Regulation by blockchain

Yeung, Karen

DOI:
10.1111/1468-2230.12399

Regulation by Blockchain:
The Emerging Battle for Supremacy between the Code *of* Law and Code *as* Law

Abstract

Many advocates of distributed ledger technologies (including blockchain) claim that these technologies provide the foundations for an organisational form that will enable individuals to transact with each other free from the travails of conventional law, thus offering the promise of grassroots democratic governance without the need for third party intermediaries. But does the assumption that blockchain systems will operate beyond the reach of conventional law withstand critical scrutiny? This is the question which this paper investigates, by examining the intersection and interactions between conventional law promulgated and enforced by national legal systems (ie the 'code *of* law') and the internal rules of blockchain systems which take the form of executable software code and cryptographic algorithms via a distributed computing network ('code *as* law'). It identifies three ways in which the code *of* law may interact with code *as* law, based primarily on the intended motives and purposes of those engaged in activities in developing, maintaining or undertaking transactions upon the network, referring to the use of blockchain: (a) with the express intention of evading the substantive limits of the law (*'hostile evasion'*); (b) to complement and/or supplement conventional law with the aim of streamlining or enhancing compliance with agreed standards (*'efficient alignment'*); and (c) to co-ordinate the actions of multiple participants via blockchain to avoid the *procedural* inefficiencies and complexities associated with the legal process, including the transaction, monitoring and agency costs associated with conventional law *('alleviating transactional friction')*. These different classes of case are likely to generate different dynamic interactions between the blockchain code and conventional legal systems, which I describe respectively as 'cat and mouse', the 'joys of (patriarchial) marriage' and 'uneasy coexistence and mutual suspicion' respectively.

I argue that the emerging response of conventional law in the first two kinds of case can be readily anticipated and understood. While the first class of case threatens to undermine the rule of law and which national legal systems can be expected to take positive action to safeguard, the second class of case does precisely the opposite: reinforcing the primacy and sovereignty of national law, and hence blockchain applications falling within this class are likely to be regarded as a welcome development by conventional legal systems. But it is the law's response to the third category of applications ('alleviating transactional friction') that is the most difficult to predict, due to the normative ambiguity of these applications. Whether the conventional law ought to intervene to oversee these systems raises fundamental tensions between the sovereignty of law in modern legal systems, including the universal coverage of the rule of law and its guarantee of security (which includes, but extends beyond, providing transactional security), on the one hand, and respect for individual autonomy and freedom of association on the other. I argue that, to the extent that the exercise of agency and freedom of association by a group of individuals results in adverse consequences for third parties and the broader public, state intervention via the code of law is normatively justified. Accordingly, the critical challenge is to identify the conditions and circumstances in which this threshold is reached in concrete contexts in order to justify the assertion of supremacy by conventional law over activities taking place on and arising out of blockchain systems.

Regulation by Blockchain:
The Emerging Battle for Supremacy between the Code *of* Law and Code *as* Law

Karen Yeung[*]

1. Introduction

The current hype concerning distributed ledger technologies, commonly referred to as 'blockchain'[1], is rooted in their capacity to enable transactions between strangers through reliance on cryptographic software algorithms run across a distributed computing network, establishing secure peer-to-peer interactions through which an immutable[2], tamper-proof shared ledger can be reconciled in real time. By obviating the need for trusted third-party intermediaries to guarantee the validity of transactions, which have, in contemporary society, taken the form of powerful institutions such as nation states or multi-national financial institutions, blockchain could radically alter the existing distribution of social and economic power[3]. It is in the developing world, where reliable, trustworthy and effective legal institutions are often absent, that blockchain may deliver the most significant transformational change. For example, the new Honduran government started creating a secure record of land title on the blockchain to address the inaccuracy and inadequacy of existing land and business records which corrupt public officials have tampered with to acquire title to property illegitimately.[4] Yet those in advanced industrialised economies are also excited by blockchain's potential, particularly in the financial services and commercial sector which could facilitate swift, secure and reliable transactions without the operational costs, delays and inefficiencies associated with conventional legal

[*] Interdisciplinary Professorial Fellow in Law, Ethics and Informatics, Law School & School of Computer Science, the University of Birmingham. I am indebted to two anonymous reviewers for their helpful comments on an earlier draft. Earlier versions of this paper were presented at UCL workshop, Blockchain and the Constitution of a New Financial Order Legal and Political Challenges, UCL Faculty of Laws, London 19 June 2017; Centre for Media & Communications Law/ Centre for Corporate and Securities Regulation & Transactional Law Research Group, Melbourne Law School, Melbourne, Australia, 13 April 2018 and 'Law and Big Data' Workshop, Bar-Illan University, Faculty of Law & Data Science Institute, Tel Aviv, Israel 14-15 May 2018.

[1] Although not all distributed ledgers technologies take the blockchain form, this article uses the term 'blockchain' refers to distributed ledger technologies whether or not in the form of a blockchain. See discussion at section 2.1 below.

[2] On blockchain immutability, see n.11 below.

[3] Many blockchain enthusiasts (sometimes known as 'blockchainiacs') believe that these technologies will fundamentally revolutionise economic and social organisation. Eg Smith, Jamie (2016) 'There Is More to Blockchain Than Moving Money. It Has the Potential to Transform Our Lives - Here's How', World Economic Forum, 9 November 2016 available at https://www.weforum.org/agenda/2016/11/there-is-more-to-blockchain-than-moving-money/ (accessed 29 November 2017). The Economist (2017) 'The Long Arm of the List', 15 July, available at https://www.economist.com/news/world-if/21724906-trust-business-little-noticed-huge-startups-deploying-blockchain-technology-threaten (accessed 4 December 2017); Boucher, Philip (2017). *How Blockchain Technology Could Change Our Lives*, European Parliamentary Research Service: European Parliament, February available at http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/581948/EPRS_IDA(2017)581948_EN.pdf (accessed 29 November 2017).

[4] Schiller, Ben. "How the Technology Behind Bitcoin Is Going to Change the Lives of the Bottom Billion." *Fast Company*, 3 May 2016. Sweden and Georgia are also experimenting with blockchain for Land Title Registry, although at the time of writing, the Honduran project appears to have stalled. See Plaster, Morgan. "Can Blockchain Title Registry Make Property Rights More Secure?" See https://www.globalrealestateexperts.com/2016/11/can-blockchain-title-registry-make-property-rights-more-sec (accessed 29 November 2017).

mechanisms.[5] Yet, as a general purpose technology[6], blockchain's potential applications reach beyond the realm of commerce and finance. For example, the UK's Chief Scientific Officer refers to blockchain's potential to help governments to collect taxes, deliver social security benefits, issue passports, record land registries, assure the supply chain of goods and ensure the integrity of government records[7] in a more transparent and accountable form.[8] By enabling new forms of social and community co-operation without a central authority, blockchain's offers the promise of decentralising and democratising collective decision-making.

But will blockchain technology operate without the need for the state as central authority, thus operating *outside* the realm of conventional law? Although this question cannot be answered definitively given that blockchain applications are in their infancy, this paper offers a hypothesis concerning how these two quite different systems for governing interactions between strangers are likely to interact. It seeks to identify and critically examine the underlying normative values and tensions that conventional law-makers and enforcement officials must confront in determining whether legal intervention into blockchain systems is necessary and justified. My analysis begins from the premise popularised by cyber-scholar Lawrence Lessig who claimed that, within cyberspace, 'code is law,' in that the internet's technical infrastructure and software code regulates, constrains and enables on-line behaviour and interaction[9]. By examining the extent to which, 'governance by blockchain' may avoid the reach of conventional law, this paper interrogates the intersection and interactions between two quite different modalities of governance: conventional law (the 'code *of* law'), on the one hand, and the internal rules of blockchain systems which take the form of executable software code and technical protocols ('code *as* law')[10], on the other. It offers a schematic map of the different kinds of interaction that are emerging, and likely to emerge, between these two forms of social ordering as the technology develops and matures.

I will argue that the belief that blockchain systems will operate outside of, and independently from, conventional law, rests on two assumptions: firstly, that the conventional state legal system is rendered redundant because blockchain provides guarantees of security of equal (or greater) effectiveness and efficiency compared to those currently provided by conventional law, and secondly, that the state will refrain from intervening in blockchain networks - either because its interests are not threatened by particular blockchain networks or applications, or, even if they are, the state nevertheless lacks the practical capacity to take effective action to forestall or mitigate these threats. My argument is that these assumptions are highly implausible: not only are legitimate state interests threatened by blockchain systems consisting of threats to the universality of the rule of law, but also because the security offered by blockchain systems is narrow and limited to 'transactional security'. Even if blockchain systems can successfully provide reliable and efficient transactional security, they are unlikely to deliver other critical security guarantees (including protection against interference with rights of property, threats to health and safety, and unfair exploitation), that are currently (albeit imperfectly) provided by conventional law.

---

5 Yeung, Karen (2017) 'Blockchain, Transactional Security and the Promise of Automated Law Enforcement: The Withering of Freedom under Law?' In Philipp Otto and Eike Graf (eds) *3TH1CS – A Reinvention of Ethics in a Digital Age*, 132-46. Berlin: iRights.Media.

6 Government Office for Science (2016). *Distributed Ledger Technology: Beyond Block Chain*. London (hereafter the 'Blackett Review 2016').

7 Blackett Review 2016, 6.

8 Blackett Review 2016, 30.

9 Lessig, L. (1999). *Code and Other Laws of Cyberspace*. New York, Basic Books.

10 In this paper, I adopt the approach taken by the Blackett Review, referring to the technical code of distributed ledger systems as including both the software (computer code) and protocols, since both are required for distributed ledgers to function: Blackett Review 41.

The remainder of this paper proceeds in four parts. First, I explain the basic technological mechanisms through which blockchain operates, noting how their decentralised nature is likely to create difficulties for conventional law-makers and enforcement officials in responding appropriately and effectively. Secondly, I identify three different ways in which the code *of* law may interact with code *as* law, based primarily on the intended motives and purposes of network participants when engaging in transactions within the network vis a vis the conventional law, and secondly on the nature, scope and magnitude of potential harms arising from particular blockchain applications. These purposes that I identify as likely to motivate participants to utilise blockchain systems are concerned to (a) deliberately evade the substantive constraints of conventional law ('hostile evasion') (b) complement and/or supplement conventional law to streamline or enhance compliance with legal standards ('efficient alignment'), and (c) to co-ordinate actions across and between multiple participants, without the procedural inefficiencies associated with the conventional legal process ('alleviating transactional friction'). Each of these three motivations can be expected to generate a particular kind of dynamic interaction between law and blockchain systems, which I describe as *cat and mouse*, *the joys of marriage* and *uneasy coexistence and mutual suspicion* respectively. The penultimate section of the paper reflects upon the deeper normative challenges and tensions underlying these predicted interactions between the two ordering systems, which are most acute in the third class of case aimed at alleviating transactional friction, and is ultimately rooted in the shifting and uncertain boundaries between the public and private realm in a continuously networked digital age. The final section concludes.

2. How will the code *of* law interact with code *as* law?

Before proceeding, a brief explanation of what blockchain is, how blockchain works, and why it apparently render third party intermediaries redundant, is required, and to which I first turn.

2.1 Distributed ledger technologies ('blockchain technology'): a brief outline

Blockchain is an append-only, distributed database that is collaboratively stored, maintained and updated across a network of computers, with each computing 'node' in the network storing an identical copy of the database[11]. Cryptographic methods enable mathematical consensus to confirm the consistency of each transaction's digital record, which is then permanently recorded on the database, preventing their alteration or deletion.[12] Information on the blockchain is represented as cryptographic tokens which guarantee the technical authenticity of the information. Blockchain systems record the allocation of these tokens among anonymous accounts, automatically recording all exchanges of these tokens between accounts and automatically updating each copy of the database at each node. The security and accuracy of the ledger is maintained through the use of computational techniques in which cryptographic 'keys' and signatures control who can do what with the shared ledger.[13] If conflict between the different copies of the database arises (for example, because someone is trying to tamper with the data) an automatic cryptographic consensus mechanism[14] is designed to

11 Blackett Review 2016.

12 This so-called 'immutability' is, however, imperfect due to the possibility of 'forking' software code, which refers to the copying of an existing open source software programme and the distribution of a modified version of it. If both the old and new versions of the software are implemented, this can result in competing versions of public blockchains with the result that two distinct ledgers are maintained. See Walch, Angela (2017) "Open Source Operational Risk: Should Public Blockchains Serve as Financial Market Infrastructures?" In David Lee Kuo Chuen and Robert H Deng (eds.), *Handbook of Digital Banking & Internet Finance, Volume 2*, forthcoming. Werbach points out that immutability is not always beneficial for trust, because it can provide false confidence. In particular, the blockchain guarantees that a transaction was recorded accurately and once only: it does not guarantee that the person making the transaction was the rightful owner of the private key, or other factors: Kevin Werbach (2016) 'Trustless Trust.' SSRN Network, accessed 9 June 2018.

13 Blackett Review 2016, 5.

ensure that only those updates get permanently recorded on the blockchain that are consistent with the earlier, stored versions of the database. Distributed ledger systems which take the blockchain form aggregate transactions into 'blocks', and these are added to a 'chain' of existing blocks using a cryptographic signature (hence the name 'blockchain')[15]. In public (or 'unpermissioned') blockchain systems[16], these records are fully transparent and can therefore be viewed by anyone on the network, thus creating a 'distributed, shared, encrypted-database that serves as an irreversible and incorruptible public repository of information.'[17]

The revolutionary potential of blockchain technologies may not be readily apparent from this thumbnail sketch of their mechanics, which lies in its capacity to provide a 'distributed yet provably accurate record'[18] without a central intermediary to ensure the veracity and accuracy of transactions and their recording on the database[19]. Blockchain has therefore been described as signifying a move to 'trustless trust'[20] in which transactional security is achieved via reliance on 'trust-by-computation' established across a decentralised computing network. Accordingly, The Economist has described blockchain as a 'trust machine'[21], with Antonopolous similarly claiming that blockchain represents a 'shift from trusting people to trusting math.'[22] Blockchain could therefore transform the internet from a powerful mechanism for transferring *information*, into an even more powerful vehicle for transferring *value*[23]: because all participants trust in the veracity and accuracy of a singular trusted state of truth without the need for trusted actors[24], value can be securely transferred via the blockchain. While Bitcoin was the first public blockchain, creating the first electronic payment

---

14 In the Bitcoin blockchain, the consensus mechanism is referred to as 'mining'. Bitcoin: The Magic of Mining (2015), *The Economist*, 10 January at 58 available at http://www.economist.com/node/2163812 (accessed 9 June 2018).

15 Blackett Review 2016, 5.

16 Blockchains can be public ('permissionless' or 'unpermissioned) or private ('permissioned'). An unpermissioned ledger, such as the Bitcoin blockchain, has no single owner and allows anyone to contribute to the data, making the ledger censorship resistant and difficult to hack: because a successful cyber-attack would require all existing copies of the ledger to be simultaneously attacked, and attempts to tamper with the ledger would be thwarted by the automatic consensus mechanism. In contrast, permissioned ledgers are closed systems which have one or multiple owners. When new records are added, the ledger's integrity is checked through a limited consensus process carried out by trusted actors who have controlling authority over the ledger: Blackett Review 2016, 17.

17 Wright, A., and De Fillipi, P. (2015) Decentralised Blockchain Technology and the rise of *Lex Cryptographia'* SSRN network, 2.

18 Werbach. *Supra* n.11.

19 Blackett Review 2016.

20 Werbach. *Supra* n 11.

21 *The Economist.* (2015). 'The Trust Machine - The Promise of Blockchain.' 31 October.

22 Antonopoulos, A. (2014). Bitcoin security model: trust by computation. *O'Reilly Radar.* 20 February, available at http://radar.oreilly.com/2014/02/bitcoin-security-model-trust-by-computation.html (accessed 10 June 2018).

23 Yaw-Owusu, F. 'Blockchain: Moving from the Internet of Information to the Internet of Value' at https://themarketmogul.com/blockchain-information-internet-value/ (accessed 21 May 2018)

24 Finck, M. (2017). 'Blockchain Regulation' Max Planck Institute for Innovation and Competition Research Paper Series No. 17-13, Available via SSRN Network, 4.

system in 2009 based on a decentralised peer-to-peer network, its underlying blockchain technology is general purpose in nature. Blockchain could therefore be employed in many different contexts in which a ledger is required, such as electronic record-keeping and registries, supply chain verification and persistent attribution for digital works.[25] Accordingly, blockchain could radically disrupt existing political and economic orders by dispensing with the need for conventional third party intermediaries, including the state, enabling peer-to-peer transactions via the blockchain without the operational inefficiencies currently associated with conventional law.[26]

Before embarking on an investigation of the interaction between blockchain systems and conventional law, two features of public blockchains arising from their decentralised form may be especially challenging for conventional law are worth highlighting: first, identifying which (if any) actors' motives, intentions, rights, interests and obligations should be ascribed legal significance, and secondly, identifying practical strategies for intervening in the operation of blockchain network, to which I first turn.

2.2 Multiple participants, interests and purposes within a decentralised system

The decentralised, distributed nature of public blockchains means there is no single, centrally controlled and integrated entity which conventional legal systems can regard as a bearer of legal rights and/or duties. This might generate difficulties for conventional law-makers and enforcement officials when considering blockchain's legal implications, and may require the identification of the interests, purposes and/or intentions of particular blockchain networks, applications and/or those who participate in and upon them, which are likely to be multiple and divergent. Although the activities of corporate entities implicate many stakeholders, with many varied interests, purposes and intentions, a corporate entity has long been recognised as a single legal entity with juristic personality. Because corporate entities are 'artificial' persons, their governance structure is mandated by law, requiring both an underlying constitutional framework (known as a company's Memorandum and Articles of Association) which specifies how the company can act: typically through its directors acting in accordance with a specified procedure. Moreover, conventional legal systems have, over time, developed settled principles and doctrines through which the intention and motives of particular individuals within the corporate entity might be legally attributed to it for particular legal purposes (including the application of criminal punishment, which typically requires proof of criminal intent).[27] Public blockchain networks may be analogous to corporate entities in that a variety of actors are directly involved in their operation, who are widely dispersed in space and time, with very distinct interests, opportunities, forms of participation and motives for their involvement.[28] These include the individual entrepreneurs who initiate and develop ideas for new blockchain applications; the software developers who devise, implement and contribute to the open source software code and cryptographic protocols upon which public blockchains generally operate (including the 'core developers' who occupy informal leadership roles based on their reputation and performance within the open source software developer community[29]); the operators of nodes (i.e. those providing the computing power, performing the cryptographic proofs and storing a copy of the ledger); the holders of private keys (i.e.

25 Blackett Review 2016; Werbach. *Supra* n.11.

26 Atzori, M. (2015). 'Blockchain Technology and Decentralized Governance: Is the State Still Necessary?' SSRN network (accessed 10 June 2018).

27 Coffee, J. (1981). 'No Soul to Damn, No Body to Kick: An Unscandalised Essay on the Problem of Corporate Punishment.' *Michigan Law Review* 79: 413-424. Ferran, E. (2011). 'Corporate Attribution and the Directing Mind and Will.' *Law Quarterly Review,* Vol. 127: 239-259.

28 It is these differential interests that are highlighted in debates about blockchain governance: see for example De Filippi, P. and B. Loveluck (2016). 'The invisible politics of Bitcoin: governance crisis of a decentralised infrastructure.' *Internet Policy Review* 5(3) doi: 10.14763/2016.3.427.

29 Walch, A. (2017). 'Open Source Operational Risk: Should Public Blockchains Serve as Financial Market Infrastructures?' D. L. K. Chuen and R. H. Deng (eds.) *Handbook of Digital Banking & Internet Finance, Volume 2.*: forthcoming, 10.

those who transact upon the network by, for example, trading in cryptocurrency) and commercial providers of 'wallet' services that provide a user-friendly interface for those wishing to transact on the blockchain network but lack the technical sophistication, capacity or confidence to do so directly[30]. Yet, unlike corporate stakeholders, participants in blockchain networks are not recognised by law as bound together in a single, centralised organisational form. For the time being, conventional law does not mandate the governance structure of blockchain systems, perhaps partly because blockchain governance structures are encoded in their software architecture, rather than being purely socially constructed, unlike the corporate entity. Accordingly, the response of conventional legal systems to questions concerning the relevance and attribution of the intentions of particular individuals involved in blockchain networks is likely to remain uncertain until the technology matures and direct encounters between them occur more frequently. Yet it is reasonable to expect that their response will depend on the particular context and question arising for consideration, including whether the operation of particular blockchain activities threatens legitimate state interests, discussed more fully at section 4 below[31]. I expect that legislators and enforcement officials will take a highly pragmatic stance, similar to their approach in exerting national legal authority over conduct occurring on internet: if law-makers and enforcement officials regard the operation of blockchain networks as significantly threatening legitimate state interests, then they are likely to attempt intervention against *any* actors that they identify as in a position to exert influence over the network and/or activities taking place upon it (whether or not it is morally appropriate to hold them responsible) in order to safeguard national interests.

A different but related practical challenge arises when conventional law-enforcement officials seek to intervene in the operation of public blockchain networks. One significant advantage of decentralised computer systems is the absence of any 'single point of failure'. Although this enhances the resilience of the network's stability and operation[32], it may be less desirable from a conventional law perspective because there is no single organisational or individual gatekeeper upon that it targeted in order to intervene in their operation.[33] These concern about the regulability of blockchain resonates with academic debates concerning the regulability of the internet taking place when the internet first emerged. Cyber-libertarians claimed that the internet's distributed, global nature rendered it essentially ungovernable by nation states and beyond the effective reach of law, owing to the possibility for anonymous participation and the high degree of mobility of participants in cyberspace, enabling them to relocate freely to other areas of cyberspace.[34] Cyber-paternalists disagreed, arguing that there was nothing inherent in the nature of cyberspace that rendered it beyond the reach of law,

---

30 In relation to the bitcoin blockchain, for example, individuals who wanted to own or transact in Bitcoin at the time of its inception in 2009 could either run the Bitcoin protocol (a Bitcoin client) on their own computer, or create an account on a website that runs the bitcoin client for its users. But because bitcoin has been designed to preserve the scarcity of bitcoins, the difficulty of running the cryptographic proof (called Bitcoin 'mining') increases as the number of coins increases, so it is no longer practically possible for individuals to mine new coins and who instead must buy bitcoins with fiat currencies through cryptocurrency exchanges, ie. firms that hold bitcoins and are willing to sell them at a specified exchange rate: Guadamuz, A. and C. Marsden (2015). 'Blockchains and Bitcoin: Regulatory Responses to Cryptocurrencies'. *First Monday* 20 (12).

31 See below discussion of the rule of law (at section 2.1) and, for example, the potential harm to human health and safety in relation to energy distribution via blockchain systems (at section 2.3), to the property interests of participants (at section 3.2) and to creditors of an insolvent company (at section 3.2).

32 For a cyber-attack to succeed, it would have to attack all the copies simultaneously.

33 The decentralised nature of the network also makes the legitimate and effective governance of blockchain networks particularly challenging, in contrast to vertically integrated bureaucratic forms of organisation: see De Filippi, P. and B. Loveluck (2016). 'The invisible politics of Bitcoin: governance crisis of a decentralised infrastructure.' *Internet Policy Review* 5(3).

34 DeNardis, L. (2014). *The Global War for Internet Governance*. New Haven, Yale University Press.

with Lessig arguing, for example, that ordinary laws that apply to behaviour in the physical world regulate behaviour in cyberspace, although the latter's effectiveness might vary depending upon the characteristics of cyberspace, and which states might also regulate through control of the code itself, or the institutions (i.e. the coders) who produce the code that shapes the contours of cyberspace.[35] As time passed and the internet matured, it soon became apparent that the predictions of the cyber-paternalists were closer to the mark.[36] It remains to be seen whether the same or similar dynamic will play out in the interactions between blockchain and conventional legal systems, to which I now turn.

2.3 Anticipated Forms of Interaction between the Code *of* Law and Code *as* Law

In this section, I develop a typology of emerging and anticipated interactions between blockchain and conventional legal systems. It springs from my view that the nature of these interactions will depend critically upon whether particular blockchain applications are likely to be regarded by the state as threatening its legitimate interests. I identify two core interests which conventional legal systems have a legitimate responsibility to protect and safeguard that particular blockchain applications might threaten: first, the rule of law and the universality of its application, and secondly, the safety and security of its citizens. Furthermore, I will suggest that the extent to which these interests are potentially threatened by blockchain is likely to depend upon at least two sets of variables: (a) first, and most importantly, the purposes and intentions of blockchain network participants concerning conventional law in seeking to engage in blockchain network activities, and (b) secondly, the nature, scope and magnitude of potential harm (both to network participants and to third parties) arising from particular blockchain applications. On this basis, I identify three different classes of blockchain applications, based primarily on the first of these variables, which I refer to as (a) *hostile evasion*, where blockchain systems are used deliberately to evade the substantive constraints of conventional law (b) *efficient alignment*, where blockchains are employed to complement and/or supplement conventional law to streamline or enhance compliance with legal standards, and (c) *alleviating transactional friction*, referring to blockchain applications aimed at co-ordinating actions between multiple participants, motivated by a desire to avoid the procedural inefficiencies, costs and complexities associated with the conventional legal process. Each of these three motivations can be expected to generate a particular kind of dynamic interaction between blockchain and conventional legal systems, which I describe as of *cat and mouse*, *the joys of marriage* and *uneasy coexistence and mutual suspicion* respectively.

2.3.1 Hostile evasion provoking on-going 'cat and mouse' interaction

(a) Using blockchain to evade substantive legal duties and obligations

We have seen how blockchain systems enable direct peer-to-peer social cooperation between strangers without the need for the state or other third-party intermediary to guarantee the security of transactions. Yet blockchain is employed deliberately to *evade* the substantive obligations imposed by conventional law, this directly threatens the rule and sovereignty of law upon which conventional legal systems are rooted. National law enforcement officials can therefore be expected to assert their legal authority to halt and deter such activities,[37] for if they fail to act against blatant attempts to evade the law, this exposes potential victims of crime to serious harm and, as the European Banking Authority has warned, could undermine the reputation of the regulator and confidence in the integrity

---

35 Wu, T. and J. Goldsmith (2008). *Who Controls the Internet?: Illusions of a Borderless World*. New York, Oxford University Press.

36 Ibid. DeNardis, *supra* n 33.

37 Ripple Inc's failure to comply with anti-money laundering requirements may or may not have been intentional, although the Statement of Facts and Violation issued by FinCEN at the time at which the settlement was announced identifies at least one instance in which a Ripple employee intentionally refrained from insisting upon completion of 'Know Your Customer' requirements in the face of a client's threat to use a competitor which did not 'require nearly as much paperwork': FinCEN *Statement of Facts and Violations,* per FinCen Press Release, *ibid*.

of the national legal system itself.[38] Accordingly, if blockchain networks, particularly those dealing in cryptocurrencies, are used intentionally to evade the *substantive* obligations imposed by tax legislation, financial market regulation, mandatory consumer protection legislation and the like, then, particularly if the magnitude of potential harm to individuals and society is considered significant, national legal systems are likely to take enforcement action against them.

One of the challenges that conventional legal systems have already confronted, however, is navigating the multiplicity of participants and their varied motivations for engaging with blockchain networks. Given the many benefits of blockchain systems, it is reasonable to expect states to allow their use for legitimate purposes, whilst clamping down on blockchain activities aimed at avoiding their substantive laws. For example, the concept Bitcoin was originally formulated by anonymous founder, Satoshi Nakamoto, as an alternative to conventional fiat currencies issued by nation states that could operate as a form of payment.[39] In and of itself, the establishment of an alternative payment system does not threaten the rule of law any more than a barter system for the exchange of second-hand goods by residents within local communities threatens the rule of law. However, the greater degree of anonymity (in contrast to conventional currencies) associated with the use of Bitcoin as a form of payment meant that it became a popular vehicle for those wishing to engage in illegal activities.

Accordingly, in circumstances where cryptocurrencies have been used deliberately to circumvent substantive legal requirements, national legal authorities have selectively sought to exert their sovereign authority over those activities (and, where possible, the participants who engage in them) on a piecemeal basis. Yet the distributed nature of the Bitcoin network and the absence of a single legal entity has meant that in clamping down on illegal activity, conventional legal authorities have targeted their enforcement activity at particular public interfaces within the broader digital ecosystem in which cryptocurrencies have been used for illegal purposes, rather than directly intervening the Bitcoin network per se. For example, US Federal Regulators moved swiftly to shut down online marketplace 'Silk Road', in which Bitcoin rose to prominence by creating a platform over which a range of illegal merchandise could be purchased and then paid for using Bitcoin, rather than attempting to directly restrict the use of Bitcoin[40]. Nor have national authorities focused solely on seeking to identify and take enforcement action against the individuals using cryptocurrencies intentionally to evade the substantive obligations arising under conventional law. Rather, they appear to have been more concerned with closing off opportunities to use cryptocurrencies to evade legal duties, pursuing a preventative and defensive strategy, rather than one focused on apprehending and punishing the primary offenders. National regulators have therefore largely avoided taking across-the-board regulatory action against Bitcoin, with Thailand being the only nation that has sought to prohibit its use in 2013 (rather unsuccessfully) while China has restricted lawful dealing in Bitcoin to commodity trading, effectively prohibiting it from being used as a form of currency[41].

Financial regulations have also sought to intervene in the cryptocurrency eco-system where participants have created opportunities for criminal and other attempts at evading the law. For example, the US Financial Crimes Enforcement Network (FinCEN) issued guidelines in 2013 indicating that decentralized currencies should comply with money laundering regulations, bringing a successful enforcement action against Ripple Labs Inc, which operated a virtual currency exchange in 2015. This action resulted in a civil penalty settlement of US$ 700,000 for alleged wilful violation of the anti-money laundering laws, while Ripple also settled a criminal investigation by the US Attorney's Office for the Northern District of California for the same anti-money laundering failures, agreeing to pay a criminal fine of US$450,000 in partial satisfaction of FinCEN's $700,000

---

38 European Banking Authority (EBA) (2014). *EBA Opinion on 'Virtual Currencies*, EBA EBA/Op/2014/08 at 36 available at https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf (accessed 4 December 2017).

39 Guadamuz, and Marsden, *supra* n 29.

40 *Ibid.*

41 *Ibid*.

penalty.[42] FinCEN's enforcement action demonstrates why conventional law-makers and enforcement officials can be expected to assert their sovereign authority over the ecosystem in which blockchain-based activities are embedded in circumstances where those activities are aimed at avoiding the reach of national law: in this case, Ripple's allegedly wilful failure to comply with money laundering regulations was regarded by FinCEN as facilitating organised crime, so that failure to act against Ripple might be interpreted as a failure to uphold the rule of law and secure its universal application.

b) A 'cat and mouse' battle for supremacy

Guadamuz & Marsden suggest that that the lack of any significant regulatory push towards outright outlawing of Bitcoin (or other cryptocurrencies) arises because governments do not presently feel threatened enough to ban its use and, more importantly, because action could prove futile given its decentralised nature[43]. Because blockchain is decentralised and distributed in structure, creating an identical ledger shared across a widely dispersed network of nodes located around the globe, many believe that public blockchains are effectively beyond the reach of sovereign state control[44]. But although the absence of a central controller inevitably makes it considerably more difficult to exert practical control over blockchain networks, these networks operate within a wider ecosystem of applications, exchanges and practices in which the network interfaces with the real world[45] and it is these key intermediaries that have been, and are likely to continue to be, the targets of regulatory intervention. Thus, FinCEN's administrative guidance and subsequent enforcement action was targeted at cryptocurrency exchanges, rather than addressed and aimed at miners who run the underlying cryptographic protocols, or at Bitcoin users.[46]

This strategy of targeting intermediaries may be effective in the short-term, although it would not, for example, reach through to blockchain activities that do not involve an exchange of currency via an intermediary, such as the spending of cryptocurrency directly on goods and services. But national legal systems could, if they desired, introduce legally enforceable restrictions on the acceptance cryptocurrencies as a form of payment by suppliers of goods and services. The resulting interaction between the code *of* law and code *as* law can thus be described as 'cat and mouse': as blockchain activities and their ecosystems evolve, conventional legal systems will need to monitor developments, continually reassessing whether additional or alternative strategies to combat blockchain activities

---

42 Financial Crimes and Enforcement Network ('FinCEN') (2015) 'FinCEN Fines Ripple Labs Inc in First Civil Enforcement Action Against a Virtual Currency Exchanger', Press Release issued 5 May, available at https://www.fincen.gov/news/news-releases/fincen-fines-ripple-labs-inc-first-civil-enforcement-action-against-virtual (accessed 29 November 2017).

43 Guadamuz and Marsden, *supra* n 20 at n 134.

44 cf Blackett Review 2016, Chapter 3, *supra* n 6.

45 Golumbia highlights the embeddedness of cryptocurrencies within existing economic and financial systems to argue that the cyber-libertarian visions will not be realized in practice. For him, '…Bitcoin fails to embody any substantial alternative to [our existing financial systems]. The reasons for this have little to do with technology and everything to do with the financial systems in which Bitcoin and all other cryptocurrencies are embedded, systems that instantiate the forms of power that cannot be eliminated through either wishful thinking or technical or even political evasion: the rich and powerful will not become poor and powerless simply because some people decide to operate alternative exchange economies. Lacking a robust account of transforming these systems of power, even without Bitcoin's flaws, a 'perfect' cryptocurrency would exacerbate, rather than address, the existing serious problems with our monetary and financial systems.' Golumbia, David (2015) 'Bitcoin as Politics: Distributed Right-Wing Extremism' In Geert Lovink, Jess van Zyl and Patricia de Vries (eds/) *Moneylab Reader: An Intervention in Digital Economy*, 118-31. Amsterdam: Institute of Network Cultures, 2015, 120.

46 Paech, Philipp (2017) 'The Governance of Blockchain Financial Networks' *Modern Law Review* 80: 1073-110.

aimed at wilfully evading legal and regulatory obligations are needed in order to protect the public interest and safeguard the rule of law.[47] In this respect, the Blackett Review was rather sanguine, stating that '(c)ontrary to public perception, the underlying architecture (of unpermissioned blockchains) makes it relatively easy to track transactions and establish the identity of people who misuse the system. Regulators have learned how to control the 'on-ramps and 'off-ramps' where value flows in and out of the system.'[48]

However, as blockchain is more widely taken up in which, for example, financial assets are moved onto blockchain networks, the role of intermediaries is likely to decrease. If so, then national authorities may need to identify alternative addressees upon whom regulatory obligations can be effectively imposed[49]. But serious doubts arise concerning whether national legal systems will develop practically viable strategies to cracking down on illicit blockchain activities in the absence of intermediaries who can constitute legitimate targets for regulatory intervention.[50] This may, however, not turn out to be a significant problem if, as Paech predicts, in the realm of blockchain financial networks we are very unlikely to see unpermissioned financial blockchain networks rolled out on a mass basis because states will recognise the critical nature of financial systems as essential public infrastructure, and may therefore prohibit regulated financial institutions from dealing with or upon them. Paech argues that blockchain financial networks are much more likely to take the form of permissioned networks, involving clear control nodes which can readily be rendered subservient to national regulatory authority[51]. Although unpermissioned blockchain networks might continue to operate, Paech suggests that states could seek to limit their interaction with the financial system by, for example, making it impossible for these networks to deal with legal tender and continuing to regulate virtual currency exchanges and other interfaces between the network and the real world[52].

In summary, where blockchain networks are used intentionally to evade substantive legal obligations intended to protect individuals and the public interest (by seeking to protect the public from harm or to help finance the operations of the state), national legal systems are unlikely to sit idly by, particularly if these activities are non-trivial in size and scale.[53] We can therefore anticipate an active

[47] See for example recent statements by the US Secretary of the Treasury that his department was scrutinizing illegal uses of Bitcoin and other cryptocurrencies, and that it is important that they are not used for 'illicit' purposes: https://www.coindesk.com/us-treasury-secretary-were-looking-carefully-at-illicit-uses-of-bitcoin/ (accessed 4 December 2017).

[48] The Blackett Review, supra n.6, at 34. See also Wright, Aaron and Primavera De Filippi (2015) 'Decentralised Blockchain Technology and the Rise of Lex Cryptographica' available via SSRN network at www.ssrn.com.

[49] Paech *supra* n.45; Boucher *supra* n.2.

[50] Paech *supra* n.45. although the Blackett review seemed reasonably optimistic about the prospects of governments finding effective ways to regulate blockchain by influencing the technical code that defines their rules: The Blackett Review, supra n 6, at 45.

[51] Paech, *supra* n.45, at 1101-1103.

[52] Peach, *ibid.* This view is supported by the Blackett review, which noted the emerging belief that the technology underpinning Bitcoin could have valuable and benign uses and enable significant future innovation. It took view the view that Bitcoin's censorship resistance is problematic from a law-enforcement and regulation perspective, and it is therefore unlikely that major corporates or banks will engage closely with Bitcoin or related technologies in the short to medium term: The Blackett Review, *supra* n. 6 at 34.

[53] As Blackett observed, in addition to the interests of system stakeholders, there may also be broader interests involved in how a distributed ledger functions. For example, regulators may wish to collect taxes, prosecute crimes and limit the use of a distributed ledger for criminal purposes. If a system is adopted to the extent that it starts to have potential knock-on effects elsewhere in society, regulators may also wish to ensure that the system is resilient against systemic risk and market failure: The Blackett Review, supra n.6 at 44.

'battle for supremacy' in which the code *of* law attempts to exert its sovereign authority over code *as* law to close off opportunities for actors to exploit the anonymised interactions which public blockchains make possible. This battle is, unlikely, however, to take the form of a single, monumental winner-take-all 'fight for survival', but a series of on-going 'cat and mouse' interactions in which national legal authorities seek to close off loop-holes that some blockchain users attempt to exploit to evade the law's substantive demands. In this dynamic interaction, the identity of the 'mice' upon whom national legal authorities set their sights may change over time. Although ideally the state might wish to target the primary culprits, that is, those who actively seek to evade substantive laws by utilising blockchain, the state is likely to find it more effective and convenient to target the intermediaries and other gatekeepers who act as interfaces between blockchain networks and the real-world[54]. But, as the need for intermediaries evaporates as more services and placed on unpermissioned blockchains, national legal systems might seek to target and impose legal responsibilities on code developers and miners directly: although whether they can do successfully in practice will, at least for the time being, remain unanswered.[55]

2.2.2 Efficient alignment

(a) Blockchain to support and enhance the efficient enforcement of conventional law

The relationship between blockchain and conventional legal systems is not necessarily hostile. On the contrary, blockchain systems can be configured to help secure compliance with substantive legal norms. These are referred to in recent policy literature as 'RegTech' (as shorthand for 'Regulatory Technology'). As the UK's Blackett Review observed:

> 'there are also opportunities to take advantage of the potential interactions between legal and technical code. For example, public regulatory influence could be exerted through a combination of legal and technical code, rather than through legal code as at present. In essence, technical code could be used to assure compliance with legal code, and in so doing, reduce the costs of legal compliance. This could provide a 'use case' for the use of technology to enhance regulation, so-called RegTech' (at p 12)[56]

54 Wright and De Filippi, *supra* n 31. Leiser, Mark, and Andrew Murray (2017) 'The Role of Non-State Actors in the Governance of New and Emerging Technologies' In Roger Brownsword, Eloise Scotford and Karen Yeung (eds.) *The Oxford Handbook of Law, Regulation and Technology*, 670-704. Oxford: Oxford University Press.

55 The Blackett review considered the possibility of regulating blockchain via technical code, noting that some technical code (comprising software and protocols) emerge from the public sector, such as TCP/IP and other core internet protocols which, together with other international multi-stakeholder processes, point to the possibility of public involvement and democratic representation in the production of technical code – public regulation of technical code as opposed to legal code. So, applied to distributed ledger systems, this could mean anything from instituting multi-stakeholder processes for maintaining technical code, to developing public standards for the code. If this allowed the governments or the public directly to attain legitimate regulatory goals by influencing the rules built into the computer code, it could lessen the need for a body of new legal code to regulate these systems. See The Blackett Review 2016, *supra* n.6, at 44-45.

56 The UK's Chief Scientific Adviser refers 'RegTech' as encompassing 'any technological innovation that can be applied to or used in regulation, typically to improve efficiency and transparency' Government Office for Science (2015) *Fintech Futures: The UK as a World Leader in Financial Technologies*. London, 47. The Report notes that, within the financial services sector, 'FinTech' (ie 'financial technologies integrate finance and technology in ways that will disrupt traditional financial models and businesses and provide an array of new services and businesses and consumers. The hybridisation of technology with the traditional processes of finance – working capital, supply chain, payments processing, deposit accounts, life assurance and so on – replaces traditional structures and ways of working with new technology-based processes' at 5) can be utilised to create new mechanisms for RegTech - by applying them to regulation and compliance to make financial regulation and reporting more transparent, efficient and effective' and to 'improve the process of regulation' at 12. The report identifies four key groups of technology advancement that it believes will enable the FinTech sector in the near and medium term: (a) machine learning and cognitive computing (b) digital currencies and blockchain (c) big data analytics, optimisation and fusion, and (d) distributed systems, mobile payments and peer

An example of blockchain-based RegTech is R3's Corda project, established by a group of regulated financial institutions (including Barclays, Royal Bank of Scotland, Credit Suisse, JPMorgan, Deutsche Bank, and UBS) which seeks to design, construct and implement a distributed ledger platform to record, manage and synchronise legal agreements between their proper parties. R3s Corda platform[57] is a permissioned system, so only the relevant parties share the transactions, and the other transactions are not known to others or made visible. Although its data structure is not actually a blockchain, and the platform does not use 'proof of work', it is a distributed ledger that operates through basic distributed consensus[58]. Unlike typical cryptocurrrencies, the Corda platform is designed to *supplement* and complement existing legal structures, so that the ledger's operation is intended to give effect to the rights and obligations expressed in legally enforceable contracts expressed in conventional linguistic text (referred to by Corda as 'legal prose'). Accordingly the platform has been designed to allow the legal prose to be attached to the node that is intended to verify and automate the execution of the obligations arising under the legal agreement.[59] In so doing, Corda's developers explicitly recognise that complex contractual disputes can and do arise, so that the legal obligations of the participants of the platform are intended to prevail in the event of a dispute entailing conflict between the legal obligations arising under the agreement and the operations taking place upon the Corda platform. In other words, the Corda platform expressly eschews the assertion that, for the purposes of the platform's operation and governance, 'code is law'.[60]

By explicitly acknowledging that the legal rights and obligations of participants arising under conventional legal contracts ultimately govern the relationship takings place upon the network, this serves Corda's overarching goal, which is 'to define a shared ledger fabric for the financial services use-cases that can be deployed within existing legal frameworks which relies on proven technologies'.[61] But Corda's vision extends beyond merely enhancing the efficiency, effectiveness and timeliness of transactions between private financial institutions, for it also seeks to bolster the efficacy of oversight by financial and other related regulators by providing a technical means through which they can access real time information about transactions taking place between the participants. So, for example, the Corda platform might permit regulators to view transactions upon it to identify any suspicious transactions in terms of fraud, money laundering or other indicators of criminal activity.[62] Corda's proposal thus represents a concrete example of 'RegTech' envisioned in several policy

to peer applications (at 7). Recommendation 10 of the report provides that: 'Regulators should engage the FinTech community in automating regulation and compliance to create a state-of-the-art regulatory reporting and analytics infrastructure, which we have called 'RegTech' (at 12).

[57] Corda version 1.0 was released on 3 October 2017 and is available on an open source basis: https://www.r3.com/blog/2017/10/03/introducing-corda-1-0/.

[58] Distributed ledgers are a type of database that is spread across multiple sites, countries or institutions and is typically public. Records are stored one after the other in a continuous ledger, rather than sorted into blocks, but they can only be added when the participants reach a quorum: see The Blackett Review, 17-18.

[59] See https://docs.corda.net/key-concepts-contracts.html accessed 10 November 2017.

[60] See https://docs.corda.net/key-concepts-contracts.html accessed 10 November 2017.

[61] Brown, Richard Gendal, James Carlyle, Ian Grigg, and Mike Hearn. "Corda: An Introduction." https://docs.corda.net/_static/corda-introductory-whitepaper.pdf. (accessed 29 November 2017)

[62] See https://discourse.corda.net/t/how-does-the-corda-prevent-using-it-for-an-illegal-purposes-e-g-for-money-laundering/1230 (accessed 10 November 2017)

documents, with the state of Illinois becoming the first government regulator to join the R3 consortium.[63]

(b) Mutually supportive interaction between code *of* law and code *as* law

Corda's founders intend that their distributed ledger should operate, in effect, as a servant of conventional law. No formal 'battle for supremacy' between these two regulatory modalities arises because the technical network is intentionally embedded within conventional law, building upon and actively supporting conventional law's authority over network participants' relationships and dealings. Nevertheless, one might anticipate informal tension to arise on occasion, at least in circumstances where either formal legal rights and obligations do not translate readily into the binary language of technical code, or if the interactions between the parties on the network fail accurately to reflect their rights and obligations arising under the legal instruments on which they rest. The resulting dynamic interaction between the two systems might therefore be described as akin to the 'joys of marriage' – within an on-going, dynamic relationship that occasionally entails disagreement and discord but ultimately seeks to provide long term mutual support and collaboration for the benefit of both partners. Because the stability of the relationship is assured by the willingness of one partner to accept and defer to the superior authority of the other, rather than a partnership of equals, the resulting dynamic is perhaps more aptly described as the 'joys of *patriarchal* marriage'. For example, as legal philosophers have long observed, there will always be an inevitable element of ambiguity and uncertainty associated with linguistic texts, including legal prose.

It is also conceivable that the contractual agreement between the parties who have sought to implement their agreement via blockchain-enabled smart contracts may have unintended adverse effects upon third parties.[64] For example, consider a master contract between two major financial institutions concerning the terms that are intended to apply to their dealings, including the terms and conditions that they propose to apply to their respective customers at the retail level. These parties may then wish to implement their legal arrangements via 'smart contracts' that can be built on top of a distributed ledger. As Finck explains, a smart contract is not in fact a legal contract, and nor are they 'smart' in that they need outside input to determine real world events. Instead, a smart contract is a computer programme code that automates the verification, execution and enforcement of certain terms and conditions of an arrangement.[65] It is conceivable that, for example, smart contracts used to execute the parties' agreement unintentionally cause harm or produce other adverse third party effects.[66] A question then arises concerning how those third parties might seek redress: if the

---

63 Rutland, Emily (2017) 'Illinois becomes first state level regulator to join R3 distributed ledger group' at http://www.r3cev.com/press/2017/3/21/illinois-becomes-first-state-level-regulator-to-join-r3-distributed-ledger-group (accessed 29 November 2017).

64 In English contract law, even if third parties are explicitly intended to benefit from a contract between two contracting parties, if they are not themselves party to the contract then there is no 'privity of contract' with the result that those third parties do not have any rights under the English common law to enforce the terms of the contract against the contracting parties.

65 M Finck, *supra* n.23, 6. Werbach describes smart contracts as, in essence, autonomous software agents, enabling a distributed ledger to function as a distributed computer, so that the same consensus algorithms that allow each node to have an identical copy of the ledger allow it to perform identical computations: Werbach, K. (2016). 'Trustless Trust.' *SSRN network*, 31. The term 'smart contract' was originally conceived by Nick Szabo, who defined a smart contract as 'a computerised transaction protocol that executes the terms of a contract'. The general objectives of smart contract design are to satisfy common contractual conditions (such as payment terms, liens, confidentiality and even enforcement), minimise exceptions both malicious and accidental, and minimize the need for trusted intermediaries. Related economic goals include lowering fraud, loss, arbitration and enforcement costs, and other transaction costs: see http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html (accessed 4 June 2018)

66 See discussion at section 3.2 below.

contracting parties are committed to fully reflecting the rights and obligations arising under conventional law in their dealings both on and off the blockchain, then one would expect them to be sympathetic to third party concerns and to seek to devise arrangements that would reflect the allocation of rights and duties that would be enforceable under conventional law. If, however, affected third parties are unable successfully to enlist the support of the blockchain community to implement an appropriate solution[67], they might look to the conventional law for assistance. If so, then such blockchain applications would no longer be appropriately classed as 'mutually aligned' with conventional law, resembling the class of case that are motivated by a desire to 'alleviate transactional friction', discussed more fully in the following subsection.

Just as some blockchain developers, such Corda's founders, have openly embraced conventional law and invited interactions between them, so also have national law makers taken active steps to welcome, and provide legal recognition of, blockchain forms of interaction, albeit also on the understanding that the code of law prevails over code *as* law. Various legislative reforms have been proposed or adopted in several jurisdictions, in which national legal regimes have sought to provide legal recognition of the validity of transactions undertaken on blockchain systems, thereby reducing legal uncertainty and bolstering their attractiveness to potential users. For example, in March 2017 Arizona passed legislation which clarifies enforceability issues associated with the use of blockchain and smart contracts under Arizona law[68], while in the Isle of Man, policy makers are proposing to amend its Proceeds of Crime Act 2008 to embrace cryptocurrencies, thus providing a safe haven for digital currency projects, with the aim of attracting blockchain start-ups in the hope that these will fuel the kind of economic boom it saw arise from its early embrace of online gambling and electronic gaming.[69] In a different but related vein, Australia's federal Parliament has passed legislation so that Australians will no longer be required to pay taxation on cryptocurrency purchases, thus bringing them into line with the tax treatment of other foreign currencies.[70] Although the motivations of law-makers underpinning these legislative measures varies in the extent to which particular jurisdictions are willing to welcome blockchain systems, from grudging acceptance through to actively seeking to attract their development, they collectively reveal an attitude of acceptance.

In summary, where blockchain systems are developed for the explicit purpose of supporting and partnering with conventional legal systems by providing mechanisms through which legally enforceable rights and obligations can be executed and implemented with considerably greater speed, efficiency, security and reliability that is currently possible via conventional legal enforcement mechanisms, the resulting dynamic interaction between the systems can be described in terms of the 'joys of (patriachial) marriage'. At the same time, at least within liberal legal regimes in which 'anything not prohibited is permitted', some conventional law-making bodies have enacted legislation to recognise the validity of transactions taking place upon blockchain systems, reflecting an attitude ranging from tolerance to encouragement. Although these measures are intended to avoid any overt 'battle for supremacy' between the code of law and code as law, implicit in this approach is an assumption that ultimately, the sovereign authority of conventional law prevails. Whether or not this position is sustainable in practice is a question which is addressed in the next section.

---

67 See discussion at section 3.2 concerning The DAO Hack, particularly the willingness of the majority of nodes to implement the 'hard fork' solution recommended by Ethereum's lead developers.

68 See https://www.coindesk.com/arizona-smart-contract-clarity-winning-startups/

69 See https://www.coindesk.com/isle-of-man-bitcoin-regulation-2015/

70 See http://www.theaustralian.com.au/news/latest-news/new-laws-stop-double-taxation-on-bitcoin/news-story/80bd73cff2abe4a86552a04e0d8240d7 accessed on 10 November 2017. Australian Tax Office (2014) Tax Determination, TD 2014/25, 'Is bitcoin a 'foreign currency' the purposes of Division 775 of the Income Tax Assessment Act 1997, available at http://law.ato.gov.au/atolaw/view.htm?DocID=TXD/TD201425/NAT/ATO/00001 (accessed 4 December 2017).

2.2.3 Alleviating transactional friction

Thus far I have identified two opposing attitudes towards conventional law that might be evinced by some blockchain participants: one concerned to *avoid* the substantive obligations imposed by conventional law, while the other seeks to *support and giving effect to* the substantive obligations imposed by conventional law. But a third set of attitudes and motivations can be identified, lying between these two poles: those motivated to use blockchain primarily to undertake novel forms of cooperation without the procedural burdens, costs and formalities of conventional forms of legal coordination. In this section, I argue that conventional legal systems will be hesitant and cautious in responding to these blockchain systems, producing a relationship dynamic of 'uneasy co-existence' characterised by an attitude of 'mutual suspicion'.

(a) Using blockchain to support novel forms of social coordination

Much of the enthusiasm for blockchain arises from its potential to enable novel forms of effective and trustworthy social cooperation between strangers without the procedural burdens and costs of conventional law. Because Bitcoin has been used by cybercriminals to extort payment from victims of ransomware attacks[71] and to pay for contraband via the darknet, it is often associated with criminal activity. But the origins of Bitcoin were rooted in a loss of faith in the convention global financial system following the 2008 Global Financial Crisis. This provoked a discussion within the crypto community about whether a currency exchange system could be developed which avoided the conventional financial system (and thus its reliance on major financial institutions and conventional legal institutions to guarantee the security of transactions). In other words, one significant advantage of blockchain to effect social coordination between strangers (including but not limited to cryptocurrency applications) is its capacity to avoid many of the weaknesses associated with conventional law to guarantee the security of transactions, particularly given that invoking the formal legal processes to enforcing legal rights and obligations is typically slow, time-consuming, labour intensive, uncertain and costly[72]. Even in highly developed, stable economic systems with well-established legal systems, the delay and expense associated with formal legal proceedings means that it is rarely invoked, regarded in practice as available only to the rich and powerful.[73]

Accordingly, one important driver of innovation in blockchain applications is a desire to avoid the procedural, economic and temporal shortcomings of conventional law, and which might, all other things being equal, plausibly be regarded as a legitimate objective. The response of conventional law to these applications is contingent on identifying whether, and in what ways, legal intervention into blockchain systems is considered necessary or desirable and practically feasible. Two recent and emerging applications illustrate the challenges faced by conventional legal systems in making this evaluation: first, crowdfunding for start-up ventures via 'initial coin offerings' and secondly, peer-to-peer energy exchange platforms. In both cases, blockchain is being utilised and imagined as a vehicle for establishing and maintaining community-based cooperation between network participants in which the *procedural* inefficiency, friction and costs associated with the conventional legal processes can be avoided, rather than (arguably) motivated predominantly by a desire to evade *substantive* legal obligations. Conventional legal systems have responded to applications of the first kind in a tentative and piecemeal fashion, resulting in ICOs occupying a 'regulatory greyzone'. The resulting interaction between the code *of* law and code *as* law can therefore be described as one of *uneasy coexistence*, outlined in the following discussion.

---

[71] Gibbs, Samuel (2017) 'Wannacry: Hackers Withdraw £108,000 of Bitcoin Ransom' *The Guardian*, 3 August at https://www.theguardian.com/technology/2017/aug/03/wannacry-hackers-withdraw-108000-pounds-bitcoin-ransom.

[72] Yeung, Karen (2017) 'Blockchain, Transactional Security and the Promise of Automated Law Enforcement: The Withering of Freedom under Law?' In Philipp Otto and Eike Graf (eds.) *3ETH1CS - the Reinvention of Ethics in a Digital Age*, 132-46. Berlin: iRights.Media.

[73] Bach, Lord Willy (2016) *The Crisis in the Justice System in England and Wales*, Interim Report." The Fabian Society, London.

(b) Initial coin offerings: a blockchain-based approach to crowdfunding

The recent proliferation of so-called 'initial coin offerings' (ICOs) vividly illustrates how blockchain is being utilised to enable novel forms of social and economic co-ordination. ICOs have, to date, been both enormously popular and highly controversial, with the New York Times reporting in July 2017 that $US 1 billion has been raised through ICOs since the beginning of that year.[74] The current crop of ICOs take one of two forms. Some are 'token sales', in which those who purchase tokens (or 'appcoins') are intended to acquire a right to participate in the activities of the token issuer, for instance, to purchase its products and services on a preferential basis once they are available. For example, a token might enable the holder to buy data storage or cybersecurity services from a new start-up that has yet to launch[75]. Other ICOs, known as 'coin offerings', are intended to confer upon those acquiring coins a form of property, sometimes in the form of fractional ownership in the underlying enterprise, or its future profits, so that coins are analogous to digital stock certificates. Trade in tokens is recorded using blockchain and investors can typically trade their tokens on secondary peer-to-peer exchanges, as investors speculate on their value.

Considerable controversy has arisen concerning the appropriate legal and regulatory response to ICOs, owing to uncertainty concerning whether they should be regarded as akin to public offerings of securities (IPOs) and thus subject to the same regulatory requirements to ensure investor protection. ICOs are financing vehicles developed to fund venture-style investments, purporting to give ordinary investors opportunities to invest in exciting start-up projects that would typically only be available to private equity investors. They have therefore been described as a 'cross between crowdfunding and a conventional equity IPO'[76] making it possible for anyone to buy 'coins' in a venture fund that is typically claimed to be fully transparent and, in many cases, purportedly under complete shareholder control, by giving coin-holders a voice in the form of voting rights concerning which products and projects to fund while receiving an equity stake in the startup's outcome. Because expected returns are directly linked both to the pooled funds of the ICO and the issuer's efforts to employ those funds to execute its proposed plans to generate returns, participants are effectively investing in the on-going commercial proposition: if the value of their appcoin holdings increases, they either earn a greater financial return by selling the tokens (capital gains) or gain more credit to access the underlying product or services. Accordingly, the rights attached to these coins can be understood as directly analogous to ordinary securities to which attendant voting rights, rights to benefits and potential involvement in management decisions attach and, owing to the risks to investors of harm and exploitation by the securities issuer, are subject to stringent legal regulation.[77] In part, controversy surrounding ICOs is rooted in recognition that the procedural burdens of securities legislation are ultimately intended to provide substantive protection to the investing public and should not be readily side-stepped by entrepreneurs using blockchain to fund their risky ventures.

---

[74] N Popper 'SEC Issues Warning on Initial Coin Offerings', *The New York Times*, 25 July 2017 at https://www.nytimes.com/2017/07/25/business/sec-issues-warning-on-initial-coin-offerings.html. (accessed 29 November 2017).

[75] N Popper 'Easiest Path to Riches on the Web? An Initial Coin Offering', *The New York* Times, 23 June 2017 at https://www.nytimes.com/2017/06/23/business/dealbook/coin-digital-currency.html?action=click&contentCollection=DealBook&module=RelatedCoverage&region=Marginalia&pgtype=article (accessed 29 November 2017).

[76] Schiller, Ben (2017) 'Can Initial Coin Offerings Give New Life to Social Good Companies?' *Fast Company*, 15 September at https://www.fastcompany.com/40456378/can-initial-coin-offerings-give-new-life-to-social-good-companies (accessed 29 November 2017).

[77] Sehra, Avtar, Philip Smith, and Philip Gomes (2017) 'Economics of Initial Coin Offerings', Allen & Overy, available at http://www.allenovery.com/publications/en-gb/Pages/Economics-of-Initial-Coin-Offerings.aspx (accessed 29 November 2017).

Regulators in major financial markets have all responded to ICOs[78], adopting a largely cautious, 'wait and see' approach to ICOs rather than treating them as all subject to, or free from, regulation as ordinary equity securities.[79] Thus both the USA's Securities and Exchange Commission (the SEC)[80] and the UK's Financial Conduct Authority (FCA) have issued warnings, essentially stating that the offer and sale of digital tokens may be regulated as securities but will be assessed on a case-by-case basis[81]. The resulting uncertainty leaves fundraisers and investors facing different rules and expectations over how ICOs will be treated in different parts of the world, prompting critics to characterise ICOs as a 'Wild West' of financial services in which ICOs constitute a form of 'workarounds' that seek to 'leverage regulatory arbitrage opportunities to execute undercover securities issuances', potentially limiting the vision and creativity required to see the true scale of what ICOs and digital tokens could represent, while blinding the industry to possible risk.[82]

---

78 Scanlon, Luke (2017) 'Regulators Playing Catch-up on Initial Coin Offerings,' *Outlaw.com*, 8 September available at https://www.out-law.com/en/articles/2017/september/regulators-playing-catch-up-on-initial-coin-offerings/ (accessed 29 November 2017).

79 See response of SEC (USA) and FCA (UK) referred to below at n.60 and n.61. See also Monetary Authority of Singapore (2017) 'MAS clarifies regulatory position on the offer of digital tokens in Singapore', 1 August, available at http://www.mas.gov.sg/News-and-Publications/Media-Releases/2017/MAS-clarifies-regulatory-position-on-the-offer-of-digital-tokens-in-Singapore.aspx (accessed 4 December 2017); Canadian Securities Administration (2017) 'Cryptocurrency Offerings', CSA Staff Notice 46-307, 24 August, available at http://www.osc.gov.on.ca/en/SecuritiesLaw_csa_20170824_cryptocurrency-offerings.htm#N_1_1_1_1 (accessed 4 November 2017); and Hong Kong Securities and Futures Commission (2017) 'Statement on initial coin offerings', 5 September, available at http://www.sfc.hk/web/EN/news-and-announcements/policy-statements-and-announcements/statement-on-initial-coin-offerings.html (accessed 4 December 2017).

80 Securities and Exchange Commission (2017) Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO, 25 July.

81 The Financial Conduct Authority (FCA) issued a consumer warning on identifying various risks, but did not offer a definitive view on how existing regulations apply to them, merely stating that 'Whether an ICO falls within the FCA's regulatory boundaries or not can only be decided case by case. Many ICOs will fall outside the regulated space. However, depending on how they are structured, some ICOs may involve regulated investments and firms involved in an ICO may be conducting regulated activities. Some ICOs feature parallels with Initial Public Offerings (IPOs), private placement of securities, crowdfunding or even collective investment schemes. Some tokens may also constitute transferable securities and therefore may fall within the prospectus regime. Businesses involved in an ICO should carefully consider if their activities could mean they are arranging, dealing or advising on regulated financial investments. Each promoter needs to consider whether their activities amount to regulated activities under the relevant law. In addition, digital currency exchanges that facilitate the exchange of certain tokens should consider if they need to be authorised by the FCA to be able to deliver their services.' Per Financial Conduct Authority (2017) *Consumer warning about the risks of Initial Coin Offerings* ('ICOs'), 12 September, available at https://www.fca.org.uk/news/statements/initial-coin-offerings (accessed 29 November 2017). In its consumer warning, the FCA said that whether an ICO would be regulated must be considered on a case-by-case basis. Although ICO issuers will be keen to avoid falling within the scope of UK regulation, given that applications for authorisation to carry on a "regulated activity" under the Financial Services and Markets Act 2000 (FSMA) are costly and time-consuming, and ongoing compliance even more so. But carrying on "regulated activities" without authorization is a criminal offence: no firm may carry on a regulated activity in the UK unless it is authorised to do so or exempted from the need for authorisation. To carry on regulated activities, the firm must be performing "specified activities" relating to "specified investments," as defined in the FSMA (Regulated Activities) Order 2001 (RAO), enacted pursuant to FSMA. For an opinion on whether ICOs are "specified activities" for this purpose, see Barber, A. (2018) 'UK regulators recognise cryptocurrency and ICO risks' available at https://www.womblebonddickinson.com/uk/insights/articles-and-briefings/uk-regulators-recognise-cryptocurrency-and-ico-risks (accessed 4 June 2018).

82 Sehra, Smith, and Gomes *supra* n.77.

2.3.3 Blockchain for cooperative energy generation, sharing and distribution

In many ways, ICOs resemble well-established public fund-raising strategies and thus neither radical nor revolutionary, at least in substance rather than form. Other emerging blockchain applications, however, better reflect the revolutionary vision that blockchain advocates seek to champion, including those aimed at enabling peer-to-peer energy generation and distribution. Various energy projects around the world[83] are currently being developed using blockchain platforms to enable people to generate, sell and buy energy directly to and from each other. For example, the 'Brooklyn Microgrid' project by TransactiveGrid[84] aims to test how blockchain technology can enable direct neighbour-to-neighbour sale of solar energy, building on the Ethereum blockchain. Since April 2016, it has been running a pilot project that seeks to integrate buildings, each with rooftop photovoltaics systems, in a decentralised peer-to-peer power grid. All energy not used by the buildings themselves is sold to five neighbouring buildings, all of which are also interconnected through the conventional power grid, with transactions managed and stored using a central blockchain.[85] The same underlying logic is evident in the ambitions of WePower, a blockchain energy start-up which, although yet to launch at the time of writing, is currently gathering together producers of renewable energy including solar, wind and hydro plants while seeking investors who pay upfront for the right to consume electricity generated by those plants by purchasing its own cryptocurrency, a token called WPR, which represents one 1kw hour of power produced and which are themselves tradeable on the platform. By tokenising renewable energy and putting it onto a blockchain, WePower seeks to make that power tradeable and accessible to anyone. In effect, people taking contracts on WePower become their own energy traders, substituting for the role utilities play in buying and selling power on our behalf. Hence, rather than showing the price of energy set by a utility company, their bills will show the price they have negotiated on the blockchain platform, although households will still have to pay the cost of grid transmission and distribution.[86]

Critical to the operation of these platforms is the fully automated smart contract.[87] In theory, smart contracts could be used to signal when to initiate a transaction based on predefined rules aimed at ensuring that all energy and storage flows are controlled automatically to balance supply and demand. For example, whenever energy production exceeds demand, smart contracts could ensure that surplus energy is automatically delivered into storage and deployed whenever demand exceeds supply. Smart

---

83 These projects include those undertaken by Power Ledger, which has several blockchain pilot projects in Australia; Drift has launched a blockchain based utility in New York; Vattenfall has launched a start-up company 'powerpeers' in the Netherlands; Various firms are involved with the Energy Web Foundation, a non-profit group founded by the Rocky Mountain Institute and Grid Singularity; and an Austrian blockchain developer focused on energy applications: see PriceWaterhouse Coopers (2016) *Blockchain - an Opportunity for Energy Producers and Consumers?* Available at www.pwc.utilities/ (accessed 29 November 2017); Schiller, Ben (2017) 'Can Initial Coin Offerings Give New Life to Social Good Companies?' *Fast Company*, 15 September at https://www.fastcompany.com/40456378/can-initial-coin-offerings-give-new-life-to-social-good-companies (accessed 29 November 2017).

84 TransactivGrid is a joint venture between L03 Energy and ConsensSys see https://lo3energy.com/ (accessed 29 November 2017).

85 Cardwell, Diane. "Solar Experiment Lets Neighbors Trade Energy among Themselves." *The New York Times*, 13 March 2017. https://www.nytimes.com/2017/03/13/business/energy-environment/brooklyn-solar-grid-energy-trading.html.

86 Schiller, Ben (2017) 'Can Initial Coin Offerings Give New Life to Social Good Companies?' *Fast Company*, 15 September at https://www.fastcompany.com/40456378/can-initial-coin-offerings-give-new-life-to-social-good-companies (accessed 29 November 2017).

87 See above at n 65 above and associated text. See also Raskin, Max (2017) 'The Law and Legality of Smart Contracts' *Georgetown Law Technology Review* 1: 305.

contracts between the energy producer and consumer could also autonomously and securely regulate both supply and payment so that if a customer fails to make a payment, the smart contract would automatically arrange for the power supply to be suspended until payment is received (provided the parties had previously agreed to include such a mechanism in their contract).[88]

These blockchain energy projects have yet to move beyond the concept or pilot stage, so that conventional law-makers and energy regulators have not needed to take a formal position on the extent to which they are subject to national law. Given that there are well-established energy laws and regulatory requirements concerned with ensuring safety and security of supply and quality, protecting vulnerable consumers, and regulating disputes between suppliers and providers, it seems highly unlikely that conventional law-makers, regulators and enforcement officials would regard these systems as beyond the reach of national law, at least if successfully scaled up to enable mass energy distribution and consumption via blockchain networks[89]. It is worth noting, however, that the technical and governance challenges associated with implementing these systems at scale are very significant.[90]

The energy sector differs critically from the financial services sector, however, in that the physical product itself (ie the electricity) must be taken into account. Transactions on blockchain energy networks involve not only values and information but also the trading of energy delivered via network infrastructure. If blockchain-based distributed energy generation and distribution systems remain at the small scale, neighbourhood level, national legal systems might be reluctant to intervene except when called upon to do so by network participants seeking the legal system's assistance to resolve a particular dispute, particularly if these systems are expressly and clearly stated to be governed exclusively by the internal rules and technical architecture of the system (which might include internal dispute resolution mechanisms). But even in the case of small-scale blockchain networks, it is highly unlikely that national legal systems would refrain from insisting that core legal obligations aimed at ensuring basic requirements to safeguard health, safety and security are complied with.

(d) A relationship of uneasy coexistence and mutual suspicion?

Initial coin offerings (ICOs) and peer-to-peer energy generation systems illustrate both the potential of blockchain to enable novel forms of peer-to-peer social and economic co-operation and the dilemma faced by conventional law-makers in responding to them. While these applications are in their infancy and their future trajectory and take-up remains unknown, conventional law-makers are keeping their powder largely dry. For the time being, they have avoided systematically attempting to exert their sovereign authority, resulting in a relationship of 'uneasy co-existence' between these two regulatory modalities. At the same time, those seeking to build novel blockchain applications are equally likely to be suspicious of conventional law, given their desire to foster and enable novel forms of social co-operation without the procedural burdens, delays and costs typically associated with conventional legal mechanisms, resulting in an attitude of 'mutual suspicion' between the two systems.

---

88 PriceWaterhouse Coopers, *supra*, n.83.

89 In the UK, following the privatization of major utilities, statutory regulation was introduced, primarily due to fears of abuse of monopoly power, but also to ensure universal service obligations are met to ensure that the poor and vulnerable members of society are not left without basic utility provision. Yet regulation did not wither away after competition in utilities market was introduced, and the utilities sector continues to be subject to regulatory oversight to ensure quality of service, disconnection, fair pricing, ensure community service obligations and the meeting of environmental targets: see Graham, Cosmo (1998) 'Is There a Crisis in Regulatory Accountability?' In Robert Baldwin, Colin Scott and Christopher Hood (eds), *A Reader on Regulation*, 482. Oxford: Oxford University Press.

90 PriceWaterhouse Coopers*, supra* n.83.

3. Normative tensions and shifting public-private boundaries: should the code *of* law win the battle for supremacy over code *as* law?

The preceding analysis has identified three different kinds of interaction between blockchain systems and conventional legal orders, determined primarily by the motives of network participants in utilising blockchain systems with respect to conventional law, represented in Table 1 (below).

Table 1

Motives of blockchain participants vis-à-vis conventional law	Dynamic interaction (battle for supremacy?)
Hostile evasion	Cat and mouse
Supportive Alignment	The joys of (patriarchal) marriage
Alleviating Transactional Friction	Mutual suspicion and uneasy co-existence

In the cases of *hostile evasion* and *supportive alignment*, the assertion of the supremacy of national law over blockchain interactions can be readily understood. In the former case, national legal systems are justified in taking coercive action against those within their jurisdiction who seek to evade substantive laws intended to protect individuals and the community from harm and exploitation. In latter case, the supremacy of conventional law over blockchain code is both intended by its developers and normatively desirable, not only to support the legitimate intention of developers, but also in strengthening the practical application and effect of legal rights and duties arising under national law. However, blockchain applications motivated by a desire to establish novel forms of cooperation via blockchain technologies that avoid the procedural and associated burdens of conventional law are more difficult to evaluate in normative terms.

3.1 How will national legal authorities balance competing claims for and against intervention?

The political claims associated with the third class of blockchain applications display similarities with those made by advocates of the 'sharing economy' that has emerged as digital aggregation platforms have proliferated. Supporters celebrate the 'freedom' these platforms provide by enabling individuals to connect with each other, untethering them from established institutions, often accompanied by triumphant claims of transition, disruption or even revolution.[91] This family of blockchain applications take this logic further, enabling direct peer-to-peer interaction by dispensing with a central intermediary altogether and replacing it with the underlying distributed computer network. Leaving aside this ideological rhetoric, they present conventional legal systems with a conundrum. On the one hand, liberal democratic constitutional systems rest on a political commitment to respect individual freedom and autonomy, but, they are also firmly committed to the rule of law and its generality, equality and the universality of its protection on the other. It is therefore not surprising that blockchain applications of this kind are jurisprudentially contestable and normatively ambiguous. The sovereignty of law in contemporary democratic orders can be understood as rooted in the idea of the social contract pursuant to which citizens willingly forgo some of their liberty in return for the state's guarantee of security[92]. This social contract is grounded in an understanding that the proper role of the state is to protect its citizens against harm caused by others to which they have not consented, in return for which citizens voluntarily cede some of their freedom. It follows that, if individuals are fully informed of the risks associated with a particular set of activities, and clearly indicate their willingness to engage in them, it is arguably *not* the role of the state to override their arrangements for this would exceed the terms of the implied social contract. Yet there are limits on the extent to which even liberal states permit individuals to voluntarily assume certain risks.[93] But

---

91 Boucher *supra* n.2.

92 Galligan, D. (2006). *Law in Modern Society*. Oxford, Clarendon Press.

93 Even John Stuart Mill conceded that the state will not countenance, for example, an individual willingly selling him or herself into slavery: Mill, J.S. (1859) *On Liberty*. 2nd ed. London: John W Parker & Son.

identifying how much liberty citizens of liberal democratic states can appropriately forgo is often a matter of intense disagreement.[94]

This uncertainty in finding the appropriate balance between respect for individual freedom, on the one hand, and the need to protect individuals from harm on the other, is arguably reflected in the cautious, tentative approach taken by national regulators in response to ICOs referred to above. One strategy that some national regulators have adopted, which helps resolve this uncertainty and allay industry and consumer suspicion, is by seeking to cultivate a cooperative relationship with blockchain developers through the use of 'regulatory sandboxes'. Pioneered by the UK's Financial Conduct Authority in June 2016 as recommended by the UK's Chief Scientific Officer[95], a regulatory sandbox is an 'experimental' approach in which the regulator provides selected firms wishing to bring innovative services that rely on new technological applications to market with an opportunity to trial their services with real customers and market participants within a designated domain for a specified period, subject to monitoring and oversight by the regulator to safeguard against undue risks and harms to the public[96]. In its recent report on lessons learned from the regulatory sandbox's first year of operation, the FCA observed that distributed ledger technologies were the most popular innovation that applicant firms sought to develop, concluding that initial evidence suggests that the sandbox had been very successful.[97]

This experimental regulatory approach has been rapidly emulated by other financial regulators, including those in Hong Kong, Malaysia, Singapore, Montreal, the Isle of Man, Australia, Bahrain, Thailand and Russia, all seeking to foster innovation in Fintech and encourage start-ups to operate within the regulatory fold.[98] National regulators hope that regulatory sandboxes, at least in the financial services sector, will enable the development of blockchain and other emerging technologies by fintech entrepreneurs that will generate social benefits, whilst addressing any associated harms and risks effects swiftly and in a cooperative fashion. In other words, by enabling the supervised testing of innovative blockchain applications, regulators might help to prevent simmering suspicion between the code *of* law and code *as* law from erupting into hostility, thereby discouraging blockchain entrepreneurs from replicating Silicon Valley's attitude towards conventional law, best epitomised in Facebook's motto, 'move fast and break things' by rolling out technological innovations into the public domain as rapidly as possible without first seeking the advice or authority of conventional legal officials, hoping that rapid mass market take- up will render it politically and practically difficult (if not impossible) for regulators to intervene to prohibit or regulate their use.[99]

---

94 See for example Feinberg, J (1989). *The Moral Limits of the Criminal Law Volume 3: Harm to Self*. Oxford University Press: Oxford.

95 Government Office for Science (2015) *Fintech Futures: The UK as a World Leader in Financial Technologies*, Go-Science, London.

96 See https://www.fca.org.uk/firms/regulatory-sandbox. The FCA opened a regulatory sandbox to applicants in June 2016, receiving 146 applications in its first year of application from which it ultimately selected 50.

97 Financial Conduct Authority. "Regulatory Sandbox Lessons Learned Report." 2017 available at https://www.fca.org.uk/publications/research/regulatory-sandbox-lessons-learned-report (accessed 29 November 2017) acknowledging that it is too early to draw robust conclusions from the experience.

98 See Cummings, Dan (2017) "Regulatory Sandboxes: A Practice for Innovation That Is Trending Worldwide." *ETHNews*, 1 March available at https://www.ethnews.com/regulatory-sandboxes-a-practice-for-innovation-that-is-trending-worldwide (accessed 4 December 2017).

99 Vaidhyanathan, S. (2011) *The Googlization of Everything: (and Why We Should Worry)*. University of California Press, San Francisco.

3.2 The rhetoric and reality of regulation by blockchain: The DAO Hack

Given continuing uncertainty concerning the application of conventional law to blockchain interactions (including the 'regulatory greyzone' that ICOs currently occupy) there are real risks that the current legal and technical regime may fail to provide effective protection and accountability guarantees to network participants.[100] These risks were vividly illuminated by the hacking incident occurring in one of the earliest attempts to crowdsource funds from the public by The DAO (shorthand for 'Distributed Autonomous Organisation') on the Ethereum Blockchain by Slock.It, its German co-founder and blockchain start-up. The resulting 'DAO Hack' drew attention to overblown claims about the so-called 'immutability' of blockchain systems, while demonstrating that the technical nature of blockchain systems does not eliminate matters of subjectivity and political judgement in their development and operation. The founders' of the DAO intended to create a for-profit entity that would establish a fund of assets through the sale of 'DAO Tokens' to investors, which would then be used to finance individual 'projects'[101] while DAO Token-holders could monetise their tokens by re-selling them on various web-based platforms that supported secondary trading in DAO Tokens. The DAO sold approximately 1.15 billion DAO Tokens during the offer period in exchange for a total of approximately 12 million Ether ('ETH'), the virtual currency used on the Ethereum Blockchain, which was then worth approximately US$150 mil. But before The DAO commenced financing individual projects, an attacker used a flaw in The DAO's computer code to divert approximately one third ($US 50 million) of The DAO's assets from The DAO's Ethereum Blockchain address to an Ethereum Blockchain address controlled by the attacker. During the 27 days following the attack (during which The DAO code prevented the movement of ETH out of the attacker's account), a lively online debate ensued within the Ethereum community concerning how to respond to the attack. Three solutions were considered and debated (1) do nothing, (2) a soft fork, which would have added a patch to the Ethereum code to freeze the diverted Ether so that it could not be used, or (3) a hard fork, which would roll back the transactions in the blockchain and effectively reverse the attack. In the event, Ethereum community members voted for the hard fork solution, which was undertaken in July 2016.

While a detailed discussion of the attack and the hard fork solution are beyond the scope of this paper, for present purposes it is worth noting how the incident provoked a number of questions concerning blockchain governance, calling into question the relationship between blockchain code and conventional law. In particular, the promotional material disseminated by The DAO's co-founders sought explicitly to oust the jurisdiction of conventional law altogether, claiming that all The DAO activities were governed solely and exclusively by the software code upon which it was to operate, emphasising that investing in The DAO was especially risky, and issuing extensive disclaimers associated with the creation of DAO Tokens[102]. Accordingly, some argued that because 'code is law' on The DAO, the attacker's success in exploiting a flaw in the code constituted a legitimate action so that the attacker was entitled to the fruit of his or her efforts, despite the fact that, from the standpoint of an ordinary investor, it constituted a naked form of theft. Because a hard fork was subsequently adopted, investors avoided significant losses and did not need to enlist the assistance of the conventional legal system to seek redress. Although the US Securities & Enforcement Commission (SEC) declined to pursue criminal enforcement action against The DAO or Slock.It[103], its investigation and report concluded that DAO Tokens satisfied the definition of 'securities' under federal legislation so that The DAO Token issue violated US securities law.

---

100 Boucher, *supra* n.2.

101 For factual background, see SEC Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO, Release No 81207, 25 July 2017.

102 Hinkes, Drew. "A Legal Analysis of the DAO Exploit and Possible Investor Rights." *Bitcoin Magazine*, Jun 21, 2016.

103 The SEC stated that 'In light of the facts and circumstances' it declined to take enforcement action seeking instead to 'caution the industry and market participants' who seek to use blockchain technologies to evade securities legislation.: https://www.sec.gov/news/press-release/2017-131

Had the Ethereum community taken no action in response to The DAO attack, whether conventional national regulators or other legal authorities would have been willing and able to reach into network to correct the effects of the attack is unknown.[104] Nevertheless, the emerging regulatory response decisively rejects the claim of hard-line crypto anarchists who advocate a rugged 'law of the jungle' approach in which the blockchain code and protocols govern the network on a sole and exclusive basis. National legal officials recognise that blockchain networks might harm participants if the network code and internal rules provide inadequate protection. Moreover, even if one accepts that investors in The DAO had voluntarily assumed the risk of flaws in the technical code being exploited (given the warnings and disclaimers of liability issued by The DAO's developers), third parties providing services to, and interacting with, The DAO could not plausibly be regarded as having consented to the disapplication of ordinary law to their dealings. As Paech has persuasively argued in the context of blockchain financial networks, because these networks pose risks to third parties and to the stability of the market, the rights of participants cannot be left entirely to the software.[105] He imagines hypothetical cases in which blockchain financial assets are held within the estate of an insolvent: if insolvency triggers the operation of smart contracts to automatically divest those assets, this may violate the pari passu principle that is foundational to conventional insolvency law, at the expense of insolvent's general creditors who should, by law, rank equally in the recovery of claims against the insolvent. In other words, although blockchain networks may purport to operate as hermetically sealed, closed systems, they invariably interface with the wider world, and thus affect the broader community who have legitimate rights, interests and expectations and which the nation state is normatively justified in protecting, if necessary through the exertion of sovereign power over the 'private' arrangements of network participants.

In many ways, the novel forms of social and economic interaction and organisation which blockchain technologies make possible exemplify how networked digital technologies are challenging existing social, political and cultural understandings and expectations of the public-private divide. By enabling new forms of allegedly trustworthy peer-to-peer interaction made possible by cryptographic algorithms run across a distributed, geographically dispersed network of computers, this threatens and destabilises established forms of organisation and existing patterns in the distribution of power that it sustains. In responding to the kinds of interaction which these new technological capacities make possible, conventional legal systems will need to do at least two things. First, they must evaluate whether activities taking place on blockchain networks should be regarded as matters that fall within the domain of the private. This will invariably require them to identify whether, and to what extent, such activities may harm both network participants and the broader public, and to exercise political judgement concerning the kinds of activities and interaction which should properly be regarded as beyond the reach of the state[106]. Secondly, if state intervention is deemed necessary and justified owing to the risk of harm associated with these networks, conventional legal systems must also find creative and practically effective ways for exerting their authority over activities upon and associated with blockchain networks.

4. Conclusion

The origins of Bitcoin, which established proof of the blockchain concept began an ideological project in the early 1990s by a group known as Cypherpunks. Their political vision was, in essence, an anarchic one: they advocated an extreme form of libertarianism in which all forms of commerce

---

104 Further unauthorised hacks have occurred in relation to other ICOs since The DAO exploit including the Coindash hack in July 2017(see https://www.coindesk.com/coindash-ico-hacker-nets-additional-ether-theft-tops-10-million/).

105 Paech supra n.45.

106 Where this line is drawn in relation to shifting cultural expectations of the public-private divide provoked by new digital technological is ultimately a matter of political culture. See Perri 6 (1998) *The Future of Privacy*. London: Demos.

existed beyond state control, enabled by advances in cryptographic software that could provide users with complete anonymity[107] made possible via a decentralized currency, which Bitcoin was intended to fulfil.[108] This political vision assumed that reliance on cryptographic algorithms to enable trustworthy peer-to-peer interaction between strangers, and the distributed nature of the underlying computing network, would render conventional law unnecessary and unable to reach into the activities taking place upon or arising out of the network's operation. This paper has subjected these assumptions to critical scrutiny, arguing that the belief that blockchain systems will operate outside of, and independently from, conventional law, rests on two assumptions: firstly, that the conventional state legal system is rendered redundant because the blockchain provides an alternative governance framework, including guarantees of security, of equal or greater effectiveness and efficiency than those currently provided by conventional law, and secondly, that the state will not intervene in these networks, because it either has no significant legitimate interests that are threatened by particular blockchain networks or applications, or, even if the state has legitimate interests that it might plausibly seek to protect, it nevertheless lacks the practical capacity to take effective remedial action to forestall or mitigate these threats.

I have argued that it is highly implausible to expect that these assumptions will be borne out in practice, owing to two critical roles currently undertaken by contemporary constitutional democratic states vis-à-vis their citizens: firstly, in safeguarding the rule of law and ensuring the universality of its protection and secondly, ensuring the basic security of its citizens. Because blockchain systems may threaten the universality of the rule of law, and because the security offered by blockchain systems takes a rather limited form, in the guise of 'transactional security' which falls short of the nature and extent of security guarantees that citizens in contemporary democratic states have come to expect, I have argued that conventional national law-makers and enforcement officials have attempted to (and are likely to continue to) assert national sovereign authority over activities taking place upon, or arising out of, the operation of blockchain code, in certain circumstances.[109] The critical question is not, therefore, whether states will attempt to exert legal authority over blockchain systems and interactions, but identifying the *conditions* in which they are likely to do so, and their success in employing strategies and techniques through which this legal authority can be successfully asserted in practice, given that the distributed nature of the network means that there is no central point of control upon which legal officials can target their enforcement efforts. This paper has offered my hypothesis concerning how conventional national legal systems are likely to respond to blockchain systems (drawing on their emerging responses to date), in order to provide a schematic map of the kind of interactions that are likely to arise between these two quite different regulatory modalities.

I have identified three different kinds of interaction between the code *of* law, and code *as* law, based on the intended motives and purposes of network participants when engaging in transactions upon the network, each giving rise to a distinctive form of interaction where blockchain is used for the purposes of:

(a) *hostile evasion*, to evade the substantive constraints of conventional law. National law enforcement authorities have asserted the superior authority of national law over blockchain-related activities of this kind, resulting in a dynamic of *cat and mouse* battle for supremacy;

---

[107] Cunningham, Alan (2016) 'Decentralisation, Distrust & Fear of the Body - the Worrying Rise of Crypto-Law' *Script-ed* 13: 235-57.

[108] Yet the motives of contemporary Bitcoin users may bear no relationship to its ideological origins, with studies identifying a range of user-motivations, ranging from strong political commitments, a desire for anonymity through to an intent to engage in illegal activities: Yelowitz, Aaron and Matthew Wilson (2015) Characteristics of Bitcoin Users: An Analysis of Google Search Data. *Applied Economics Letters* 22: 1030-36.

[109] I share the Blackett review's belief that the interests of nation states in exerting authority over blockchain systems will prove impossible to resist so that nation states will at least *attempt* to extend the reach of their sovereign authority in the form of conventional law to the transactions and interactions taking place: The Blackett Review 2016, Chapter 3, *supra* n 6.

(b) *efficient alignment*, with conventional law, by seeking to streamline or otherwise enhance compliance with legal standards. No battle for supremacy between the law vs code arises because network participants willingly accept and voluntarily submit themselves to the jurisdiction of conventional law. Yet because informal tensions are likely to arise between these two forms of ordering, I describe the resulting dynamic as *the joys of (patriarchal) marriage* – sometimes harmonious, at other times rather tense and fractious, but ultimately rooted in a shared commitment to deriving the benefits of long term mutual support and cooperation and in which the supremacy of conventional law is expressly acknowledged;

(c) supporting novel forms of peer-to-peer co-ordination and cooperation to *reduce transactional friction* associated with the legal process, including the transaction, monitoring and agency costs associated with conventional law. Here I suggest that the resulting dynamic between the two codes can be characterised as one of *uneasy co-existence*. Whether national law enforcement authorities will attempt to assert their authority over activities undertaken on a particular blockchain network will depend upon whether those activities are considered likely to cause significant harm to third parties and/or those transacting on the network. But unless and until an explicit attempt is made by conventional legal systems to reach into blockchain-based activities, the resulting uneasy coexistence between the code *as* law and the code *of* law may be characterised as one of *mutual suspicion* and uncertainty.

My analysis has highlighted the underlying normative challenges and tensions that can be expected to shape the interactions between the two ordering systems, which are most acute in the third class of case, and ultimately grounded in the shifting and uncertain boundaries between the public and private realm in a continuously networked digital age. As blockchain technologies mature and new applications emerge, both kinds of code will be faced with at least three points of tension, and which are likely to influence their on-going interactions and the extent to which they are predominantly antagonistic or co-operative in character. First, blockchain developers committed to a vision in which the blockchain code can be relied upon exclusively to govern network interactions, are bound to be disappointed. As legal scholars have long observed in their analysis of rules in the form of linguistic text as guides for future behaviour, rules are inevitably and inescapably imperfect[110]. No amount of careful and detailed drafting is able to predict future events, and hence unanticipated situations will arise which existing rules are unable comfortably to accommodate[111]. At the same time, the way in which rules have been drafted, whether in linguistic or computational form, will at times fail to reflect the intentions and expectations of their drafters. In these situations, how the rules ought to apply will be a matter of interpretive debate and require human judgement, as The DAO Hack vividly illustrates. If network participants are unhappy with the way in which such disputes are resolved within the blockchain community, then they may well turn to conventional law to remedy the perceived injustice.

Secondly, even if blockchain networks can live up to their promise of enabling new forms of more democratic, peer-to-peer interaction than is currently possible through reliance on traditional modes of social organisation, they cannot in practice operate as hermetically sealed systems detached from the broader community beyond the network and the wider social world. There will inevitably be differences in the size and significance of these external effects on the broader community, but it will fall to conventional legal systems to ensure that the legitimate rights, interests and expectations of the wider community are duly protected, in accordance with the terms of the implied social contract between the state and its citizens. National legal systems will then be required to identify, evaluate and trade-off the balance of legitimate interests of those within the network with those operating outside the network, and this may require them to exert sovereign power over the putative 'private' arrangements of network participants. In other words, even if blockchain systems can successfully provide reliable and efficient transactional security, they are unlikely to deliver other critical security guarantees (including protection against interference with rights of property, threats to health and safety, and unfair exploitation), that are currently (albeit imperfectly) provided by conventional law.

---

110 Black, Julia. *Rules and Regulators*. Oxford: Clarendon Press, 1997.

111 Hart, H L A. *The Concept of Law*. New York: Oxford University Press, 1961, 124-130.

Thirdly, network developers, participants and users will learn, whether through experiences such as The DAO Hack or otherwise, that software code is an imperfect and limited instrument of governance. Not only is code prone to software bugs, but because rules themselves are imperfect guides for future action, requiring revision and updating as the economic, social and political context changes along with the needs of its users. Accordingly, national legal systems will be required to identify the extent to which they are willing and able to respond to these deficiencies in order to protect network users and those outside the network, which necessitates reliance on human judgement. In addition, blockchain's decentralized structure presents additional operational risks. As Angela Walch has observed, the decentralised nature of public blockchains means that no one is responsible for keeping the Blockchain software operational, so that even if a crucial repair is needed to prevent complete collapse of the software, no one could be required to perform the repair. Even core developers who have been voluntarily working to maintain the blockchain could decide not to help in a moment of crisis, perhaps deeming their continued to involvement to be personally risky. And without any formally defined power, authority or accountability structure, although anyone with a suggested resolution to a crisis may propose a solution, it may take too long to achieve buy in from other members of the blockchain community to successfully implement the solution, either in an emergency or otherwise.[112] As the Blackett Review reminds us, even unpermissioned blockchains do not exist independently of human rule-making and governed only by mathematical algorithms.

> Just like legal code, technical code needs to be produced and maintained by humans who define the rules that the code embodies….Like any software, Bitcoin needs to be regularly updated to address bugs, security issues, and changes in the operating environment. Such an update can in principle change any aspect of the software, including accounting and ownership rules. Who gets to write the software and how that process is governed is therefore critically important to all participants in a DLS.[113]

These observations also highlight the lack of any existing laws mandating minimum internal governance requirements that public-facing blockchain networks must satisfy, so that users remain largely at the mercy of the network's founders and developers in devising the basic framework for internal governance of the network and for implementing them via technical code. My guess is that, in time, minimum standard to ensure that basic principles of good blockchain governance will emerge, although they might not take the form of mandatory legal standards. In short, the success of blockchain will depend on effective and legitimate governance structures, which will require *both* the code that controls the operation of digital technologies (code *as* law) as well as the conventional rules provided by national legal systems (code *of* law). In other words, the challenge is to find sustainable, stable yet flexible equilibrium in which legal and technical code can avoid engaging in an unhelpful battle for supremacy but enables them to coexist and collaborate in order to sustain valuable forms of social, economic and political interaction without posing unacceptable risks of harm to network participants or the wider community.

Accepted version 13.6.18 **(14553 words without footnotes)**

Revised and shortened 1.7.18 (12,969 words without footnotes less 565 words of abstract = **12404 words**)

---

112 Walch, Angela (2017) 'The Bitcoin Blockchain as Financial Market Infrastructure: A Consideration of Operational Risk'. *Journal of Legislation and Public Policy* 18: 837.

113 The Blackett Review 2016: 43