BREAKING THE CODE: CRYPTOCURRENCY AND PROGRAMMING PROPOSAL

Allan C. Hutchinson*

The problem to be faced in regulating cryptocurrency is the general thrust of the 'governance paradox'[1]—how do you regulate an innovative scheme that demands some regulation in the public interest, when you know that any regulation will transform the very features of that scheme that not only makes it what it is, but also makes it especially useful and attractive to that same public? More specifically, how do you regulate an off-the-grid, decentralized and distributed scheme without making it into an on-the-grid, centralized and undistributed scheme? This is the challenge to be met in devising any kind of proposal to create a tailored and efficacious regulatory regime for cryptocurrency. Consequently, in making this effort, it will be important to remember that regulation is not a technical end in itself, but a means to a larger and more substantive end. As regards cryptocurrency, this means that regulation must serve to advance and protect broader social and democratic goals—the shared notion of putting ordinary people and their interests at the heart of any regulated society, not those of many civic or state-controlled institutions that tend to put their own interests ahead of others. Accordingly, any proposals to regulate cryptocurrency must be guided by that broader and more encompassing ambition.

In this paper, I explore how to go about that exciting and, some might say, daunting task of designing and implementing such a regulation scheme. In the first section, I examine the present self-regulatory arrangements that underpin cryptocurrency; it is important to appreciate where things presently stand if there is any chance of making progress forward. In the second section, I pull back the institutional curtain and reveal the people and processes that maintain the blockchain technology that drives cryptocurrency; the nature of its operation and alleged consensus-based character are examined. The third section looks at some of the objections that are made to any effort to monitor the work of the code-makers and programmers; an important distinction is made between what is possible and what is desirable. In the fourth section, I draw comparisons and contrast between programmers and corporate directors with an eye to adopting some disciplinary strategies from corporate governance. The fifth section examines the difficulties to applying a

* Distinguished Research Professor, Osgoode Hall Law School, York University, Toronto, Canada. I am grateful to Taylor Trottier, Eyoel Negaye, Murad Wancho and, especially, Eliza Coogan for critical assistance and intellectual support. Thanks as always to Jennifer Leitch. I am grateful to the faculty and students at UNB Law School for the generosity and hospitality around the delivery of the 2020 Viscount Bennett Memorial Lecture.

[1] Kevin Werbach, *The Blockchain and the New Architecture of Trust* (Cambridge, MA: The MIT Press, 2018) at 133–38.

modified fiduciary duty to the work of programmers. Throughout the chapter, the goal is to lay bare the inner workings of cryptocurrency so that a better and more effective job can be made of regulating it in a sensible and sensitive manner. Taking seriously Lessig's notion that 'code is law',[2] I strive to bring the code-makers into the disciplinary fold.

In Those We Trust

Cryptocurrency is not so much an unregulated domain, but a self-regulated sphere of activity. While this kind of regulation is not the kind of central or governmental intervention that engages and enrages critics and supporters, it is a foundational aspect of cryptocurrency. In so many ways, cryptocurrency is entirely dependent on blockchain technology and, therefore, those who create, organise and maintain it. There can be no cryptocurrency without a very structured and sustained set of programs, codes and protocols that combine to form the underlying blockchain-technology of cryptocurrency. As such, one of the primary and neglected entry-points for possible regulation is the small, but influential group of programmers who have so far largely flown under the regulatory radar. With the power to maintain and change the codes and protocols of the blockchains, they are the heirs to Satoshi Nakamoto's originating vision and have enormous responsibility and power, especially within permissionless systems. Even if the credo of crypto-programmers is to "reject kings, presidents and voting,"[3] they will, if only by default, assume those royal and almost autocratic powers.

Although cryptocurrency users do not need to trust any central intermediary or other transacting party, they have no other choice than to trust the technology itself. Indeed, as a way to alleviate the need to trust others, the blockchain demands that you trust the system of algorithmic and cryptographic proofs and the software that enables the blockchain platform to underpin cryptocurrency transactions. This can be termed the *lex cryptographica*: it is an informal governance tool that both enables and puts limitations on what can and cannot be done. Indeed, it is the code and protocols that comprise the network itself that must be trusted. Of necessity, it determines the nature of people's interaction within the network by channeling and constraining those interactions; there is no network without a code to realise it and there is no cryptocurrency without a network. As such, the defenders of cryptocurrency as a trust-free mode of interaction and financing must stake their claims on the controversial assertion that "technology is much more trustworthy than people."[4] There are obvious

[2] Lawrence Lessig, *Code: And other Laws of Cyberspace, Version 2.0* (New York: Basic Books, 2006) at 1.

[3] Niels ten Oever & Kathleen Moriarty, "A Novice's Guide to the Internet Engineering Task Force" (8 November 2018), online: *Internet Engineering Task Force* <www.ietf.org/about/participate/tao/>.

[4] Mingxing Xu, Ying Tian & Jiyue Li, *Blockchain, An Illustrated Guidebook to Understnading Blockchain,* translated by Jie Liu (New York: Skyhorse Publishing, 2018) at 15. See also Jean Bacon et al, "Blockchain Demystified: A Technical and Legal Introduction to Distributed and Centralized Ledgers" (2018) 25:1 Rich JL & Tech 1.

problems with this, especially if compared and contrasted with the operation of more traditional financial institutions, like banks.

First, it seems axiomatic that there are all modes of technology are vulnerable to error or manipulation in one way or another. Indeed, the short history of cryptocurrency itself demonstrates that distinct possibility. The Mt Gox fiasco in 2014 is perhaps the most well-known. Hackers were able to infiltrate this busy Tokyo-based Bitcoin exchange (with about 75% of all Bitcoin transactions); not only were millions in Bitcoin lost, but it destabilised the entire global cryptocurrency market. Although on a lesser scale, the antics of Quadriga resulted in investors losing C$200M; the death of the sole founder and operator left investors with no way to access the various e-wallets in which the company's passwords were held. Secondly, unquestioning faith in the trustworthiness of cryptocurrency's technology drives home the crucial point from a regulatory point of view that technology is only as good as those who design, run and maintain it; the programmers and code-makers must be trusted to fulfil their responsibilities and exercise their powers in a professional, competent and scrupulous manner. However (and again), experience teaches that, no matter how professional, competent or scrupulous those people are, there will be mistakes and errors. Of course, if the code-makers are not professional, competent and scrupulous (as in the Mt. Gox and Quadriga situations), trouble and turmoil will lie ahead. In such circumstances, the introduction of some regulation of programmers seems to be not only wise, but close to essential; the legitimacy of the cryptocurrency demands nothing less.

Accordingly, it is with programmers that regulatory efforts might be able to intervene at ground-zero in the cryptocurrency world. By addressing the work and world of the code-makers, a more innovative mind-set might be able to intervene in ways that are both effective and consensual. The regulatory impulse might be able to influence the *lex cryptographica* and engineer the kind of changes, like a scaling-back of the system's pseudonymous characteristics, that might be demanded. Indeed, whatever crypto-purists might demand and defend, the maintenance of such a characteristic is both unwarranted and indefensible.[5] In short, any agency or institution entrusted with regulatory responsibilities agency might seek to nudge and chivy the software guardians of the blockchain to design and build code that instantiates and reflects the kind of values and incentives that would be thought to best advance the goals of a more fairly and lightly regulated cryptocurrency world. Indeed, by so acting, these latter-day heirs to Nakamoto might begin to instantiate in the overall and animating benevolent spirit of that originating genius. This holistic approach to regulation would allow a blend of the *lex cryptographica* with what might be termed the *lex traditionis* for the mutual benefit of each.

Importantly, any intervention that targeted the programmers and core developers would also have a very significant and attractive effect—it would permit the blockchain to remain its own regulator by continuing and developing an internal

[5] It is extremely difficult to understand why cryptocurrency should be relieved of criminal and tax obligations. However, a degree of protection might be appropriate and possible by the imaginative use of judicial screens and similar institutional devices. See Allan C Hutchinson, *Paying The Price: Cryptocurrency and the Regulatory Challenge* [forthcoming 2020].

mode of algorithmic governance.[6] This is a tantalising prospect. Despite the arguments put forward by the good faith defenders of the status quo (as opposed to its less savoury and ill-intended ones who seem keen to protect illicit activity), the present structure and operation of permissionless systems of cryptocurrency can be enhanced by the right kind of regulation. The main arguments against directing regulatory initiatives—'free speech' and impracticality—do not hold water. They are diversionary and last-ditch tactics more than they are genuine and serious obstacles to regulation. As such, the effort to bring the code-makers within the regulatory field of consideration are worth pursuing; they hold the potential to both unlock and boost the beneficial possibilities of targeting the work and influence of programmers.

Before recommending how to go about this challenging task of regulating the programmers and protocol-makers, it is important to explain who these people are and how they operate. For a process that is touted for its transparency and 'trust-free' qualities, there is a definite amount of mystery that swirls around how the technological integrity and maintenance of the system is achieved. Indeed, the identities of the core developers are far from simple to discern and their modus operandi is also far from transparent to the uninitiated eye. Nevertheless, as they are located at the dynamic heart of the cryptocurrency enterprise, it would be foolish not to look more deeply into the code-makers' mandate and canvass the possibilities for bringing them more squarely into the regulatory fold.

At The Core

The first core developer (and, therefore, first regulator), of course, was Satoshi Nakamoto. He/she/or they created and implemented the blockchain technology in January 2009. However, Nakamoto's involvement in this development role only lasted for about 22 months until December 2010. At that time, Nakamoto had over 1 million Bitcoins in their name; these remain inactivated and are now worth close to US$1 billion. Their activation would have a serious and negative effect on the price of Bitcoin. During Nakamoto's short tenure as the chief code-maker, Nakamoto made several small alterations to the blockchain software that maintained its efficiency and security, but did not affect its basic operating process and workings. Nakamoto's last e-mail message was in April 2011 and they have not been heard from (or identified) since then. In effect, Bitcoin and blockchain technology has its own ironic and myth-making genesis-story; Nakamoto plays the role of benevolent creator.

When Nakamoto bowed out in 2010, the responsibility for maintaining and taking care of the source-code and operating protocol was handed over to five people. This process of the existing developer or developers deciding who gets to be part of the core development team has become part of the Bitcoin tradition. Programmers are invited into the core group as a result of having built up a strong reputation as highly competent and solidly reliable within the existing group of core developers: it seems

[6] See generally Primavera De Filippi & Aaron Wright, *Blockchain and the Law: The Rule of Code,* (Cambridge, MA: Harvard University Press, 2018) at 193–204; Werbach, *supra* note 1 at 157–60.

very much an inside or elite practice for an overall enterprise that is supposed to be open and distributed. Since 2010, there have been only 14 core developers who have access to the software to maintain, modify and update the blockchain programs. There are presently six core developers—Wladimir van Der Laan, Pieter Wuille, Jonas Schnelli, Marco Falke, Samuel Dobson and Michael Ford. Among this group, one of them is entrusted with the considerable power and responsibility to lead the overall project and coordinate any modifications or developments. After Nakamoto, Gavin Andresen took on this role until April 2014. It is now occupied by Wladimir van der Laan; he is funded by the Digital Currency Initiative at the Massachusetts Institute of Technology (MIT).

However, as powerful as this group are, it would be misleading to give the impression that this elite band of core developers amount to a technocracy that wield absolute power and exercise untrammelled authority. The convention is that these programmers are only supposed to act and make changes to the basic blockchain technology when there is sufficient consensus among the larger group of contributors (of which there are presently around 600 or so) and the larger community of Bitcoin users. As such, in order to assess the power of the core developers and possibilities for regulating them, it is essential to have a better grasp of when and how changes to the basic source-code can be implemented.

There exists what is termed a Bitcoin Improvement Proposals (BIPs) process. All of this occurs through a communications platform, titled the *GitHub* repository where BIPs can be proposed and discussed. This is a relatively elaborate and involved process that can be generally understood as comprising five distinct and important phases:

- *Submission of proposals*—anyone is free to make a proposal for changes to the Bitcoin network's code and protocols provided that they follow the standardized process as outlined on GitHub. There are presently about 600 or so contributors to Bitcoin Core. Since Bitcoin's creation, there have been 10s of thousands of proposals. Only a relatively small number of them are ultimately accepted for implementation. However, it is estimated that more than 75% of Nakamoto's original source-code has been changed or discarded in its 10 years of existence;

- *Discussion and editing*—once a BIP is made, there is considerable discussion and commentary about the proposed changes on GitHub. Again, anyone can contribute and suggest revisions or alterations to the proposal to make it more feasible or likely to obtain approval and implementation. By relying on the participation and insights of other contributors, there is intended to be a greater degree of accountability and cooperation. However, not surprisingly, more weight is given to the proposals and comments of those contributors who have a strong track-record and lengthier involvement than others. The ambition of this discussion is to garner sufficient support for particular proposals so that a momentum is generated to improve the chances of community consensus;

- *Community consensus*—in order to have a chance at success, any BIP must be able to generate a rough consensus. Exactly what this amounts to is not entirely clear. In generating this level of collaboration and agreement, the views and interest of miners are given special consideration; there are about 20 mining pools with a total of over 2,000 miners involved. Their participation and approval is vital because they are the ones who validate transactions and, thereby, create more Bitcoins. Without them, the whole process would stagnate. Consequently, it appears that there needs to be a very high threshold of miners who are on-board with a particular BIP—as much as 95%—before it can receive the necessary degree of community consensus;

- *Implementation*—once the code has been reviewed and generated the required rough consensus, the core developers will take a sterner look at the BIP to ensure that it is compatible with the general principles of the overall Bitcoin project and that it will enhance the performance and technical integrity of the Bitcoin protocol. This confers considerable power on the core developers because not all BIPs with a rough community consensus make it through to implementation.[7] Those BIPS that are accepted by the core developers are then implemented and made available for public adoption; and

- *Community upgrade*—even if a change is implemented to the governing code, it will not automatically become part of the users' network by way of a centralized decree. Each node operator must take steps to update and upgrade the code that they run and are operating with. Consequently, even after discussion and review, the users have the final say on the acceptability of any new change or alteration. For those who champion the truly decentralized, consensual and bottom-up nature of Bitcoin technology, this user-oversight is a vital feature of the system's set of checks and balances.

The rationale for proceeding in this way is that, as an open-source and distributed network, the fate of Bitcoin depends on its continuing security, enhanced technological integrity, broad participation, and effective decentralization. The challenge is to ensure that no person or group can hijack Bitcoin and make changes that do not serve or adversely affect the interests of the Bitcoin community. However, the reality is not so comforting. Despite the general and genuine sense of community spirit, Bitcoin (and other related blockchain-based entities) are more of a faux-democracy. They are long on rhetoric, but short on action. For instance, although the

[7] See Forking Off below.

leading core developer, van der Laan, insists that changes are made by the core developers in a "janitorial" or housekeeping way, he also stated that the "GitHub repositories are not democratic… [and] difficult technical issues are not solved by popular voting."[8] This is far from a democratic commitment or even the appearance of one.

Nevertheless, there is much in this system of upgrading and modifying that warrants serious respect and attention. In particular, it makes the regulatory task even more challenging and difficult; this is especially so with the practice of giving users the ultimate ability to accept or reject any implemented changes. In light of this, some throw up their hands and hold that regulation is unfeasible—the only choice is between an outright ban on permissionless cryptocurrency or a complete hands-off stance to it. Accordingly, my favoured approach of regulation-lite becomes even more impractical and even impossible in some people's eyes, whether they are supporters or critics of cryptocurrency. However, I remain chastened, but undaunted. Behind the front of impregnability and distributed power, I maintain that there is still a viable and pragmatic possibility for regulation. Moreover, I also insist that such regulatory interventions can actually improve cryptocurrency's operation and facilitate its broader acceptance. This is no easy task, but is an achievable one.

Forking Off

The first and most serious objection to targeting programmers or code-makers is that, whatever its claimed benefits and advantages, such regulation is simply not possible. They are constrained by and held hostage to the wishes and control of the broader cryptocurrency community. In other words, they are simply amanuenses or janitors who respond to and do the bidding of their communal bosses and leaders. Moreover, whatever they decide to do, they are open to correction and admonition by those very same community members; users can simply refuse or fail to adopt any changes made by the core developers to the operating platform and protocols. In short, the select group of core developers follow, not lead; they are not kings, but king-makers. Consequently, it is argued that it would be pointless and a waste of organisational resources to take steps to reorganise or monitor their programming behaviour. This is no small hurdle to surmount for any attempt at regulation. However, it is important to remember that there is a vital difference between what can be done and what programmers (and users) think can be done or would want to be done.

The past decade offers several examples of both what programmers or core developers can do and how those efforts are received by users. There have been two general kinds of change that have been made—soft forks and hard forks. As regards soft forks, these are small and incremental changes to the code that help with the overall functionality of the existing system (e.g., readability and memory usage). These changes are backwards compatible in that the blockchain itself is not changed

[8] Danny Bradbury, "Why Bitcoin's Core Developers Want Multiple Versions" (19 October 2014), online: *Coindesk* <www.coindesk.com/bitcoins-core-developers-want-multiple-versions>.

and can move forward in the same way that it has done before. There have been a great many of these changes or soft forks; they are usually uncontroversial and are almost universally accepted by users as they do not affect the consensus rules that go more to the operating heart of the blockchain technology. Nevertheless, these changes accumulate over time and have likely caused a change in over 75% of Nakamoto's original source-code.

The other and more controversial kind of changes are hard forks. These have more significant effects on Bitcoin's operation because they generally change the consensus rules (i.e., those that demand almost universal). The consensus rules are the technical rules that all Bitcoin clients must adhere if the network is to continue working properly. A hard fork, therefore, is one that makes changes or up-grades that are not backwards compatible with the previous version and, therefore, demand a break with or fork from the existing blockchain. There are two well-known examples of this. In August 2017, there was a deep-seated disagreement over how to handle increasing congestion on the blockchain. A contentious change was implemented that obliged users to decide whether they wanted to stay with the original blockchain (Bitcoin) or to go with the new blockchain (Bitcoin Cash). Because one only recognised 1MB blocks as valid and the other recognised 8MB blocks, the two were incompatible. In 2018, Bitcoin Cash itself forked into two cryptocurrencies—Bitcoin Cash, and Bitcoin SV. The core developers, of course, played a major role in all this and, depending whose side you were on, were either the heroes or villains of the piece.

Some draw upon these examples to support their argument that the core developers are simply not a viable target or entry-point for regulatory intervention. Because their power and impact are conditional at best, it would be futile to hinge regulation on their programming efforts. Whether the core developers do or do not implement changes to the basic protocols and operations of the blockchain by way of a change to the consensus rules, the users get to decide whether they adopt them, ignore them or implement their own changes. The ultimate option for users is to fork and establish their own version of a blockchain-enabled cryptocurrency that is incompatible with other versions and does not have a shred history with earlier versions: the original core developers will not have access to or involvement in the new operating software. Examples of this possibility are Litecoin and Dogecoin; they did not split the blockchain itself, but altered the source-code so that new blockchains were created entirely. All of this demands that users, if they are to exercise this ultimate control, must be aware of any changes, appreciate its significance, be prepared to take a stand, and persuade others to get on board with them. Importantly, none of this was antithetical to Nakamoto's original vision. Indeed, it can be argued that it fits aptly within the original vision of a truly decentralised, distributed and user-empowering system.

So where does this leave any recommendations to focus on the programmers as a major entry-point for regulation efforts? How is it possible and effective, let alone desirable, to bring programmers and their programming products into a regulatory framework that can be circumvented by users? Many might say that this leaves my project nowhere: programmers and particularly users will end-run any efforts at regulation. They will either set up new versions of cryptocurrency or refuse to migrate to new versions of the operating program. This response is all well and good in theory: it is true that users can do much to evade the regulatory reach of any more centralised or state-connected organisation. However, this response begins to lose much of its traction and force when placed in a more realistic and practical context. When this is done, a sensitive and light-handed approach to putting programmers in the regulatory mix becomes more realisable and possible.

There are only so many forkings that can occur without undermining the whole utility of the cryptocurrency market. As the number of cryptocurrencies on offer grows further, they will become less attractive to both transactional users and investors. For the transactional users, the attraction of a widely-used digital coin is that they will be less restricted in using it for commercial purposes among a larger community of users; niche-cryptocurrencies have much less appeal for trading and transacting. Consequently, although the option of constantly shifting loyalty between different crypto-brands is available, it will sooner or later become less attractive and viable from a user's own cost-benefit perspective: the avoidance of regulatory intervention at some point becomes self-defeating. Of course, that might not be the case for those who want to engage in money-laundering or related illicit activity; they will want to be beyond regulatory surveillance at almost all costs. However, this can hardly count as an argument against regulation; it is exactly those kind of activities that need to be rooted out and prevented.

For those who use cryptocurrencies for investment purposes, the constant fragmentation into more and more alternative digital products is likely not only to increase the existing price-volatility of cryptocurrencies, but also to drive many existing and would-be investors from the crypto-market entirely. Indeed, the brief history of cryptocurrency to date suggests that, despite the hard forks and new alt-coins that result, Bitcoin will continue to remain the primary and leading cryptocurrency: it is more likely to consolidate its dominant position than lose it. As such, it is fair to say that users seem to have calculated that the costs of moving away from Bitcoin are greater than the costs of remaining with it. In short, the greater technological sophistication or functionality of other cryptocurrencies that might elude regulatory reach is insufficient to offset the relative stability and reliability of remaining with Bitcoin. Consequently, it is far from clear, even from the users' standpoint, that regulatory engagement and focus on programmers will be the bane that many crypto-insiders predict or fear, especially if such regulation is built more around innovative incentivisation than interventionist commands.

At bottom, therefore, a more realistic dilemma for users, whether of a transactional of investor-oriented kind, is not a choice between remaining with regulated and unregulated cryptocurrencies. Instead, it is a choice between staying with cryptocurrencies, as litely-regulated, or shifting back to the traditional system of banking and financing. Understood in this way, some will contend that such a regulated crypto-sphere will be tantamount to making it a permissioned network. This is not the case. Bitcoin will still remain entirely open; users will be free to join at any time and without anyone's approval or permission. For some, of course, this will be a rank betrayal of Nakamoto's vision; the ideological (and also criminally-facilitating) appeal of cryptocurrency is its private and unregulated nature. There is little to say to such purists or ideologues. However, looked at from a more balanced and pragmatic perspective, a subtle and supportive scheme of regulation might actually be viewed as a way to strengthen, not subvert cryptocurrencies like Bitcoin. As with private property generally, the value and benefit of a person's resources are enhanced and even made possible by the involvement of the state and its regulatory arm.

Finally, the other objection to the regulation of programmers is more principled in nature. The basic claim is that any effort to regulate the programmers or code-makers will be an infringement of their rights to free speech. This is a stretch. The argument is that they simply design different technological platforms and protocols; it is the users of these processes who, for good or bad purposes, use the software and, therefore, should be responsible for their activities. The defensive analogy relied on is that between knife-makers and knife-users—it would be unfair and inappropriate to make a knife-maker liable for the knife-wielding actions of a criminal. Although the analysis of that knife-using situation seems persuasive, it misses the main point of the analogy with crypto-code. First, there is no suggestion that the code-maker will be liable for the illicit use of code for criminal purposes: their liability will be by way of administrative fine or discipline.[9] The basis for a regulatory imposition of responsibility is that programmers are aware that such activities occur and cannot deny that they are facilitating this in a reasonably direct way. Those who act criminally through the cryptocurrency platforms can and should be dealt with directly. Secondly, there are ample and entirely legitimate regulations imposed upon knife-makers; they are required to manufacture knives to a high standard of quality (and can be sued for bad craftsmanship) and they are prohibited from producing certain kinds of dangerous knives. Accordingly, while it is important to respect the bona fides and skills of many code-makers, there is no plausible or compelling argument to insulate them from appropriate regulatory oversight as a result of their alleged speech rights.

Code Duties

Code-developers and miners are at the heart of the blockchain process and operation. Although there already exist several checks upon their authority and possible abuses of power (e.g., decentralisation, consensus requirements, and the like), it seems sensible to consider whether there are sufficient safeguards in play to protect the interests of crypto-users. After all, there is considerable disparity in power between code-developers (and, to a lesser extent, miners) and crypto-users. In actuality, this places the crypto-users in a position where they have to place trust in the code-developers that they will act in good faith and for the benefit of all sectors of the

[9] The UK is considering applying anti-money laundering and counter terrorist financing regulations "to impose data collection and reporting requirements on not only cryptocurrency developers, but all open-source software developers and those who facilitate the peer-to-peer exchange of crypto-assets." See James Foust, "Hot Takes" (10 June 2019), online: *Coincenter* <www.coincenter.org/link/coin-center-submitted-comments-to-her-majesty-s-treasury-defending-uk-citizens-right-to-develop-and-publish-open-source-software>. See generally UK, *Transposition of the Fifth Money Laundering Directive: April 2019* (Consultation Paper) (London: Crown Copyright, 2019), online (pdf): *HM Treasury* <assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/795670/20190415_Consultation_on_the_Transposition_of_5MLD__web.pdf>.

crypto-community. Indeed, not only is there an insiders/outsiders dynamic in play, but there are also huge asymmetries of technological knowledge and expertise between code-developers and most crypto-users. Accordingly, in order to appreciate the relation between code-developers and crypto-users and its potential regulation, it is helpful to look at other similar relations and ask whether the disciplinary tools utilised there have any pertinence to the cryptocurrency context.

The obvious, although far from identical, comparison is with the situation of corporate directors. There is an established and sophisticated jurisprudence that addresses the dynamic relation between directors and shareholders; it explores the details of that relation, lays out standards of behaviour that are expected from directors, and examines the remedies available to shareholders if those are breached. The basic notion is that directors owe a duty to act in the best interest of the corporation. As such, they stand in a fiduciary relation to the company's shareholders; they must place the interests of those they represent and at whose behest they hold power ahead of their own interests. This can be unpacked into a variety of sub-obligations, including the avoidance of conflicts of interest and the effecting of statutory compliance. The board of directors, therefore, is be held, as the inimitable Cardozo put it, "to something stricter than the morals of the marketplace; ... only thus has the level of conduct for fiduciaries been kept at a level higher than that trodden by the crowd."[10] Suitably modified to their technological circumstances, this is far from being an onerous or inappropriate duty that might be placed on code-developers.

Code-developers, of course, are not corporate directors: there is a vast difference between their respective roles and responsibilities. The most important are that there is no centralized organisation that is in any way analogous to the corporation in the decentralized world of cryptocurrency, that code-controllers have no direct control over the crypto-users' property (i.e., the crypto-asset) and that they do not act as the agents of individual crypto-users or the group as a whole. Nevertheless, allowing for these important differences, it is still useful to canvass whether a similar regime to that in corporate governance, suitably adapted and tweaked, might be imported into the technological world of cryptocurrencies. That said, if there is to be a transplant of legal doctrines and rules from the corporate to the crypto-world, at least two caveats will be necessary—such fiduciary duties ought not to be enforceable by way of private litigation, and there should be some kind of cap on the liability of code-developers to crypto-users individually or collectively.

The idea that code-developers are in a fiduciary relationship with crypto-users and have a duty to act in the best interests of crypto-users, not their own, is not difficult to sustain. In brief, they provide services (in contrast to products) that demand a certain reliance by crypto-users on the code-developers' superior knowledge and influence whose exercise carries significant risks to crypto-users if they are not performed properly. Because of this imbalance, the beneficiary/crypto-user is vulnerable and needs protection from the possible untrustworthy and self-serving

[10] *Meinhard v Salmon*, 164 NE 545 at 464 (NY 1928), Cardozo J. For my own take on corporate governance generally, see Allan C Hutchinson, *The Companies We Keep: Corporate Governance for a Democratic Society,* (Toronto: Irwin Law, 2005).

actions of the fiduciary/code-developers Traditional relationships recognized as giving rise to a fiduciary duty include lawyer/client, physician/patient, and trustee/beneficiary. In an important sense, this fiduciary approach treats code-developers as being in the same position as other skilled professionals and asks that they be judged by the same standards as them.[11] Consequently, by being obliged to turn their focus to more 'public' and less private ends, the managers of the cryptocurrency universe will be required to bring themselves more in line with the regulatory goals of improved governance, systemic stability, user protection and financial legitimacy.

However, as with most regulatory or legal regimes, the devil is in the details. It will be important to ensure that a reasonable standard is imposed upon code-developers in fulfilling this responsibility. As in the corporate world, the expectation is that they will owe uncompromised loyalty to the corporation and its shareholders, take professional care in fulfilling their responsibilities, and make decisions in good faith. This is not an absolute standard of behaviour and action, but it does demand a close attention by code-developers to the interest of all those involved in and affected by their decisions and actions. As one Canadian court has nicely phrased it in regard to corporate officials,

> [the law] looks to see that the directors made a *reasonable* decision *not a perfect* decision. Provided the decision taken is within a range of reasonableness, the court ought not to substitute its opinion for that of the board even though subsequent events may have cast doubt on the board's determination. As long as the directors have selected one of several reasonable alternatives, deference is accorded to the board's decision.[12]

Consequently, mindful of the influence and power that they have, code-developers should be expected to have their conduct scrutinised and to be held responsible to other members of the crypto-community, especially users, for their actions. As with all other large and complex institutions, the crypto-challenge for a crypto-regulatory agency will be to introduce structures and measures which will contribute to 'closing the gap' between those relative few entrusted with authority to make decisions and those relative many affected by those decisions. To do this, it will be essential to the well-being of the crypto-community as a whole that code-developers appreciate and act upon the imperative to advance as far as practicable all the combined and often competing interests of the different stakeholders. This is no easy task, but it is one that must be assumed or imposed. Whether said by Voltaire or

[11] See generally Tamar Frankle, *Fiduciary Law* (Oxford: Oxford University Press, 2010). For arguments in favour of treating Code-developers as fiduciaries, see Angela Walch, "In Code(Rs) We Trust: Software Developers As Fiduciaries In Public Blockchains" in Georgios Dimitropoulos et al, eds, *The Blockchain Revolution: Legal and Policy Challenges* (Oxford: Oxford University Press, 2018). See also Philipp Hacker, "Corporate Governance for Complex Cryptocurrencies? A Framework for Stability and Decision Making in Blockchain-Based Organizations" in Georgios Dimitropoulos et al, eds, *Regulating Blockchain: Techno-Social and Legal Challenges* (Oxford: Oxford University Press, 2019).

[12] *Maple Leaf Foods Inc v Schneider Corp* (1998), 42 OR (3d) 177 at 192, 44 BLR (2d) 115 (CA). There is likely less of a case for miners being held to the same standards, although they should have some responsibility to act in the general interest of users as much as their own interests.

Spiderman's uncle Ben, it ought to be axiomatic that 'with great power comes great responsibility'.

An Unfair Burden?

The argument to treat code-developers as fiduciaries will, of course, not persuade everyone. There are those who maintain that the realms of corporate directors and code-developers are so different that the rules in the former should not be used in the latter; the differences far outweigh the similarities. Apart from the general disposition against public intervention of any kind, the primary thrust of this resistance to introducing a fiduciary duty is two-pronged—that skilled programmers will be discouraged from becoming code-developers (and that will work to everyone's disadvantage); and that there are sufficient safeguards in place to prevent the typical abuse of authority that fiduciary duties are intended to control against.[13] Both objections are genuine and need to be taken seriously, but they are over-stated. The first concern is true for anyone who assumes a degree or power and authority. The code-developers' assumption of responsibility will come with costs and liabilities as it does for doctors, lawyers and trustees: there is no evidence that this has dried up the supply of those professional ranks. The challenge will be to ensure that code-developers receive adequate recognition and benefits (acknowledgements, prestige, rewards and otherwise) to off-set such legal liability.

The second concern about existing safeguards is also wide of the mark. The argument made is that code-developers have no real capacity to bind and, therefore, harm the interests of crypto-users because any changes to the blockchain and its accompanying software must be approved by those users. As such, any changes that are proposed and are assessed by users to be for the benefit of code-developers and against their own will be rejected. Again, while there is some force to this objection (i.e., users are free to run any forked version of the software that they choose), it fails to confront the realities of both the corporate and crypto worlds. Like disgruntled shareholders who can sell their holdings, crypto-users can opt out and deploy their funds elsewhere. But, as in the corporate world, this is not in itself a stand-alone reason for code-developers to forego the imposition of a fiduciary duty; 'exit' is not the only or optimal solution. Mindful of the information and technical asymmetry between code-developers and users, the addition of a 'voice' option by way of a fiduciary mandate seems to be both necessary and desirable.[14] If crafted and implemented in a sensitive way, placing a fiduciary duty on code-developers will not only protect users from any self-serving or anti-communal behaviour, but it will also fill the trust-gap that is created by the present programming arrangements and changes.

[13] See e.g. Raina S Haque et al, "Blockchain Development and Fiduciary Duty" (2019) 2:2 Stan J Blockchain L & Pol'y 139.

[14] See Albert O Hirschman, *Exit, Voice, and Loyalty: Responses to Decline in Firms, Organizations, and States* (Cambridge, MA: Harvard University Press, 1970).

Accordingly, as part of the regulatory *quid pro quo*, the code-developers must be given rights and discretion that will allow them to plot the best course for the crypto-community in light of its multiple constituencies. As in the corporate context, the code-developers would not be the agents of the users: their lodestar would be the best interests of the crypto-community as a whole, not only those of the largest coin-holders or users. At the same time, they should have strong responsibilities placed upon them which will ensure that they appreciate that their power is provisional and dependent on those they serve and those to whom they ought to be accountable. In short, the introduction of a fiduciary duty will give substance to the oft-claimed notion by code-developers that "we reject kings, presidents and voting." In a manner of speaking, this will go some of the way to requiring code-developers to put their money where their technological mouths are—establishing "rough consensus and running code".[15] As such, the main challenge is to encourage the code-developers to remain innovative and creative, but to do so in a responsible and reasonable manner for the crypto-community at large.

Of course, achieving this will demand some difficult trade-offs and delicate compromises; there is no simple metric for measuring such a feat. However, two prominent recommendations come to mind that will go most of the way to assuaging some of the more obvious concerns:

- *No private right of action*—it would seem sensible, at least as a first step, to enforce a fiduciary duty by way of administrative process and compliance. A crypto-regulatory agency would monitor the code-developers' behaviour; the infractions of any stipulated standard would be dealt with by means of fines, suspensions de-certifications or other administrative steps. Such a restriction on private litigation and judicial intervention would contain and hopefully reduce the scope for expensive and lengthy disputation; and

- *No open-ended compensatory remedy*—this follows from the first. The penalties for infringing the code of practice would be broad and inventive—reprimands, supervision, fines, appointment bans, and the like. In taking such a line, the paralyzing challenge of quantifying the nature and extent of users' losses brought about by code-developers' malfeasance would be obviated; the reliance on litigation caps and other such devices would not be needed. This would work as the beneficial *quo* to the liability *quid.*

As always (and as even critics contend), a more sophisticated appreciation of the range and character of regulation suggests that the most telling contrast is not between heavy-handed government intervention and an entirely hands-off *laissez-faire* approach. While the state possesses a wide range of repressive powers to discipline its subjects, there is a much wider and more subtle set of institutions, practices and, as cryptocurrency reminds us, technologies that shape and influence, as

[15] Oever & Moriarty, *supra* note 3.

Foucault put it, 'the order of things'.[16] Within such a modern world, the choice is between how to mix and match these various and often competing protocols for achieving an optimal state of affairs. This suggest that, when it comes to regulating cryptocurrency and blockchain technology, the critical decision will be how to balance public processes and procedures with the various private tools of regulation. My recommendations are intended as a first-cut at such a balance.

Conclusion

As George Orwell might have put it in *Animal Farm* (his justly famous parable about totalitarian government), "all … are equal, but some are more equal than others" in the technological farmyard of cryptocurrencies·[17] This would seem to be the case with code-makers and programmers. Although they claim to be neither kings nor presidents in their work and approach (and, therefore, are no more equal than others), their commitment to voting and consensus is not entirely genuine. Like most politicians, they say one thing, but on important occasions do another; the posture of selfless servants of the public interest is unconvincing. Consequently, any serious effort to regulate cryptocurrency must entail some genuine willingness to focus on the work and influence of the code-makers. Without bringing them into the regulatory equation, the chances of advancing and attaining a democratic and progressive agenda for the regulation of cryptocurrency will be thwarted.

[16] Michel Foucault, "Truth and Power" (1979) 4:13/14 Critique of Anthropology 131.

[17] George Orwell, *Animal Farm,* (London, UK: Penguin Books, 1989) at 90.