THROUGH A DIGITAL GLASS DARKLY: CRYPTOCURRENCIES AND THE REGULATORY CHALLENGE

Allan C. Hutchinson[*]

As a social process that places great stock in its stability and predictability, law does not deal as easily or as well with change as it might wish. In a modern world that is in a constant and extensive state of flux, law is being placed under considerable stress in its efforts to fulfill its task as a primary regulator of social and economic behaviour. This challenge is particularly acute in the realm of technology and its profound ramifications for social and economic behaviour. The innovative Techno-Age not only offers fresh ways of handling old problems, but also throws up entirely new problems; traditional ways of thinking about and responding to these old and new problems and their optimal resolution are no longer as tenable as many once thought. One such example is the burgeoning world of cryptocurrencies – this peer-to-peer digital network presents a profound challenge to the status quo of the financial services sector, to the established mode of state-backed fiat currency, and to the regulatory authority and reach of law. Taken together, these related challenges demand the urgent attention of jurists, lawyers and law reformers. It is the future and relevance of legal regulation as much as cryptocurrency that is at stake.

In this article, I want to propose an approach to regulating cryptocurrency that recognises and retains its innovative and transformative potential, but also identifies and deals with some of its less appealing qualities and implications. In so many ways, the term 'cryptocurrency' is misleading, especially from a legal and definitional point of view. By characterizing itself as a currency, it begs the very question that needs to be answered – what is the nature of cryptocurrency and, as such, how should it be regulated, if at all? I maintain that cryptocurrency is sufficiently special and different in its dynamics and character that it warrants a regulatory approach that is equally special and different in approach and implementation. Although secondary aspects of cryptocurrency's workings and structure lend themselves to similar and selective regulation to currencies, commodities or securities, the primary ambit and operation of cryptocurrency deserves its own *sui generis* regulation. So, rather than be content with canvassing possibilities, I will plumb for a particular style, scheme and substance of regulation. This is a tall order, but it is necessitated by both the unique challenges and opportunities that cryptocurrency and its enabling blockchain technology present.

This article has four main parts. In the first part of the article, I sketch the beginnings of cryptocurrency, the forces that gave rise to it, the working of this technological innovation, and the challenges it now faces. The second part looks to the regulatory challenge more generally by considering the tools available, the normative ends of regulatory schemes, and the fit of different regulatory initiatives with different activities. In the third part, I explore the different categories of existing regulatory schemes – property, securities, currency and commodities -- that might be relied upon to deal with cryptocurrency. The fourth part works towards suggesting a regulatory

---

* Distinguished Research Professor, Osgoode Hall Law School, York University, Toronto, Canada. I am grateful to Peter Blaha, Joshua Harriott, Dale Lastman, Jennifer Leitch, Taylor Trottier, **, and other friends and colleagues for critical assistance and intellectual support.

approach that respects and enhances the essential character of cryptocurrency, but also wrestles with its shortcomings as a more general and transformative mode of digital trading. Throughout the article, my overriding and constructive ambition is to grapple with and confront the basic challenge of any regulatory scheme -- to regulate something in such a way that, after regulation, that something is essentially the same and better than it was rather than having it become something different and worse.

A. GOING SECRET

1. Banking on It

Trade and commerce are as old as civilisation itself. The need to exchange goods and services is a continuing and vital social feature. However, influenced by innovators and entrepreneurs, how this has been done has changed significantly and frequently over the centuries. Bartering was once the most common forms of commerce. However, the idea and practice of utilising 'money' as a medium of exchange recommended itself as a convenient and reliable system that could overcome the inefficiencies and limitations of a bartering system; it would serve to broaden, deepen and diversify trading practices.[1] At first, there was commodity money (e.g., salt), but this soon gave way to the issuance of representative or paper money. Whether state-backed or not, the overall function of such money is to provide a commodity that can be saved and held with confidence, whose value will remain stable, and that it can be retrieved when needed and used as a reliable medium of exchange. After a long run, the almost exclusive reliance on paper money is now under threat by the rise of digital money or cryptocurrencies.

As representative or paper money became the convenient currency of commerce, the first banks began to appear. Indeed, modern banking still resembles the early institutions of the Medici family in 15th Century Florence. Their role was to act as a trusted intermediary between buyer and seller by facilitating trade and sharing the risks that are inherent in the use of money as a unit of account, a repository of value, and a medium of exchange. In performing that task, banks (and other financial institutions) have themselves become lucrative and powerful trading bodies; they make money on handling other people's money. The core business of banks is to hold accounts for customers, facilitate the uses of that account for payments and deposits, and to extend credit to borrowers. As well as user fees, banks make money on the difference between loan/credit interest charged and deposit/account interest paid by borrowers. As the old joke goes, bankers were happy if they could follow the 3-6-3 rule – interest paid at 3% on money deposited, interest earned at 6% on money lent, and on the golf-course at 3:00. Although they have now branched out and their activities are more diverse and widespread, the basic institutional logic remains much the same.

At the heart of the bank's power is their valued and valuable activity of creating and validating a ledger that keeps a trustworthy record of all transactions so that double-spending (i.e., that people would use the same resources or money more than once to buy goods or services) and other fraudulent and dubious practices were avoided. Most importantly, although originating as

[1] NOBLE HOGGSON, BANKING THROUGH THE AGES (1926) and FREDERIC MISHKIN, THE ECONOMICS OF MONEY, BANKING, AND FINANCIAL MATTERS (2007).

trusted facilitators and guaranteed ledger-keepers of trade and commerce, a bank-centric approach to financial services has become both a major drain on the economy and financial transactions generally and a de-stabilizing institutional force. The convoluted and costly nature of this intermediary role is considerable. With sometimes 5 or 6 intermediate dealers between buyer and seller, the banking system adds up to 8% to all transactions made and it takes up to a week to clear and settle most transactions. Indeed, the payment card industry (e.g., Visa, Mastercard, and Diners Club) processes about $20 trillion in volume and generates almost $300 billion in fees each year.

Although there remains a crucial role for banks and bank-like institutions, those institutions have developed and grown to such an extent that they threaten the original basis for their existence -- to facilitate efficient exchange and provide trusted security in handling money. Apart from a continuing history of bank failures and collapses,[2] financial institutions and banks have become self-serving entities who any real lack of transparency and utilize informational asymmetry to their advantage. Indeed, banks foster and benefit from the false idea that they are not simply one more economic corporate entity, but that they occupy a special and semi-public role that sets them aside from the usual profit-making priorities of other market actors. In short, the whole financial services industry tends to serve its own as much as the public's interests. Although they have turned to technology and e-commerce to perform their roles, they have not embraced more fully the possibilities of a truly digital and transformed style of banking. As such, the rise of cryptocurrencies is not only a response to the dominating role of banks (and governments), but also presents a genuine threat to the centralising role of banks in the burgeoning world of trade and commerce.

2. Blocking Efforts

Imagine a way of transacting one's life and business in which everyone that you dealt with was part of the same bank. All the people that you deal with are account-holders of that same bank; this will reduce a number of risks and costs that presently weigh upon your capacity to act speedily, safely and cheaply in making payments for goods and services. But not only that, imagine that you and all the other account-holders were also the exclusive managers and owners of the bank; there was no middleperson to orchestrate or benefit from your efforts. Moreover, imagine that there is the added attraction of being able to be both account-holder and manager in a largely confidential and semi- or pseudo-anonymous manner; other account-holders that you transact with would not be able to know your business or spending habits (or you theirs). This arrangement would mean that many issues of trust could be handled better, risks could be more contained, and costs could be further reduced.

[2] For example, between 2008 and 2012 alone, over 450 U.S. banks failed. See K. CONNORS, THE HISTORY OF BANKING: THE HISTORY OF BANKING AND HOW THE WORLD OF FINANCE BECAME WHAT IT IS TODAY (2017) and ANDREW ROSS SORKIN, TOO BIG TO FAIL: THE INSIDE STORY OF HOW WALL STREET AND WASHINGTON FOUGHT TO SAVE THE FINANCIAL SYSTEM--AND THEMSELVES (2010).

This scenario is one way to think about cryptocurrencies. They came into being on 3rd January, 2009 under the genius and guidance of the fabled Satoshi Nakamoto. He or she (or perhaps they, as Nakamoto's identity remains unknown) set out to develop a scheme that was intended to be an entirely borderless, decentralised, unmediated (without banks), pseudo-anonymous, self-regulating and politically-neutral medium. In particular, it needed to be capable of solving the double-spending problem that made the existence of ledger-maintaining banks desirable. This originally involved the still-dominant mode of cryptocurrency entitled 'Bitcoin'. In the intervening decade or so, there have been more than 1000 different types of cryptocurrency created and put into use. Over half of them are still trading actively on unregulated or registered exchanges. At present, there are approximately 17.5 million bitcoins in circulation. While it initially traded at approximately US$0.003 per bitcoin, it is currently valuated at approximately US$3800, with a market capitalization of over US$67 Billion.

At its most basic, therefore, cryptocurrency is a self-contained and decentralised system that allows for peer-to-peer transactions in a digital space that is free from outside control, safe from exploitive meddling, and is unrestricted by national borders. Anyone can join by downloading the free software and becoming part of the process; there are presently millions of computer-users in 90 or so jurisdictions. Because it does not have an underlying or anchoring asset, its price is determined purely by the supply and demand for bitcoins. The appeal of such a system of transacting and banking is obvious to people of very different backgrounds (both poor and rich) and with very different interests for doing so (both legal and illegal).[3] The challenge is to devise a cryptocurrency process that operates in a secure, inexpensive, confidential and dependable way. In short, that it will work better than the existing banking system

Nakamoto offered "a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions."[4] What does this mean for the ordinary person? The task was to generate a system that cut out the role of the middle-person by replacing institutions, like banks and credit card distributors, with a process whereby a universal ledger was established and validated by individual users who would be incentivised to maintain, run and authenticate the system through their own computers. People would transact using bitcoins; these are digital markers. They are held in a personal e-wallet on a computer that is encrypted and can only be opened by the owner through a private key of or password. These bitcoins can be used in much the same way as any currency to buy and sell products and services from other bitcoin users. In that sense, the bitcoin cryptocurrency is a closed and consensus-based digital system in that is only usable by and through other members on the system. Of course, as the number of bitcoin users increases, so will the utility and reach of the system. Today, there are over four million bitcoin users globally with over 20 million e-wallets between them; over 20,000 transactions are made daily. However, the combined total of their crypto-holdings account for only about 3% of the combined assets of the world's leading central banks.

---

[3] The best and most accessible account of the workings of bitcoin and blockchain is PAUL VIGNA AND MICHAEL CASEY, THE AGE OF CRYPTOCURRENCY: HOW BIT COIN AND THE BLOCKCHAIN ARE CHALLENGING THE GLOBAL ECONOMIC ORDER (2016). See also ARVIND NARAYANAN ET AL., BITCOIN AND CRYPTOCURRENCY TECHNOLOGIES: A COMPREHENSIVE INTRODUCTION (2016) and CRAIG K. EWELL ET AL., CONG. RESEARCH SERV., R43339, BITCOIN: QUESTIONS, ANSWERS, AND ANALYSIS OF LEGAL ISSUES 1 (2015).

[4] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf.

The whole process of cryptocurrency is contained within a software program that keeps a corroborated and immutable record of all transactions made -- blockchain.[5] Every time someone enters a new transaction and pays by or is paid with bitcoin, that transaction is checked and measured against all the existing transactions ever made with bitcoin. It is only then that the transaction can be recorded and e-stamped as being unique and, therefore, legitimate. This process takes a few minutes (as compared to the week or so that it takes banks to clear and settle transactions). Because there is no central server or controlling third-party, this distributed process allows all users to be involved in and, therefore, responsible for guaranteeing that each and every transaction that has ever occurred is unrepeated: the blockchain can only be added to, not revised retroactively. If one or series of computers are compromised, there are still large numbers of users with a complete record.[6] Further, all transactions are open to view, but only by way of the encrypted and pseudonymous e-addresses of users. This overcomes the double-spend problem, ensures the trusted integrity of the overall system, reduces payments to third-party intermediaries, and preserves users' confidentiality.

However, there are, at least, two particular challenges with this cryptocurrency process – who controls the supply of bitcoins? And how are users incentivised to do the necessary authenticating work? Nakamoto had the ingenious idea of linking these two issues together. When the first bitcoin was released in January 2009, a secured stash of 21 million bitcoins was also created. The stash was programmed to be released over a 130-year span. This release is scaled so that the amount of bitcoin made available in each block was reduced to 25 per 10 minutes after 2012 and then halved every four years after that. This means that the total supply of the 21 million bitcoins will not be exhausted until 2140. Also, bitcoins are divisible into smaller units known as *satoshis*; each satoshi is worth 0.00000001 (10^{-8}). As well as providing incentives for security and performance, this arrangement also ensures that the value of bitcoins is not vulnerable (at least within the digital universe)[7] to devaluation by unanticipated releases of more bitcoins or by intervening governmental and corporate policies. Secondly, in order to earn bitcoins, users or 'miners' have to do the essential work of confirming the legitimacy of existing bitcoin transactions as they happen by solving randomly-generated and complex mathematical problems. If successful, these miners are rewarded by obtaining a block of the 50 coins that are released every 10 minutes; they can also charge an optional fee (as low as 0.00001 bitcoin).

An unfortunate side-effect of this is that 'mining' has become a far from simple or cheap activity. Indeed, it has been deliberately made mathematically more difficult as the regular supply

---

[5] For an expansive look at the broader potential of blockchain technology, see DON TAPSCOTT AND ALEX TAPSCOTT, BLOCKCHAIN REVOLUTION: HOW THE TECHNOLOGY BEHIND BITCOIN IS CHANGING MONEY, BUSINESS, AND THE WORLD (2016). For example, it is now being used by some American sates as part of their election process. See Coingeek, Denver to apply blockchain technology in upcoming elections, https://coingeek.com/denver-to-apply-blockchain-technology-in-upcoming-elections/ (March, 2019).

[6] There is the problem of the so-called 51% attack. This when a group might ambush the network by commandeering over half the computer network, take control and approve illegitimate transactions. This is becoming increasingly expensive and is now likely prohibitive so at about $1.5 billion. See Osato Avan-Nomayo, Bitcoin 51% Attack is Unrealistic, https://bitcoinist.com/bitcoin-51-percent-attack-study/.

[7] There is, of course, the vulnerability of the boom-and-bust cycle of bitcoin valuation in terms of traditional fiat currencies. See infra pp.**-**.

of bitcoins reduces. As well as attracting a techno-geek clientele that has access to sophisticated and expensive computers, the search for bitcoins requires a huge investment in electrical resources to be done properly. This has had a couple of very significant effects. First, big business has become involved in mining and begun to squeeze out the small and local enthusiasts who were in on the ground-floor of the cryptocurrency start-up; as few as 10 groups or so now dominate mining. This development has changed the overall thrust of the cryptocurrency market and turned it into as much a vehicle for investment or speculation as an alternative mode of banking and transacting. Secondly, in order to facilitate the use of cryptocurrencies as an investment tool and to allow the less technically-sophisticated to enter the cryptocurrency sector, a secondary market has developed in which bitcoin can be exchanged for traditional fiat currency. There now exist a variety of sites and institutions, like that Bitstamp, Binance and Kraken, that work as cryptocurrency exchanges. This turn of events has not only largely transformed how cryptocurrencies are viewed and used, but also has created a new set of problems and challenges for those who maintain that regulation is demanded.

Bitcoin is the dominant, but by no means only mode of cryptocurrency. There are over 1000 different kinds of cryptocurrency that can be acquired and traded. Utilised for a variety of purposes and with varying degrees of technological similarities to bitcoin, they tend to be closed or permissioned schemes that require certified membership to participate and that are overseen by the controlling entity; Paypal is an example. In the past few years, these Initial Coin Offerings (ICOs) have generated more than $4 billion in revenue. Although they are an adjunct to cryptocurrency rather than an integral part of it, these sites are the public and often troubled face of cryptocurrency. Moreover, these sites have become the profitable intermediaries that cryptocurrency was intended to challenge and do away with.

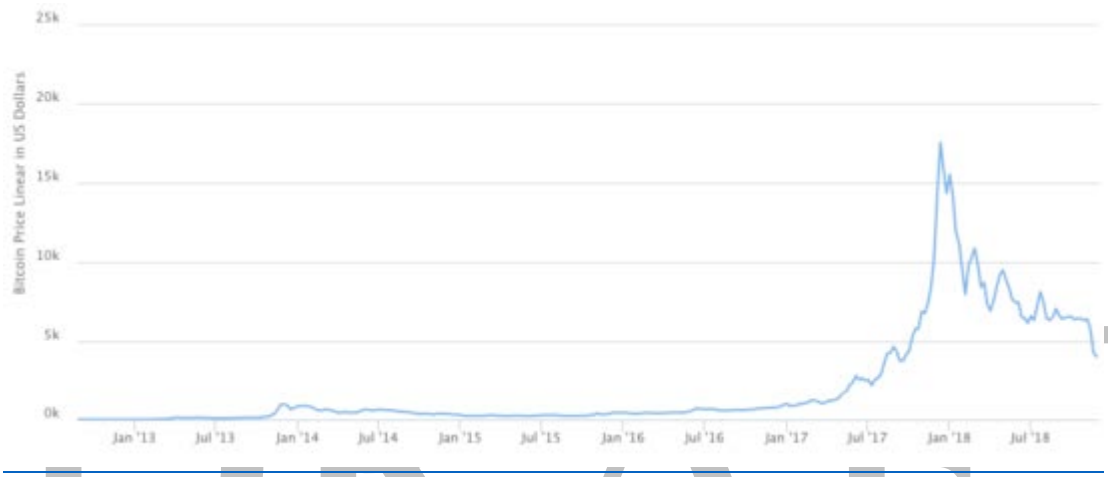
3. Booming and Busting

One of the major bones of contention about cryptocurrency is that it is perceived by a number of respected commentators and critics as a fad or flash in the pan. While it has a certain innovative and trendy appeal, it is condemned because, in failing to respect the cautionary logic of basic economics, it will soon fall victim to its own surreal success. In more technical terms, it is seen as a hyper-mode of speculative investing in an untethered asset or commodity that has no state-backing; the basic bitcoin has no intrinsic value to anchor it in reality so its over-inflated pricing is a boom waiting to go bust if and when its users' confidence wobbles or wanes. As such, it is very vulnerable to a 'pumps and dumps' cycle of valuation. In many ways, therefore, crypto-sceptics predict that the cryptocurrency market will end in tears and trouble like The Dutch Tulip Mania of 1634-37, the British South Sea Bubble of 1720 or even Bernie Madoff's Ponzi scheme of 2008.[8] There is some basis for these claims in that the price of bitcoin raced to a high of $19,783 in December 2017 and then proceeded to crash to $3,756 a year later; it is a much more volatile entity than gold, fiat currency or most stocks and shares. However, for all the dooms-saying, there is, as it were, another side to the coin.

---

[8] Nouriel Roubini, Blockchain Isn't About Democracy and Decentralisation, https://www.theguardian.com/technology/2018/oct/15/blockchain-democracy-decentralisation-bitcoin-price-cryptocurrencies and Paul Krugman, Transactions Costs and Tethers: Why I'm a Crypto-Sceptic, https://www.nytimes.com/2018/07/31/opinion/transaction-costs-and-tethers-why-im-a-crypto-skeptic.html.

Despite its admitted volatility as a partial result of its more than 200-times smaller market than global stock markets ($300 billion to $75 trillion), cryptocurrencies have not been the disastrous investment that some have forecast. The collapse that many have predicted has not happened, at least for now. Despite the boom-and-bust effects of 2018, the value of bitcoin has tended to stabilise to a more modest, if still high price in the mid-$3,500. This price is not to be scoffed at. Anyone who invested in 2009 would be still benefitting enormously from a very high rate of return on their investment today, even if they did not reap the extravagant rewards of late 2018. Most revealingly, on an average basis, someone who invested in bitcoin in the last few years would still be doing much better than someone who invested in the stock market; they would have increased their initial investment thousands-fold.



Bitcoin price since 2009 to 2018. The historical chart shows the changes of price of Bitcoin (BTC).

No one is pretending that cryptocurrency does not come with its own share of perils and pitfalls. It would a naïve and foolish investor who did not invest in bitcoin without a strong sense of anticipated adventure that could offer great losses as well as great rewards; the higher the possible rewards, the greater the actual risk. It is ironic, in light of cryptocurrency's anti-establishment posture, to expect government to protect such speculators in this off-the-grid region. That said, the problem with all this for defenders of cryptocurrency is that it was never intended to be one more vehicle for high-risk speculation; the basic idea of cryptocurrency in its purer Nakamoto-form was to be an alternative mode of doing business that did not rely on fiat currency and banks. At its inception in 2009, there was no sense or expectation that it would become a speculative vehicle for investing: it was about finding a truly trustworthy and unmediated medium that did not have the very problematic history of banks, central and otherwise.[9] Indeed, insofar as bitcoin became a target for wealthy investors, it seemed to be exactly the kind of traditional financial wheeling-and-dealing that cryptocurrency was intended to abandon and set itself apart

[9] See Satoshi Nakamoto, Bitcoin Open Source Implementation, http://p2pfoundation.ning.com/ forum/topics/bitcoin-open-source (February, 2009).

from. In other words, the primary function of cryptocurrency as a medium of exchange has been supplemented, if not supplanted by its secondary use as an investment vehicle.

This distinction between primary and secondary markets in cryptocurrencies is hugely significant in thinking about law and regulation. Whereas the primary market of cryptocurrency exchange is separate and apart from the tradition financial markets, the secondary market is more fully a part of it. Transactions that occur through and on blockchain are to the side of traditional markets in terms of the self-selected participants involved, the contained purposes for which cryptocurrency can be used, and the internal process utilized for recording transactions. Governed by consensus and encrypted security, cryptocurrency is an alternative to, not an adjunct of the traditional market. However, the secondary market – coin exchanges, ICOs, and other related trading activities – is intended to function as a limb of the traditional market that facilitates interactions between cryptocurrencies and fiat currencies. Inside cryptocurrency, bitcoin rules. But, on the edges of the traditional market, the dollar rules.

B. THE REGULATORY CHALLENGE

1. Beyond The Technical

Regulation comes in many shapes and sizes. Society is constructed and constituted by the different modes of regulation that are adopted or in place. These can span a broad spectrum from criminalisation and command-and-control laws through delegated authority and market competition to self-regulation and tax incentivization. Indeed, there has been a general move away from the traditional command-and-control model to less coercive and more cooperative types of regulation. Of course, there is no one tried-and-trusted formula by which to determine what kind of regulation best suits what kind of activity. The prevailing rationales are seen to be about correcting for market failures and power caused by informational asymmetries, lack of competition, interest group capture, and the like; the goal is treated as being the need to create regulatory processes that encourage transparency, efficiency, confidence, and accountability.[10] However, these choices of appropriate tacks and tools are not simply technical matters or considerations; they involve formative values and bigger choices that raise matters of deeper normative commitments.

As such, it is a mistake to view regulation as being the exclusive domain of technicians and bureaucrats. For example, centralized regulatory devices or decentralized ones are not to be considered as ends in themselves, but as means to achieve larger and more encompassing objectives. Nor is it simply a matter of calibrating regulatory responses in terms of market efficiency; this already builds upon a hidden and set of normative values and assumptions: it assumes that an efficient market is self-evidently the gold-standard of regulatory schemes. The choice of regulatory design or instruments, therefore, is framed by broader and more contested issues that go to the heart of the civil compact -– who should be responsible for ordering social

[10] See, for example, ROBERT BALDWIN AND MARTIN CAVE**,** UNDERSTANDING REGULATION: THEORY, STRATEGY, AND PRACTICE ch.4 (1999); John Braithwaite, Rewards and Regulation, 29 J.L. & SOC'Y 12 (2002); and *I.A. MOOSA*, GOOD REGULATION, BAD REGULATION (2015).

practices?; who needs to be protected and from whom?; what kind of society do we want to move away from and towards?; and how are we going to get that done? At bottom, the choice of regulatory processes, organisations and tools is a matter of politic engagement and ideological alignment.

In light of these considerations, it would be wrong to begin with the notion, as many do, that cryptocurrencies are presently unregulated. While there is no outside or independent regulatory bodies over cryptocurrency that claim to be acting in the broader public interest, a more accurate description would be to say that cryptocurrency is self-regulated through its blockchain code. This is the so-called *lex cryptographica*.[11] Although this is a mode of regulation, it is not a public or governmental set of intervening rules that require or only incentivise cryptocurrency to act in certain ways. It consists of the code and protocols that comprise the network itself. By necessity, these software designs determine the nature of people's interaction within the network by channeling and constraining what can and cannot be done and how it can be done; there is no network without a code to realize and sustain it. As such, the technology of blockchain is a kind of regulation. In the same way that, there is no game of chess without the rules of chess, there is no cryptocurrency without the architectural imperatives of blockchain technology.

If there is to be a move away from this self-regulated world of cryptocurrency (as with any other self-regulated activity), there is a range of questions and challenges that must be addressed:[12]

- *Context* – What are the existing conditions and parameters of the activity to be regulated that might recommend or constrain the nature and type of regulation to be introduced?;
- *Stakeholders* – What are the identities and competing interests of the various actors that participate in the activity to be regulated?;
- *Objectives* -- What is the need for and purpose of interventions from a social, economic and/or political perspective?; and
- *Tools* – What modes of intervention are available and likely to be effective in addressing the behavior to be regulated?

These challenges do not recommend or lend themselves to easy answers. However, they do offer a framework for thinking about and organising an appropriate scheme of regulation. Any scheme of regulation that is to have any chance of success must be able to confront and have responses to them.

---

[11] See PRIMAVERA DE FILIPPI AND AARON WRIGHT, BLOCKCHAIN AND THE LAW: THE RULE OF CODE 32 (2018) and LAWRENCE LESSIG, CODE: VERSION 2.0 (2006). Whether this amounts to 'law' is, of course, an open question. For an introduction to the perennial preoccupation of jurists and legal theorists with these definitional challenges, see H.L.A. Hart, Definition and Theory in Jurisprudence, 70 L.Q.R.. 37 (1954) and Allan Hutchinson, Coming Home (Again): A Jurisprudential Exploration 1 SORBONNE L.J. 56-84 (2018)

[12] I have relied upon and modified the ideas in ALBERTO ASQUER, REGULATION OF INFRASTRUCTURE AND UTILITIES 31-32 (2018).

Accordingly, any effort to design a useful, fair and responsible process of regulation for cryptocurrencies must begin by taking a stand on the broader political matters that underpin both cryptocurrency and regulation generally. It is only when that is done by way of preface that the proposed nuts and bolts of regulation can be taken seriously. No scheme of regulation (including self-regulation) is perfect or even close to it; what works at any particular time and place will be a matter of normative contestation and institutional design. As the economist Andrei Shleifer put it, there is a need to seek a "trade-off between dictatorship and disorder."[13] As such, the regulatory challenge is not only both political and technical, but also involves an acknowledgement of their mutually-sustaining relationship.

2. A Political Beginning

The origins of cryptocurrency are important and revealing. Although there is no one universal or accepted creation-story, its genesis is clearly to be found in a techno-generation reaction to prevailing conditions and alliances. There are two main culprits in this story – the banks and the government. Brought to a head by the financial and global crisis of 2008, the banking sector was under great suspicion and opprobrium as it sought and received government bail-outs. For some, this was further evidence that there needed to be some attempt made to break out of the cycle of boom-and bust that both fueled and, in some cases, felled the financial establishment. Indeed, in developing his radical ideas, Satoshi Nakamoto offered his digital peer-to-peer bitcoin innovation as a riposte to both the government's and banks' untrustworthiness and exploitive behaviour in handling currency and people's finances.[14]

Although perhaps more than a little romantic and nostalgic in its intentions, there was an attempt to make good on the original promise of the internet to act as a democratic medium that had been betrayed or sullied by the new techno-aristocracy of the Googles, Amazons and Facebooks of the early 21st Century. As some of cryptocurrency's early advocates insisted, it was birthed by cyberpunks as a direct challenge to the hegemony of the financial establishment and Big Brother. This has persuaded some that cryptocurrency is or was part of a radical anarcho-libertarian movement that was motivated to take back and reinvigorate popular control over those institutions that now exerted enormous and self-serving economic and social power. While there is no doubt much to this depiction, it is also unnecessary to frame all supporters of cryptocurrency as being aligned with such a political orientation and momentum. Indeed, whatever its specific roots and realities, the world of cryptocurrency is now treated as a semi-alternative haven for many disparate actors from the oppressive practices of the financial and fiscal establishment. It has befriended and galvanised supporters from across the political spectrum; it has its advocates from both the political right and left as well those in the middle-of-the road.[15]

---

[13] Andrei Shleifer, Understanding Regulation, 11 EUROPEAN FINANCIAL MANAGEMENT 439 at 51 (2005).

[14] See Nakamoto, supra note **.

[15] A good summary of views can be found in Bitcoin And Other Cryptocurrencies Are Useless, THE ECONOMIST, August 30th, 2018 and Nigel Dodd, The Social Life of Bitcoin**,** CULTURE & SOCIETY **(**2017). The fact that Steve Bannon, President Trump's former Chief of Staff, considers it an aspect of "disruptive populism" and that "it takes control back from central authorities" is not necessarily a strike against it for those not on the far-ish right. Also, there can be little doubt that the wider possibilities of blockchain technology have been embraced by all manner of political activists. See generally Tapscott and Tapscott, supra note **.

After almost a decade of life, cryptocurrency has begun to experience the trials and tribulations of coming-of-age in the larger world of financial services. Whatever the original motivations for its creation, real or mythical, bitcoin and its relatives have come to feel and occasionally succumb to the pressures of Big Business – mining has been taken over by large and highly-funded corporations; Wall Street (and even government) has begun to co-opt the technological innovation of cryptocurrency; exchange markets have prospered as a means to turn cryptocurrency into fiat currency; and investment and wealth has become the seeming measure of cryptocurrency's success, not innovation and freedom. In short, what began as an effort to offer a genuine alternative to traditional banking and finance has itself become vulnerable and almost hostage to those very same forces and institutions. Also, government has become suspicious of the global reach and subversive qualities of cryptocurrency; the fact that cryptocurrency has no borders has made it more resistant to the state's territorial sovereignty. Taken together, the banks' and government's anxiety and desire to protect their own turf threaten to stifle the enormous potential of cryptocurrency as a viable and valuable alternative mode of banking and finance.

Within such an environment, it is not surprising that there are both sceptics and true believers. Those who cling to the almost New Techno-Age-appeal of cryptocurrency are confronted by the hard-nosed economic realists who foresee a further and avoidable crisis waiting to happen. Those who forecast its imminent collapse are confounded by the real-world persistence of cryptocurrency as an alternative mode of exchange. As is often the case, this heated and polarised debate is in need or a cooler and more measured assessment. If cryptocurrency is not the salvation that its supporters claim, nor is it the devil incarnate that its opponents suggest. The truth lies somewhere in the middle or, at least, in a mix of the two.

This elusive space or mixture can be found in the notion that people of different political affiliations can agree that a shift of financial power from a concentrated centre to a more dispersed margin and from institutional intermediaries to individual users is no bad thing. Cryptocurrency offers one way to help bring that about. It has the potential to transform as well as destabilize the whole banking and financial system. However, in the process of any makeover, there is a genuine need to avoid throwing out the baby with the bathwater. The strengths of the traditional system of banking and currency regulation must be retained at the same time that its failings are being overcome. Accordingly, any effort to regulate cryptocurrency must be clear in its political assumptions and ambitions – the shared notion of putting ordinary people and their interests at the heart of any regulated society, not those of many civil or state-controlled institutions that tend to put their own interests ahead of others. This is a democratic and popular mandate that can garner broad political support.

3. Legitimating Regulation

In order to achieve that political goal, it will be necessary for supporters of cryptocurrency to shelve or suspend their varying degrees of antagonism toward government. The reality of contemporary politics dictates that the choice is not between regulation and no regulation, but between different kinds of regulation, strong or lite; there is no real possibility of the continuing status quo of self-regulation (or, at least, self-regulation in its present mode) unless there is a willingness for cryptocurrency insiders to put their own house in some decent order. Ironically, while cryptocurrency was created as a strike against government, it will require something of

government's imprimatur if cryptocurrency is to resist heavy-handed regulation and the encroachment of banks and other financial intermediaries.[16] However, the opposition to any kind of regulation comes from two very different sources.

The first are those anarcho-libertarians who were in at the introduction of digital peer-to-peer innovation. These die-hards view any kind of government intervention as a sell-out and entirely unacceptable. For them, to agree to any regulation would be considered to be the equivalent to make a deal with the devil. However, these true believers seem at their happiest when they are on the outside looking in: they are perpetual and habitual renegades who need an establishment to rail against. As such, in their world of constant opposition, no plan of regulatory action or compromise will ever be acceptable. The second are a group of traditionalists who maintain that regulation will only add further legitimacy to the very dubious and scam-like arrangement that is cryptocurrency. This is also a dubious and impractical stance. There are many things that are allowed and regulated in today's society that it would likely be better off to do without. Gambling is an obvious one. Although there is little to no redeeming social value to it, gambling is not only allowed, but is heavily regulated. Indeed, government often is not only the major regulator of gambling activity, but is also its major beneficiary by way of taxes and fees.

Others have been more open to regulation-lite. Ironically (in light of its laissez-faire origins), some self-styled cryptocurrency purists have welcomed the prospect of more invasive regulation; they claim that it will allow cryptocurrency to get back to its original purposes as a legitimate and alternative mode of private ordering and be consistent with its technology's potential as an unburdened and experimental medium for innovative entrepreneurialism. Although a tad idealistic and naive, there is substantial appeal to such an undogmatic and pragmatic anti-establishment ethic. After all, one of the great attractions of cryptocurrency is that it will "dispel much of the enormous cost that a bank-centric model of payments imposes."[17] Yet, how to regulate crypto-currencies, even with a light and sensitive touch, is by no means obvious. There are some deep and perilous shoals to be navigated in the already treacherous cross-waters of technology and high finance. In particular, the central challenge will be to generate and implement ways of regulating cryptocurrencies that curb its secretive and illicit excesses, but preserve its innovative and decentralised strengths as an alternative market to so-called fiat money. This is no easy task.

In designing and implementing a regulatory regime, therefore, it is important to take a broader institutional view. To ban or gut the cryptocurrency system, like China and other countries are doing, would be a serious mistake (as would ignoring it entirely). Indeed, over-regulating would play into the hands of the very institutions that are most threatened by and have most to lose from the existence of an entirely borderless, decentralised, unmediated, self-regulating and neutral medium – the established structures and private financial institutions. The challenge, therefore, is to split the debilitating alliance of banks and government in their control over currency and financial services. By so doing, it might be possible to enlist government support for ensuring that

[16] The widespread use of the internet was proceeded by and perhaps facilitated by government regulation of the internet. See JACK GOLDSMITH AND TIM WU, WHO CONTROLS THE INTERNET? ILLUSIONS OF A BORDERLESS WORLD ** (2006).

[17] Vigna and Casey, supra note ** at 295.

the alternativeness of cryptocurrency schemes is secured and the suffocating hold that the banks and similar institutions have over the financial services sector is released or loosened. This can only be done if some of the excesses of a self-regulated digital peer-to-peer process are dealt with. In particular, there is no reason why criminals and others should be able to utilise blockchain technology of cryptocurrency to hide and/or launder funds, evade taxes, circumvent currency restrictions, and the like. Nor are there any serious reasons as to why users of cryptocurrency should be able to shield their transactions from being open to similar kinds of taxation as other similar financial dealings.

Accordingly, if cryptocurrency is to survive and even thrive, it must accept that regulation is not only around the corner, but might be helpful. To resist that conclusion would be a form of institutional suicide. Of course, realizing that ambition will not be simple or straightforward. At a minimum, regulators will have to abandon typical command-and-control and top-down approaches to regulation. Indeed, the effort to meet the challenge of regulating cryptocurrency presents an opportunity to match cryptocurrency's innovative technological achievement with an equally innovative regulatory approach. This will involve developing and implementing a regulatory regime that is matched to the unique openings and deep pitfalls of a digitalised financial world. Whatever route is taken, there is a clear and looming notion that some regulation of crypto-currency is both wise and timely.[18] After all, despite the prognostications of some economic commentators, the world of crypto-currency is a reality. The move away from self-regulation towards a more cryptocurrency-sensitive style of regulation can only contribute to improving its chances of survival and even growth.

Of course, any legal intervention will not occur in a vacuum. There are a whole range of regulatory regimes and options that are already in play to cover a wide range of activities and actors. A first step, therefore, in working towards a suitable regulatory scheme for cryptocurrency is to canvass the existing regulatory landscape and evaluate whether they can or should be used to tackle the specific challenges of cryptocurrency regulation. This will demand attention to the context, stakeholders, objectives and tools of such regulation. It is to that comparative and difficult task that I now turn.

C. REGULATORY REGIMES

1. Sameness and Difference

The task of determining whether something is or is not like something else is a staple tool of legal analysis. But, as quotidian as it, this does not make it a simple task; the whole process is fraught with complexities and challenges. For example, in deciding whether two people have a relationship that would be sufficient to allow one person to be described as a 'child' of another is deceptively difficult. Imagine I am out with my young grand-daughter, teenage step-daughter and her friend; we meet someone who asks me 'are these your children?' There is no easy answer; much will depend on who asked, why they asked, and what follows from my answer. So my

[18] For instance, at the recent G20 Summit in Argentina in December 2018, member countries announced that they would be taking concerted action to regulate the cryptocurrency. See infra, pp.**-**.

answer might be all, none or a couple of them – am I responsible for them while out with them?; are they part of my family?; are they my dependents?; do we look alike?; and are they my blood relative? In short, it depends on why it is important to determine who is a child of someone and, as importantly, what follows from deciding if a person is or is not a child of someone. These two matters – context and consequence – are pivotal to any effort to provide and apply definitions or analogies.

These taxonomic challenges apply acutely to the question of whether cryptocurrency is sufficiently like other entities or activities that it warrants the same or a similar type and style of regulation. While it seems reasonable to assume that cryptocurrency is 'property', it is a matter of some uncertainty about what category of property it falls into. For present purposes, there are three possible options that might profitably be explored –is cryptocurrency a currency?; is cryptocurrency a security?; and is cryptocurrency a commodity? In order to resolve those questions, it is necessary to pay close attention to the context for making the inquiry (i.e., whether and how to regulate) and the consequences of so finding (i.e., the particulars of the regulatory scheme to be applied). As such, context and consequence are related issues that give rise to important and competing analyses.

So, what is cryptocurrency? The answer is that it is a little bit of this and a little bit of that. It has characteristics that permit it to be thought of as a currency, a commodity or a security. As such, it might feasibly be understood to be any or all of them. However, it is important to recognize what flows as a regulatory matter from treating them as either property, a currency, a security or a commodity. As I have suggested, cryptocurrency does not lend itself well to an exclusive treatment as a currency, a security or a commodity. Consequently, the optimal approach is not to force cryptocurrency into one of these categories and apply the relevant regulatory tools and processes as if it were fully and centrally part of that categorization. Instead, it is much better and more productive to think about cryptocurrency as demanding a different and separate regulatory approach and apparatus that fits and responds to its specific and, in some ways, unique characteristics. This might well entail borrowing and blending aspects from all three regulatory regimes and perhaps adding new approaches to boot. By so doing, it might be possible to achieve an integrated set of regulatory solutions that are sufficiently efficacious and balanced that it will accommodate a broad range of political interests.

2. Is It Property?

Like most other legal concepts, the idea of 'property' is not a fixed or transcendental entity. It is a functional device that shifts and changes to meet the demands of different and changing social, economic and political conditions. As such, it is more a site for contestation as it is a solution to it. From this less formalistic standpoint, property is not about things, but about the relationship between persons and things.[19] So understood, it is a metaphysical notion as much as

[19] See Wesley Hohfeld, Fundamental Legal Conceptions as Applied in Judicial Reasoning, 23 YALE L.J. 16 (1913) and C.B. MACPHERSON, PROPERTY: MAINSTREAM AND CRITICAL POSITIONS (1978). There is debate about whether the cryptocurrency is a non-private space and, therefore susceptible to the 'tragedy of the commons'. See Garrett Hardin, The Tragedy of The Commons, 162 SCIENCE 1243(1968). However, this is a distraction as cryptocurrency is neither public (it is entirely controlled by private actors) nor private (it is open to anyone who joins); it is a hybrid space.

a physical entity. The status of property, therefore, can attach to 'things' that may be tangible (e.g., land) or intangible (e.g., ideas). Consequently, whatever the physical status of cryptocurrency, the question of whether bitcoins can be counted and treated as property will not solely be resolved by determining what pieces of computer code actually are. Whether they are or are not like other kinds of property in some essentialist sense will not be the crucial determinant. Instead, the focus is upon why something is to be treated as property and what follows from that designation will be central to any definitional inquiry.

Although there is much debate by judges and jurist over the nature of digital information as property, there is a growing consensus that cryptocurrency (or, at least, the bitcoin itself as opposed to the overall blockchain process or any related activity) is best treated as private property for various legal and regulatory purposes.[20] In traditional terms, a bitcoin can be controlled by one person and its use can be exclusively reserved to one person; it is a valuable digital asset that can be held or transferred as the owner sees fit . Like information, it can be shared with and used by others. As such, but unlike information and more like money, it can only be used by one person at one time; it cannot be used simultaneously by others. While control is exercised by the use of an encrypted key or password rather than through physical possession of the bitcoin itself, this is insufficient in itself to defeat the argument that is it best understood as private property. Accordingly, the main issue is not so much whether bitcoin is property: it is. More importantly, the focus of debate is about how should such property be regulated as a legal matter.

The designation of cryptocurrency as property, therefore, might end one particular debate, but it opens up other and more important debates about what follows from that determination. There is no rigid formula for deciding that question; it is not a one-size-fits-all resolution. For instance, when it comes to matters of taxation, there are different applications of taxing measures that might be adopted in different jurisdictions even though there is general agreement on the status of cryptocurrency as property.[21] Or the fact that it is to be classified as property might be sufficient for one purposes (e.g., the crime of money laundering), but not for another (e.g., the sale of securities).[22] This means that, although cryptocurrency is to be recognised and understood as property, it is necessary to take the next step and explore what particular legal regime might best be suited to its regulation – is cryptocurrency to be treated as a currency, a security, or a commodity? And, of course, these questions do not lend themselves to straightforward or ordained answers; they are normative and contested as much as technical and objective.

3. **Is it A Currency?**

[20] See, for example, OBG Ltd. v. Allan, [2008] 1 A.C. 1; Kremen v. Cohen, 337 F.3d 1024 (U.S. C.A. 9th Cir., 2003); and Tucows.Com Co. v. Lojas Renner S.A., (2011) 336 D.L.R. (4th) 443 (Ont. C.A.). See generally Joshua A. T. Fairfield, BitProperty, 88 S. CAL. L. REV. 805 (2015) and Petter Hurich, The Virtual is Real: An Argument for Characterizing Bitcoins as Private Property, 31 BANKING & FINANCE L. REV. 573 (2016).

[21] Compare the approach of the American IRS with that of the Canadian CRA. See IRS, Notice 2014-21 *5-6 (Mar 25, 2014), online at http://www.irs.gov/pub/irsdrop/n- 14-21.pdf and **.

[22] See, for example, United States v. Ulbricht, 31 F. Supp. 3d 540 (S.D.N.Y 2014) (cryptocurrency is money for the purposes of laundering).

The most obvious place to begin the classificatory exercise is with the question of whether cryptocurrency is a currency. The fact that it is called 'cryptocurrency' should in itself not be dispositive of the issue of whether it is a currency and should be regulated as a currency for legal purposes. There are a number of clear ways in which cryptocurrency does function as a currency. It is a medium of exchange, a unit of account and store of value. Because it is not backed by any underlying asset, its value is determined by supply and demand alone. In this way, cryptocurrency is very similar to standard fiat currencies, like the US dollar, the Euro or the British pound. However, despite its similarities to fiat currency, there are very significant differences that recommend that cryptocurrency is of a very dissimilar kind and warrants a distinct regime of regulation. Only one country, Japan, to date has designated cryptocurrency as 'legal tender' and, therefore, susceptible to direct and equivalent regulation as a fiat currency. As always, it is a matter of context and consequences.

The major difference between cryptocurrency and fiat currency is that the latter is state-backed and its supply is determined by government. Indeed, the very nature of cryptocurrency is that it is intended to be and work as an alternative form of currency; it is a private and decentralized medium and, as such, immune to government's monetary policy. Although it is personal chattel, albeit of a non-physical form than coins or notes, it has a different property-like status than fiat currency. Also, it moves across geographical and state-defining borders; it is an international medium that eludes control by any one national (e.g., the American and Canadian dollar) or bloc government's (e.g., the Euro) central bank. While it is convertible into fiat currency, it is not itself fiat currency.[23] However, distinguishing cryptocurrency from fiat currency does not in itself exempt its users from tax obligations; the use, sale and holding of cryptocurrency are amenable to appropriate and relevant tax principles and rules. Indeed, in some jurisdictions, like Canada and the United States, it has been specifically determined that, although cryptocurrency functions in much the same way as fiat currency and money generally, only coins issued by the national mint and under the authority of law should be treated as legal tender and, therefore, regulated as official currency.[24]

In short, while cryptocurrency and fiat currency have important family resemblances and, as it were, cryptocurrency is not not a currency, their underlying origins, operation and rationale are more than sufficiently different to warrant a different approach and method in terms of their regulation. Indeed, the scheme and purposes of the existing regulatory structures seem ill-designed to confront and contain the challenges of cryptocurrencies: they are premised entirely on the idea that currency is a state-backed and state-controlled entity and that the state has an unfettered monopoly in such matters.[25] While there are lessons to be learned from the history and practice

---

[23] See, for example, Reuben Grinberg, Bitcoin: An Innovative Alternative Digital Currency, 4 HASTINGS SCI. & TECH. L.J. 159, 160 (2011); Kevin Tu and Michael Meredith, Rethinking Virtual Currency Regulation in The Bitcoin Age, 90 Wash L Rev 271 (2015); and Oleg Stratiev, Cryptocurrency and Blockchain: How to Regulate Something We Do Not Understand, 33 BANKING & FINANCE L. REV. 173 (2018).

[24] See https://www.irs.gov/pub/irs-drop/n-14-21.pdf and https://www.canada.ca/en/revenue-agency/services/ forms-publications/publications/t4037/capital-gains-2016.html#P279_29831.

[25] In the United States, the Constitution extends to the federal government an exclusive right to issue currency and coin money. See U.S. CONST. art. I, § 8 and also the Stamp Act of 1862. In Canada, 'currency and coinage' is in the exclusive control of the federal government. See Constitution Act 1867, s.91(14) and the Currency Act in 1985 and the Bank of Canada Act in 1985.

of currency regulation by governments, they do not offer a very useful or framework for regulating cryptocurrency. Cryptocurrency is its own kind of currency and should be regulated as such.

4. Is It A Commodity?

Deciding whether cryptocurrency is or is not a commodity is much like the discussion about whether it is or is not a currency. There is no black and white answer, but only a shifting series of gray responses. For some purposes, it does share important characteristics with and function as a commodity, but for others it does not. Indeed, when it is appreciated that currencies have been classified for some legal and regulatory purposes as a commodity, the difficulty of pinning down whether cryptocurrency is or is not a commodity can be understood becomes clearer. Indeed, throughout history and across societies, many commodities (e.g., gold and salt) have served as a currency. In short, the question of whether cryptocurrency is a commodity depends on the context for asking and answering it and the consequences that flow for such a determination.

The general understanding of what is a 'commodity' is broad and diffuse. At one level, commodities are simply goods and articles that can be commercially traded. This has traditionally included metals, energy, livestock, and agricultural products. Cryptocurrency does not square up easily with these kinds of property. However, recent understandings of what counts as a commodity have expanded to include mortgages, foreign currencies, and communication bandwidths. Like all commodities, cryptocurrency can also be bought or sold like a commodity; the price of bitcoin is based on supply and demand. The volatility of cryptocurrencies is very much like that of commodities; commodities investors invest in futures contracts rather than purchase the commodity. A connecting thread seems to be that commodities, like gold or pig-bellies, have value not only as an investment device, but also as a usable product; cryptocurrency does not. Moreover, because the value of cryptocurrency is not backed by anything other than itself, it differs from traditional commodities. Nevertheless, even though its initial and perhaps primary purpose is to act as a medium of exchange, currency can be treated as a commodity because it can be purchased and sold as an investment and, thereby, benefit from ups-and-downs in currency exchange rates.

In comparing cryptocurrency and commodities, the main practical issue is with the use of commodities as a speculative investment by way of future trading: most regulatory efforts are devoted to monitoring and constraining such activities. However, cryptocurrency is not like other commodities in that, when functioning as a currency, it is exchanged directly and momentarily. Also, unlike more usual futures commodity trading, the user of cryptocurrency as a currency is an exclusive owner; they have more than a contractual option to trade the underlying asset in question. That said, it can also, like currency, be utilized as an investment tool to hedge risk and speculate. When used in this way and traded for future consideration, it does potentially fall within the regulatory authority of the U.S. Commodity Futures Trading Commission (CFTC), a federal regulatory agency. Indeed, the CFTC has always insisted that that bitcoin and other digital currencies are commodities and, therefore, within its regulatory reach: this stance has been

confirmed by the courts.[26] Furthermore, the Canadian Revenue Agency has characterized cryptocurrency as a commodity, not a government-issued currency for the purposes of taxation.[27]

From a regulatory standpoint, the issue has become one of jurisdictional competence and priority. The central rivalry over the nature and identity of cryptocurrency is between the CFTC (as a commodity) and the Securities Exchange Commission (as a security). The decision whether to allocate regulatory responsibility to one, the other or both has significant consequences for the focus and substance of any regulations imposed. However, rather than opt for one or even both bodies as the regulatory agency of choice, a more preferable approach might be to treat cryptocurrency as property of its own kind, a little bit currency and a little bit commodity. This would allow the development of a regulatory scheme that is specifically designed for cryptocurrency and its peculiarities rather than squeeze it into a regulation scheme that clearly did not have in mind even the possibility of there being cryptocurrencies when its rules and regulations were developed. Accordingly, the more telling question is not whether cryptocurrency is a commodity (or anything else for that matter), but what is the most suitable and effective kind of regulation for cryptocurrency.

5. Is It A Security?

Perhaps the most settled definitional issue is that cryptocurrency can and should be considered to be a security. Appropriate regulatory agencies have determined that, whatever else they might be as well, bitcoin and other cryptocurrencies count as securities. However, this determination has limited and specific scope. Rather than treat cryptocurrency as a security at all times and for all purposes, the general consensus among securities regulators has been that the initial establishment of a cryptocurrency scheme or a cryptocurrency exchange comes within their regulatory mandate. In other words, the use of digital coin within the bitcoin process of exchange is not a practice to be regulated by securities agencies, but the venue for and practices of converting these coins into fiat currency through initial coin offerings (ICOs), initial token offerings (ITOs), or by selling securities of cryptocurrency investment funds is.[28]

---

[26] CFTC, Retail Commodity Transactions Involving Virtual Currency, Proposed Interpretation, 82 Fed. Reg. 60335 (December 20, 2017), https://www.cftc.gov/sites/default/files/idc/groups/public/@lrfederalregister/documents/file/2017-27421a.pdf. See CFTC v. McDonnell in the Eastern District of New York (August, 2018) where it was held that bitcoin and other cryptocurrency fell within the definition of a 'commodity' under the Commodity Exchange Act of and, therefore, fell within the regulatory jurisdiction of the CFTC. See also In re Coinflip, Inc., CFTC No. 15-29, 2015 WL 5535736 (Sept. 17, 2015) where then court on an expansive definition of commodity so that markets can be properly policed and traders appropriately protected. See also Nicole Swartz, Bursting the Bitcoin Bubble: The Case to Regulate Digital Currency as a Security or Commodity, 17 TUL. J. TECH. & INTELL. PROP. 319 (2014) and Hadar Jabotinsky, The Regulation of Cryptocurrencies - Between a Currency and a Financial Product, SSRN-id119591 (March, 2018).

[27] See https://www.canada.ca/en/revenue-agency/services/forms-publications/publications/t4037/capital-gains-2016.html #P279_2983.

[28] See, for example, https://www.sec.gov/news/public-statement/statement-clayton-2017-12-11#_ftnref8 and Canadian Securities Administrators, "CSA Staff Notice 46-307: Cryptocurrency Offerings", 40 OSCB 7233 (Toronto: OSCB, 24 August 2017) at 7231 [CSA Staff Notice] and SEC Statement on Potentially Unlawful Online Platforms for Trading Digital Assets (March 7, 2018), https://www.sec.gov/news/publicstatement/enforcement-tm-statement-potentially-unlawful-online-platforms-trading.

Although the meaning of what counts as a security for the purposes of regulation is not entirely fixed, it has long been accepted that there are several main elements to this categorization – the entity in question must involve an investment of money in a common enterprise with the expectation of profits that will be solely from the efforts of others.[29] While this definition encompasses the secondary and later market of cryptocurrency as an investment exercise, it does not apply too well to the original use of cryptocurrency itself as a medium of exchange; there is no real or necessary expectation of profits through the efforts of others. This becomes more apparent when the consequences of deciding that cryptocurrency is or is not a security for regulatory purposes are considered.

The effect of classifying something as a security and bringing it within the purview of the appropriate regulatory agency is that an array of governing principles and rules will apply. These include dealer registration, full disclosure, no insider trading, record keeping, auditing, investor protection and the like. The purpose of these requirements is to ensure that investors are appraised of all relevant information and that the market is able to price the securities appropriately. As regards, the secondary market of coin offerings and investment funds (e.g., Coinbase and Poloniex), these regulations seem to be warranted, even if some more subtle tweaking of those rules and their application would be beneficial and helpful. Similarly, these regulations do not adapt well to the regulation of the cryptocurrency itself; there is no investment or capital market that is in need of regulation and there is no form of asset representation other than the cryptocurrency unit itself. In this sense, the use of cryptocurrency as an exchange medium is more aptly thought of as a piece of personal property that functions more as currency than a security.

It is revealing that some of the most well-known fiascos around cryptocurrency involve the failure of these secondary organizations. In early 2014, Mt. Gox placed exchanges in the glare of publicity and alerted people to the risks of an unregulated market around cryptocurrency; losses were around $400M. More recently, the collapse the Canadian cryptocurrency exchange, Quadriga CX has revived concerns about the unruly operation of such institutions; unexplained losses remain at around $200M. Both of these affairs speak to the need for more serious regulation of the secondary market around cryptocurrency.[30] However, this leaves unresolved issues of how to deal with the primary operation of cryptocurrency. Efforts by the New York state Department of Financial Services to impose a BitLicense framework are a beginning.[31] But more in needed if cryptocurrency is to be used as a reliable and responsible zone of digital trading.

---

[29] See SEC v. W.J. Howey Co., 328 U.S. 293, 301 (1946). This definition has been adopted by the supreme court of Canada in Pacific Coast Coin Exchange of Canada v. Ontario (Securities Commission), [1977] 80 DLR (3d) 529, [1978] 2 SCR 112. See also Swartz, supra, footnote ** and Thomas Witteveen, Future Crypto-Concerns for Canadian Securities Regulators, 33 BANKING AND FINANCE L. REV. 265(2018).

[30] See Jake Adelstein and Nathalie-Kyoko Stucky, Behind the Biggest Bitcoin Heist in History: Inside the Implosion of Mt. Gox, http://www.thedailybeast.com/articles/2016/05/19/behind-the-biggestbitcoin-heist-in-history-inside-the-implosion-of-mt-gox.html and Allan Hutchinson, The Lesson Of Quadriga Are Not As Obvious as Many Think, https://www.theglobeandmail.com/business/commentary/article-lessons-of-quadriga-fiasco-not-as-obvious-as-many-think/.

[31] New York State Department of Financial Services (July 17, 2014). "NYDFS Releases Proposed BitLicense Regulatory Framework for Virtual Currency Firms. See https://web.archive.org/web/20140923054843/http://www.dfs.ny.gov/about/press2014/pr1407171.html.

D. A SEPARATE REGIME

1. A Special Agency

The problem to be faced in regulating cryptocurrency is the general issue of the 'governance paradox'[32] – How do you regulate an innovative scheme that demands some regulation, but know that any regulation will transform the very features of that scheme that makes it what it is as well as what makes it unique and useful? 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 regulatory regime for cryptocurrency. Consequently, in doing so, 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 -- the shared notion of putting ordinary people and their interests at the heart of any regulated society, not those of many civil or state-controlled institutions that tend to put their own interests ahead of others.

As I have been at pains to demonstrate, cryptocurrency is its own kind of activity and, therefore, should be regulated as such. it is an item of property that a little bit currency, a little bit security, and a little bit commodity. While it is conceivable that a patchwork quilt of regulatory agencies might be tasked with regulating cryptocurrency in the hope that this will produce a thorough and comprehensive scheme of regulation, this is highly unlikely. Indeed, the chances are that this will produce the worst of all worlds. Not only will administrative agencies vie for control, they will be doing so as a result of competing ambitions and by way of conflicting devices. This is a recipe for regulatory disaster; it will result in a heavy-handed, ill-suited and untidy mish-mash of regulations. Instead, it seems much more practical and useful to develop a regulatory approach to cryptocurrency that is as special and different in approach and implementation as cryptocurrency is in nature and operation. Of course, this might well entail borrowing and blending aspects from different and existing regulatory regimes and perhaps adding new approaches to boot. By so doing, it might be possible to achieve an integrated and coherent set of regulatory solutions that are sufficiently efficacious and balanced that they will advance the main goal of regulating cryptocurrency so that it is a better version of itself, not a lesser one.

The first move towards this goal is to establish an agency that will have primary and sole responsibility for regulating cryptocurrency in all its manifestations. In the spirit of cryptocurrency's decentralised philosophy, such a body should not be a typical and traditional government agency, like the SEC or CFTC. While it will be essential to include government representatives, they need not and should not comprise the majority of members. This would be a certain kind of quasi-autonomous non-governmental organisation (a QUANGO).[33] The idea is that this would be separate from government, but have ties to and representation from government. It would occupy that important, but neglected space between public authority and private autonomy. Working as a go-between for the cryptocurrency community and the broader society, its members would have a degree of tenure and, even if government appointees, have an arms-length relation

[32] KEVIN WERBACH, THE BLOCKCHAIN AND THE NEW ARCHITECTURE OF TRUST 133-38 (1918).

[33] Alan Pifer, The Quasi Nongovernmental Organization (Carnegie Corporation, 1967). For instance, while more popular in the United Kingdom, these organizations might include bodies like the US Federal Reserve. See PAUL KRUGMAN, THE AGE OF DIMINISHED EXPECTATIONS: US ECONOMIC POLICY IN THE 1990s 99 (1997).

to government. The ambition here would not be to produce neutral or apolitical recommendations, but to balance the often competing interests of its various constituencies.

Of course, it is important for both the legitimacy and efficacy of such an agency that it be populated by a full range of stakeholders from both inside and outside the cryptocurrency community. These might include software developers, miners, coin-holders, financial services representatives, cryptocurrency exchange operators, CFTC and SEC representatives, and the like. Also, in the spirit of the cryptocurrency community, the members would strive to attain rough consensus in its deliberations and policy initiatives. By populating such a regulatory body in this way, it might be possible to generate the kind of technological expertise, regulatory experience, and political savvy that is needed to pull off its ambitious mandate of regulating cryptocurrency in a way that holds true to its transformative possibilities and opportunities. This would entail the usual regulatory responsibilities of developing standards for registration, certification, sound practices, security, database management and the like.

This endeavour to create such a cryptocurrency quango, populate it representatively and define appropriately its mandate can draw upon the efforts of some organizations that already exist, even if they are in a somewhat embryonic state. For instance, there is the fledging ICO Governance Foundation (IGF). This is a decentralized, global and non-profit organization whose mission is to establish a protocol-based community that regulates ICOs in capital markets; it seeks to create and enforce global standards for disclosures as part of a voluntary registry.[34] Also, there is the Virtual Currency Association (VCA). An initiative of the Winklevoss twins, it is similar to the IGF in its non-profit and independent structure, but has a broader self-created mandate: it seeks to establish a global standards and best practices for the U.S. virtual currency industry, specifically virtual commodity exchanges and custodians. As a self-regulatory organization, it models itself on other similar groups, like the National Futures Association,, and plans to work with established regulators, like the SEC or CFTC.[35]

Both the IGF and VCA are non-public initiatives that offer some flavour of what a new cryptocurrency agency might look like or, at least incorporate. Rather than liaise with government bodies, the agency being proposed would combine the IGF and VCA with those public bodies and create a new quango that would replace them all. Although these kind of quangos are more common in the United Kingdom and Canada than in the US, they have much potential in cryptocurrency context. Although not without risks and flaws (i.e., if not properly constructed, they are open to government- and/or industry-capture), such a quango-like agency would be an important step in kick-starting an appropriate regulatory process for cryptocurrency.

2. A Balancing Mandate

[34] Miko Matsumura, ICO Governance: A Protocol-Based Self-Regulation of Token Sales in Decentralized Capital Markets, November 27, 2017. See https://icogovernance.org/wp-content/uploads/2017/12/Governance_of_Token_Sales_in_Decentralized_0.91.pdf.

[35] Cameron Winklevoss, A Proposal for a Self-Regulatory Organization for the U.S. Virtual Currency Industry (March 13th, 2018). See https://medium.com/gemini/a-proposal-for-a-self-regulatory-organization-for-the-u-s-virtual-currency- industry-79e4d7891cfc.

While the mandate of a Cryptocurrency Agency would be broad and comprehensive, it would be for the members to decide how to exercise and fulfil it. Nevertheless, there are certain issues that will have to be addressed and confronted. The crux of the matter will involve some evaluation of those characteristics that go the heart of the cryptocurrency enterprise and those that do not. It is only by engaging in this important exercise that it might be possible to address properly, if not entirely resolve fully the 'governance paradox' – to regulate, but not to negate the basic structure of the cryptocurrency process. To do this, tough decisions will have to be made about what is core and what is not. Also, it will be important to approach the regulatory task with the enigmatic Satoshi Nakamoto's admonition to early bitcoin users about the blockchain technology – "there's no reliance on recourse. It's all prevention."[36]

The primary characteristics of cryptocurrency are that it is it was intended to be an entirely borderless, decentralised, unmediated (without banks), pseudonymous, self-regulating and politically neutral medium. To be blunt, which of these characteristics, if any, can be interfered with or altered without eviscerating the whole cryptocurrency project? One way to come at this is to ask how it might be possible to deal with one of its main perceived failings – its use for illegal and even criminal activity. Insofar as there are a variety of legal provisions in play in the financial sector that are intended to prevent or punish activities like money laundering, tax, evasion, terrorist funding, currency limitations, and the like, there are no compelling reasons why cryptocurrency should be exempt from their reach or application. Indeed, it seems a reasonable complaint by established members of the financial services sector, especially banks, that cryptocurrency should not escape the prevailing legal frameworks for detecting and deterring such activities; ordinary people and traders would be harmed by such an exemption. It was surely not a central purpose of the Nakamoto and his colleagues to develop a process to facilitate such activities.[37]

If that all is the case, the challenge becomes how to prevent such activities while, at the same time, allowing the use of cryptocurrency to continue in its primary and defining initial format. While anonymity is a positive good, it is also a negative charge in that it allows criminal activities to proceed and go unchecked. At present, it is not so much that transactions are entirely anonymous, but that they are ascribable to a particular account by way of a cryptic pseudonym or password; the particular coin-holder is known, but not their real world identity. Indeed, the whole benefit of blockchain technology is that not only does it record and confirm all transaction, but it also does by knowing who transferred coins to who. The crunch issue, therefore, is whether it is possible to abandon or modify the semi- or pseudo-anonymity of present cryptocurrency transactions without irreparably changing their basic structure? Although purists will argue that it is not possible, I maintain that the answer to this is that it can be. In other words, cryptocurrency can remain cryptocurrency without being crypto.

---

[36] Satoshi Nakamoto, Re: Bitcoin P2P e-cash paper, https://www.mail-archive.com/cryptography@metzdowd.com/msg10006.html (November 17th, 2008).

[37] A question of relative importance is whether cryptocurrency is any more or less vulnerable to criminal activities than other trading or banking process. Although the predominant view seems to be that it is, some argue that cryptocurrency is less vulnerable because all transactions are viewable and, as such, cryptocurrency might be more capable of protecting against criminal activity than cash or fiat currency. See Tapscott and Tapscott, supra, note ** at 275-77.

The underlying integrity of cryptocurrency is founded on the notion of it bringing into existence a non-hierarchical system that is bottom-up, not top-down in its operational philosophy and regulatory structure. Moreover, because it was intended to challenge the hegemony of the banks and offer a viable alternative to them and other financial sector actors, its primary dynamic was motivated by a desire to create a decentralized, unmediated, self-generating and distributed process. If the characteristic of anonymity was to be cut back or reduced, it is not obvious that the *raison d'être* of the whole process of cryptocurrency trading would be fatally impaired. Indeed, ensuring that the process was less open to criminal or illegal use might actually enhance the wider reputation and attractiveness of the process and encourage more people to become participants. Divested of the stigma of illegality, cryptocurrency might better slip out of the relative shadows into a brighter and less marginal future.

Of course, achieving this, without doing substantial damage to the overall cryptocurrency process, is not a simple task. It will take a series of subtle and targeted interventions. In keeping with a commitment to regulation-lite, it will be useful to move well beyond the command-and-control mentality of traditional regulatory efforts. Instead, the cryptocurrency situation would best be handled, at least initially, with a range of more 'nudge-like' initiatives.[38] Indeed, regulation of cryptocurrency seems to be one of those activities that would benefit from a more-carrots-than-sticks approach. As such, a Cryptocurrency Agency might adopt measures like best practices, incentivization, voluntary registration and the like. If these proved ineffective, then a sterner and more directive set of interventions might be considered.

A particular and related challenge in regulating cryptocurrency is that, unlike in other similar areas and activities, there is no central authority or organizing lynchpin when it comes to cryptocurrency. Because cryptocurrency is a truly decentralized and distributed process, no one entity is fully tasked with the responsibility to make or implement decisions that are prescribed by a regulatory agency. Even if a gentler and more suggestive approach is adopted, there is the continuing problem of how such recommendations will be introduced across the cryptocurrency board. This is where a more innovative mind-set can intervene in ways that are both effective and consensual. The regulatory impulse might be able to influence the so-called *lex cryptographica* and engineer the kind of changes, like a scaling back of the system's semi-anonymous characteristics, that might be demanded.[39] In short, it might be possible to nudge and chivy the software guardians of the blockchain to design and build code that incorporates the kind of values and incentives that would be thought to best advance the goals of a more fairly and lightly regulated cryptocurrency world. These latter-day heirs to Nakamoto might be acting in the benevolent spirit of that originating genius.

Mindful that the blockchain code used is the heartbeat of cryptocurrency, the idea would be to take steps that would incentivise the code-makers to alter the operating software so that the identities of coin-holders could be retrieved and stored. As holders' pseudonyms must presently be recorded and known in order to allow the blockchain to validate transactions, it would be a relatively small step to develop a data-store of the real identity of the pseudo-anonymous users of cryptocurrency. There is no need for all other holders to be aware of a holder's identity: conditions

---

[38] RICHARD THALER AND CASS SUNSTEIN, **

[39] See supra, pp.**-**.

and constraints can be in place that preserve the limited confidentiality of such a data-store. Moreover, limited access in limited circumstances might be granted to certain existing government agencies, like those entrusted to handle taxation and money-laundering; such a scheme might be judicially-administered so as to balance and protect persons' individual rights. This overall kind of regulatory approach would allow a blend of the *lex cryptographica* with what might be termed the *lex traditionis* for the mutual benefit of each. Importantly, this would also permit the blockchain to remain its own regulator by continuing and developing an internal mode of algorithmic governance.[40]

Another approach that is attuned to and based upon the particular characteristics of a blockchain-enabled cryptocurrency system is the use of 'smart contracts'. These are self-executing agreements that require no third-party intermediary for enforcement and are based upon the autonomous code of existing blockchain technology. As such, they offer similar advantages to cryptocurrency generally – heightened cyber-security and lower transaction costs.[41] They are already used within or on top of the bitcoin network to facilitate a number of transactions, like escrow accounts, payment channels, multi-party security, and others. These innovative digital contracts can be utilized to regulate the use of cryptocurrency by organizing and verifying the operation of the data-store. Also, they could be customized to allow a tax-at source protocol that levied and transferred a certain sum upon each transaction to the appropriate tax authority; this would prevent the kind of extended litigation that is presently wending its way through the courts.[42]

Accordingly, the challenge of regulating an enterprise that has no central hub, is entirely technology-driven, creates its own enforced practice of trust, and prides itself on its reliance on distributed consensus can be achieved. Of course, these suggestions are only the beginning of a continuing and, through the cryptocurrency quango, an almost open-source of regulation. The most important feature is that the means and target of such regulation is compatible with both the nature and spirit of cryptocurrency and its blockchain protocols. Also, although some will resist this possibility, such regulation can make cryptocurrency a better and safer place to trade, transact and do business.

3. Across Borders

A distinctive feature of cryptocurrency is that, among others, it is a borderless process that operates in its own public domain. There are two dimensions to this problem in regard to regulation. The first is the border between the primary sphere of cryptocurrency as a trading process and its secondary province as an investment device. The second is the task of recognising that cryptocurrency is intended be a global innovation that does not acknowledge national boundaries and so can more easily evade the regulatory reach of any one jurisdiction. While the

---

[40] See generally DE FILIPPE AND WRIGHT, supra, note ** at 193-204 and WERBACH, supra, note ** at157-60.

[41] See MICHAEL CASEY AND PAUL VIGNA, THE TRUTH MACHINE: THE BLOCKCHAIN AND THE FUTURE OF EVERYTHING 2018) and Tapscott and Tapscott, supra, note **. The primary smart-contract platform is Ethereum that is public, not permissioned site and has its own cryptocurrency: 'ether' is the most common and valuable cryptocurrency after bitcoin.

[42] See, for example, **.

former regulatory challenge is easier to meet, the latter will require more concerted and cooperative efforts.

There seems to be a strong consensus within and outside the cryptocurrency community that some form of regulation is need for the secondary market of coin exchanges, initial coin offerings (ICOs), and other related trading and investment activities. Because these entities and occurrences function as part of the traditional market by facilitating various interactions between cryptocurrencies and fiat currencies, it is appropriate to recommend the introduction and enforcement of a regulatory regime that requires much the same set of principles and rules as the traditional market itself. The existing approaches of SEC and CFTC can be borrowed and amended in ways that a cryptocurrency regulatory agency would see fit.[43] As things stands, the usual requirements of registration, adequate record-keeping candid disclosure, auditing, client transparency principles, 'know your customer' rules, insurance, conflicts checks, and the like seem to be apposite and pertinent. Although some will contend that these requirements will be unduly onerous and stymie innovation, they do seem to be recommended on the same basis as existing securities and futures regulation – the protection of investors and other stakeholders.

A telling example of what can happen in an unregulated environment and what regulation might do to improve matters is offered by the recent collapse of the Canadian crypto-exchange, QuadrigaCX. When the creator and sole operator of the company, Gerald Cotten, died in mysterious circumstances, there was apparently no way to access his laptop or off-line USBs (so-called 'cold wallets') on which a suspected C$200 million of assets from almost 100,000 clients were stored: no one knew or could replicate his encrypted key. There were also suggestions that the funds had been embezzled. To make matters worse, there were no enforced regulations about registration, auditing, record-keeping and the like in effect: Cotton was running a truly off-the-grid operation. Ironically, this state of affairs confirms the hyper-security of cryptocurrency. Nevertheless, even if speculative users of QuadrigaCX were naïve in much the same way as investors in Bernie Madoff's too-good-to-be-true scheme,[44] they were entitled to some regulatory supervision and protection that might have avoided such a fiasco.

The other challenge is how to handle and respond to the borderless ambitions and actual operations of cryptocurrency. As with tax evasion and dubious banking, the possibility of simply moving off-shore to avoid unwanted regulations is real. This should not discourage jurisdictions from taking the regulatory task seriously; many crypto-enthusiasts will remain local in their trading and business, especially in the United States. At present, there is a patchwork of national procedures for such monitoring. Some countries, like China, have taken a no-cryptocurrency position, while others, like Malta and Japan, are enthusiastically open for business. Obviously, this is not a desirable situation: a multi-national approach is a much better option.

---

[43] In Europe, the regulatory framework under the Markets in Financial Instruments Directive (MiFID) has been held to apply when crypto-assets qualify as transferable securities or other types of financial instruments. See ESMA Advice – Initial Coin Offerings and Crypto-Assets (January 9, 2019), https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf.

[44] See DIANA HENRIQUES, THE WIZARD OF LIES: BERNIE MADOFF AND THE DEATH OF TRUST (2017). On the QuadrigaCX debacle, see Mystery as Quadriga crypto-cash goes missing, https://www.bbc. com/news/technology-47454528 and Hutchinson, supra, note **.

At the recent G20 Summit in Argentina in November 2018, the member countries agreed that they would be taking concerted action to regulate cryptocurrency. With guarded praise for its technological innovations that have led to significant benefits to the global economy, a call was made for some substantial and serious regulation to deal with money laundering, terrorist funding, excessive risk speculation, and the coordination of cross-border taxation. The basic plan is to rely on the standards created by the Financial Action Task Force (FATF), established by the G7 in 1989.[45] However, the G20 is unlikely to exercise a light touch in regulating crypto-currency. In combatting criminal and terrorist activity, there will likely be a more heavy-handed approach. Innately suspicious of any effort to evade public scrutiny and oversight, governments will find it difficult to forebear from introducing a raft of restrictive and intrusive measures. However, as I have recommended, that impulse should be resisted. When it comes to cryptocurrency, the more that is done in plain sight will be better than pushing it further to the shadowy margins.

E. Conclusion

If the effort to regulate cryptocurrency is to be successful, it will be important that the cryptocurrency community is not the only one open to some changes and enhancements. It is also vital that the legal and regulatory community approach this task as an occasion to change and challenge its own traditional ways of doing things. The style, tools and substance of legal regulation must adapt to cryptocurrency as much as cryptocurrency must adjust to regulatory interventions. On both sides, there are beneficial and mutually-reinforcing opportunities for transformation and improvement. A heavy-handed approach would be counter-productive and work to the advantage of the very established financial institutions that are most threatened by the efficient innovation of an entirely borderless, decentralised, unmediated, self-regulating and politically-neutral medium for doing business and trading. By adopting lighter and more sensitive modes of regulatory policy, both cryptocurrency (and other new technological inventions) and law can evolve and serve better the interests of the broader public.

[45] Financial Action Task Force, Public Statement: Mitigating Risks from Virtual Assets, http://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-[assets-interpretive-note.html

.