COMPUTER LAW & SECURITY REVIEW 34 (2018) 843–846

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/CLSR

Computer Law & Security Review

Blockchain and law: Incompatible codes?

*Christopher Millard**

Centre for Commercial Law Studies, Queen Mary University of London, London, UK

ARTICLE INFO

Article history:

Keywords:
Blockchain
Distributed ledger
DLT
Bitcoin
Smart contract
Data protection
Privacy
GDPR
European Union
EU

ABSTRACT

Blockchain has recently joined a long line of technological innovations that have been characterised as disruptive to, and possibly even subversive of, fundamental legal principles. This article looks behind the hype to examine how blockchain might – or might not – be compatible with established legal and regulatory models. Data protection is discussed as an example of an area of law that some have claimed cannot be reconciled with blockchain. Various other conflicts are also identified and concerns about blockchain are placed in the context of wider historical debates about new technologies vs law.

The history of technologies, not least information technologies, is replete with claims that a particular development will be highly 'disruptive' and will render obsolete established legal norms and regulatory frameworks. Perhaps the most dramatic illustration is the enthusiastic reception that cyber-libertarians gave the public Internet in the mid-1990s. At the time, some forecast not merely that specific legal constructs would be challenged, but that nation states would become obsolete. In that debate, the most famous example was the late John Perry-Barlow's 1996 'Declaration of the Independence of Cyberspace'.[1] This included assertions that:

> *"Governments of the Industrial World… You have no sovereignty where we gather…. Your legal concepts of property, expression, identity, movement, and context do not apply to us. They are based on matter, and there is no matter here."*

This rallying cry was wildly popular and many early web sites reproduced the full text or at least linked to it. Reports of the death of sovereignty were, however, exaggerated. When asked in 2004 to comment on his revolutionary tract, Barlow responded simply: "We all get older and wiser". In fact, there has long been evidence that 'online' activities are likely to be subject, at least nominally, to more legal rules, and broader regulatory oversight, than comparable 'offline' activities.[2] Admittedly, new technologies do not always fit easily into

* Corresponding author: Christopher Millard, Centre for Commercial Law Studies, Queen Mary University of London, 67-69 Lincoln's Inn Fields, London WC2A 3JB, UK.

E-mail address: c.millard@qmul.ac.uk

[1] John Perry Barlow, 'A Declaration of the Independence of Cyberspace', 8 February 1996, available at: https://www.eff.org/cyberspace-independence.

[2] See discussion of 'Cyberspace and the "no regulation" fallacy' in Christopher Millard and Robert Carolina, 'Commercial transactions on the global information infrastructure: a European perspective', *John Marshall J. Computer & Info. Law*, Vol. 14, 269 (1996).

https://doi.org/10.1016/j.clsr.2018.06.006

existing legislative and regulatory paradigms, and enforcement may be challenging, but lawmakers, regulators, and courts have so far managed to adapt, albeit with a time lag, to each wave of innovation.

A recent technological development that is provoking agitated debates, and attracting a lot of media attention, is blockchain. Most of the current hype about blockchain relates to crypto-currencies, especially Bitcoin, and related financial products such as Initial Coin Offerings (ICOs). Concerns have been raised that, like the early Internet, blockchain-based financial systems may be unregulated, and possibly even 'unregulatable'. Less visibly, but probably far more importantly in the long run, a great deal of investment is going into the development of a broad range of blockchain applications in contexts ranging from asset registration (including land) to self-executing ('smart') contracts. Notwithstanding widespread confusion about what exactly blockchain is or might become, blockchain and distributed ledger technologies (DLT) have caught the imagination of governments, businesses and private investors, and they are increasingly a focus of attention for legislators and regulators worldwide.

An example of an apparently intractable legal challenge concerns how data protection concepts and rules will apply to blockchain. Is it possible to build and deploy compliant blockchain platforms to the extent that they involve the processing of personal data? Jan Philip Albrecht, an MEP who played a prominent role in the development and finalisation of the EU's General Data Protection Regulation (GDPR), has suggested it is not. In his view:

> *"Certain technologies will not be compatible with the GDPR if they don't provide for [the exercising of data subjects' rights] based on their architectural design. This does not mean that blockchain technology, in general, has to adapt to the GDPR, it just means that it probably can't be used for the processing of personal data."*[3]

Albrecht's negative view of blockchain as a technology for processing personal data seems premature and simplistic. As is the case with many other technologies, whether personal data may be processed using blockchain technology in a manner compatible with the GDPR will depend on the specific technical and organisational model that underpins a particular blockchain application. Before we explore this further, however, we need greater clarity regarding the term blockchain.[4]

Unlike some other recently deployed technologies, such as cloud computing, there is not yet a widely accepted definition of blockchain.[5] This is perhaps not surprising given the unorthodox origins of the first popular blockchain application,[6] the rapid pace at which blockchain technologies are evolving, and the fact that the term is used to cover a broad range of models for establishing and managing a ledger of transactions.

It may be helpful to distil the concept down into three fundamental elements. At its most basic, a blockchain can be understood as a system:

(i) for recording a series of data items (such as transactions between parties)
(ii) that uses cryptography to make it difficult to tamper with past ledger entries, and
(iii) that has an agreed process for storing one or more copies of the ledger and adding new entries.

The first element is simply another way of saying that a blockchain is a kind of ledger. As regards the second element, commentators often assume that the way in which blocks are formed and chained makes a blockchain 'immutable' and 'irreversible'. To be more precise, a blockchain is a series of blocks, with each block containing data about various transactions together with a header that includes a 'hash value' for the previous block, which in turn has a header that includes the hash of the block before that, and so on. Together, these blocks form a chain linked through their hashes. This means that any attempt to tamper with data in a particular block in the chain will be obvious, as the hash of its data will no longer match the hash value included in the next block, thereby breaking the chain. So, strictly speaking, a change may be made to a particular record in a block within a blockchain, but it will be obvious that a change has occurred (hence a blockchain is 'tamper evident' rather than 'tamper proof').

The third element (the 'agreed process') is usually called 'consensus'. Again, confusion can arise from interchangeable use of the terms 'blockchain' and 'distributed ledger technology' (DLT). DLT refers to a particular type of blockchain 'technology' in which a 'ledger' is 'distributed' across several, potentially many, 'nodes' (i.e. individuals or organisations that hold a copy of the ledger). In a distributed system a mechanism is needed to ensure consistency between the various copies of the ledger. Such 'consensus' may be achieved in several different ways. These include the cumbersome and energy intensive 'proof of work' model used by Bitcoin, whereby 'miners' compete to solve increasingly difficult computational

[3] David Mayer, 'Blockchain technology is on a collision course with EU privacy law', IAPP Privacy Advisor, 27 February 2018. Available at: https://iapp.org/news/a/blockchain-technology-is-on-a-collision-course-with-eu-privacy-law/.

[4] The introduction to blockchain that follows is inevitably only a high-level overview of the topic. For a more detailed technical explanation of blockchain technology and platforms, and a more thorough exploration of the data protection and other legal issues mentioned in this article, see Jean Bacon, Johan David Michels, Christopher Millard, and Jatinder Singh, Blockchain Demystified (December 20, 2017). Queen Mary School of Law Legal Studies Research Paper No. 268/2017. Available at: https://ssrn.com/abstract=3091218.

[5] In the case of cloud computing, 'The NIST Definition of Cloud Computing' had reached its 16th, and final, version by September 2011. Available at: https://csrc.nist.gov/publications/detail/sp/800-145/final.

[6] Although the idea of using a hashed chain of blocks to create a secure ledger dates back to the early 1990s, the concept only received widespread attention with the publication in 2008 of a white paper entitled 'Bitcoin: A Peer-to-Peer Electronic Cash System', authored by an unknown person or person using the name Satoshi Nakamoto. See Arvind Narayanan, Joseph Bonneau, Edward Felton, Andrew Miller and Stephen Goldfeder, 'Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction' (Princeton University Press, 2016). The Nakamoto paper is available here: https://bitcoin.org/bitcoin.pdf.

puzzles as a basis for adding a new block to a chain, with the winner being rewarded in Bitcoin for doing so. Other key characteristics of Bitcoin are that it is 'open' and 'permissionless', which means that anyone may, without authorisation, use Bitcoin and, indeed, may participate in the network as a node. Widespread distribution of copies of the ledger, together with a consensus process that does not require any centralised intermediary to manage the ledger, make Bitcoin and similar DLTs attractive as platforms for use by large numbers of parties who do not trust, and indeed may not even be able to identify, each other.

It is, however, this very openness, lack of permissioning, and potential anonymity that make public blockchain systems like Bitcoin problematic from a legal and regulatory perspective. Indeed, these characteristics echo some of the ideals and aspirations of early cyber-libertarians such as John Perry Barlow. For example, how do pseudonymous Bitcoin transactions fit with anti-money laundering (AML) and know your customer (KYC) rules? How might a financial services regulator check whether such rules are being complied with if token transfers take place without involving any central entity or other intermediary that can be regulated and audited?

Data protection law raises further difficult questions in four interrelated areas:

(i) Identifying data controllers and processors: Is each node that holds a copy of the distributed ledger a controller in respect of all personal data in the ledger? What is the status of the users of an open blockchain application? If they store personal data in the blockchain, are they then also controllers? If so, might they be exempt from regulation provided they are only processing data in the course of a purely personal or household activity?
(ii) Controller and processor relationships: How can controllers give instructions to processors regarding the processing of personal data when the parties may not even know whom they are dealing with? Indeed, if thousands of nodes hold copies of data relating to transactions between millions of users how could they all contract with each other anyway?
(iii) International data transfers: Given that a node or user may be anywhere on the planet, must it be assumed that any personal data in a distributed ledger might be transferred worldwide?
(iv) Data minimisation and data subject rights: Is the proliferation of copies of data in a DLT compatible with the data minimisation principle? What happens if a data subject wishes to exercise an individual right, for example to correction or erasure of data, if the relevant data are stored in an 'immutable' blockchain?

Given the proliferation of such difficult questions, it is perhaps unsurprising that many commentators are asserting that blockchain is somehow fundamentally incompatible with existing legal and regulatory models, with data protection often cited as an obvious example. Should we then just adopt Albrecht's position and conclude that blockchain probably cannot be used for the processing of personal data?

Not necessarily. Let us step away from the Bitcoin model and return to the core elements of blockchain as a tamper-evident ledger that is established and maintained according to some kind of consensus protocol. Based on these fundamental elements, might it be possible to develop and deploy a blockchain platform that is compatible with data protection by design principles? Perhaps. For example, instead of being public and permissionless, the blockchain might be set up by a consortium that is governed by rules that establish the basis on which each party will process any personal data that is included in the blockchain. Moreover, instead of a distributed consensus mechanism such as proof of work, the parties might agree to use some kind of 'consensus by authority' whereby one or more participants has the authority to add blocks to the chain, for example by each taking turns to do so. Indeed, that role might be outsourced to a trusted third party, perhaps a cloud service provider that offers Blockchain as a Service (BaaS).[7] This would make identifying controllers and processors and structuring their relationships much more straightforward. It may even be possible to design a blockchain that is 'redactable' or 'editable' without undermining the core characteristic of being a tamper-evident ledger.[8] This could make it simpler to comply with data subject requests for rectification or erasure of data.

So, as with many issues that arise in data protection law, the appropriate answer to the question of whether a blockchain may be used to process personal data is not binary but rather "It depends". Undoubtedly, there remains a lot of work to be done not just in relation to personal data but also regarding other legal implications of blockchain, including the role of contract law in managing 'on-chain' and 'off-chain' assets and relationships.[9] Perhaps not surprisingly, cryptocurrencies and ICOs have received particular attention from lawmakers and financial services regulators, with approaches ranging from attempted bans to constructive engagement.

Just how disruptive will blockchain be in terms of established legal norms and regulatory frameworks? At this stage in its development, blockchain looks like yet another technology that gives rise to complex challenges in terms of interpretation, application and enforcement[10] of existing rules. The case

[7] See Jatinder Singh and Johan David Michels, 'Blockchain as a Service: Providers and Trust', Queen Mary School of Law Legal Studies Research Paper No. 269/2017. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3091223.

[8] For example, personal data might be stored 'off-chain' and be reflected on the blockchain only in the form of a one-way hash. Deletion of the off-chain-stored personal data would then render the hash value meaningless. Alternatively, in a closed, permissioned, environment with a limited number of nodes the participants might agree a process for forking the blockchain to create a new version in which the relevant data have been corrected or from which the data have been removed. See also Accenture, *Editing the Uneditable Blockchain: Why Distributed Ledger Technology Must Adapt to an Imperfect World*, Accenture Press Release, 2016, (20 Mar. 2018). Available at: https://newsroom.accenture.com/content/1101/files/Cross-FSBC.pdf.

[9] See Chris Reed, Uma Sathyanarayan, Shuhui Ruan and Justine Collins, "Beyond Bitcoin: legal-impurities and off-chain assets", *International Journal of Law and Information Technology*, Vol. 26(1), 160.

[10] As with regulation of online content, enforcement of specific rules against blockchain participants may be require novel approaches. As is the case with enforcement of rules relating to online content, where platform and other service providers are often

has not been made, however, for blockchain technology precipitating an imminent 'paradigm shift' of the type predicted by the early cyber-libertarians.[11]

However, over the longer term, blockchain may end up driving changes in the way in which legal rules work. One of the many interesting features of blockchain technology is that it is not only rules-based (like many information technologies) but that it can be deployed so as to automate the operation of rules-based processes both to trigger and to document events in novel ways and on a very large scale. Two decades ago, Joel Reidenberg suggested the time had come for 'Lex Informatica'.[12] His core thesis, radical at the time, is apposite to our assessment of blockchain. Having observed a few years earlier that technical choices in network designs may result in new legal norms,[13] he went on to argue that "policymakers … should pursue Lex Informatica norms as an effective substitute for law where self-executing, customised rules are desirable." So-called 'smart contracts' built on blockchain technologies may prove to be the most important example yet of "self-executing, customised rules". In this context, it remains to be seen whether the further development and deployment of blockchain platforms will promote beneficial changes, probably subtle at first, to the way in which lawmakers, courts and regulators deal with commercial transactions and other legal arrangements.[14] If this is indeed the outcome, then the apparent tensions between blockchain and law may prove to be a catalyst for positive developments rather than a chilling factor for innovation.

The process of reconciling new technologies with established legal principles and regulatory models is often messy and protracted. As was the case when 'computer law' began to emerge as a discipline in the 1980s, and often since, current debates surrounding blockchain demonstrate that lawyers still have a lot to learn from specialists in other disciplines, and vice versa. However, it is this fertile ground for collaboration that makes it so rewarding to work in the field of technology law and regulation. Over the past 33 years, thanks to the pioneering work of its founding editor, the *Computer Law and Security Review* has played a crucial role as an inter-disciplinary forum where potential clashes, and synergies, between technology and law can be identified and explored. When I started out as a 'computer lawyer' in 1982, Stephen Saxby was one of a handful of scholars worldwide who were already immersed in the field. I will always be grateful for the leadership he has demonstrated and for all the support and encouragement he has provided to me and so many other colleagues over the years. I congratulate him, and Elsevier, on the publication of this special 200th issue.

Acknowledgement

The author is grateful to Microsoft for supporting the research on which this paper is based and to colleagues in the Cloud Legal Project for comments on an earlier draft. Responsibility for views expressed, however, remains with the author.

targeted, blockchain intermediaries (such as software wallet and exchange providers) are also likely to become targets for regulation.

[11] That is, a paradigm shift in the sense of a change so fundamental that it is revolutionary, as described by Thomas Kuhn in his highly influential book *The Structure of Scientific Revolutions* (University of Chicago Press, 1962).

[12] Joel R. Reidenberg, 'Lex Informatica: The Formulation of Information Policy Rules Through Technology', *Texas Law Review*, Vol. 76, 553 (1998). Reidenberg's theory provided an important foundation for Larry Lessig's popular book *Code and Other Laws of Cyberspace* (Basic Books, 1999) and its successor *Code Version 2.0* (Basic Books, 2006).

[13] Joel R. Reidenberg, 'Rules of the Road for Global Electronic Highways: Merging the Trade and Technical Paradigms', *Harvard Journal of Law and Technology*, Vol. 6, 287 (1992–1993).

[14] For an interesting discussion of the potential for improved governance systems based on blockchain, see Aaron Wright and Primavera De Filippi, Decentralized Blockchain Technology and the Rise of Lex Cryptographia (March 10, 2015). Available at: https://ssrn.com/abstract=2580664.