THE FIDUCIARIES OF PUBLIC BLOCKCHAINS

Angela Walch

INTRODUCTION

Blockchain euphoria is in full bloom, with luminaries of all stripes hailing the technology as a solution to virtually every human problem in existence, from financial inclusion, to identity management, property and health records, and most prominently, currency and essential finance functions.

If blockchain technology achieves even a small portion of its projected potential, then it is possible that it may soon undergird many critical infrastructures within our societies, from property records, to payment and voting systems. The World Economic Forum, in a prominent report canvassing the possible financial use-cases for the technology, has gone so far as to state that distributed ledger technology (DLT, an alternative term for blockchain technology, as the vocabulary of the space evolves) "should be viewed as one of [the] technologies that will form the foundation of nextgeneration financial services infrastructure."[1] Giancarlo Bruno, head of financial services industries at the WEF, said that "blockchain will become the beating heart of [the finance industry," in a news release issued with the report.[2]

If blockchain technology ends up enabling our most basic financial market infrastructures, then the governance processes for creating, maintaining, and altering the technology deserve careful scrutiny, as they will affect the resilience of the technology, as well as the infrastructure that comes to rely on it.[3] If blockchain technology is widely used in financial infrastructures, that will mean that large swathes of people are relying on and trusting in its ongoing operation, meaning that it matters who is running it and how they do it.

This paper focuses on the governance of public blockchains, like that of Bitcoin or Ethereum.[4] With the decentralized software that operates these data structures, governance

[1] *World Economic Forum*, The Future of Financial Infrastructure: An ambitious look at how blockchain can reshape financial services, p. 18, August 2016.

[2] Nathan Popper, http://www.nytimes.com/2016/08/13/business/dealbook/bitcoin-blockchain-banking-finance.html?smid=tw-dealbook&smtyp=cur&_r=0.

[3] *See* Angela Walch, *The Bitcoin Blockchain as Financial Market Infrastructure: A Consideration of Operational Risk*, 18 NYU J. Legis. & Public Policy 837 (2015).

[4] The governance of 'private' or 'permissioned' blockchains deserves its own careful scrutiny, but is beyond the scope of this paper. Private (permissioned) blockchains are common ledgers shared amongst a known group of parties with only certain parties having the ability, or permission, to make changes to the ledger. Public (permissionless) blockchains like Bitcoin's are publicly available common ledgers that allow anyone who runs the Bitcoin software to participate in making changes to the ledger. *See* BITFURY GROUP & JEFF GARZIK, PUBLIC VERSUS

occurs through the software development and transaction verification processes. This paper explores what obligations the software coders and transaction verifiers of public blockchains should owe to those who rely on them to keep the systems functioning properly (and to determine what it means for the system to function "properly"). Recent events in the blockchain space, including the July 2016 Ethereum hard fork and the Bitcoin block size debate, indicate how important it is to understand the existing governance structures and the risks that flow from them.

This paper compares the role of the dominant software developers and transaction processors to a general definition of a fiduciary and finds many likenesses between the two.[5] Given this resemblance, a deeper consideration of the categorization is merited. The paper lays a foundation for this discussion by providing an outline of reasons for and against such a classification, and identifying many practical questions that would need deeper consideration, including the scope of the category and enforcement difficulties. This paper seeks to *begin* the discussion of how to deal with the governance structures of public blockchains, and does not purport to offer a complete resolution of this complex issue.

In Part I, I describe the activities that the dominant software developers and transaction verifiers perform, and explain how those activities function as the *de facto* governance of public blockchains. In Part II, I evaluate the implications of this concentration of power in the core developers and the dominant transaction verifiers, and analogize the *de facto* governance structure of public blockchains to a broad definition of the legal conception of a fiduciary. In Part III, I discuss the pros and cons of treating these parties as fiduciaries of certain participants in the blockchains they manage. In Part IV, I

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

[5] I am not the only person who has noticed the relevance of the fiduciary concept to what blockchain technology developers are doing. During the course of writing this paper, I found Austin Hill and Christopher Allen of the company Blockstream referring to "fiduciary code" due to their recognition of the high-stakes, public infrastructural rule that public blockchains play. To my knowledge, neither has proposed that the people behind the blockchains be considered fiduciaries.

discuss the complexities involved with the categorization, including the difficulties of determining precisely which individuals in a given blockchain should be considered fiduciaries, and to whom they should owe these duties. Finally, I offer concluding thoughts and suggestions for further research.

I. NOMINAL DECENTRALIZATION / *DE FACTO* GOVERNANCE

In this Part, I describe how the core developers and dominant miners of public blockchains function as the *de facto* governance of public blockchains, and demonstrate that public blockchains' reputation for decentralized transaction verification and software development is undeserved, as identifiable parties dominate (and therefore centralize) each process.

One of the defining features of public blockchains is that they are said to be **decentralized.**[6] In theory, this means that there is no central entity that creates or maintains them. Rather, they operate on a peer-to-peer basis through the running of open-source software. The network of computers that operates the blockchain has the job of maintaining and adding new entries to the distributed ledger that *is* a blockchain, and thus plays a crucial role in the system's operation. Changes to the ledger are made once 51% of the computer network agrees – equivalent to a voting process.[7] The participants in this computer network are often referred to as "miners," as they are generally rewarded for the services they provide with new units of the cryptocurrency of the system.[8]

Even though anyone in the world may download software and become a miner, the mining network of both Bitcoin and Ethereum is quite centralized. This has happened through an arm's race in the processing power needed to complete transactions more quickly, and thereby obtain the mining rewards. In both Bitcoin and Ethereum, transaction processing is dominated by businesses devoted to mining and mining consortiums (known as

[6] *See* ANDREAS M. ANTONOPOULOS, MASTERING BITCOIN: UNLOCKING DIGITAL CRYPTOCURRENCIES 18 (2014). Mr. Antonopoulos is a well-respected figure in the Bitcoin community and has taught university courses on digital currencies. I have chosen to cite his December 2014 book on Bitcoin for many of the basics of Bitcoin's operation because he is an identifiable, seemingly credible person, while the website that purports to be "behind" Bitcoin (bitcoin.org) does not come from a unified, identifiable source. *See About bitcoin.org: Who owns bitcoin.org?,* BITCOIN.ORG, https://bitcoin.org/en/about-us (last visited Oct. 21, 2015) ("Bitcoin.org was originally registered and owned by Bitcoin's first two developers, Satoshi Nakamoto and Martti Malmi. When Nakamoto left the project, he gave ownership of the domain to additional people, separate from the Bitcoin developers, to spread responsibility and prevent any one person or group from easily gaining control over the Bitcoin project. . . . Bitcoin.org is not Bitcoin's official website. Just like nobody owns the email technology, nobody owns the Bitcoin network. *As such, nobody can speak with authority in the name of Bitcoin.*") (emphasis added).

[7]

[8]

"pools."[9] In both of these public blockchains, individual mining pools hold fluctuating amounts of significant percentages of the network power, allowing them to effectively control the path of the blockchain. This becomes most evident when a new version of the software is released by the developers, and the miners choose whether or not to upgrade to the new version. A new release does not become operable on the network until a certain percentage of transaction processors adopt it, meaning that miners essentially block or approve each substantive change to the software.

The software development process for public blockchains is also said to be decentralized, as is typical of open-source software projects. There is no central entity that is officially responsible for maintaining or updating the software.[10] A mix of 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."[11] The code is publicly available on github,[12] and anyone in the world may propose a change through a standardized proposal process. Indeed, many coders from across the globe have made proposals.

Although there is no central entity that issues and stands behind the software, not all developers of the code are equal. A team of "core developers" leads the software development process, as is typical in open-source projects. This means that although this group of people is not united under the roof of an entity structure, they function as the leaders and decision-makers for the code. This power manifests in the ways in which they differ from rank-and-file developers. With Bitcoin, for example, core developers have the ability to send emergency messages to all nodes in the network,[13] and are the only developers who have "commit keys" that allow them to make actual changes to the software code.[14]

[9] https://www.cryptocoinsnews.com/ethereum-miner-consolidation-problem/.

[10] *Id*. at 1.

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

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

[13] The emergency message power "allow[s] the core developer team to notify all bitcoin users of a serious problem in the bitcoin network, such as a critical bug that require[s] user action." ANTONOPOULOS, *supra* note 3, at 157. Alerts have "only been used a handful of times, most notably in early 2013 when a critical database bug caused a multiblock fork to occur in the bitcoin blockchain." *Id.* The password that allows the sending of the network-wide emergency messages is held only "by a few select members of the core development team." *Id.*; *see also* ARTHUR GERVAIS ET AL., IS BITCOIN A DECENTRALIZED CURRENCY? (2014), http://eprint.iacr.org/2013/829.pdf (arguing that giving the emergency alert power only to the core developers "gives these entities privileged powers to reach out to users and urge them to adopt a given Bitcoin release").

[14] *See* Tom Simonite*, The Man Who Really Built Bitcoin*, MIT TECH. REV., (Aug. 15, 2014), http://www.technologyreview.com/featuredstory/527051/the-man-who-really-built-bitcoin/ (describing how only the core developers have the power to "change the code behind Bitcoin and merge in proposals from other

(I.e., other developers can propose changes, but a core developer ultimately decides which ones reach the core code.) The core developers also shape how the public blockchains are viewed by regulators and the public at large, as they have met privately with many international regulators (including in the United States),[15] and are often quoted in the press on their opinions of what should happen with the particular blockchain they represent and the technology as a whole.[16]

A series of concrete examples best demonstrates the concentrated power wielded by core developers and large miners. As in most cases, true power is revealed in a crisis, so I focus on Bitcoin's March 2013 hard fork and its current block size debate, as well as Ethereum's July 2016 hard fork in response to The DAO's $60 million heist. Hard forks occur 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.[17] As the most celebrated innovation offered by blockchain technology is the creation of a single, reliable ledger by a decentralized network of computers, a hard fork is indeed a crisis moment for this type of technology, as a single "true" ledger can fracture into several, with human discretion required to determine which of the surviving ledgers should be recognized as true or reliable.

Bitcoin's March 2013 Hard Fork

In March 2013, Bitcoin experienced a hard fork in the software, with the effect that two separate ledgers were being simultaneously maintained by computers within the network.[18] The fork was "due to nodes using two different versions of the bitcoin protocol."[19] 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, with these miners suffering the consequence of "sacrific[ing] significant amounts of money."[20] With that change made, the network gradually returned to a single ledger.

volunteers"); *see also* GERVAIS ET AL., *supra* note 7, at 6 ("This [software development process] limits the impact that users have, irrespective of their computing power, to affect the development of the official Bitcoin [software].").

[15]

[16]

[17] (Distinction between hard forks (non-backwards compatible) and soft forks (backwards-compatible).

[18]

[19]

[20]

This episode spotlights the exercise of power by both the core developers and miners with a significant amount of hashing power. The core 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 core developers also chose which ledger should be authoritative, which created financial winners and losers amongst the miners, based on which ledger fragment they had been processing during the fork. And 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 that can be cast by a miner, and the more lobbying required by core developers to obtain the result they seek.

Ethereum's July 2016 Hard Fork

The Ethereum blockchain faced an existential crisis this summer (2016) when an application built on top of its blockchain platform suffered a $60 million theft. 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 (in effect recovering the funds by rewriting the ledger so that they were never transferred), the Ethereum core developers decided to pursue a hard fork that would recover the funds. This meant that 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.] Only a very small percentage of Ether holders or miners voted in the advance poll, but the Ethereum core developers decided to proceed with the hard fork.

And it worked. Enough miners upgraded to the revised software, and the ledger followed them, taking the Ethereum name and core developers with it.

Or so it seemed until a group of software developers and miners decided to keep the original ledger (reflecting the theft) going. Dubbing the surviving chain "Ethereum Classic", this group has issued a Declaration of Independence from Ethereum, and is making a go of operating a competitive ledger.

Regardless of the ultimate outcome (whether two ledgers/networks will continue to exist or not), the hard fork demonstrates the power exercised by the core developers and the significant miners. The core developers made the decision whether to treat the hack in 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. Charges that the core developers recommended the hard fork because some of their own money had been stolen in the hack flew around Twitter and reddit. Vitalik Buterin, the wunderkind founder of Ethereum and one of its core developers, was likened to a medieval pope, who had decided he was infallible.

The passion, drama, and anger surrounding the Ethereum hard fork shows how much was at stake for the Ethereum community, investors in Ether, and 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.

Bitcoin Block-Size Debate

Finally, although it has yet to culminate in a hard fork, the slow-motion crisis of the Bitcoin block size debate also demonstrates the power held by the core developers and significant miners.

A political debate cloaked as a technical dispute, the block size debate deals with how Bitcoin should change to be able to accommodate higher numbers of transactions per second, as it would need to if it became more widely used as a currency or as infrastructure of financial or other systems. The political issue at the heart of the debate is whether it is desirable or problematic for the Bitcoin mining network to become more centralized as the system increases in scale, as one of the proposals will likely raise the cost of mining, leading to increased consolidation and centralization as it becomes cost-prohibitive for all but the biggest to participate. The community is also debating whether it is better to attempt to fix the scaling problem all at once, or to fix it little by little. There is a serious worry about hard forks among a substantial number of Bitcoin software developers, though other members of the ecosystem (e.g., the owners of prominent exchanges) have been more relaxed about this risk. The risk profiles of the advocates for each stance have been on full display as the debate has droned on since the summer of 2015.

The way in which the block size debate has played out has emphasized that certain people within the decentralized Bitcoin system have more power than others. For instance, a delegation of core developers traveled to China to discuss resolution of the block size debate with the powerful miners there (i.e., owners of significant percentages of the network's hashing power). This summer, an invite-only retreat of core developers and dominant miners was held in California to allow the parties to socialize together and discuss solutions to scaling Bitcoin. The gathering was memorialized by [Dan Azure], but held under Chatham House rules, which prohibit attribution of comments made during the event.

These elite gatherings make sense when one acknowledges that this small group of people controls the destiny of the Bitcoin blockchain, and are making choices that will affect everyone who has invested in Bitcoin, built on top of the Bitcoin blockchain, or services parties that have built on Bitcoin.

These examples of power exercised in connection with crisis reveal that centralized decision-making exists within nominally decentralized public blockchains. When the entire premise of the technology is based on decentralization and eliminating the need to trust third parties, it is controversial to even suggest that a centralized group of people are making crucial decisions on behalf of others. Yet, from the moment these public blockchains were created (including the creation process), a small group of people has been making decisions about which policies should be reflected in the code (a limited number of tokens or unlimited? transaction fees or creation of new tokens?) and how those policy choices should technically achieved through the code. Many people have been impacted by the decisions of this select group, even though it is taboo to suggest it. And, the more widely used public blockchains become, whether as cryptocurrencies or as infrastructure undergirding other systems, the greater the number of people who rely on the decision-making of this small subset of people.

II. If It Looks Like a Fiduciary…

In Part I above, I demonstrated how the core developers and dominant miners exercise power within public blockchains. In this Part, I explore the implications of this concentration of power, and analogize these central decision-makers to fiduciaries. When using a general definition of "fiduciary," the governors of public blockchains show a strong resemblance.[21]

The fiduciary concept is ancient, and is based most fundamentally around trust. Familiar fiduciaries include doctors, lawyers, financial advisors, trustees, and corporate officers and directors. We frequently put our fate in the hands of others – others whom we count on to provide considered and competent advice, perform tasks that we can't 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.

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

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

1) "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 or misuse the entrusted power or they will not perform the promised services adequately…

4) …there is likelihood that (1) the entrustor will fail to protect itself from the risks involved in fiduciary relationships; (2) the markets may fail to protect entrustors from these risks; and that (3) the costs for the fiduciaries of establishing their trustworthiness may be higher than their benefits from the relationships."[22]

Those who govern public blockchains arguably resemble fiduciaries in all of the ways identified by Frankel. Below, I apply each of Frankel's factors in turn, first to the core developers and then to the significant miners of public blockchains.

1) *Providing Socially Desirable Services that often require Expertise*

Frankel's first factor is that fiduciaries provide services (as opposed to products) to the "entrustors"[23] and that the services are typically "socially desirable" and "often require expertise."

Core Developers: As described in Part I, the software developers who work on public blockchains provide services to the users of that blockchain. These services include reviewing the code, proposing conceptual changes to the code, reviewing changes proposed by other coders, drafting new code and revising existing code, security-testing new code, compiling code into new releases, and communicating about the project with other developers, among others. There is certainly a conceptual question as to whether software code is a "product,"[24] 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

[22] Tamar Frankel, *Fiduciary Law*, p. 6.

[23] I use here Frankel's terminology, which she uses to refer to those whom fiduciaries serve.

[24] See caselaw/articles on treating software as a product for product liability and other purposes.

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.

Further, one can 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." Further, the services provided by the software developers clearly "require expertise." Only those skilled in 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 risen to the status of core developer have the privilege of making changes to the actual code.

Significant Miners: Again, as described in Part I, the miners provide the absolutely essential service of processing changes to the distributed ledger that *is* a blockchain. They provide the service or the blockchain ceases to exist. There is less argument here that miners provide a product rather than a service. In addition to the simple processing of transactions, though, the miners perform other services that require judgment. They determine whether or not to adopt software upgrades, which implement policy choices made by the core developers, enabling them to determine the path of the blockchain.

It is also definitely arguable that significant miners provide socially desirable services. Again, if we think public blockchains are on balance beneficial to society, then the miners who operate them are providing a socially desirable service. The expertise factor is more complicated with miners. The simple processing of transactions is solely dependent on a computer running blockchain software; however, the owners of the computers exercise judgment in determining whether or not to upgrade to a new software release, arguably using their special knowledge and expertise to make that decision.

2) *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."[25]

Core Developers

[25] Frankel, *Fiduciary Law*, p. 26.

As Part I explained, the core 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, core developers are constantly making impactful choices. In the 2013 Bitcoin hard fork, the core 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, the core 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, some people lost money, based on the core developers' decisions.

Users of the software and those who build businesses on top of these public blockchains do not get to approve these decisions – once they have chosen to participate in the blockchain, the only way to escape the core developers' power is to abandon the investment (whether in the cryptocurrency or the blockchain-related business). Unfortunately, the core developers' decisions could reduce the value of an investment in the blockchain to zero (as we have seen with the falling value of Ether since the Ethereum hard fork) before an investor is able to get out.

In all of these ways, core developers are entrusted with power by all parties who rely on the blockchain.

Significant Miners: As discussed above, the miners are entrusted with the power to choose whether or not to use a particular version of the blockchain code. This means that all people who rely on a blockchain (whether holders of the applicable token or an investor who has built on top of the blockchain) are dependent on the miner's decisions, much like minority shareholders are tied to the choices of the majority shareholders. The vast amount of power exercised by dominant miners is the reason why core developers have summits and meet-and-greets with the miners – they are lobbying the miners support their political and technical choices embedded in a new software release.

Significant miners also have the power to block specific transactions if they are able to obtain (or band with others to control) 51% of the hashing power in the network. The bigger the chunk of hashing power controlled by a miner, the more power it has to control what occurs in a blockchain. As with core developers, those who count on the blockchain's ongoing operation, or its operation consistent with certain stated philosophies, are unable to escape the miner's exercise of power without leaving the network altogether.

3) *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 or misuse the entrusted power or they will not perform the promised services adequately…"[26] This factor deals with both trustworthiness (the possibility of exploitation by the fiduciary) and competence (performing the promised service to an acceptable standard).

Core Developers

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

As with any position of power, conflict of interest situations can and do arise for core developers. These crop up most obviously with their compensation. Although open-source software is generally developed by software coders 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 the core developers for their time. [With Ethereum, a Swiss non-profit company called the "Ethereum Foundation" was created and crowd-funded, and pays salaries for [x] developers, along with other administrative and advisory staff.] With Bitcoin, there have been a variety of ways of compensating the core developers, including having them work at the MIT Media Lab and for private companies within the Bitcoin ecosystem (e.g., Blockstream, BitPay).

As I have argued previously,[27] this compensation structure sets up a clear conflict of interest for core developers, who may feel pressured to make decisions about the blockchain that favor 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 core developer might make, meaning that conflicts of interest among the core developers are relevant to anyone relying on the applicable blockchain.

This is not purely hypothetical, as core developers are regularly accused of being improperly influenced by those who pay their salaries, or by their own financial interests. [examples, including Bitcoin devs employed by private companies and Ethereum devs said to have had investments in the DAO and chose to fork to get own money back.]

A risk of exploitation of the position could also arise through the core developers' interactions with regulators on behalf of the blockchain. Many of these meetings have been held behind closed doors, so users of the blockchain must simply trust that the core developers are acting in their interest rather than their own in these meetings.

[26]

[27] Walch, *Bitcoin Blockchain as FMI paper.*

There are infinite ways in which the core 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 (as the Ethereum core developers may have in recommending the hard fork that resulted in two competing blockchains), 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 as well as those building businesses in connection with a blockchain are vulnerable to both untrustworthiness and lack of competence by core developers.

Significant Miners

Significant miners similarly expose users of blockchains to the risk that the miner will be untrustworthy or incompetent.

As discussed in Part I, because the miners determine which changes are made to the ledger based on the hashing power they control, their actions can seriously harm users. For instance, if a miner obtained (or colluded with other miners to obtain) a 51% stake of the blockchain's hashing power, it could manipulate the ledger by blocking transactions or approving false ones. Blockchain proponents argue that engaging in such an attack would be against the miner's economic interests, but that does not mean the threat to users does not exist.

It is also possible for a miner's decision on whether to upgrade to a new software release could be compromised by a conflict of interest or even a bribe by an interested party.

A miner's lack of competence could also expose blockchain users to harm. For example, if a miner miscalculated the risks of a software upgrade, its decision to either upgrade or not could have negative effects on the blockchain users (as has arguably happened when a majority of the miners upgraded to pursue the Ethereum hard fork). Presumably miners should be engaging in as many security and accuracy audits of proposed new releases as the software developers do, as they cannot reasonably decide to upgrade without such review. [Check if this is common practice.]

The important decisions that miners make on behalf of blockchain users means that both their trustworthiness and competence are of crucial importance to blockchain users.

5) *Difficulty or Failure of Entrustors to Protect Themselves from Fiduciary Risks*

> …there is likelihood that (1) the entrustor will fail to protect itself from the risks involved in fiduciary relationships; (2) the markets may fail to protect entrustors from these risks; and that (3) the costs for the fiduciaries of establishing their trustworthiness may be higher than their benefits from the relationships."[28]

Expertise barrier means difficult for users to protect themselves from these risks – especially if public blockchains underlie any financial infrastructures.

There is nothing that prevents people who lack software expertise from becoming involved with blockchain technology, whether through the purchase of tokens or by investing in or creating a business tied to the blockchain. Anyone who lacks expertise in the particular code of the blockchain will have a difficult time protecting themselves from the actions of the developers or the miners, as they will be unable to meaningfully evaluate the software code and any proposed changes to it. They simply have to count on the developers and miners to make good decisions.

[Frankel's factor about the possibility that it may be costlier for the fiduciary to establish his/her trustworthiness than the benefits from the relationship] [to come]

* * *

Once we acknowledge that these people resemble fiduciaries, even if not a perfect likeness, the instincts that people have had all along make sense. For instance, many of the core developers (e.g., Gavin Andresen) have made efforts to be transparent to the community in advising it that he would be presenting on Bitcoin to various Federal agencies and other regulators, even posting the power point slides he presented on various message boards. This instinct towards transparency suggests that the core developers realize that they are acting on behalf of others and owe those they represent transparency on their actions. There have been a number of comments from core developers that indicate they appreciate the heavy responsibility they bear to keep the blockchain running. Further, the discussions about the compensation of core developers, and the concern about the power held by large mining pools are all indicators that all parties (developers, miners, and blockchain users) have recognized how much power the developers and miners exercise in relation to users.

Finally, a reminder of what is at stake in these public blockchains. The core developers and miners are determining through their decisions and actions what happens to the money and financial resources of others. Though this paper focuses on the financial uses of blockchain technology, the technology is being discussed as the foundation of record-keeping in virtual every critical public domain, from identity management, to health care and property records. In the non-blockchain setting, when people entrust others with the

[28] Tamar Frankel*, Fiduciary Law*, p. 6.

responsibility to affect their financial and personal affairs, we have no trouble calling them fiduciaries. It is worthwhile here to focus on substance over form in evaluating the governance of public blockchains.

III. PROS AND CONS OF FIDUCIARY CHARACTERIZATION

Although there are many ways that core developers and significant miners resemble fiduciaries, the analysis here would be incomplete without considering the costs and benefits of such a categorization. In this Part, I provide an initial sketch of these pros and cons, and leave exhaustive exploration of them to further research.

Pros

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. 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 those governing public blockchains, characterizing the core developers and significant miners as fiduciaries would theoretically have the following impacts.

- The core developers and significant miners 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 of code and all other actions they take in acting on behalf of the blockchain.

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

- Less particularized due diligence of individual core developers and miners would be needed by those relying on the blockchain, meaning users would not have to keep track of the current cast of core developers and significant miners and do exhaustive research on each one in an ongoing evaluation of continued participation in the blockchain. This minimizes the resources needed to evaluate participation in the blockchain, increasing efficiencies.

- There would be an acknowledgement that core developers and big miners are making high-stakes decisions on behalf of others, on critical matters such as finance and money, and are accountable in a way that more closely approximates the stakes involved. 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.[29]

Costs

Of course, there are reasons not to view core developers and big miners as fiduciaries, and these reasons are all the arguments that are commonly made against the idea of regulation itself.

1) The primary argument against categorizing core developers and big miners 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 do not need to 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) It would be impossible to tell when core developers and big miners have met the fiduciary standard, given the large potential pool of beneficiaries who will have differing interests. The core developers and big miners may have a duty to the public at large for these public infrastructural technologies.

[29] Michael Scott law review article summarizing difficulties of holding people responsible for software harms.

5) Treating core developers and big miners 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, discouraging people from doing proper due diligence in 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 core developers and big miners, as participants in these public blockchains may not have had such accountability expectations when they decided to participate.

8) Core developers and big miners 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 core developers and big miners.

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

The outcome of this discussion turns on whether one prizes innovation for its own sake, without scrutiny, or believes that the subject matter of the innovation should inform how it is treated.

IV. 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?"[30]

As Justice Frankfurter noted in *SEC v. Chenery Corp*. in 1943, the discussion is not concluded by stating that a party is a fiduciary. Many more questions remain to be answered, and that is true here as well.

[30] *SEC v. Chenery Corporation*,[14] Frankfurter J.

In this Part, I identify some of the nuances and practical matters that would need to be considered and resolved if a legislature or a court were to decide to treat the governing bodies of public blockchains as fiduciaries. In some instances, I suggest appropriate resolutions, but in-depth research beyond the scope of this paper would be necessary to draw informed conclusions.

Identifying the Fiduciaries

I have suggested that the core developers and big miners resemble fiduciaries in their role in public blockchains, but this does not resolve the question. As anyone can become a developer or a miner, these broader categories are always in flux. It seems problematic to consider *any* software developer who participates in blockchain code development to be a fiduciary, as only the core developers actually control what makes it into the released code. It is the distinctions in power between the core developers and the other developers that make the core developers look more like fiduciaries, akin to the officers and directors of a corporation. Similarly, it feels wrong to consider a minor with a *de minimis* portion of the hashing power of the network to be a fiduciary, as that minor lacks a meaningful way to influence the operation of the blockchain. But, there is a threshold at which a miner does obtain more meaningful influence in the blockchain, similar to a controlling shareholder of a corporation. Determining that threshold (10%, 20%, more?) requires further research.[31]

Identifying the Entrustors

Thus far, I have been somewhat imprecise about who, precisely, are the parties to whom core developers and big miners would act as fiduciaries. In Frankel's parlance, who are the "entrustors?"

There are a variety of parties who inhabit the blockchain ecosystem. In addition to the software developers and miners already identified, we see 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), and companies that are using the underlying blockchain as a platform for other forms of record-keeping, 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 swathe of the public could unknowingly rely on the operation of public blockchains, if they become part of underlying record-keeping infrastructures that are not seen by the public.

[31] Check CS papers for mining analyses.

The trick here will be to determine which of these groups are considered "entrustors" and entitled to the protections of 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. A full spelling-out of these arguments is beyond the scope of this paper, but would be a helpful area for further research.

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 the core developers and big miners are most like the fiduciaries of officers, directors, and controlling shareholders, having analogous fiduciary duties seems to make sense. A more fulsome analysis would look at whether the protections of the "business judgement rule" used in the corporate setting make sense here.

The duties of care and loyalty fall in neatly with the fiduciary definition provided by Frankel above. As discussed in Part II, 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 the core developers, miners, and those counting on the blockchain already have.

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 problematic code is located, it may be difficult to pin it to a particular developer. What happens if a bit of code was fine until a later update made it problematic? Further, 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 do regularly. This type of behavior would help to demonstrate that the fiduciary had fulfilled its responsibilities.

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. This means that core developers and big miners could be subject to liability from an enormous number of people – users of the applicable cryptocurrency, along with businesses building on and servicing the blockchain. And, despite any cryptocurrency that they may have previously managed to cash out, it would likely be very difficult for any of these parties to satisfy their liabilities – the cost of making whole an entire blockchain would simply be too great.

Enforcement Practicalities

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, so a duty does not have any bite unless it is able to be enforced.

Enforcement of such a 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 a 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.

* * *

As always, the devil is in the details, and it is clear that 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. But, the inquiries remain worthwhile despite the challenges they present.

V. Broader Implications and Concluding Thoughts

This article focuses on the behaviors of coders and transaction verifiers 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 paper opens the door to further research on the matter.

We need to be alert 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 what they call themselves. If the developers had formed a corporation to issue 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). But, 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 coders and miners must recognize that they are not just building simple, fun technology like Wikipedia or Napster.

It is insufficient to focus attention exclusively on the companies building on top of the Bitcoin blockchain and mining network. 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. And 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, etc.

This heralds a need to reexamine the responsibilities of software developers generally, and in a separate ongoing project, I consider whether software developers should owe fiduciary-like duties to the public, akin to public accountants, architects, or engineers. Though the software development industry has resisted professionalization and accountability since its inception [50-60] years ago, it is now performing grown-up functions, and it may well be time for it to grow up and take responsibility for what it builds.