2018

Blockchain versus Data Protection

Fred H. Cate
Indiana University Maurer School of Law, fcate@indiana.edu

Christopher Kuner
Vrije Universiteit Brussel, Brussels

Orla Lynskey
London School of Economics

Christopher Millard
Queen Mary University of London

Nora Ni Loideain
University of London

See next page for additional authors

Authors
Fred H. Cate, Christopher Kuner, Orla Lynskey, Christopher Millard, Nora Ni Loideain, and Dan Jerker B. Svantesson

Editorial

Blockchain versus data protection

Christopher Kuner*, Fred Cate**, Orla Lynskey**, Christopher Millard**, Nora Ni Loideain** and Dan Svantesson**

It is not uncommon for technological developments to give rise to debates as to whether existing legal norms and regulatory frameworks will be disrupted or undermined. A recent, high-profile, example is blockchain.

Most of the popular excitement about blockchain, so far at least, relates to crypto-currencies, especially Bitcoin, and related financial products such as Initial Coin Offerings (ICOs). Less visibly, but probably 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 registration of assets (including land) to self-executing ('smart') contracts. Notwithstanding widespread confusion about what exactly blockchain is or might become, blockchain and distributed ledger technologies (DLTs) have caught the imagination of governments, businesses, and private investors, and they are increasingly a focus of attention for legislators and regulators worldwide.

Of specific relevance to this Journal is the question of how data protection concepts and rules will apply to blockchain and, indeed, whether it might prove to be impossible to build and deploy compliant blockchain applications to the extent that that they involve the processing of personal data. Indeed, Jan Philip Albrecht, a Member of the European Parliament who played a prominent role in the development and finalization of the European Union's General Data Protection Regulation (GDPR), has asserted just that. 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.[1]

We consider Albrecht's views on blockchain as a technology for processing personal data to be overly negative. Whether personal data may be processed legitimately using blockchain technology will depend on the specific technical and organizational model that underpins a particular blockchain application. Before we can go any further, however, we need to clarify what we mean by the term blockchain.

Unlike some other recently deployed technologies, such as cloud computing, as yet there is no widely accepted definition of blockchain. This is perhaps because blockchain technology is evolving rapidly and the term is used to cover a broad range of models for establishing and managing a ledger of transactions. Moreover, the term blockchain is often used interchangeably with other concepts such as DLT (see below regarding this concept). Above all, the lack of technical precision that often characterizes discussions of cryptocurrencies such as Bitcoin has resulted in widespread confusion as to what should, and should not, be regarded as an implementation of blockchain technology.

It may be helpful to pare the concept down into three fundamental components. For our purposes, a blockchain is (i) a system for recording a series of data items (such as transactions between parties) that (ii) uses cryptography to make it difficult to tamper with past ledger entries, and that (iii) has an agreed process for storing one or more copies of the ledger and adding new entries. This process is usually called 'consensus', though that term may also be misleading. DLT refers to a particular type of blockchain system that is 'distributed' across several, potentially many, 'nodes' (ie individuals or organizations that hold a copy of the distributed ledger). '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 puzzles as a basis for adding a new block

* Editor-in-Chief.

** Editor.

1 D Mayer, 'Blockchain Technology is on a Collision Course with EU Privacy Law' IAPP Privacy Advisor <https://iapp.org/news/a/blockchain-technology-is-on-a-collision-course-with-eu-privacy-law/ > accessed 27 February 2018.

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 authorization, 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 centralized, trusted, intermediary to manage the ledger, make Bitcoin and similar DLTs attractive as platforms for use by large numbers of parties who do not trust, indeed may not even be able to identify, each other.

It is, however, the very openness, lack of permissioning, and potential anonymity that make public blockchain systems like Bitcoin problematic from a legal and regulatory perspective. For example, how can a financial services regulator check that anti-money laundering (AML) and know your customer (KYC) rules are being complied with if a large number of parties can transfer tokens between each other without involving any regulated entity or other intermediary that can be audited? In terms of data protection compliance, is each node that holds a copy of the distributed ledger a controller in respect of all personal data in the ledger? Might each node also, or instead, be a processor for the operator of every other node? What is the status of the users of an open cryptocurrency? Are they also all controllers and, if so, in what circumstances might they be excused from data protection compliance obligations because of an exemption such as that for processing in the course of a purely personal or household activity? How can controllers give instructions to processors regarding the processing of personal data when the parties may not even know who 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? 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? Is the proliferation of copies of data in a DLT compatible with the data minimization principle? What happens if a data subject wishes to exercise an individual right, eg to correction or erasure of data if the relevant data are stored in an 'immutable' blockchain?

Very few commentators have gone beyond identifying a selection of these questions and then concluding that data protection compliance in relation to blockchain is highly problematic, or simply impossible. Does this mean that Albrecht is right and 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 being 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 system 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, eg by each taking turns to do so. Indeed, that role might be outsourced to a trusted third party, perhaps even a cloud services provider that offers Blockchain as a Service (BaaS). 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. These are not just hypothetical suggestions; blockchain arrangements are currently being established that have some or all of these features.

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.'[2]

doi:10.1093/idpl/ipy009

2 For a more detailed explanation of blockchain technology, and an exploration of the data protection and other legal issues raised in this editorial, see J Bacon and others, 'Blockchain Demystified' (Queen Mary School of Law Legal Studies Research Paper No 268/2017). <https://ssrn.com/abstract=3091218> accessed 20 December 2017; see also M Finck, 'Blockchains and Data Protection in the European Union' (2018) 4(1) European Data Protection Law Review 17–35.