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.