KEY POINTS

- Academics have suggested that the peer-to-peer nature of some distributed ledger technologies, with all nodes linking directly to each other, could lead to the system being considered at law to be one of several legal entities, including a joint venture, a multi-party contract and a partnership.
- Commentators have considered whether a particular class of participants, such as smart contract code developers, miners or nodes, should be liable for losses.
- Academics have argued against the "code as law" suggestion for regulation on the basis that the law covers all relations among people and property; analysis of blockchain by definition must fit within the existing framework.

Feature

Authors Charles Kerrigan and Siobhan McKeering

Laws and legal principles relating to blockchain and distributed ledger technologies: a taxonomy

In this article the authors consolidate and categorise the legal issues so far identified in relation to blockchain and distributed ledger technologies, setting out broadly the areas in which issues can be said to fall.

Blockchain and other distributed ledger technologies (DLT) are approaching the mainstream. Technology companies offer products for commercial projects. IBM's Blockchain Platform references "500+ client engagements to date". Financial institutions use them. HSBC said in January 2019 that it settled $250bn worth of foreign exchange trades using blockchain during 2018. They are used in fundraising in the syndicated lending and capital markets. In November 2018 BBVA arranged a $150m syndicated loan using DLT arranged over a private blockchain network. In August 2018 the World Bank launched the world's first public bond created and managed using only blockchain in a A$100m transaction designed to test how the technology could improve practices in the industry.

Although there is still some way to go before blockchain lives up to the claims of its most optimistic adherents, organisations in both the private and public sectors are actively taking steps to develop blockchain-based solutions.

The legal community is involved in these developments. Lawyers in businesses and at external law firms work in development and implementation. Academic lawyers and lawyers at policymakers provide analysis and expert guidance on the issues arising.

We believe that it would now be useful to consolidate and categorise the legal issues that have so far been identified in relation to blockchain and distributed ledger technologies. The list of categories below is not exhaustive. It sets out broadly, however, the areas in which issues can be said to fall.

First it is necessary to clarify a point on terminology and scope. Permissionless systems are public and do not rely on a network owner. Permissioned systems are private and access to the network is granted by a network owner. Most commercial examples of systems are permissioned. The analysis in this article applies to permissionless systems. There is no existing legal analysis that is definitive in this area. The analysis applies more or less to permissioned systems depending on the extent to which developers or courts choose to or need to make use of the benefits of permissionless or decentralised architecture (eg efficiency, transparency, resilience).

And as a second housekeeping point, it will be obvious that the notes below are very short paraphrases of the sources that are credited by reference. These are not a substitute for the original material.

1. "BLOCKCHAIN LAW"

Some jurisdictions have legislated specifically in relation to blockchain, DLT and crypto-assets.

In July 2017, the Delaware General Corporations Law was amended to recognise the creation and maintenance of corporate records on "distributed electronic networks or databases".

In April 2018, Arizona State in the US passed a "blockchain law" (HB 2417) to allow Arizona corporations to hold and share data on a blockchain and to clarify certain enforceability issues in relation to the use of smart contracts.

In July 2018 Malta passed three Bills (the Malta Digital Innovation Authority Act, the Virtual Financial Assets Act and the Innovative Technology Arrangements and Services Act) establishing a regulatory framework for blockchain, cryptocurrency and DLT.

In February 2019 Luxembourg passed Bill 7363 into law to facilitate the use of blockchain technology in financial services.

In February 2019, the state of Wyoming passed a law (SF 125, effective 1 July 2019) which, among other things, classifies digital consumer assets as intangible personal property for certain purposes. Wyoming has also enacted a series of other blockchain-specific legislation.

Many other jurisdictions are considering or implementing similar rules. These rules are generally directed towards clarifying certain specific administrative or regulatory points. They also demonstrate (and are usually intended to do so) an openness to the use of the technology. They leave open, however, many of the more theoretical legal points associated with the technology, as noted below.

2. LEGAL NATURE OF BLOCKCHAIN AND DLT SYSTEMS: IDENTIFICATION, IMPLICATIONS, PARTICIPANTS AND THIRD PARTIES

D A Zetzsche, R P Buckley and D W Arner (in 'The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain' (2018)

University of Illinois Law Review) provide the most comprehensive analysis of the nature of these systems and distinguish DLT systems from "traditional business networks" (such as franchise systems, credit card networks and supply chains). The latter follow a "hub and spokes", centralised model. In the absence of express contractual provisions, individual participants, such as franchisees, are only connected to each other through the "hub" (that is, the franchisor). Participants do not owe loyalty to the network as a whole.

Zetzsche, Buckley and Arner distinguish the decentralised model which exists in some DLT systems. They argue that the peer-to-peer nature of these systems, with all nodes linking directly to each other, is "the tipping point at which a loose assembly of self-interested entities turns into a group of entities legally tied together". There is also a common purpose in DLT systems, which goes beyond economic interests. The participants in the system share the aim of the joint performance of the ledger.

Zetzsche, Buckley and Arner suggest that these features of a DLT system could lead to it being considered at law to be one of several legal entities, including a joint venture, a multi-party contract and a partnership. For example, the authors suggest that the group that sets up the code design and governs the ledger could be considered a joint venture and that this could extend to nodes or even simple users of the ledger depending on the extent of their participation. Alternatively, the DLT system could be considered as a multi-party contract, with the group that sets up the code design and nodes under a contractual obligation to maintain the system's security and operations.

Potential legal structures will differ depending on the relevant jurisdiction. Under English law there is no distinct legal concept of a "joint venture". Instead, that term covers legal structures such as a general partnership, a limited partnership, a limited liability partnership, a private limited company, and an unincorporated contractual arrangement.

Depending on the nature of the legal structure, Zetzsche, Buckley and Arner say that liability may arise under contract law, tort, partnership law or under specific legislation or regulation. Such liability may be "internal network liability" (that is, between the participants to the DLT system) and "external network liability" (that is, liability to third parties).

J Bacon, J D Michels, C Millard and J Singh, (in 'Blockchain demystified: a technical and legal introduction to distributed and centralised ledgers' (2018) 25(1) *Richmond Journal of Law & Technology*) note that elements of Decentralised Autonomous Organisations (DAO) may replicate those of a company. For example, a DAO could have a smart contract which allows the spending of funds based on approval by two-thirds of nodes (or members). In contrast, a DAO would not need a management team to exercise control over the DAO and its capital as this would be done by nodes and according to the code. Significantly, however, in the UK a DAO may not qualify as a recognised legal person (because it is not registered as a legal company with Companies House) or offer shareholders limited liability. Therefore, unlike a private company, participants in a DAO may face significant legal risk.

Several factors may therefore influence the potential legal structure of a DLT system, including, but not limited to:

- whether there is an agreement which specifies the legal structure;
- whether the system is permissioned or permissionless;
- the express or implied purpose of the system (if any);
- whether there is a pre-existing relationship between the parties;
- the consensus mechanism employed by the system.

3. LEGAL PERSONALITY

Determining whether a system has legal personality has implications for many of the questions considered in relation to this topic.

In 'Horizon Scanning – Blockchain: The Legal Implications of Distributed Systems', the Law Society questions what legal status attaches to DAOs. An answer to this is needed to be able to answer questions such as who or what is claimed against in the context of a legal dispute.

Tendon and Ganado (in 'Legal Personality for Blockchains, DAOs and Smart Contracts') highlight the idea proposed by the government of Malta permitting the grant of legal personality in the form of a newly designed type of legal entity incorporating a blockchain and/or smart contract arrangements.

This shows another approach – that is to create a new legal entity through legislation. A consultation paper published in Malta in February 2018 by The Parliamentary Secretary for Financial Services, Digital Economy and Innovation, ('The establishment of the Malta Digital Innovation Authority; the Framework for the Certification of Distributed Ledger Technology Platforms and Related Service Providers; and a Virtual Currency Act') briefly raised the possibility of a "technology arrangement" (broadly defined as including DLT software and architecture, and smart contracts and related applications) having legal personality.

Ultimately, the Maltese legislation has not provided that an innovative technology arrangement could have its own legal personality. However, Tendon and Ganado (M Ganado, 'Maltese Technology Foundations – Initial Thoughts on an Important Proposal' (August 2018); S Tendon, M Ganado, 'Legal Personality for Blockchains, DAOs and Smart Contracts', *Revue Trimestrielle de Droit Financier Corporate Finance and Capital Markets Law Review* No 1-2018) have argued that such an approach has clear advantages. It could deal with allocation of liability and provide:

- protection to counterparties, consumers and developers/designers/coders;
- protection against damage caused by anonymous or bankrupt designers;
- opportunities to impose compliance requirements; and
- opportunities to introduce an element of jurisdiction to the DLT system, as the innovative technology arrangement would be required to be registered with the regulator in Malta.

Of course, these advantages should be weighed against the financial cost of compliance and registration, which may affect innovation and willingness to register a DLT system in the first place. (P L Athanassiou, 'Tokens and the regulation of distributed

ledger technologies: where Europe stood in the last quarter of 2018', 34(3) *Journal of International Banking Law and Regulation*).

4. LIABILITY ISSUES: CATEGORIES OF RISK, CLASSES OF PARTICIPANTS, TYPES OF TRANSACTION

One of the key consequences of the analysis of the legal structure of a DLT system is for the allocation of liability where loss has occurred. The use of DLT systems provides the potential for transactions to take place automatically, without human intervention. However, the use of these systems is neither failsafe nor fool proof. For example, Zetzsche, Buckley and Arner outline the different categories of liability risk associated with DLT systems, including risks of problematic coding and negligent performance. The Law Society (in 'Horizon Scanning – Blockchain: The Legal Implications of Distributed systems') notes the problem of liability management relating to systems where there is an inability to control and stop the functioning of public blockchains.

Businesses using DLT systems, and their lawyers, should be acutely aware that these risks raise questions as to where losses will lie. Although parties are likely to mitigate against losses through commercial documents where possible, it is worth reviewing the various ways in which liability for damage could be considered.

The question of allocation of liability could be analysed by reference to the participants in the system. Commentators have considered whether a particular class of participants, such as smart contract code developers, miners or nodes, should be liable for losses. Commissioner Brian Quintenz of the US CTFC, has talked about the "key players essential to powering smart contracts on the blockchain". In the context of CTFC regulations, Commissioner Quintenz posited that smart contract code developers should be held liable in some circumstances, and that the appropriate question is whether they "could reasonably foresee, at the time they created the code, that it would likely be used by US persons in a manner violative of CTFC regulations".

P De Filippi and A Wright (in 'Blockchain and the law' (2018), Ch 11) consider different modes of regulation that could be applicable, including in the context of liability questions.

Another way of looking at liability is by reference to the type of transaction taking place on the DLT system. For example, it has been suggested that if the existing law does not specify how losses should be allocated, it may be appropriate to let the losses lie for commercial contracts but not for consumer contracts. In 'Smart contracts: legal framework and proposed guidelines for lawmakers' (October 2018), the European Bank for Reconstruction and Development and law firm Clifford Chance note that regulators and legislators could impose a requirement that transactional documents used in a DLT system must allocate liability.

It is also possible to consider questions of liability and loss through the lens of any legal structure of a DLT system. Depending on the view taken on the points in section 2 above, different answers to this question present themselves.

5. EXISTING LEGAL CONCEPTS

Most commentators consider the relevance and applicability of existing legal concepts to those systems. The analysis often involves making a choice between:

- existing contract theory (generally considering the enforceability of smart contracts by mapping the elements of a contract onto new systems); or
- the operations of the new technology, generally considering the question which is often framed as "code as law" (borrowing from Lawrence Lessig in *Code and other laws of cyberspace* (1999)).

We take two examples of the different approaches.

In the first case, Herbert Smith Freehills (in 'Hashing Out the Implications of Smart Contracting under English law') provides a walk-through analysis of each element of a conventional contract in the context of a blockchain system. Although outside the scope of the HSF note there is, however, scope for applying the elements of a contract to DLT technology if viewed from the perspective of the technology rather than the contract. This would include, for example establishing consideration for a contract through the "cost" of membership of the network.

In this second case, Zetzsche, Buckley and Arner argue against the "code as law" suggestion for regulation. Their view is that the law covers all relations among people and property. It is exhaustive and so analysis of blockchain by definition must fit within the existing framework.

6. JURISDICTIONAL ISSUES

Many commentators note that true decentralisation implies that enforcement of obligations must be effected through the system. A permissioned system may include conventional governing law and jurisdiction provisions within a contractual framework established by terms and conditions or an agreement between parties establishing a network. A permissionless system must rely on non-contractual remedies, such as remedies in the system, because it is extremely complex to establish jurisdiction.

Lord Hodge, a UK Supreme Court Justice (in a speech made at East China University of Political Science and Law in October 2018) notes issues with the cross-jurisdictional nature of DLT. He notes, among other things, the role that international arbitral bodies would perform.

The Law Society (in 'Horizon Scanning – Blockchain: The Legal Implications of Distributed systems') notes that "jurisdictional confusion" may be caused by servers and nodes being in multiple jurisdictions.

The Financial Markets Law Committee has considered questions of governing law and the application of conflict of laws rules, proposing several potential solutions ('Distributed Ledger Technology and Governing Law: Issues of Legal Uncertainty' (March 2018)).

7. REGULATION

Developments in this area are of interest to regulatory lawyers since the technology is used by businesses that operate in regulated environments, such as financial services and technology businesses. Commentators have identified numerous issues:

A Sotiropoulou and D Guegan (in 'Bitcoin and the challenges for financial regulation') note that regulators must put in place frameworks to protect against risks but in a way that does not restrain innovation.

They identify aspects of bitcoin that may be subject to regulation:

- the Bitcoin system itself;
- the uses of Bitcoin; and
- the members of the Bitcoin system.

In the UK, a joint report by HM Treasury, the FCA and the Bank of England Cryptoassets Taskforce notes that cryptoassets are a particular concern and will be monitored closely by them. It states that the most immediate priorities for the authorities are:

- to mitigate the risks to consumers;
- market integrity; and
- to prevent the use of cryptoassets for illicit activity.

The report highlights key risks including:

- risks of financial crime;
- risks to consumers;
- risks to market integrity; and
- financial stability.

Following the Cryptoasset Taskforce report, the FCA has consulted on cryptoassets guidance (January 2019) and plans to make a Policy Statement on cryptoassets in summer 2019, as well as publishing a consultation on potentially banning the sale to retail customers of derivatives linked to certain cryptoassets (in 2019). (https://www.fca.org.uk/firms/cryptoassets).

Trevor I Kiviat (in 'Beyond Bitcoin: Issues in Regulating Blockchain Transactions') notes that current blockchain regulation is focussed towards the application of blockchain for virtual currency and that guidance and regulation outside the financial sector may be required. He states that it is important for regulators to establish risk mitigating provisions, but these must not be so wide as to prevent innovation and the use of blockchain's non-financial utility.

An ISDA White Paper titled *Smart Derivative Contracts: From Concept to Construction* notes that frameworks will need to be devised in relation to the future direction and regulation of these systems.

8. GOVERNANCE

In an area where there are questions about the legal structure of what is being analysed, inevitably there are questions about the possible approaches to governance and which is most appropriate.

Nouriel Roubini (in 'The Big Blockchain Lie', October 2018) states that code as law is not viable because it hands too much power to developers. This suggests that a truly decentralised and autonomous system would be problematic precisely because it leaves no room for governance in the traditional sense.

Nir Kabessa, President of Blockchain at Columbia University, (in 'After Ethereum Classic Suffers 51% Hack, Experts Consider – Will Bitcoin Be Next') states that, while difficult, attacks on the larger cryptocurrencies are no longer out of reach. This suggests that any governance system would involve inherent risk as a consequence of the nature of the underlying technology.

Zetzsche, Buckley and Arner note that new technology may redefine old words. "Governs", includes "*de facto*" governance, that is, the group that controls the ledger by having the "technical ability and opinion leadership to prompt a 'hard fork' of the system".

9. REMEDIES: IN PRINCIPLE

The original Bitcoin White Paper stressed the importance of transactions not being reversible. Irreversibility is a function of Bitcoin, deliberately designed to reduce transaction costs and improve efficiency.

Tatiana Cutts of the London School of Economics and Political Science (in 'Modern Money Had and Received', *Oxford Journal of Legal Studies*) sets out the nature of remedies in relation to "bank money" (contrasted with physical cash) which provides very useful analytical background to this topic in its widest sense.

Tendon and Ganado note that consumers could be protected under the mooted Maltese system by requiring the innovative technology arrangements to meet certain requirements (including, for example, insurance) before being registered as a legal person, building on their analysis as noted in sections 2 and 3 above.

10. REMEDIES: TORTS RELATING TO DIGITAL ASSETS

As the law develops the courts may be asked to find remedies for perceived wrongs inflicted by or in connection with the systems. These may include duties of care that could address questions of implications of the systems for those established by contract.

11. REMEDIES: EQUITY, UNJUST ENRICHMENT

In a permissionless system, there is no contract framework to address unexpected outcomes. Lord Hodge sees a case for unjust enrichment to provide a remedy: "it is unlikely a court could interfere with the running and performance of self-operating code, the law of unjust enrichment is suggested as a possible remedy". There may be other equitable remedies, or extensions of equitable remedies that could be applied to the question of these systems, for example, in the nature of trusts arising by operation of law, equitable tracing, rectification, fiduciary obligations or equitable compensation, for example. But, of course, not all jurisdictions recognise such remedies.

Professor Sarah Green suggests that the equitable remedy of rectification is likely to become more significant (Sarah Green, 'Smart contracts, interpretation and rectification' (2018) 2 *Lloyd's Maritime and Commercial Law Quarterly* 234-251).

12. PROPERTY RIGHTS AND DIGITAL ASSETS

The status of digital assets generally and in the context of property laws is not settled but is coming to the top of the list of issues for policymakers.

Lord Hodge notes that it will be necessary to achieve a degree of international legal consensus on the nature of digital assets as property rights.

Cutts argues that recognition of digital assets would enable clearer analysis of remedies.

Bacon, Michels, Millard and Singh consider the legal classification of digital assets and suggest that until this question is

Biog box

Charles Kerrigan is a partner in the Banking & Finance group at CMS London. Email: charles.kerrigan@cms-cmno.com

Siobhan McKeering is a team lawyer in the Commercial and Common Law team at the Law Commission of England and Wales. Email: siobhan.mckeering@lawcommission.gov.uk

settled by case law or legislation, it will cause consternation for lawyers in a wide range of cases (in 'Blockchain demystified: a technical and legal introduction to distributed and centralised ledgers' (2018) 25(1) *Richmond Journal of Law & Technology*).

In the recent decision in *B2C2 v Quoine Pte Ltd* [2019] SGHC (I) 03 (concerning the reversal of crypto currency trades), the parties appear to have been prepared to assume that both Bitcoin and Ethereum should be treated as property. Simon Horley LJ said that he considered that was the correct approach, considering the definition of a property right in *National Provincial Bank v Ainsworth* [1965] 1 AC 1175. However, given that this was not disputed by the parties, the judge did not need to consider the question further.

13. DATA PROTECTION

The European General Data Protection Regulation raises at least two issues in particular in this context. First: is pseudonymous information personal data? Second: how can a "right to be forgotten" be consistent with an immutable ledger? Other jurisdictions have legislation raising similar questions (highlighted, for example, by the French data protection authority, the CNIL, in October 2018). See also G Spindler and P Schmechel, 'Personal Data and Encryption in the European General Data Protection Regulation' (2016) vol 7(2) *Journal of Intellectual Property, Information Technology and E-Commerce Law* 163.

Other issues include how the immutable nature of blockchain can be reconciled with principles of data minimisation and storage limitation and the potential difficulty of identifying the data controller and processor in DLT systems (see European Bank for Reconstruction and Development and Clifford Chance, 'Smart contracts: legal framework and proposed guidelines for lawmakers' (October 2018), and Bacon, Michaels, Millard and Singh, 'Blockchain demystified: a technical and legal introduction to distributed and centralised ledgers' (2018) 25(1) *Richmond Journal of Law & Technology*).

There is a need for a clear and internationally consistent solution, particularly with regards to public blockchains.

14. COMPETITION, ANTI-TRUST AND CONSUMER PROTECTION

Again, consumer protection rules differ by jurisdiction. The European Union in particular has devoted time to this issue.

In November 2017 the Council of the European Union issued regulation 2016/0148 stating that:

> "Effective consumer protection needs to respond in particular to the challenges of the digital economy and the development of cross-border retail trade in the EU."

The regulation is part of the policy work connected to the Digital Single Market. The aim is to "strike a balance between the interests which are protected as fundamental rights such as a high level of consumer protection, the freedom to conduct business and the freedom of information".

In April 2018 a proposal was brought forward to update the European Union Consumer Rights Directive to address "various consumer issues, including penalties for infringements, transparency on online marketplaces, protection for consumers of 'free' digital services, the right of withdrawal and dual quality of products".

These regulations and proposals have some relevance to blockchains and DLT but it will be apparent that this is only indirect. In particular, it may be appropriate to look beyond direct effects on retail customers by extending the scope of parties deserving of protection in this context and to consider the impact of indirect effects.

In the US a more directly interesting question has recently been considered by a regulator. This concerns the situation where the operation of algorithms developed by multiple parties has the effect that the systems collude in fact but not by design and that no persons are directly involved in the collusive practices.

Maureen K Ohlhausen, Acting Chairman of the US Federal Trade Commission (in United States of America Federal Trade Commission, 'Should We Fear The Things That Go Beep In the Night? Some Initial Thoughts on the Intersection of Antitrust Law and Algorithmic Pricing') suggests it may be the case that no breach of anti-trust rules is committed.

One of the reasons that this is interesting is that it suggests that in order for there to be some prospect of allocating responsibility and liability in these cases, the system should have legal personality, at least so far as is needed to bring a suit against it. Otherwise there will be lacunae.

15. TAXATION

Taxation policy in a digital economy is one of the most intensively considered topics in this area. The UK government's consultation on *Corporate tax and the digital economy* closed in January 2018 and results are due to be published shortly. The basis of the debate relates to the ability of businesses to manage their tax affairs in relation to digital services and intangible assets by taking advantage of the ability to choose the location from where these services are provided. Decentralised systems that are not "owned" by any person will only complicate the debate further. ■

Further Reading:

- Mapping the landscape: cryptocurrency disputes under English law: Part 2 (2019) 5 JIBFL 290.
- Smart contracts: can they be aligned with traditional principles or are bespoke norms necessary? (2018) 8 JIBFL 479.
- LexisPSL: Banking & Finance: Practice Note: Blockchain – key legal and regulatory issues.