-Source Operational Risk: Should Public Blockchains Serve as Financial Market

In section II, I describe the types of activities that software developers perform and explain how these activities function as a significant part of the governance of prominent public blockchains, like Bitcoin and Ethereum.[12] In section III, I evaluate the implications of this concentration of power in certain developers and apply Tamar Frankel's conception of a 'fiduciary' to their actions. In section IV, I discuss the pros and cons of treating these parties as fiduciaries of certain participants in the blockchains they manage. In section V, I discuss some of the complexities involved with the categorization, including the difficulties in precisely determining which individuals in a given blockchain function as fiduciaries and to whom they should owe corresponding duties. In section VI, I provide an overview of the continuing experimentation in public blockchain governance and of existing scholarly approaches. Finally, in section VII, I offer concluding thoughts and suggestions for further research.

As I perform this analysis, I am aware that analogizing software developers to fiduciaries is controversial, as treating these parties as fiduciaries directly contests the dominant narrative of decentralization of public blockchains and would almost certainly reduce innovation in the public blockchain space. However, sometimes consideration of taboo ideas is necessary to illuminate the trade-offs we make in our existing legal paradigm of protecting innovation by minimizing accountability. A discussion of the accountability of those who govern technology is particularly salient given the current, active debate over the governance of Facebook, Uber, and other technology companies that have significant effects on society.

II. Nominal Decentralization—De Facto Governance

In this section, I describe the role developers play in the governance of certain public blockchains and explore public blockchains' overstated reputation for decentralized software development, given that identifiable parties dominate (and therefore centralize) the process.[13]

One of the defining features of public blockchains is that they are said to be *decentralized*.[14] In theory, this means that there is no central entity that either creates or maintains them.[15] Rather, they operate on a peer-to-peer basis through the running of open-source software by a network of computers. The software development process for public blockchains is also said to be 'decentralized', as is typical of open-source software projects.[16] There is no central entity that is officially responsible for maintaining or updating the software. A mix of

Infrastructures?' in *Handbook of Blockchain, Digital Finance, and Inclusion*, edited by David Lee Kuo Chuen and Robert Deng (Vol. 2, Elsevier Academic Press 2017), explores the operational risks raised by the use of grassroots open-source software development practices in the use of public blockchains as financial market infrastructures.

[12] Each public blockchain has its own unique characteristics, so it is theoretically possible that some public blockchains may not have software developers who serve as fiduciaries. However, I am sceptical that the elimination of trusted software developers will actually occur, so believe the analysis in this chapter will be useful to the understanding of most, if not all, public blockchains.

[13] A great deal of experimentation is happening with public blockchains, with new variations introduced almost daily. This chapter does not specifically address each variation of governance but provides an overarching analytical framework. I highlight some recent variations of public blockchain governance in Part VI. It may be possible that new variations of public blockchains have no developers filling the role of fiduciaries, but I am sceptical that this will be the case.

[14] Adam E. Gencer, Soumya Basu, Ittay Eyal, Robbert van renesse, and Emin G. Sirer, 'Decentralization in Bitcoin and Ethereum Networks' (*arXiv.org*, 2018) https://arxiv.org/pdf/1801.03998.pdf.; Peter van Valkenburgh, 'What Could "Decentralization" Mean in the Context of the Law?' (*CoinCentreBlog*, 15 June 2018) https://coincenter.org/entry/what-could-decentralization-mean-in-the-context-of-the-law.

[15] Gencer (n 14). The mining networks of public blockchains, like Bitcoin and Ethereum, are quite centralized, which is relevant to the governance role miners play in these networks. More extensive discussion of this phenomenon is beyond the scope of this chapter.

[16] For a discussion of the software development process of public blockchains, see Walch, 'Open-Source Operational Risk' (n 11), 252–54.

volunteer and paid software developers write and update the software, determining how to revise the code through 'informal processes that depend on rough notions of consensus and that are subject to no fixed legal or organizational structure'.[17] The code is publicly available,[18] and anyone in the world may propose a change through a standardized proposal process. Indeed, many developers from across the globe have made proposals.

Furthermore, there may be people involved who help shape the code but do not actually write it—these may include people reviewing it or doing research and making recommendations about the policy and technical goals of the system. As mentioned earlier in footnote 4, my use of the term 'developer' in this analysis is intended to encompass those making decisions about the policy choices to be embedded in the code, how best technically to manifest those choices, and then actually crafting and reviewing the code to achieve those policy and technical choices. Within 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 the leaders and decision makers in relation to the code.[19] This power manifests in the ways in which they differ from rank-and-file developers. With Bitcoin, for example, core developers, until recently, have had the ability to send emergency messages to all nodes in the network[20] and are the only developers who have 'commit access' that allow them to make actual changes to the software code,[21] i.e. other developers can propose changes but a core developer's password or access code is ultimately needed to put that change in a new code release. Prominent developers also shape how public blockchains are viewed by regulators and the public at large. Certain developers have met privately with various international regulators or leaders[22] and often comment publicly on what should happen with the particular blockchain they represent and the technology as a whole.[23]

[17] Shawn Bayern, 'Of Bitcoins, Independently Wealthy Software and the Zero-Member LLC' (2014) 108 *Northwestern University Law Review Online*, 257, 259.

[18] The GitHub pages for Bitcoin and Ethereum, the two most prominent public blockchains, are found at https://github.com/bitcoin/bitcoin and https://github.com/ethereum/, respectively.

[19] Vitalik Buterin, creator of Ethereum, stated in a January 2017 interview about Ethereum's governance: 'It is kind of technocratic in some ways, because right now there is a small group of people that really deeply understand all the different Ethereum technical considerations—a lot of decisions do tend to get made by a small group. But in the longer term that is definitely something we are looking to democratize.' This statement is from Joon Ian Wong, 'Ethereum's Inventor on How "Initial Coin Offerings" are a New Way to Fund the Internet' (*Quartz*, 14 September 2017), Interview with Viterik Buterin, https://qz.com/1075124/ethereum-founder-vitalik-buterin-discusses-initial-coin-offerings-the-consensus-algorithm-and-the-most-interesting-apps/.

[20] Andreas M. Antonopoulos, *Mastering Bitcoin: Unlocking Digital Cryptocurrencies* (2nd edn, O'Reilly 2017), 157: the emergency message power 'allow[ed] the core developer team to notify all Bitcoin users of a serious problem in the Bitcoin network, such as a critical bug that require[s] user action'. The password that allowed the sending of the network-wide emergency messages was held only 'by a few select members of the core development team'. Also see Arthur Gervais, Ghassan O. Karame, Srdjan Capkun, and Vedran Capkun, 'Is Bitcoin a Decentralized Currency?' (2014) http://eprint.iacr.org/2013/829.pdf, which argues that giving the emergency alert power only to the core developers 'gives these entities privileged powers to reach out to users and urge them to adopt a given Bitcoin release'.

[21] Tom Simonite, 'The Man Who Really Built Bitcoin' (2014) *MIT Technology Review*, http://www.technologyreview.com/featuredstory/527051/the-man-who-really-built-bitcoin/, describes how only the core developers have the power to 'change the code behind Bitcoin and merge in proposals from other volunteers'. Also see Gervais et al. (n 20), 6: 'this [software development process] limits the impact that users have, irrespective of their computing power, to affect the development of the official Bitcoin [software]'.

[22] For example, Gavin Andresen met with the Central Intelligence Agency in the United States when he served as the lead developer of Bitcoin in 2011. Vitalik Buterin, the creator of Ethereum, met with Russian president Vladimir Putin in 2017 as sourced from Ilya Khrennikov, 'Vladimir Putin is Getting Interested in Bitcoin's Biggest Rival' (*Bloomberg*, 6 June 2017) https://www.bloomberg.com/news/articles/2017-06-06/putin-eyes-bitcoin-rival-to-spur-economic-growth-beyond-oil-gas.

[23] Quoting of Bitcoin core developer Wladimir van der Laan on plans for funding Bitcoin software development found in Stan Higgins, 'Bitcoin Core Opens Doors to Outside Funding with Sponsorship Program' (*CoinDesk*, 6 April 2016) http://www.coindesk.com/bitcoin-core-opens-doors-to-outside-funding-with-sponsorship-program/;

Power is often most visible during a crisis and examining what has happened in crisis moments of public blockchains shows us the power that a small group of developers wields. Below, I briefly describe Bitcoin's March 2013 hard fork and Ethereum's July 2016 hard fork. A 'hard fork' occurs when at least two non-compatible versions of software are running on a network, meaning that different ledgers are being generated by different portions of a previously cohesive network.[24] Hard forks are significant moments in public blockchains as they result in two separate networks; if the hard fork is unintentional, it can require human discretion and action for the networks (and their ledgers) to reunite.[25]

A. Bitcoin's March 2013 hard fork

In March 2013, Bitcoin experienced a hard fork in the network, with the effect that two separate ledgers were being maintained by different computers within the network.[26] The fork happened because nodes within the network were running two different versions of the Bitcoin software; some had upgraded to a new release whilst others had not yet done so. When the software developers realized that the fork was occurring, they quickly contacted miners on the network to persuade them to support one of the two disparate ledgers. This required some of the miners to downgrade to the prior software version, 'sacrificing significant amounts of money' as a result.[27] With that change made, the network gradually returned to a single ledger.

This episode spotlights the exercise of power by both the key developers and miners with a significant amount of hashing power. The developers were able to correspond with, and persuade, particular miners to alter the software they were running, which had the effect of creating a 'winning' ledger. The developers involved also chose which ledger should be authoritative; this created financial winners and losers amongst the miners, based on which ledger fragment they had been processing during the fork. Miners with a threshold percentage of power within the network were able to sway the outcome through their choice of which version of the software to run. The more network power, essentially, the more 'votes' a miner could cast, and the more lobbying required by developers to obtain the result they sought.

B. Ethereum's July 2016 hard fork

The Ethereum blockchain faced an existential crisis in the summer of 2016 when the DAO, an application built on top of its blockchain platform, suffered a $50+ million theft.[28] Presented with the choice of allowing the thief to keep the stolen ether to preserve the ledger's 'immutability' or to craft new code that would reverse the objectionable transactions, the Ethereum

transcribing of an interview with Vitalik Buterin about public blockchain governance and funding found in Wong (n 19).

[24] A 'hard fork' (i.e. a split into more than one network) can result from the use of incompatible software by different portions of a public blockchain network, whereas a 'soft fork' results from the release of new software to the network that is compatible with prior versions so that the network continues to produce a single blockchain record. Bruno Biais, Christophe Bisière, Matthieu Bouvard, and Catherine Casamatta, 'The Blockchain Folk Theorem' (2018) Toulouse School of Economics Working Paper No. 17-817, 14, https://www.tse-fr.eu/sites/default/files/TSE/documents/doc/wp/2017/wp_tse_817.pdf.

[25] For a more in-depth discussion of hard forks of public blockchains, see Walch, 'Open-Source Operational Risk' (n 11), 259–66; Biais et al. (n 24), 13–17.

[26] Walch, 'The Bitcoin Blockchain as FMI' (n 11), 873; Biais (n 24), 14–16.

[27] Walch, 'The Bitcoin Blockchain as FMI' (n 11), 873.

[28] Joon Ian Wong and Ian Kar, 'Everything You Need to Know About the Ethereum "Hard Fork"' (*Quartz*, 18 July 2016) https://qz.com/730004/everything-you-need-to-know-about-the-ethereum-hard-fork/.

developers decided to pursue a hard fork that would recover the funds.[29] They determined how to code revised software that would achieve the fork as well as persuaded a majority of the network's hashing power (held and exercised by miners) to adopt the revised software. The preparations for the hard fork included explanatory missives from the core developers and an advance poll of the Ethereum miners to see how likely the hard fork was to succeed.[30] Only a very small percentage of ether holders or miners voted in the advance polls but the Ethereum developers decided to proceed with the hard fork.[31]

It worked. Enough miners upgraded to the revised software, and the ledger followed them, taking the Ethereum name and primary developers with it. However, a splinter group of software developers and miners decided to keep the original ledger (reflecting the theft) going. Dubbing the surviving chain 'Ethereum Classic', this group issued a Declaration of Independence from Ethereum[32] and has since been operating a competing blockchain.

This hard fork demonstrates the power exercised by certain developers and significant miners. The developers made the decision whether to treat the hack of the DAO application as theft (meaning that it should have some sort of remedy) or as an exploitation of code intended to run without human involvement (meaning no remedy would be appropriate). The proposal to engage in the hard fork split the Ethereum community, with some arguing passionately for immutability no matter what, and others arguing that the hacker must be punished. Allegations that the dominant developers recommended the hard fork because some of their own money had been stolen in the hack[33] made the rounds on Twitter and Reddit.[34]

The passion, drama, and anger surrounding the Ethereum hard fork show how much was at stake for the Ethereum community, for investors in ether, and for those who built applications and companies atop the Ethereum blockchain. Yet only a small number of developers and miners in this 'decentralized' system decided what the resolution of the DAO hack would be, in effect determining the financial fortunes of all those relying on the Ethereum blockchain, whether or not they had invested in the DAO.[35]

These examples of power reveal that centralized decision making exists within nominally decentralized public blockchains.[36] There are countless other examples demonstrating the exercise of power by a small subset of developers—arguably every single bit of code actually

[29] ibid. [30] ibid.

[31] Vitalik Buterin, 'Notes on Blockchain Governance' (Vitalik Buterin's website, 17 December 2017) https://vitalik.ca/general/2017/12/17/voting.html.

[32] Ethereum Classic, 'The Ethereum Classic Declaration of Independence, 20 July 2016', https://ethereumclassic.github.io/assets/ETC_Declaration_of_Independence.pdf.

[33] Ray Jones, 'Ethereum Protocol Developer Holds $114,877 Worth of DAO Tokens' (*Reddit*, 29 June 2016) https://www.reddit.com/r/ethereum/comments/4qiqq8/ethereum_protocol_developer_holds_114877_worth_of/d4th8ce/: 'The simplest solution would be for all people in positions of influence who are in favor of a hard fork to openly declare their DAO token holdings.' Aakil Fernandes, 'Ethereum Protocol Developer Holds $114,887 of DAO Tokens' (*Reddit*, 29 June 2016) https://www.reddit.com/r/ethereum/comments/4qiqq8/ethereum_protocol_developer_holds_114877_worth_of/d4tm9o5/: 'We *should* care when people have conflicts of interest. That applies to lawyers, judges, bankers, politicians and yes it applies to developers. Humans are humans.'

[34] See, e.g., Justin Camarena, 'I'd agree with a rollback for protocol level hacks ... But this isn't that at all. Core devs own DAO' (*Twitter*, 17 June 2016) https://twitter.com/juscamarena/status/744008754459475968; Justin Camarena, 'they are unfairly slanted to HF'ing to regain their money ... might as well just have a private chain' (*Twitter*, 17 June 2016) https://twitter.com/juscamarena/status/744008863091941376; Fernandes (n 33).

[35] A counter-argument to the argument that Ethereum developers and miners exercised power is that parties who did not wish to proceed were able to continue with the Ethereum Classic blockchain. However, Ethereum Classic had much less mining power devoted to it, making it more vulnerable to attack, and it had to assemble a new slate of software developers to keep it going.

[36] Some may argue that these examples of power exercised in connection with a hard fork are no longer relevant because they happened in 2013 and 2016, respectively. However, nothing relevant appears to have changed about the software development governance models in Bitcoin or Ethereum since these events.

released to the network is an exercise of power. Since the moment these public blockchains were created (including the idea development and creation process), small groups of people have been making decisions about which policies should be reflected in the code (e.g. a limited or unlimited number of tokens? Transaction fees or the creation of new tokens?) and how those policy choices should technically be achieved through the code. These decisions have impacted upon significant numbers of people, and the more widely used public blockchains become, whether as cryptocurrencies or as infrastructure undergirding other systems, the greater will be the number of people who rely on the decision making of a small set of developers.

III. If It Looks Like a Fiduciary...

In section I, I described how developers exercise power within public blockchains. In this section, I explore the implications of this concentration of power and analogize these central decision makers to fiduciaries.[37] When using a general definition of 'fiduciary', certain developers of public blockchains bear a strong resemblance.[38]

The fiduciary concept is ancient and is fundamentally based on the concept of 'trust'. Familiar fiduciaries include doctors, lawyers, financial advisors, trustees, and corporate officers and directors.[39] We frequently put our fate in the hands of others—others whom we count on to provide considered and competent advice, perform tasks we cannot do for ourselves (like open-heart surgery!) and to manage our funds or investments to our benefit. We expect these parties to put our interests before their own in this role and to perform their duties competently and honestly.

Tamar Frankel, the pioneering and leading scholar on fiduciary law, has written that all fiduciaries share the following attributes:

> 1) They offer mainly services (in contrast to products). The services that fiduciaries offer are usually socially desirable and often require expertise, such as healing, legal services, teaching, asset management, corporate management and religious services. 2) In order to perform these services effectively, fiduciaries must be entrusted with property or power. 3) Entrustment poses to 'entrustors' the risks that the fiduciaries will not be trustworthy. They may misappropriate the entrusted property, misuse the entrusted power or they will not perform the promised services adequately. 4) There is a likelihood that [a] the entrustor will fail to protect itself from the risks involved in fiduciary relationships; [b] the markets may fail to protect entrustors from these risks; and that [c] the costs for the fiduciaries of establishing their trustworthiness may be higher than their benefits from the relationships.[40]

Certain developers of public blockchains arguably resemble fiduciaries in all of the ways identified by Frankel. Below, I apply each of Frankel's factors in turn.

[37] Szabo, 'Money Blockchains' (n 1), analogized miners to fiduciaries and noted the significant trust placed in blockchain software developers: 'Miners are partially trusted fiduciaries, and those who are not expert developers or computer scientists who have invested a great deal of time in learning the design principles and codebase of a blockchain must place a great deal of faith in the expert developer community, much as non-specialists who want to understand the results of a specialized science do of the corresponding scientists.'

[38] This is not a jurisdiction-specific legal argument, but rather a consideration of the broad conception of a fiduciary. I am not claiming that in a particular jurisdiction, the core developers or dominant miners would be considered fiduciaries based on that jurisdiction's existing law.

[39] In recent years, legal scholars have examined whether expansion of the fiduciary category may be merited, including in the technology sector. See, e.g., Jack M Balkin, 'Information Fiduciaries and the First Amendment' (2016) 49 *University of California Davis Law Review*, 1183, who argues that tech companies holding personal data should be deemed 'information fiduciaries'. D. Theodore Rave, 'Politicians as Fiduciaries' (2013) 126 *Harvard Law, Review*671 argues that politicians function as fiduciaries. Ethan Leib, David L. Ponet, and Michael Serota, 'A Fiduciary Theory of Judging' (2013) 101 *California Law Review*, 699, apply the fiduciary concept to judges.

[40] Tamar Frankel, *Fiduciary Law* (Oxford University Press 2011), 6.

A. Providing socially desirable services that often require expertise

Frankel's first factor is that fiduciaries provide services (as opposed to products) to the 'entrustors'[41] and that the services are typically 'socially desirable' and 'often require expertise'.

As described in section I, the software developers who work on public blockchains provide services to the users of that blockchain. These services include conducting research, reviewing the code, proposing conceptual changes to the code, reviewing changes proposed by other developers, drafting new code and revising existing code, security-testing new code, compiling code into new releases, and communicating about the project with other developers. There is certainly a conceptual question as to whether software code is a 'product',[42] but it is common practice that when companies license software to other parties, they can choose whether or not to provide the service (sold under a services or maintenance agreement) of ongoing software maintenance. While one could argue that the software itself is a product, the work that the developers do to maintain and change it is a service.

Furthermore, one could certainly argue (and I imagine that all software developers working on these blockchains would agree or they would not be working on these projects) that the services provided are 'socially desirable'. If one believes that public blockchains offer some benefits to the public or to their users, then the services performed to create and maintain them are arguably 'socially desirable'. In addition, the services provided by the software developers clearly 'require expertise'. Only those skilled in designing, reading, evaluating, and crafting software code can perform these services. Although the project is open-source, which typically means that the development process is open to anyone who wants to contribute, only developers who have at least a minimum amount of expertise in the relevant software languages and design techniques can realistically participate. And, only those who have earned the privilege of 'commit access' have the privilege of making changes to the actual code that will be released for use in the system.

B. Entrusted with property or power

According to Frankel, the second hallmark of a fiduciary is the ability to use his or her discretion on behalf of entrustors, as 'fiduciaries must be entrusted with property or power'.[43]

Developers exercise discretion on behalf of others in virtually every task they perform in connection with their blockchains. From decisions about which changes should be put into a new software release (reflecting both policy and technical choices) to decisions about the stance to take when speaking to regulators on behalf of the blockchain, developers are constantly making impactful choices.[44] In the 2013 Bitcoin hard fork, leading developers determined which of the forked ledgers should be recognized as true and persuaded particular miners to achieve their goals. In the 2016 Ethereum hard fork, key developers decided to treat the DAO hack as a theft and to reverse the transaction by issuing a new release of the code. In each of these cases, based on the developers' decisions, some people lost money.

Holders of public blockchain tokens and those who built businesses on top of these public blockchains did not get to explicitly approve these decisions[45]—once they chose to participate in the blockchain, the only way to escape the developers' power would be to abandon

[41] ibid., Introduction. I use Frankel's terminology, which she uses to refer to those whom fiduciaries serve: 'they entrust to fiduciaries property and power'.

[42] See David Berke, 'Products Liability in the Sharing Economy' (2016) 33 *Yale Journal on Regulation*, 609–18, which provides a recent description of the legal status of software as a product for products liability purposes.

[43] Frankel (n 40), 6 and 26.

[44] Note that some of the variations on public blockchain governance described in Part V incorporate 'on-chain' governance (e.g. Tezos), which provides for holders of the applicable token to vote on software changes. This may not affect the fiduciary analysis as any voter who is not an expert in the relevant technology or code will likely rely on the recommendations of an expert to cast a vote.

[45] ibid.

the investment (whether in the cryptocurrency or the blockchain-related business) or to persuade a group of people to create a new token by forking off the original blockchain (as happened with Bitcoin Cash and Bitcoin Gold in 2017).[46] Unfortunately, the developers' decisions could reduce the value of an investment in the blockchain to zero before an investor is able to get out (by selling the cryptocurrency to a willing buyer). Much is made of token-holders' 'right to exit' via the forking process or selling the token;[47] however, 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 they are still owed fiduciary duties by officers and directors of the company.

One could also argue that developers are in some ways entrusted with property, given the trend to view cryptocurrency tokens as commodities or digital assets.[48] Developers are essential to maintaining the existence of these digital assets—if they mess up the coding (deliberately or unintentionally), the digital asset could cease to exist, analogous to what happened with the famous Parity bug in 2017, when millions of dollars of the cryptocurrency ether became inaccessible.[49] In this way, developers are important caretakers of other people's money.

C. Risk to entrustors that fiduciaries may not be trustworthy

Frankel's third indicator of a fiduciary is that 'entrustment poses to entrustors the risks that the fiduciaries will not be trustworthy. They may misappropriate the entrusted property, misuse the entrusted power or they will not perform the promised services adequately.'[50] This factor deals with both trustworthiness (the possibility of exploitation by the fiduciary) and competence (performing the promised service to an acceptable standard).

There are many ways in which developers could exploit their positions or fail to act with competence, in both cases harming those who rely on the relevant blockchain.

As with any position of power, conflict-of-interest situations can and do arise for key developers. These crop up most obviously with their compensation. Although open-source software is generally developed by software developers in their spare time as an unpaid hobby, the public blockchains of Bitcoin and Ethereum have worked differently. Keeping multi-billion-dollar systems working 24/7 is too demanding for hobbyists, so people involved with Bitcoin and Ethereum have found ways of paying important developers for their time. With Ethereum, a Swiss non-profit company called the 'Ethereum Foundation' was created and crowd-funded through the first initial coin offering ('ICO'), and pays for the salaries of some developers, along with other administrative and advisory staff.[51] With Bitcoin, there have

[46] Recent 51% attacks against Bitcoin Gold, a forked network from the original Bitcoin chain, demonstrate that a forked network may have different (in this context, lesser) properties than the original network, including potentially less security if it has less mining power devoted to it or less experienced software developers. See Daniel Oberhaus, 'Cryptocurrency Miners are Sabotaging Blockchains for Their Personal Gain' (*Motherboard*, 25 May 2018) https://motherboard.vice.com/en_us/article/a3a38e/what-is-a-51-percent-attack-silicon-valley-bitcoin-gold-verge-monacoin-cryptocurrency.

[47] E.g. Jeffery Atik and George Gerro, 'Hard Forks on the Bitcoin Blockchain: Reversible Exit, Continuing Voice' (2018) 1 *Stanford Journal of Law and Public Policy*, analyse the availability of shareholder concepts of voice and exit in hard forks of the Bitcoin blockchain.

[48] See *In re Coinflip Inc.*, CFTC Docket No. 15-29 (17 September 2015); *Commodity Futures Trading Commission v. McDonnell*, F. Supp.3d 213 (E.D. NY) (2018); Chris Burniske and Jack Tatar, *Cryptoassets: The Innovative Investor's Guide to Bitcoin and Beyond* (McGraw-Hill 2018).

[49] See Giuseppe Destefanis, Michele Marchesi, Marco Ortu et al., 'Smart Contracts Vulnerabilities: A Call for Blockchain Software Engineering' (2018) IEEE Conference paper, http://dspace.stir.ac.uk/bitstream/1893/27135/1/smart-contracts-vulnerabilities-3.pdf, which conducts a case study of the Parity wallet hack and proposes a special category of 'Blockchain Software Engineering' with higher standards than non-blockchain software development.

[50] Frankel (n 40), 6.

[51] See Joseph Young, 'Vlad Zamfir: Sharding is the Only True Blockchain Scaling Solution' (*BinaryDistrict*, 13 November 2017) https://journal.binarydistrict.com/vlad-zamfir-sharding-is-the-only-true-blockchain-scaling-solution-/: 'Although initial coin offerings (ICOs) and independent blockchain projects have created many millionaire Ethereum developers, Zamfir explained that most Ethereum core developers earn salaries that are much

been a variety of ways of compensating the core developers, including having them work at the MIT Media Lab, for private companies within the Bitcoin ecosystem (e.g. Blockstream, BitPay), and/or under a sponsorship model.[52]

As I have previously argued,[53] this compensation structure sets up a clear conflict of interest for developers, who may feel pressured to make decisions about the blockchain that favour their salary payer's interests. A quick scan of Twitter, Reddit, or any blockchain message board reveals that there are vastly different opinions on virtually every decision that a developer might make, meaning that conflicts of interest among the key developers are relevant to anyone relying on the applicable blockchain.

This is not purely hypothetical. Leading developers have been accused of being improperly influenced by those who pay their salaries[54] or by their own financial interests.[55] A risk of exploitation of the position could also arise through key developers' interactions with regulators or policy makers on behalf of the blockchain. For instance, Ethereum founder Vitalik Buterin famously met with Vladimir Putin and Gavin Andresen met with the Central Intelligence Agency/Federal Bureau of Investigation when he was the leading core developer of Bitcoin.[56] Meetings with regulators or policy makers may not be open to the public, so users of the blockchain must simply trust that the developers are acting in users' interests rather than their own in these meetings.

There are infinite ways in which key developers could fail to act with competence on behalf of those who rely on the blockchain. A few quick examples include failing to discover and fix a security flaw in the code, misjudging the risks of a proposed change to the software, or acting in a way that causes regulators to lose faith in the blockchain, all of which could seriously damage those relying on the blockchain.

It is clear that users of blockchain tokens and any financial products based on them, as well as those building businesses in connection with a blockchain, are vulnerable to both untrustworthiness and lack of competence by key developers, particularly those users who do not have expertise in blockchain software development.

D. Difficulty or failure of entrustors to protect themselves from fiduciary risks

Frankel's fourth characteristic of fiduciaries is:

> there is likelihood that [a] the entrustor will fail to protect itself from the risks involved in fiduciary relationships; [b] the markets may fail to protect entrustors from these risks; and that [c] the costs for the fiduciaries of establishing their trustworthiness may be higher than their benefits from the relationships.[57]

This factor deals with the vulnerability of entrustors to fiduciaries and the likelihood that neither they nor markets will provide protection from this vulnerability.

It is likely that in public blockchains, certain entrustors will fail to protect themselves from the risks involved in a fiduciary relationship with developers. This is due to the expertise

lower than the market standard. "I agree with the general statement that core developers are not sufficiently incentivized", he noted. "Some Ethereum developers are paid by the Ethereum foundation, but at what are now below market salaries. I think core developers provide a huge amount of value as a public good", added Zamfir. "Public goods are inherently difficult to fund, because the non-excludable nature of their benefits means that even those who don't pay get to enjoy the benefits."'

[52] Walch, 'The Bitcoin Blockchain as FMI' (n 11), 878–79. [53] ibid.

[54] See, e.g., Whalecalls, 'Fact or FUD: Blockstream, Inc. is the Main Force Behind Bitcoin (and Taken Over)' (*Medium*, 1 December 2017) https://medium.com/@whalecalls/fud-or-fact-blockstream-inc-is-the-main-force-behind-bitcoin-and-taken-over-160aed93c003, discusses the common statement that the company Blockstream controls Bitcoin software development because it employs several core developers.

[55] See nn 33 and 34. [56] See n 22. [57] Frankel (n 40), 6.

barrier between blockchain software developers and users who cannot evaluate software code themselves. In 'permissionless' systems like public blockchains, there is nothing that prevents people who lack software expertise from becoming involved with a given blockchain, whether through the purchase of tokens or token-based financial products, or by investing in or creating a business tied to the blockchain. Anyone who lacks expertise in the particular code of the blockchain (some of which are coded in newly developed software languages like OCaml)[58] will have a difficult time protecting themselves from the actions of developers, as they are unable to meaningfully evaluate the software code and any proposed changes to it. They simply have to count on the developers to make good policy and technical decisions. The counter-argument to this is that if non-technical people want to use public blockchains, they should be willing to pay to have the code vetted and warrantied for them or accept that any use of the blockchain is *caveat emptor*. This may be somewhat persuasive when talking about direct purchasers of public blockchain tokens but is unpersuasive in the case of public blockchains serving as infrastructure, when people do not have a meaningful choice about their reliance on the blockchain. It is also impractical for entrustors to vet the loyalty and character of each influential developer of a public blockchain in order to evaluate whether they have a conflict of interest on certain issues.

Furthermore, 'fiduciaries that serve numerous entrustors in a standardized manner [as is the case with developers of public blockchains] acquire power that is greater than the power of fiduciaries that serve individuals'.[59] This is true in public blockchains because the decisions and actions of developers affect an entire blockchain system, rather than a single person. Moreover, 'the entrustors' ability to control their fiduciaries is weakened with the rise in the entrustors' number. The entrustors may not be well organized and may have different interests and different ideas about the benefits that their fiduciaries must pursue.'[60] This manifests in public blockchains as entrustors (token holders, businesses providing blockchain-related services, and systems building atop a blockchain) have extremely divergent views on the decisions and actions developers should take, which may dilute the control they exercise over developers.

There are arguments on both sides as to whether the market is likely to protect entrustors from the risks involved in trusting developers. One could argue that users of tokens who can evaluate software code will serve as market guidance to the entrustors who cannot evaluate code, as code-savvy people will signal their belief in the software code quality and the philosophy embedded in it by using the applicable token, or by building businesses related to the token. If tech-savvy people do not believe in the quality of the developers or their code, they will avoid a particular blockchain and non-tech-savvy people will pick up on these signals and also avoid that blockchain. Unfortunately, however, this argument seems to have been disproven by events in the cryptocurrency and ICO space in 2017–2018. Investors have poured billions into ICOs, though in many cases, little detail has been provided on the technology or the development team behind the technology.[61] Despite warnings from numerous regulators and policy makers, many scams have occurred, suggesting that market signals may not enable entrustors to responsibly evaluate a public blockchain and its developers.[62]

Finally, the costs for software developers serving as fiduciaries of establishing their trustworthiness may be higher than their benefits from the relationship. This may be particularly true in public blockchains that rely on grassroots open-source software governance, with uncertainties of how the work of software developers is funded.[63] Developers

[58] Tezos is coded in OCaml. [59] Frankel (n 40), 11. [60] ibid.

[61] David Floyd, '$6.3 Billion: 2018 ICO Funding Has Passed 2017's Total' (*CoinDesk*, 19 April 2018) https://www.coindesk.com/6-3-billion-2018-ico-funding-already-outpaced-2017/.

[62] See De Nikhilesh, 'SEC Halts Mayweather-Endorsed ICO, Charges Founders with Fraud' (*CoinDesk*, 2 April 2018) https://www.coindesk.com/sec-halts-mayweather-endorsed-ico-charges-founders-fraud/.

[63] Walch, 'Open-Sourced Operational Risk' (n 11), 256–59.

must spend significant time and effort gaining credibility and respect for their competence in order to be granted 'commit access' rights. Yet, as discussed in section IIIC, the mechanics of compensation for these efforts are uncertain and evolving, with no established way of paying developers for their extensive time and effort. A recent example of this phenomenon occurred in the Zcash public blockchain when a key developer threatened to quit working on Zcash wallet software (for which he was the sole maintainer and which could potentially affect thousands of users) and to create a competing blockchain because he was not being paid for his work, resulting in money quickly being contributed to the developer.[64]

* * *

Once we acknowledge that certain developers resemble fiduciaries, even if there is not a perfect likeness, the instincts that people have had all along make sense. For instance, there has been discussion about the need for increased transparency from the Ethereum Foundation, which apparently funds development of Ethereum, but provides very little public information about its structure, governance, or funding.[65] This instinct towards transparency suggests that the developers realize that they are acting on behalf of others and owe those they represent transparency about their actions. There have been comments from key developers that indicate they appreciate the heavy responsibility they bear to keep the blockchain running.[66] Recently, one of six core developers of Ethereum software resigned from his role because he was concerned about personal legal risk.[67] Finally, discussions about the compensation of core developers and commentary about conflicts of interest suggest that some have recognized the power certain developers exercise in relation to users.[68]

If certain people are functioning as fiduciaries, the question becomes 'What do we war to do about it?' From a policy perspective, there are clear arguments that those who ac as fiduciaries should be legally accountable as fiduciaries. However, treating these par ties as fiduciaries with concomitant liability would go against our existing liability framework for software systems, which generally enables those who create software to disclaim liabilities for its flaws or harms it causes[69] and has been resistant to characterizing those creating, designing, or building software as professionals subject to claims of professional malpractice.[70]

[64] Rachel O'Leary, 'Zcash Pays Off Developer to Avoid Blockchain Split' (*CoinDesk*, 22 June 2018) https://www.coindesk.com/zcash-pays-off-angry-developer-avoid-blockchain-split/.

[65] See Ethereum Foundation Website, https://ethereum.org/foundation. It lists three members of the Ethereum foundation but provides no information concerning governance, funding, or relationship to Ethereum software development. For discussion of lack of transparency, see Bob Summerwill, Tweets on Ethereum Foundation opacity (*Twitter*, 29 December 2017) https://twitter.com/BobSummerwill/status/946760015322398720. These state that 'there is no public list of who works for the Ethereum Foundation. There is no list of the projects which the Foundation funds or how much it funds them. There is no public information on the governance of the EF ... There is no public information on the legal entities within or funded by the EF. There is no public information on the composition of the board of the EF or voting structure. There is no public information on who advises the EF.'

[66] See Jonas Schnelli (Bitcoin core developer), Tweets (*Twitter*, 15 November 2017) https://twitter.com/_jonasschnelli_/status/930680174697381888: '4 developers have currently commit access: @orionwl @pwuille @MarcoFalke and myself. It's a burden. It's for those who are willing to review and test code and keep up with the ~80 github comments per day. It's not always fun and it's certainly not a privilege.'

[67] Rachel O'Leary, 'Ethereum Developer Resigns as Code Editor Citing Legal Concerns' (*CoinDesk*, 15 February 2018) https://www.coindesk.com/ethereum-developer-resigns-as-code-editor-citing-legal-concerns/.

[68] See nn 33 and 34.

[69] For a recent overview of the 'unusual liability cocoon' that software vendors enjoy, see Marian Reidy and Bartlomiej Hanus, 'It is Just Unfair Using Trade Laws to Out Security Software Vulnerabilities' (2017) 48 *Loyola University Chicago Law Journal*, 1111–14.

[70] Michael D. Scott, *Scott on Information Technology Law* (3rd edn, 2nd Supplement, Aspen 2018), Section 15.09[A]: 'whether computer designers or programmers are professionals in the legal sense is still an open question'.

IV. Costs and Benefits of Fiduciary Characterization

Although there are many ways that dominant developers resemble fiduciaries, the analysis here would be incomplete without considering the costs and benefits of such a categorization. In this section, I provide an initial sketch of these costs and benefits (in a non-quantitative sense) and leave exhaustive exploration of them to future work.

A. Benefits

The benefits of the fiduciary categorization go back to the roots of the fiduciary relationship: society gains when people can enter into relationships of trust, knowing that the trusted party has certain underlying obligations to them. These benefits include:

1. ensuring that the fiduciary takes the performance of his or her services seriously, and, thus, performs them with deliberation and care;
2. reducing harms caused by people, on whom others rely, acting without care or competence, or exploiting those that rely on them;
3. increasing efficiency and economic activity due to a reduction in the investigation and due diligence that has to be done before every transaction with a fiduciary[71]—if one has fiduciary duties, the entrustor does not have to exhaustively research the person before entering into a transaction with him or her;
4. the creation of an accountability standard that matches the seriousness of the services performed by the fiduciary.

Connecting these benefits more closely with public blockchains, characterizing certain developers as fiduciaries would theoretically have the following impacts.

(a) Developers would seriously consider the consequences of their policy and technical choices, obtain advice from expert sources when needed and use great care in drafting and reviewing code and all other actions they take whilst acting on behalf of the blockchain.

(b) Greater care would result in better decisions by developers, about both conflicts of interest and substantive coding matters, meaning that those relying on the blockchain would likely be harmed less.

(c) Less particularized due diligence of individual developers would be needed by those relying on the blockchain, meaning users would not have to keep track of the current cast of developers and do exhaustive research on each one in an ongoing evaluation of continued participation in the blockchain. This would minimize the resources needed to evaluate participation in the blockchain, which, in turn, would increase efficiencies.

(d) There would be an acknowledgement that certain developers are making high-stakes decisions on critical matters, such as finance and money, on behalf of others and so are accountable in a way that more closely approximates the stakes involved. (As mentioned in the concluding paragraph of section III, it is notoriously difficult to hold anyone liable for problems caused by software, in part due to the 'economic loss' rule in tort law and in part because software licenses generally disclaim all liability for anything related to the software.)[72]

[71] Frankel (n 40), 271–72. [72] See Reidy and Hanus (n 69).

B. Costs

Of course, there are reasons not to view any developers as fiduciaries, many of which are commonly made against the idea of regulation itself.

1. The primary argument against categorizing certain developers as fiduciaries is that the categorization could inhibit innovation. If these parties have to be worried about the effects that their actions would have on others, this will stifle their creativity and hold back development in the area because people will be afraid to try things that might go wrong. It is too early to intervene in the development of blockchain technology.
2. We need not worry about the governance of public blockchains because they are 'platform' technologies and legal intervention is only appropriate at the application level or with intermediaries, such as wallet companies or exchanges.
3. A fiduciary characterization is too extreme and too high a duty to place on these people. It would not be fair to treat them as fiduciaries based on what they are doing here.
4. Given the large pool of potential beneficiaries who will have differing interests, it would be impossible to tell when developers have met the fiduciary standard. A more general duty to the public owed by certain developers may be more appropriate for these public infrastructural technologies.
5. Treating certain developers as fiduciaries could deter them from participating in what may be socially beneficial projects as they will fear potential liability.
6. Protecting those who rely on public blockchains through a fiduciary categorization is paternalistic and discourages people from doing proper due diligence when evaluating their participation in public blockchains. This discourages self-reliance and personal accountability in decision making.
7. It would be unfair to set such a high standard for developers as participants in these public blockchains may not have had such accountability expectations when they decided to participate.
8. Developers are not compensated at a level consistent with the high accountability standard of a fiduciary. If their accountability risks increase, they will demand more money to provide the services.
9. Too little is at stake now with public blockchains to bother with a fiduciary standard of performance by developers.

Perhaps, in the end, the costs of the fiduciary categorization to innovation are balanced in the aggregate by the harms that are avoided by, and investigations that entrustors would otherwise have to do before, relying on the fiduciary's actions. Further research in this domain would be useful.

V. Sorting Out the Details

> To say that a man is a fiduciary only begins the analysis; it gives direction to further inquiry. To whom is he a fiduciary? What obligations does he owe as a fiduciary? In what respect has he failed to discharge these obligations? And what are the consequences of his deviation from his duty?[73]

As Justice Frankfurter noted in *SEC v. Chenery Corp.* in 1943, one does not conclude an analysis by simply stating that a party is a fiduciary.[74] For any given public blockchain, a tailored

[73] *SEC v. Chenery Corp.*, 318 U.S. 80 (1943), 85–86. [74] ibid.

evaluation would be necessary to determine whether a particular developer is acting as a fiduciary.

In this section, I identify some of the nuances and practical matters that would need to be considered and resolved if a legislature or a court were evaluating whether to treat particular software developers of a public blockchain as fiduciaries. In some instances, I suggest appropriate resolutions but further work beyond the scope of this short chapter is necessary to draw firmer conclusions.

A. Who are the fiduciaries?

I have suggested that certain developers resemble fiduciaries in their role in public blockchains but this does not resolve the question. It seems problematic to consider *any and every* software developer who participates in blockchain code development to be a fiduciary as only a small subset (probably including the core developers) actually determine what makes it into the released code. Similarly, it would be problematic to focus solely on those who craft the code, ignoring those who may determine the policy choices to be reflected in the code, which is why I have incorporated these types of parties into my use of the term 'developer' in this chapter.[75] In a spectrum of 'fiduciary-ness', those developers who make the most decisions on behalf of others look a lot like fiduciaries, while those who occasionally make code proposals do not. Fiduciary developers would likely include developers who initially design and/or launch the system, those involved in decision making around new releases of software, including policy and technical choices as well as code review, and those who make decisions about how to address a crisis faced by the system (e.g. a critical bug or an attack on the system).

B. Who are the entrustors?

Thus far, I have been somewhat vague about who, precisely, are the parties to whom key developers would act as fiduciaries. In Frankel's parlance, who are the 'entrustors'?

There are a variety of parties who inhabit a blockchain ecosystem. In addition to the software developers and miners already identified, there are owners of the native tokens (cryptocurrencies) of a blockchain (e.g. bitcoins and ether), businesses that service those who own and trade in cryptocurrencies (exchanges, wallets, payment processors, financiers), and companies that are using the underlying blockchain as a platform for other forms of recordkeeping, such as trading or property records. All of these parties rely on the successful ongoing operation of the relevant public blockchain. In the future, a wider swath of the public could unknowingly rely on the operation of public blockchains, if they become part of underlying recordkeeping infrastructures that are not seen by the public.[76] Further, as Bitcoin, Ethereum, and other tokens are now being described as 'crypto-assets' with financial products like futures being tied to them, the holders of these cryptocurrency-based financial products also rely on developers.

The trick here will be to determine which of these groups are considered 'entrustors' and entitled to the protections of, and obligations imposed by, fiduciary duties. Users of the applicable cryptocurrency appear to have the most reliance on the blockchain, but there are arguments that the other businesses within the ecosystem do as well. Ultimately, the fact that the public could be impacted if public blockchains become infrastructure, or if cryptocurrencies become systemically important to the financial system, may mean that

[75] See n 4.

[76] There is much discussion about how blockchains will ultimately just be invisible to the public, much as the internet infrastructure is largely opaque to the public now.

these fiduciary duties run to the public at large, similar to how certified public accountants are obligated to act to 'serve the public interest [and] honor the public trust'[77] or perhaps through the common law doctrine of public trust, which 'imposes on governing bodies fiduciary duties toward the public'.[78] With much discussion of how public blockchains are analogous to sovereign entities,[79] the doctrine of public trust may also be a useful lens through which to view their governance processes.[80] A full spelling-out of these arguments is beyond the scope of this chapter but is an important area for further research.

C. What are the duties owed?

As Justice Frankfurter noted, we must ask what obligations one owes as a fiduciary. Again, deeper analysis is merited but the basic fiduciary duties of care and loyalty are a good starting point. Since leading developers look a lot like officers or directors of a corporation (if one views tokens as shares of stock in the corporation) having analogous fiduciary duties may make sense. A more fulsome analysis would look at whether the protections of the 'business judgment rule' used in the corporate setting would be appropriate here.[81]

The duties of care and loyalty fall in neatly with the fiduciary definition provided by Frankel above. As discussed in section III, both competence (as part of the duty of care) and acting on behalf of the entrustor rather than oneself (as part of the duty of loyalty) are expectations that leading developers are probably already trying to live up to, and blockchain users expect them to uphold.

D. How might fiduciary status of developers arise?

Perhaps the most difficult question to answer around the fiduciary characterization is how exactly the status would arise. As Frankel has noted, 'one cannot find a clear answer to the question of whether a relationship is fiduciary'.[82] Yet software developers and public blockchain advocates are quick to point to the open-source software licenses under which public blockchain software is issued, which generally disclaim liability for any claims arising from the software.[83] Furthermore, foundations associated with public blockchains may separately attempt to disclaim liability for claims related to the blockchain for the foundation

[77] American Institute of CPAs Code of Conduct, Section ET 53 Article II https://www.aicpa.org/research/standards/codeofconduct.html.

[78] See Frankel (n 40), 36 ('in the case of professional services, entrustors may include not only particular persons or groups but also the public and society'), 36–37 ('The fiduciary relationship of financial intermediaries may sometimes include a relationship to the financial system'), and 125.

[79] See Marcella Atzori, 'Blockchain Technology and Decentralized Governance: Is the State Still Necessary?' (2017) 6 *Journal of Governance and Regulation*, 45, who analyses claims of blockchains to represent new forms of governance as alternatives to sovereign states; Sarah Manski and Ben Manski, 'No Gods, No Masters, No Coders? The Future of Sovereignty in a Blockchain World' (2018) 29 *Law Critique*, 151, who discuss claims of sovereignty around blockchains.

[80] See Frankel (n 40), 279–87 for a discussion of government officials' fiduciary duties to the public. See also Ethan J. Leib, David L. Ponet, and Michael Serota, 'Translating Fiduciary Principles into Public Law' (2013) 126 *Harvard Law Review Forum*, 91, for an overview of the 'burgeoning field' of 'fiduciary political theory'.

[81] The fluctuating scrutiny of directors' actions in corporate law depending on the significance of the event may have resonance for developer fiduciary status. Director actions receive enhanced scrutiny when they relate to facilitating or fending off a change of control, for instance, which is analogous to a hard fork in a public blockchain. See *Revlon Inc v. MacAndrews and Forbes Holdings, Inc.*, 506 A 3d 173 (Delamere 1986); *Unocal Corp. v. Mesa Petroleum Co.*, 493 A 2d 946 (Delamere 1985). Carla Reyes notes this analogy in a draft paper, Carla Reyes, 'Corporate Crypto Governance' (26 January 2018) Blockchain Works-in-Progress Workshop, at Cardozo Law School.

[82] Frankel (n 40), 77.

[83] See, e.g., MIT License, https://opensource.org/licenses/MIT; GNU General Public License, https://www.gnu.org/licenses/gpl-3.0.en.html.

and any software developers employed by or contracted with the foundation.[84] One could argue that any potential liability as a fiduciary is already disclaimed so there is little point in discussing the matter further.

However, the presence of legal disclaimers in these documents does not resolve the question. Fiduciary duties can arise in a number of ways—by contract, by statute,[85] by acting as a fiduciary in the eyes of a court, or by status. Indeed, there is an ongoing debate in fiduciary law over whether fiduciary categorization is based solely on contract (and may be contracted out of by the parties) or whether there are situations in which fiduciary status arises by virtue of relationship or status and may not be disclaimed.[86] This has implications for the treatment of developers in public blockchains.

If one views fiduciary status as being purely contract-based, then one could argue that a broad liability disclaimer and failure to affirmatively create a fiduciary relationship by contract would mean no fiduciary status or liability could attach to a developer. One may attempt to argue that the contract between users and developers implies a fiduciary status[87] but it may be difficult to persuade a court of such. However, there is no certainty that the open-source software licenses will be enforced[88] and there are questions about which particular parties would be bound to the licenses. Not all owners of bitcoins, ether, or other cryptocurrencies actually run the software themselves and many may never see the related open-source software license. They may obtain their cryptocurrencies through intermediaries, like exchanges, or they may be exposed to what happens to cryptocurrencies through derivatives like futures contracts or investment funds. This raises questions about whether a given user of a cryptocurrency was on notice of the license terms and is, therefore, bound to them. Overall, though, it could be difficult to show that a fiduciary relationship was established by contract between developers and entrustors (whoever those entrustors are).

However, we may not need to show a contract establishing a fiduciary relationship for developers to be treated as fiduciaries, and even if the liability disclaimers around the software are upheld, they may not apply to breach of fiduciary claims.[89] A court could view developers to be acting as fiduciaries, due to the characteristics identified in section III, and be willing to treat them as such. Courts are generally reluctant to create new types of fiduciaries but it does happen, often over a period of time.[90] Frankel has identified spouses, mediators,

[84] See, e.g., Ethereum Legal Agreement, (*ethereum.org*), https://www.ethereum.org/agreement, which disclaims liability for both the Ethereum Foundation and software developers employed by or contracted with the Ethereum Foundation.

[85] For example, the Employee Retirement Income Security Act of 1974 (ERISA) 29 USC 1002(21)(A) statute deems certain parties to be fiduciaries.

[86] For the contractarian view, see Frank H. Easterbrook and Daniel R. Fischel, 'Contract and Fiduciary Duty' (1993) 36 *Journal of Law and Economics*, 425; Henry N. Butler and Larry E. Ribstein, 'Opting Out of Fiduciary Duties: A Response to the Anti-Contractarians' (1993) 65 *Washington Law Review*, 1. For the anti-contractarian view and a summary of the contract/status debate, see Frankel (n 40), 229–39.

[87] See Dirk Zetzsche, Ross Buckley, and Douglas Arner, 'The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain' (2018) *University of Illinois Law Review*, 1392–96, which analyses contract-based claims against parties involved with public blockchains, including developers.

[88] There has been little case law around the enforceability of open-source software licenses (and their liability disclaimers) thus far.

[89] See *Northeast Gen. Corp. v. Wellington Adv.*, 82 NY 2d 158, 172. Hancock, J., dissenting: 'It is fundamental that a fiduciary duty "is not dependent solely upon an agreement or contractual relation between the fiduciary and the beneficiary but results from the relation.' See Deborah DeMott, 'Beyond Metaphor: An Analysis of Fiduciary Obligation' (1988) *Duke Law Journal*, 887: 'contractual obligations are controlled by the parties' manifest intention; fiduciary obligation sometimes operates precisely in opposition to intention as manifest in express agreements. The terms of an express agreement are surely not irrelevant to the fiduciary obligation analysis, but once a court concludes that a particular relationship has a fiduciary character, the parties' manifest intention does not control their obligations to each other as dispositively as it does under a contract analysis.'

[90] See *Lash v. Cheshire County Savings Bank*, 474 A 2d 980 (NH 1984), which found a fiduciary relationship between a bank official and a bank customer in connection with confidential information entrusted by the customer to the official despite no explicit contractual agreement regarding the fiduciary nature of the relationship; *Martinelli Bridgeport Roman Catholic Diocesan Corp.*, 10 F Supp 2d 138 (D Conn 1998), which found a fiduciary relationship between a church and its parishioner based on 'an approach [of examining] the power relationship

and mortgage brokers among others, as emerging fiduciaries,[91] and more recently, Jonathan Zittrain and Jack Balkin have proposed treating tech companies who hold personal data as 'information fiduciaries'.[92] As I have argued throughout this chapter, there are many reasons why courts might be willing to view certain developers of public blockchains as fiduciaries, including the superior expertise and skill needed for public blockchain software design and development,[93] as well as the fact that public blockchains purport to embed and transfer value (cryptoassets or cryptocurrencies) for an entire blockchain system, thereby making developers' actions highly consequential for potentially large numbers of people.

Finally, developers could be deemed fiduciaries of a public blockchain by statute. With virtually every law-making body and regulatory agency worldwide considering how to treat blockchain technology and cryptoassets/cryptocurrencies, this is not an impossibility. As developers continue to take fiduciary-type actions within public blockchains and with the current questioning over power and ethics in the tech sector generally such a statutory designation becomes more likely.

E. How would a breach of duty be identified?

Identifying a breach of duty here would be challenging but perhaps no more challenging than it is in other complex tort problems. One of the primary challenges would be establishing that a particular action caused harm. It can be hard to identify which lines of code cause a problem as there are complex interactions that occur in the running of the software. Even once the problematic code is located, it may be difficult to pin it to a particular developer. What happens if a portion of code is fine until a later update makes it problematic? Furthermore, what happens if a core developer recommends a hard fork that turns out to do great damage to the blockchain and its users?

Presumably, if such a fiduciary standard existed, those subject to the standard would document their investigation of issues and the rationale for their decisions, much like lawyers regularly do. This type of behaviour would help to demonstrate that the fiduciary had fulfilled its responsibilities. Of course, taking action to avoid liability arguably leads to wasted efforts demonstrating compliance with the standard and could steal time from more productive use. However, a good amount of documentation around the process of proposing and evaluating changes to software code is a common part of open-source software development through sites like GitHub, so there may be few significant changes required in practice.

F. What are the consequences of a breach of the duty?

The consequences of a breach of such a fiduciary duty would arguably be that the 'entrustors' (whichever parties are deemed to fall in that bucket) would have a cause of action against the fiduciaries for the breach.[94] This means that fiduciary developers could, depending on who is deemed an entrustor, be subject to liability claims from an enormous number of people—users of the applicable cryptocurrency, potentially along with businesses building

and its potential for abuse'. For a discussion on how courts recognize new types of fiduciaries, see Frankel (n 40), 220–22.

[91] Frankel (n 40), 53–58.

[92] Jack M. Balkin and Jonathan Zittrain, 'A Grand Bargain to Make Tech Companies Trustworthy' (*The Atlantic*, 3 October 2016) https://www.theatlantic.com/technology/archive/2016/10/information-fiduciary/502346/.

[93] Destefanis et al. (n 49).

[94] Claims for breach of fiduciary duty are sometimes treated as tort claims and other times as contract claims, with a wide variety of remedies possible. Depending on the situation, monetary damages (compensatory or punitive), equitable remedies (like injunctions), rescission, or disgorgement of any profits made by the fiduciary as part of breaching the duty, may be available. See Dan Dobbs, Paul Hayden, and Ellen Bublick, *Dobbs' Law of Torts*, (2nd edn, Thomson West, June 2017 update), Section 699.

on and servicing the blockchain. Despite any cryptocurrency that they may have previously managed to cash out, it would likely be very difficult for any of these fiduciary developers to satisfy their liabilities—the cost of making whole an entire blockchain would simply be too great. This situation—the fact that the economic (or other) harms caused by parties deemed fiduciaries may be too great for them to cover—could cast doubt over whether the fiduciary categorization is worthwhile, if the entrustors are unlikely to ever be made whole.

Working out the consequences of a breach of fiduciary duty may lead to varying proposals, such as requiring some sort of malpractice insurance or directors' and officers' (D&O) insurance or bond for those with the fiduciary duties, or requiring a certification or licensure to engage in high-stakes, high-trust positions like those of leading developers. Indeed, a recent computer science paper called for a higher standard of software engineering for blockchain software development, given its particularly difficult nature and the high stakes involved with errors.[95]

Potential for liability claims may also incentivize developers to form a more traditional legal organizational structure for a public blockchain, such as a corporation or limited liability company. (Of course, adopting a traditional legal structure goes fundamentally against the core ideal of decentralized governance in public blockchain systems.)

G. Could a fiduciary standard be enforced?

Many who work with public blockchains do so based on an ideology of libertarianism or even anti-government or anarchic beliefs. Escaping government altogether through the technology is of great significance; a duty does not have any bite unless it is able to be enforced.

Enforcement of a fiduciary duty, when the fiduciaries are spread across the globe and perform their services from numerous different jurisdictions, would be complicated. Threading this needle would require recognition of the fiduciary relationship by the appropriate legal authorities as well as actually tracking down the people involved, some of whom may perform their services anonymously. Attempting to bring accountability to infrastructures on which the public relies could drive those wishing to avoid accountability further into the shadows. However, those who wish to legitimize the technology may be willing to step up and acknowledge the appropriateness of accountability in this area.

Opinions diverge on whether nation states can actually hold parties operating public blockchain systems accountable.[96] The matter remains unsettled but states have been able to enforce laws in cyberspace so I would expect them to work out a way to do the same in 'blockchain space'.

* * *

As always, the devil is in the details and many questions still need answers before this issue is resolved. Most of the questions will not have clear answers; rather, they will require a careful balancing of costs and benefits, fairness, public policy concerns, etc. However, the inquiries remain worthwhile despite the challenges they present.

VI. Ongoing Experiments in Governance and Accountability

The public blockchain world is incredibly fast-moving, with new blockchain systems constantly being created and existing ones working to fix governance issues as they are revealed. A number of blockchain systems have now explicitly incorporated governance into their

[95] Destefanis et al. (n 49).

[96] DeFilippi and Wright (n 7), 181–83, discuss government regulation of blockchain software developers and enforcement challenges.

designs from the outset; some of these new systems may structure the power of software developers differently than Bitcoin or Ethereum. Additionally, legal scholars, along with researchers in the blockchain community, have begun to weigh in with initial analyses of and proposals for public blockchain governance.

Tezos,[97] EOS,[98] Decred,[99] and Dfinity[100] are examples of public blockchains using or planning to use alternative governance processes, with variations in the powers of validators in the network or how changes to software are made. After starting out eschewing the need for governance entirely, those working on public blockchain networks have recognized the critical role governance plays in a system's success.[101] A field of study called 'cryptoeconomics' is being developed to design incentive structures intended to result in transaction processors providing security (resistance to attack) for a blockchain.[102] These 'consensus mechanisms' (or, rules for coming to agreement) for transaction processors play a significant role in the governance of public blockchain systems, indicating just how rich, complex, and nascent this area of study remains.

Legal scholars have begun to grapple with the governance questions raised by public blockchains. For example, Philipp Hacker has proposed fitting a corporate governance framework onto blockchains.[103] Carla Reyes has proposed that a business trust may be a suitable form of legal entity for blockchain developers and other players in the system to take advantage of limited liability without having to formally create a corporation or limited liability company.[104] Each of these analyses, in acknowledging the role that software developers play in the governance process of public blockchains, implicitly acknowledges that certain software developers fulfil roles of trust and power in public blockchain systems.[105]

All of this is to say that public blockchain governance and the theorizing around it remain works in progress. Nevertheless, I feel pretty comfortable predicting that systems based on software will continue to require software developers to create code (with all the processes, decisions, and judgement calls that are involved). (And yes, I hear those of you saying, 'But AI ...').

VII. Broader Implications and Concluding Thoughts

This chapter focuses on the behaviours of software developers in the public blockchain context. They provide a neat example of a potentially new type of fiduciary acting in today's world and my hope is that this chapter opens the door to further research on the matter and also alerts regulators and policy makers to the need to press hard on the 'decentralized' reputation of public blockchains.

[97] Tezos website, https://tezos.com/. [98] EOS website, https://eos.io/.

[99] Decred website, https://www.decred.org/. [100] Dfinity website, https://dfinity.org/.

[101] See, e.g., Fred Ehrsam, 'Blockchain Governance: Programming Our Future' (*Medium*, 17 November 2017) https://medium.com/@FEhrsam/blockchain-governance-programming-our-future-c3bfe30f2d74; Vlad Zamfir, 'Against On-Chain Governance' (*Medium*, 1 December 2017) https://medium.com/@Vlad_Zamfir/against-on-chain-governance-a4ceacd040ca.

[102] See Josh Stark, 'Making Sense of Cryptoeconomics' (*Medium*, 28 August 2017) https://medium.com/l4media/making-sense-of-cryptoeconomics-c6455776669. A helpful compilation of resources on cryptoeconomics is available at https://github.com/jpantunes/awesome-cryptoeconomics.

[103] See Philip Hacker, chapter 7 in this volume.

[104] Carla Reyes, 'If Rockefeller Were a Coder' (forthcoming) 87 *George Washington Law Review*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3082915.

[105] Other researchers have examined the potential liability of software developers of public blockchain systems. See Zetzsche et al. (n 87); Tim Swanson, 'Who are the Administrators of Blockchains?' (*OfNumbers Blog*, 19 October 2017) http://www.ofnumbers.com/2017/10/19/who-are-the-administrators-of-blockchains/; Ciaran Murray, 'Are Public Blockchain Systems Unlicensed Money Services Businesses In Disguise?' (*Rules of the Game Blog*, 12 October 2017) http://rulesofthegame.blog/2017/10/12/are-public-blockchain-systems-unlicensed-money-services-businesses-in-disguise/.

We must be vigilant as to how our legal and social concepts need to change as our technologies and practices change. As we experiment in technology and with new methods of governance, our legal concepts need to expand to accommodate these experiments. It may be helpful to focus on the function and activities performed by a party, rather than on what they call themselves. If the developers had formed a corporation to launch and operate these public blockchains (rather than having separate foundations to pay developers), no one would question that the officers, directors, and controlling shareholders of that corporation had fiduciary duties in their leadership roles and that the corporation should be accountable for harms that it causes (like Volkswagen is accountable for its deceptive emissions code). Yet, we seem mystified by the nominally decentralized governance and unable to see that a spade is still a spade (is still a fiduciary).

Blockchain technology has jumped into the deep end very early in its life. The functions that its proponents expect it to perform are critical, infrastructural functions in our societies. As coding becomes infrastructure building and maintenance, it is very much akin to building bridges, or nuclear reactors, or national security structures. And those building and maintaining and making decisions about these core infrastructures must take what they are doing seriously. Blockchain developers must recognize that they are not just building fun technology like Wikipedia or Napster, where a system failure has few significant social consequences.

Furthermore, it is insufficient to focus exclusively on the companies building on top of public blockchains. This approach ignores the people involved in creating and running the network upon which others are building. The *foundations* of this new infrastructure are being built by *people*, people who are making decisions that will impact the operation and success of the new infrastructure. It takes a great deal of expertise to successfully implement these decisions, much less to make the policy choices that the implementation reflects. These are not simply technical decisions being made—there are also, inevitably, policy choices, risk assessments, economic decisions, and ethical judgements happening.

The bottom line is that trust in particular, identifiable people remains fundamental to using 'trustless' public blockchains. The crucial question is—are we willing to acknowledge its existence?

VIII. Bibliography

American Institute of CPAs Code of Conduct, Section ET 53 Article II, https://www.aicpa.org/research/standards/codeofconduct.html, accessed on 9 January 2019.

Antonopoulos Andreas M., *Mastering Bitcoin: Unlocking Digital Cryptocurrencies* (2nd edn, O'Reilly 2017).

Atik Jeffery and Gerro George, 'Hard Forks on the Bitcoin Blockchain: Reversible Exit, Continuing Voice' (2018) 1 *Stanford Journal of Law and Public Policy*, 24.

Atzori Marcella, 'Blockchain Technology and Decentralized Governance: Is the State Still Necessary?' (2017) 6 *Journal of Governance and Regulation*, 45.

Balkin Jack M., 'Information Fiduciaries and the First Amendment' (2016) 49 *University of California Davis Law Review*, 1183.

Balkin Jack M. and Zittrain Jonathan, 'A Grand Bargain to Make Tech Companies Trustworthy' (*The Atlantic*, 3 October 2016) https://www.theatlantic.com/technology/archive/2016/10/information-fiduciary/502346/, accessed on 9 January 2019.

Bayern Shawn, 'Of Bitcoins, Independently Wealthy Software and the Zero-Member LLC' (2014) 108 *Northwestern University Law Review Online*, 1485.

Berke David, 'Products Liability in the Sharing Economy' (2016) 33 Yale Journal on Regulation 603.

Bitcoin GitHub Page, https://github.com/bitcoin/bitcoin, accessed on 9 January 2019.

Biais Bruno, Bisière Christophe, Bouvard Matthiue, and Casamatta Catherine, 'The Blockchain Folk Theorem' (2018) Toulouse School of Economics Working Paper No. 17-817, 14, https://

www.tse-fr.eu/sites/default/files/TSE/documents/doc/wp/2017/wp_tse_817.pdf , accessed on 9 January 2019.

Burniske Chris and Tatar Jack, *Cryptoassets: The Innovative Investor's Guide to Bitcoin and Beyond* (McGraw-Hill 2018).

Buterin Vitalik, 'Notes on Blockchain Governance' (*Vitalik Buterin's Website*, 17 December 2017) https://vitalik.ca/general/2017/12/17/voting.html, accessed on 9 January 2019.

Butler Henry and Ribstein Larry, 'Opting Out of Fiduciary Duties: A Response to the Anti-Contractarians' (1993) 65 *Washington Law Review*, 1.

Camarena Justin, 'I'd agree with a rollback for protocol level hacks... But this isn't that at all. Core devs own DAO' (*Twitter*, 17 June 2016) https://twitter.com/juscamarena/status/744008754459475968, accessed on 9 January 2019.

Camarena Justin, 'they are unfairly slanted to HF'ing to regain their money ... might as well just have a private chain' (*Twitter*, 17 June 2016) https://twitter.com/juscamarena/status/744008863091941376, accessed on 9 January 2019.

Compilation Resource on Cryptoeconomics, https://github.com/jpantunes/awesome-cryptoeconomics, accessed on 9 January 2019.

De Filippi Primavera and Wright Aaron, *Blockchain and the Law: The Rule of Code* (Harvard University Press 2018).

De Nikhilesh, 'SEC Halts Mayweather-Endorsed ICO, Charges Founders With Fraud' (*CoinDesk*, 2 April 2018) https://www.coindesk.com/sec-halts-mayweather-endorsed-ico-charges-founders-fraud/ , accessed on 9 January 2019.

Decred website, https://www.decred.org/, accessed on 9 January 2019.

DeMott Deborah, 'Beyond Metaphor: An Analysis of Fiduciary Obligation' (1988) *Duke Law Journal*, 879.

Destefanis Giuseppe, Marchesi Michelle, Ortu Marco et al., 'Smart Contracts Vulnerabilities: A Call for Blockchain Software Engineering' (2018) IEEE Conference Paper, http://dspace.stir.ac.uk/bitstream/1893/27135/1/smart-contracts-vulnerabilities-3.pdf, accessed on 9 January 2019.

Dfinity Website, https://dfinity.org/, accessed on 9 January 2019.

Dobbs Dan, Hayden Paul, and Bublick Ellen, *Dobbs' Law of Torts*, (2nd edn, Thomson West, June 2017 update).

Easterbrook Frank and Fischel Daniel, 'Contract and Fiduciary Duty' (1993) 36 *Journal of Law and Economics*, 425.

Ehrsam Fred, 'Blockchain Governance: Programming Our Future' (*Medium*, 17 November 2017) https://medium.com/@FEhrsam/blockchain-governance-programming-our-future-c3bfe30f2d74, accessed on 9 January 2019.

Employee Retirement Income Security Act of 1974 (ERISA), 29 USC 1002(21)(A).

EOS website, https://eos.io/ , accessed on 9 January 2019.

Ethereum Classic, 'The Ethereum Classic Declaration of Independence, 20 July 2016', https://ethereumclassic.github.io/assets/ETC_Declaration_of_Independence.pdf, accessed on 9 January 2019.

Ethereum Foundation website, https://ethereum.org/foundation, accessed on 9 January 2019.

Ethereum GitHub page, https://github.com/ethereum/, accessed on 9 January 2019.

Ethereum Legal Agreement (*ethereum.org*) https://www.ethereum.org/agreement , accessed on 9 January 2019.

Fernandes Aakil, 'Ethereum Protocol Developer Holds $114,887 of DAO Tokens' (*Reddit*, 29 June 2017) https://www.reddit.com/r/ethereum/comments/4qiqq8/ethereum_protocol_developer_holds_114877_worth_of/, accessed on 9 January 2019.

Floyd David, '$6.3 Billion: 2018 ICO Funding Has Passed 2017's Total' (*CoinDesk*, 19 April 2018) https://www.coindesk.com/6-3-billion-2018-ico-funding-already-outpaced-2017/, accessed on 9 January 2019.

Frankel Tamar, *Fiduciary Law* (Oxford University Press 2011).

Gencer Adam E., Basu Soumya, Eyal Ittay, Renesse Robbert van, and Sirer Emin G., 'Decentralisation in Bitcoin and Ethereum Networks' (*arXiv.org*, 2018) https://arxiv.org/pdf/1801.03998.pdf., accessed on 9 January 2019.

Gervais Arthur, Karame Ghassan O., Capkun Srdjan, and Capkun Vedran, 'Is Bitcoin a Decentralized Currency?' (2014) http://eprint.iacr.org/2013/829.pdf, accessed on 9 January 2019.

GNU General Public License, https://www.gnu.org/licenses/gpl-3.0.en.html, accessed on 9 January 2019.

Hacker Philipp, 'Corporate Governance for Complex Cryptocurrencies? A Framework for Stability and Decision Making in Blockchain-Based Organizations', this volume, chapter 7.

Higgins Stan, 'Bitcoin Core Opens Doors to Outside Funding with Sponsorship Program' (*CoinDesk*, 6 April 2016) http://www.coindesk.com/bitcoin-core-opens-doors-to-outside-funding-with-sponsorship-program/ accessed on 9 January 2019.

Hinman William, 'Digital Asset Transactions: When Howey Met Gary (Plastic)' (Speech, 14 June 2018) https://www.sec.gov/news/speech/speech-hinman-061418, accessed on 9 January 2019.

Jones Ray, 'Ethereum Protocol Developer Holds $114,877 Worth of DAO Tokens' (*Reddit*, 29 June 2016) https://www.reddit.com/r/ethereum/comments/4qiqq8/ethereum_protocol_developer_holds_114877_worth_of/d4th8ce/, accessed on 9 January 2019.

Khrennikov Ilya, 'Vladimir Putin is Getting Interested in Bitcoin's Biggest Rival' (*Bloomberg*, 6 June 2017) https://www.bloomberg.com/news/articles/2017-06-06/putin-eyes-bitcoin-rival-to-spur-economic-growth-beyond-oil-gas, accessed on 9 January 2019.

Leib Ethan, Ponet David, and Serota Michael, 'A Fiduciary Theory of Judging' (2013) 101 *California Law Review*, 699.

Leib Ethan, Ponet David, and Serota Michael, 'Translating Fiduciary Principles into Public Law' (2013) 126 *Harvard Law Review Forum*, 91.

Manski Sarah and Manski Ben, 'No Gods, No Masters, No Coders? The Future of Sovereignty in a Blockchain World' (2018) 29 *Law Critique*, 151.

MIT License, https://opensource.org/licenses/MIT, accessed on 9 January 2019.

Murray Ciaran, 'Are Public Blockchain Systems Unlicensed Money Services Businesses in Disguise?' (*Rules of the Game Blog*, 12 October 2017) http://rulesofthegame.blog/2017/10/12/are-public-blockchain-systems-unlicensed-money-services-businesses-in-disguise/, accessed on 9 January 2019.

O'Leary Rachel, 'Ethereum Developer Resigns as Code Editor Citing Legal Concerns' (*CoinDesk*, 15 February 2018) https://www.coindesk.com/ethereum-developer-resigns-as-code-editor-citing-legal-concerns/, accessed on 9 January 2019.

O'Leary Rachel, 'Zcash Pays Off Developer to Avoid Blockchain Split' (*CoinDesk*, 22 June 2018) https://www.coindesk.com/zcash-pays-off-angry-developer-avoid-blockchain-split/, accessed on 9 January 2019.

Oberhaus Daniel, 'Cryptocurrency Miners are Sabotaging Blockchains for Their Personal Gain' (*Motherboard*, 25 May 2018) https://motherboard.vice.com/en_us/article/a3a38e/what-is-a-51-percent-attack-silicon-valley-bitcoin-gold-verge-monacoin-cryptocurrency, accessed on 9 January 2019.

Rave D. Theodore, 'Politicians as Fiduciaries (2013) 126 *Harvard Law Review*, 671.

Reidy Marian and Hanus Bartlomiej, 'It is Just Unfair Using Trade Laws to Out Security Software Vulnerabilities' (2017) 48 *Loyola University Chicago Law Journal*, 1099.

Reyes Carla, 'Corporate Crypto Governance' (26 January 2018) Working Paper presented at Blockchain Works-in-Progress Workshop at Cardozo Law School.

Reyes Carla, 'If Rockefeller Were a Coder' (forthcoming) 87 *George Washington Law Review*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3082915, accessed on 9 January 2019.

Schnelli Jonas, Tweets (*Twitter*, 15 November 2017) https://twitter.com/_jonasschnelli_/status/930680174697381888, accessed on 9 January 2019.

Scott Michael, *Scott on Information Technology Law* (3rd edn, 2nd Supplement, Aspen 2018).

Simonite Tom, 'The Man Who Really Built Bitcoin' (2014) *MIT Technology Review*, http://www.technologyreview.com/featuredstory/527051/the-man-who-really-built-bitcoin/, accessed on 9 January 2019.

Singh Jatinder and Michels Johan D., 'Blockchain as a Service: Providers and Trust' (2017) Queen Mary, Univeristy of London, School of Law Legal Studies Research Paper No. 269/2017, https://ssrn.com/abstract=3091223 , accessed on 9 January 2019.

Stark Josh, 'Making Sense of Cryptoeconomics' (*Medium*, 28 August 2017) https://medium.com/l4-media/making-sense-of-cryptoeconomics-c6455776669, accessed on 9 January 2019.

Summerwill Bob, Tweets on Ethereum Foundation opacity, (*Twitter*, 29 December 2017) https://twitter.com/BobSummerwill/status/946760015322398720, accessed on 9 January 2019.

Swanson Tim, 'Who are the Administrators of Blockchains?' (*OfNumbers Blog*, 19 October 2017) http://www.ofnumbers.com/2017/10/19/who-are-the-administrators-of-blockchains/, accessed on 9 January 2019.

Szabo Nick, 'The Dawn of Trustworthy Computing' (*Unenumerated*, 11 December 2014) http://unenumerated.blogspot.com/2014/12/the-dawn-of-trustworthy-computing.html, accessed on 9 January 2019.

Szabo Nick, 'Money, Blockchains and Social Scalability' (*Unenumerated*, 9 February 2017) https://unenumerated.blogspot.com/2017/02/money-blockchains-and-social-scalability.html, accessed on 9 January 2019.

Tezos website, https://tezos.com/, accessed on 9 January 2019.

Van Valkenburgh Peter, 'What Could "Decentralization" Mean in the Context of the Law?' (*CoinCentreBlog*, 15 June 2018) https://coincenter.org/entry/what-could-decentralization-mean-in-the-context-of-the-law, accessed on 9 January 2019.

Walch Angela, 'The Bitcoin Blockchain as Financial Market Infrastructure: A Consideration of the Operational Risk' (2015) 18 *New York University Journal of Legislation and Public Policy*, 837.

Walch Angela, 'Call Blockchain Developers What They Are: Fiduciaries' (2016) *American Banker*, https://www.americanbanker.com/opinion/call-blockchain-developers-what-they-are-fiduciaries, accessed on 9 January 2019.

Walch Angela, 'Open-Source Operational Risk: Should Public Blockchains Serve as Financial Market Infrastructures?' in *Handbook of Blockchain, Digital Finance and Inclusion*, edited by David Lee Kuo Chuen and Robert Deng (Vol. 2, Elsevier Academic Press 2017).

WhaleCalls, 'Fact or FUD: Blockstream, Inc. is the Main Force Behind Bitcoin (and Taken Over)' (*Medium*, 1 December 2017) https://medium.com/@whalecalls/fud-or-fact-blockstream-inc-is-the-main-force-behind-bitcoin-and-taken-over-160aed93c003, accessed on 9 January 2019.

Wong Joon Ian, 'Ethereum's Inventor on How "Initial Coin Offerings" are a New Way to Fund the Internet' (*Quartz*, Interview with Vitalik Buterin, 14 September 2017) https://qz.com/1075124/ethereum-founder-vitalik-buterin-discusses-initial-coin-offerings-the-consensus-algorithm-and-the-most-interesting-apps/, accessed on 9 January 2019.

Wong Joon Ian and Kar Ian, 'Everything You Need to Know About the Ethereum "Hard Fork"' (*Quartz*, 18 July 2016) https://qz.com/730004/everything-you-need-to-know-about-the-ethereum-hard-fork/ , accessed on 9 January 2019.

Young Joseph, 'Vlad Zamfir: Sharding is the Only True Blockchain Scaling Solution' (*BinaryDistrict*, 13 November 2017) https://journal.binarydistrict.com/vlad-zamfir-sharding-is-the-only-true-blockchain-scaling-solution-/, accessed on 9 January 2019.

Zamfir Vlad, 'Against On-Chain Governance' (*Medium*, 1 December 2017) https://medium.com/@Vlad_Zamfir/against-on-chain-governance-a4ceacd040ca, accessed on 9 January 2019.

Zetzsche Dirk, Buckley Ross, and Arner Douglas, 'The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain' (2018) *University of Illinois Law Review*, 1361.