Blockchain: Developing Regulatory Approaches for the Use of Technology in Legal Services

Dr Anna Donovan

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Distributed ledger technologies ('DLT') offer enormous opportunities for the legal services sector. Beyond economic growth, DLT has the potential to enhance market competition, improve access to justice and strengthen trust in the legal system. Nevertheless, the technology also raises a number of important and increasingly pressing questions that are of concern to legal services regulators, including how best to realise the benefits of DLT whilst protecting public and consumer interests. This report provides an overview of DLT and its implications for the legal sector. In doing so, it explores the global DLT regulatory landscape before setting out a series of considerations for sectoral regulators to consider when developing their strategic approach to this technology.

DLT has received considerable media and industry attention, with numerous claims being made about the capabilities of the technology and its likely impact. Whilst this publicity has helped to encourage critical debate, it can sometimes obscure the true characteristics of DLTs particularly as misleading narratives, such as absolute immutability, can be promulgated. Against this, there is a risk amongst market participants of both over and under-confidence as to the use cases for DLT and a lack of clarity as to its interplay with existing legal principles and legislative frameworks. This opacity has far reaching consequences for the profession, not least a potentially stultifying impact on innovation predicated on legal and technical uncertainty. As such, sectoral regulators have an important role to play in understanding the nature and impact of DLT for their sector and thereafter supporting their constituents through education and training programmes. For legal services regulators this role is potentially two-fold, not only ensuring that legally trained service providers have the requisite technical understanding to discharge their professional obligations but also helping to support DLT developers to appreciate the legal implications (and foundations) of the products that they are building.

The potential value and transformative impact of DLTs is such that there is now acute international attention and regulatory activity in this space (which is explored in part three of the report). Whilst much of this activity has been legislative in nature, many lessons can be learned that are relevant to legal services regulators. As part three highlights, regulation to date raises the perennial challenges of when to regulate a new technology, how to define new (and continually developing) technologies, the risk of over or under regulating and whether to regulate the technology itself or to adopt a technology-neutral approach (that focuses on the relationships that are created, not a specific technology). These questions emerge at a time when a number of technological advances are being made and this raises a further consideration as to the extent to which a jurisdiction can adopt a coherent and principled approach to disruptive technologies more generally.

Against this background, part four advocates a cautious approach to regulating nascent technologies (although some type of intervention will no doubt be needed to provide, if nothing else, clarity as to the classification of DLT activities thereby providing certainty as to the application of existing frameworks). Instead it offers a continuum of activities that regulators can consider, including supporting multi-disciplinary research projects, offering education and training programmes and standards setting. These activities are complementary, with one building on the other. Together they enable the creation of a multi-disciplinary network of stakeholders that can collaborate to identify real risks and opportunities whilst supporting the sustainable development of the DLT ecosystem. In doing so, legal services regulators can play a key role in ensuring that the sector is (and is seen to be) a vital constituent that supports, rather than impedes, DLT innovation and investment whilst protecting public and consumer interests.

INTRODUCTION

Distributed ledger technology ("**DLT**") has the potential to fundamentally disrupt how individuals and businesses engage with each other. It facilitates the disintermediation of services that have traditionally relied upon the use of a trusted third party, enables the automation of contractual performance and offers a reliable store of data that could transform how we register, record and transfer title.[1] These capabilities offer significant opportunities for those in the legal services sector, facilitating the reduction of transaction costs,[2] increasing access to justice and supporting greater competition within the market. However, the use of DLTs does carry certain risks that raise increasingly pressing questions of regulatory intervention, content and design. For legal services regulators, these questions can be particularly acute, necessitating not only a consideration of the general principles of better regulation,[3] but also a careful balancing of the regulatory objectives,[4] some of which may stand in seeming conflict with each other in this context.

The focus of this report is to explore the potential impact that DLT has for the sector to help legal services regulators structure their response to this particular technology.[5] However, a general note of caution should be raised from the outset. Increased DLT adoption by traditional service providers has occurred at the same time as the introduction of a number of other disruptive technologies, artificial intelligence being a prime example.[6] Whilst each technology raises its own, specific, concerns (that should be addressed accordingly) it is important that these technologies are considered in the round to ensure that a coherent and, where appropriate, consistent regulatory framework is adopted. This minimises the risk of a piecemeal and patchwork governance structure emerging, which could undermine certainty, potentially inhibit innovation and, crucially, restrict the ability to respond to new developments in a principled manner as the technologies mature.

In this regard, whilst the report raises a number of specific issues to consider in respect of DLT regulation, these coalesce around the following four general themes, which underpin the continuum of regulatory considerations outlined in part four:

- The first is the fundamental importance of ***education and training***. Whilst DLT expertise is developing across pockets of the legal services sector (including consumers of legal services), this is by no means absolute and a significant proportion of the community has

[1] See for example HM Land Registry's Digital Street initiative.

[2] Including the 'mental' transactions costs incurred in anticipating, and negotiating the consequences of, a breach of contract. See: Nick Szabo, 'Formalizing and Securing Relationships on Public Networks,' (1 September 1997) 2(9) First Monday available at <https://firstmonday.org/ojs/index.php/fm/article/view/548/469.DOI:http:/dx.doi.org/10.5210/fm.v2i9.548> accessed 29 March 2019.

[3] Namely, that regulation should be 'transparent, accountable, proportionate, consistent and targeted' (Legal Services Act 2007, s 3(3)(a)).

[4] Legal Services Act 2007, s 1.

[5] As with all strategic decisions such as this (although this is, perhaps, particularly acute when considering nascent technologies), any such response will need to be kept under review, both periodically and in response to trigger events.

[6] These technologies have, of course, been available for many years. However, it is only recently that we have seen their widespread adoption by the profession. For more details on legal services adoption see: Legal Services Board, 'Technology and Innovation in Legal Services – Main Report,' (November 2018) available at < https://research.legalservicesboard.org.uk/wp-content/media/Innovation-survey-2018-report-FINAL-2.pdf> accessed 19 May 2019. For general adoption and investment trends in DLT see: Michael del Castillo, Blockchain 50: Billion Dollar Babies (16 April 2019, Forbes) available at <https://medium.com/blockdata/breaking-down-the-forbes-blockchain-50-2f44e9902537> accessed 19 May 2019.

limited engagement with the technology. This lack of common knowledge exposes consumers to potential risk, creates a wariness towards or, conversely, misplaced confidence in, adoption and can impede innovation in developing and deploying DLT in the sector.

- Building on this first theme, the second issue concerns the (actual or perceived) ***lack of legal and commercial certainty*** relating to DLT activity. This raises a broad range of issues that are outside the scope of this report, such as the legal status and classification of cryptoassets or smart contracts.[7] However, it also encompasses concerns as to how sector-specific regulators are going to address the issue of DLTs and decentralised applications. Commonly, a technology-neutral approach to regulation is adopted and this is an approach that, for example, the Financial Conduct Authority ('**FCA**') has confirmed that it is currently continuing to take with regard to DLT.[8] Nevertheless, this does not of course obviate intervention, giving rise to questions as to when regulators might intervene, what form such intervention will take (a number of regulators have, for example, issued guidance notes to provide clarity as to whether decentralised applications fall within the remit of existing regulatory frameworks),[9] who may be subject to regulatory attention and for what purpose.

- The third theme of the report addresses the ***speed of technological development***, our concomitant (and changing) understanding of this nascent technology and the implications that this has for regulatory decision making. This relates to what Roger Brownsword describes as a 'dynamic'[10] regulatory environment. That is, the rapid development of both DLT and our perception of it is such that the regulatory parameters and concerns that exist today may look very different in six months' time. Thus, whilst not a bar to regulation, it is crucial that we are cognisant of our own state of knowledge (and that of the market) before pursuing a legislative strategy, whilst remaining cognisant of the fact that intervention (if needed) should not be left so late that a resistance to regulation has developed.[11]

- Finally, and aligned with this third concern, the report highlights the critical need for ***multi-disciplinary stakeholder engagement***. Adopting an early, inclusive, thorough (and ongoing) approach to stakeholder consultation will be crucial to ensure that regulator activities are comprehensively debated, predicated on robust technical understanding, respond to genuine commercial activities and reach the right balance between protecting consumer interests and supporting market innovation. However, stakeholder consultation is more than an exchange of information. It is an important component in building a community of

[7] These questions are the subject of a consultation currently being undertaken by the UK Jurisdiction Taskforce of the UK LawTech Delivery Panel, available: <https://www.lawsociety.org.uk/news/stories/cryptoassets-dlt-and-smart-contracts-ukjt-consultation/> accessed 19 May 2019.

[8] FCA, *Guidance on Cryptoassets* (Consultation Paper CP19/3, January 2019), 3.

[9] Ibid. See also: the Securities and Exchange Commission's *Report of Investigation on Coin or Token Offerings* (Release No. 81207, 25 July 2017) and their 'Spotlight on Initial Coin Offerings' 22 February 2019 <https://www.sec.gov/ICO> accessed 29 March 2019.

[10] Roger Brownsword and Karen Yeung 'Regulating Technologies: Tools, Targets and Thematics' in Roger Brownsword and Karen Yeung (eds.) *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes* (Hart Publishing 2008), 5.

[11] See Roger Brownsword's discussion of Collingridge's Dilemma in: Roger Brownsword, 'The Regulation of New Technologies in professional Service Sectors in the United Kingdom: Key Issues and Comparative Lessons' (July 2019), 13. Available at: < https://www.legalservicesboard.org.uk/our-work/current-work/technology-and-regulation> accessed 25 July 2019.

interested parties, who feel adequately consulted and represented, thereby enhancing the legitimacy of regulators' activities.[12]

Against this background the report proceeds as follows. Part one provides an overview of distributed ledger technology. Mindful of the fact that this report cannot present an exhaustive analysis of all technical aspects of DLT and distributed applications, it nevertheless sets out a detailed distillation of the characteristics that are particularly pertinent for legal services and that have the greatest implications for the regulatory objectives (such as blockchain's proof-of-work consensus mechanism).[13] It also explains the distinction between permissionless and permissioned ledgers, the latter being the dominant architecture currently engaged by financial and legal services providers. Part one also includes a discussion of some of the more general barriers to adoption, such as the public perception of DLTs and the increasing importance of the narrative that has emerged when discussing the technology, particularly in the legal sector.

Having outlined the underlying platform technology in part one, part two introduces the key applications of DLT, such as smart contracts and initial coin offerings. It should be made clear that it is the *applications* that are built on the technology, rather than the underlying ledger technology itself, that are likely to be of immediate concern to regulators (although as part one explains, understanding ledger technology is crucial to identifying the regulatory implications of such applications). In discussing these applications, part two explores the key opportunities and risks that DLTs present to the sector together with their relevance to legal services regulation. For example, DLT has significant potential to reduce transactions costs, increase access to justice and support access to new capital markets. However, it also gives rise to concerns such as the current lack of consumer knowledge and a perceived opacity as to the application of existing rules and regulations to DLT based transactions. As outlined above, this uncertainty risks not only consumer harm but also the delay of DLT adoption and development.

Part three sets out a high level overview of international regulatory approaches to DLT. Given that DLT is an emerging technology, this part does not focus on the responses of legal services regulators (which have been limited and generally take the form of advisory communications),[14] instead it outlines the broad landscape of DLT regulation. This enables an examination of the variety of regulatory approaches that have been engaged and the policy decisions that underpin them. When considering these regulatory responses the mischief that they seek to address and the potential unintended consequences of any legislative response must be kept in mind. For example, providing

---

[12] Victor Bekkers and Arthur Edwards 'Legitimacy and Democracy: a Conceptual Framework for Assessing Governance Practices' in Victor Bekkers, Geske Dukstra, Arthur Edwards and Mennonite Fenger (eds.) *Governance and the Democratic Defecit: Assessing the Democratic Legitimacy of Governance Practices* (Ashgate Publishing 2007), 35.

[13] For a detailed, technical, discussion of the technology see: Paolo Tasca, 'Digital Currencies: Principles, Trends, Opportunities and Risks' (2015) Ecurex Research Working Paper 23. <https://papers.ssrn.com/sol3/papers2.cfm?abstract_id=2657598> accessed 29 March 2019.

[14] Although note that Germany's Free Democratic Party has recently proposed regulating LawTech firms and, in particular, applying oversight and liability to those offering automated legal consultations (something that the Bundestag rejected in 2018). See: Philipp Plog, 'German Politicians Seek to Regulate 'Legal Tech' Companies,' (3 June 2019, Artificial Lawyer) available at <https://www.artificiallawyer.com/2019/06/03/german-politicians-seek-to-regulate-legal-tech-companies/> accessed 3 June 2019. In France, recent regulatory reforms potentially restrict the use of judicial data in litigation prediction services (article 33 Justice Reform Act, reforming the Commercial Code, to prohibit the use of judicial identity data for the purpose of, *inter alia*, predicting decision making). See: 'France Bans Judge Analytics, 5 Years in Prison' (4 June 2019, Artificial Lawyer) available at <https://www.artificiallawyer.com/2019/06/04/france-bans-judge-analytics-5-years-in-prison-for-rule-breakers/> accessed 4 June 2019.

regulatory clarity as to the characterisation of a token for the purposes of securities regulation is helpful. However, care is needed to ensure that defining 'DLT' and 'smart contracts' in one context does not have an unintended impact in another domain (such as the tax and property implications of any such classification). There is also the perennial challenge of defining terms such as this. If drawn too narrowly, a definition (and related provisions) risks being inaccurate, ineffective and can quickly become outdated whilst being susceptible to creative compliance. If the term is too broad, it risks ambiguity and fails to deliver market or consumer confidence. The brief overview of regulatory activity set out in part three helps to demonstrate the increasing pace of global regulatory intervention in this space and it is for this reason that a second note of caution is required. DLT is, of course, a technology without geographical borders. To the extent possible, having a symbiotic global regulatory approach will help support innovation in this space (for example, by facilitating interoperability and minimising the risk of regulatory arbitrage). Part four concludes the substantive parts of the report by setting out a continuum of potential responses that legal services regulators in this jurisdiction may wish to consider, ranging from education and training activities to direct regulation.

PART ONE: DISTRIBUTED LEDGER TECHNOLOGY

To provide context to the discussion of what DLT is, it is helpful to first address the problem that distributed technology is trying to solve.[15] Namely, how can third parties coordinate their behaviour without reliance on a centralised intermediary? Put another way, how can we disintermediate transactions to enable direct contracting between the parties, facilitating faster, cheaper and potentially more accessible and transparent interactions? Accurately quantifying the benefit of solving this issue is difficult at this stage. However, an indication of the potential value that smart contracts offer to the market can be seen from Cap Gemini's estimate that in the personal motor insurance sector alone, the automation and disintermediation offered by smart contracts represents potential global annual costs savings of $21 billion.[16]

Traditionally, most transactions are dependent on a trusted third party such as a bank. Under this model, parties do not need to trust each other, as they are reliant instead on the fact that the intermediary will act in accordance with its instructions whilst maintaining an accurate ledger of account. For example, if Alice wants to transfer funds to Bob, Alice and Bob rely on the fact that: (i) the bank will check that Alice has sufficient funds to make the transfer; and (ii) that having verified Alice's account the bank will only transfer the amount of funds that Alice has asked it to. Thereafter, Alice, Bob and subsequent third parties that Alice might engage with, rely on the fact that the bank will update Alice's record of account to reflect the transfer (avoiding a subsequent 'double-spend' of funds). There are three critical challenges with this model. First, not everyone can access the intermediary, for example there are large numbers of people who do not have access to traditional banking services. Secondly, it can be inefficient, with multiple points of friction and manual intervention. As such, it is not only a time-consuming operation (sometimes taking several days to complete a payment transfer for example) but it also involves relatively significant transaction costs. Finally, as a centralised (as opposed to distributed) system, it is more susceptible to single points of weakness or failure.[17]

[15] This question looks at the functional issue of centralisation, rather than the broader philosophical foundations that for some drive the adoption of decentralised technologies.

[16] Cap Gemini, 'Smart Contracts in Financial Services: Getting from Hype to Reality,' available at < https://www.capgemini.com/consulting-de/wp-content/uploads/sites/32/2017/08/smart_contracts_paper_long_0.pdf> accessed 22 July 2019.

[17] Although as set out in part 1(ii) permissioned ledgers are similarly susceptible to risks arising from centralised control models.

Against this, the problem that DLTs sought to address was whether a system could be developed that 'manufactured'[18] trust between the parties directly, such that a centralised third party was no longer required. That is, the trust vested in the system itself, not a single entity. However, this distributed model is not without its own challenges.[19] In particular, a crucial issue that DLT had to address was to ensure that the information that the system relies upon to achieve consensus is accurate and that network participants can be trusted.[20] It is the solution that DLTs developed to address this question (such as the proof-of-work mechanism adopted by the bitcoin blockchain) that gives DLTs such transformative potential and that are explained in more detail below.

(i) Permissionless (and public)[21] ledgers

DLT first came to public attention in 2008 when Satoshi Nakamoto[22] published the white paper 'Bitcoin: A Peer-to-Peer Electronic Cash System' (the '**White Paper**').[23] The White Paper described the key features of the cryptocurrency 'bitcoin,' which was designed to facilitate relatively low-cost and fast online payments (including micro-payments) without the need for a financial intermediary.[24] However, the importance of the White Paper for legal services was not the cryptocurrency *per se* but the solution that the White Paper offered to the double-spend problem that would otherwise still exist (even with cryptocurrencies). That is, the White Paper outlined the use of a DLT platform (that came to be known as the 'blockchain')[25] that relied upon 'cryptographic proof instead of trust,'[26] supported by publicly announced and time-stamped transactions.

In high level terms,[27] like its off-chain counterparts, the blockchain operates as a ledger of account but rather than being held by a single, central, server it is distributed and replicated across all of the computers in the network (known as 'nodes'). Whilst the bitcoin blockchain is concerned with recording ownership of bitcoin, DLTs can (like off-chain ledgers) record any type of data. For example home ownership,[28] asset provenance[29] and voting records.[30] On the blockchain, the ledger

[18] Don Tapscott and Alex Tapscott, *Blockchain Revolution, How the Technology Behind Bitcoin is Changing Money, Business and the World* (Portfolio Penguin 2016), 5.

[19] This is in addition to the general criticism that can be levied, namely that DLT is sometimes promoted for use in situations where existing technology would suffice.

[20] This is the so-called 'Byzantine General's Problem.' See: Leslie Lamport, Robert Shostak and Marshall Pease, 'The Byzantine General's Problem' (1982) 4(3) ACM Transactions on Programming Languages and Systems, 382.

[21] Public has been included in parentheses as whether a ledger is public or private is separate to the question of whether it is permissionless or permissioned. Whether a ledger is public or private concerns whether permission to *view* the ledger is required. In contrast, as this part explains, whether a ledger is permissionless or permissioned refers to the consent (or otherwise) required to *submit* a transaction to the ledger. Whilst not universally the case, permissionless ledgers are generally public whereas permissioned ledgers are commonly private.

[22] Satoshi Nakamoto is a pseudonym, the identity of the author(s) is not known.

[23] (2008) https://bitcoin.org/bitcoin.pdf accessed 29 March 2019. The term 'white paper' is used here in its colloquial sense to describe a high-level proposal or explanatory document. To be clear, the bitcoin white paper has no governmental association.

[24] Nakamoto (n 23), 1.

[25] The terms 'blockchain' and 'DLT' are often, erroneously, used interchangeably. However, they are in fact distinct (albeit similar) technologies.

[26] Nakamoto (n 23), 1.

[27] For a more detailed analysis see: Anna Donovan '(Shadow) Banking on the Blockchain: Permissioned Ledgers, Interoperability and Common Standards' in Iris Chiu and Iain MacNeil (eds.) *Research Handbook on Shadow Banking* (Edward Elgar 2018), 314.

[28] See for example HM Land Registry's first end-to-end freehold title transfer using DLT as part of its Digital Street research initiative. For more details see: Lauren Tombs, 'Could Blockchain be the Future of the Property

comprises of 'smaller datasets referred to as "blocks"'[31] with a new block being added approximately every ten minutes regardless of whether there have been any independent transactions (besides the coinbase).[32] Importantly, the ledger operates on an append-only basis; blocks are added in chronological order and joined together via the hash (or digest) of the immediately preceding block. In this way, a chain of cryptographically linked blocks is created, hence 'blockchain.'

The hashing function is central to the operation of the blockchain, providing the basis for the proof-of-work consensus mechanism (discussed below) and the characterisation of the ledger as 'immutable.' Hashing is the process by which the hashing algorithm (in the case of blockchain 'SHA-256') is applied to input data (of any length) to turn it into an output of a fixed length (the 'hash' or 'digest'). Save in very rare circumstances, the hash is unique to the corresponding input data; if the same input data is used the same hash will be produced.[33] Conversely, if different input data is used (even if only by one digit) then a different hash will be produced. As such, the hash can be thought of as a digital fingerprint and it is this digital fingerprint that links the blocks in the chain together.

As figure 1 demonstrates, the input data (that is, the data contained in any one block) that generates the hash for any given block is comprised of: (i) a time stamp; (ii) the transactions for the relevant time period;[34] (iii) the hash (or digest) of the previous block; and (iv) the 'nonce' (an abbreviation for 'number only used once,' which is discussed further below). The consequence of this is that if any aspect of these components is changed, then the hash for that block will change (as a change to the input data results in a change to the output or hash). However, if the block has already been 'sealed,' namely the block's data has been hashed and the next block added to the ledger, then no further changes to the original block are possible. This is because the original hash of the first block has already been included in the next block (and effectively each subsequent block thereafter as each block's hash forms part of the input data for the following block). It is this feature that renders the blockchain, in practical terms, immutable.[35] If a malicious actor wants to tamper with an earlier block (changing the input data and therefore the hash of that block), it would also need to amend every subsequent block to reflect the change in hash of the altered block. Whilst it is technically possible to alter the chain in this way, as we shall see next, blockchain's proof-of-work consensus mechanism effectively prohibits this type of fabrication (due to the sheer size of computing power it would require), rendering the ledger virtually immutable.[36]

Market,' (24 May 2019, HM Land Registry) <https://hmlandregistry.blog.gov.uk/2019/05/24/could-blockchain-be-the-future-of-the-property-market/> accessed 26 May 2019.

[29] See for example: www.everledger.io that uses DLT to track the provenance of diamonds, keeping records of payment transactions, details of each individual diamond (including photographs and serial numbers) and certificates of authenticity.

[30] For example, West Virginia used a blockchain based voting system for those citizens eligible to use online voting pursuant to the Uniform and Overseas Citizens Absentee Voting Act.

[31] Aaron Wright and Primavera De Filippi, 'Decentralized Blockchain Technology and the Rise of Lex Cryptographia,' (2015) 6 <https://ssrn.com/abstract=25806642> accessed 29 March 2019.

[32] The coinbase transaction is mandatory for all blocks and refers to the payment of the block reward to the successful miner pursuant to the proof of work consensus mechanism (see text accompanying footnote 37).

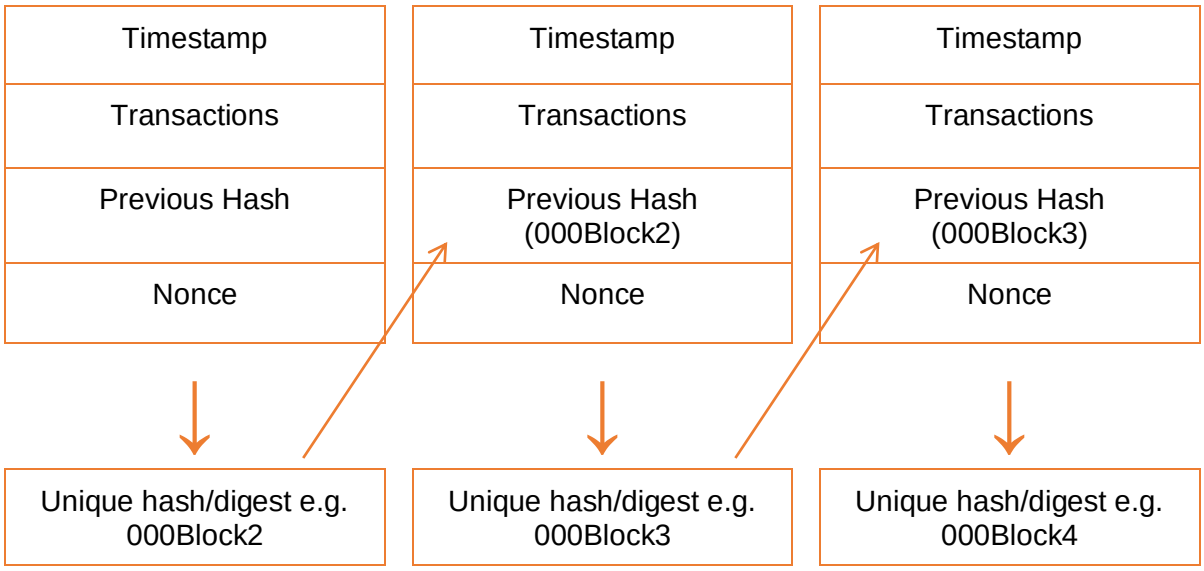
[33] Whilst 'hash collisions' (i.e. two different data sets producing the same hash) are possible these are rare. See: Ralph C Losey, 'Hash: the New Bates Stamp' (2007) 12 Journal of Technology, Law and Policy 13

[34] More accurately, this is a hash of a data structure known as a 'Merkle tree' that stores the transactions in the block. For a more detailed explanation of this see: Ethereum White Paper, 'A Next-Generation Smart Contract and Decentralized Application Platform' <https://github.com/ethereum/wiki/wiki/White-Paper#applications> accessed 29 March 2019 (the '**Ethereum White Paper**').

[35] Although see the discussion on hash attacks below.

[36] The exception being where a miner (or group of miners) controls the majority of the network's nodes, introducing the risk of a 'hash attack,' discussed in part 1(ii).

Figure 1: Abbreviated Example of Blockchain's Hash Function (SHA-256)



To validate a block (thereby sealing it and adding it to the ledger of account), blockchain adopts a proof-of-work consensus mechanism.[37] That is, to verify a block nodes on the network (known as 'miners') compete to complete a proof-of-work exercise. This is where the 'nonce' referred to above becomes relevant. Miners, who possess the other data components of the block (that is the transactions relating to that block and the hash of the previous block), compete with each other to identify an effective nonce (an arbitrary number) to complete the input data and produce the requisite hash. The hash to be calculated is specified at a certain difficulty to help regulate the network (to keep block additions at approximately ten minute intervals). This is achieved by requiring that the hash must have a specific number of zeros at the beginning; the greater the number of zeros the more difficult it is to calculate.

For a block's hash to be generated, miners compete to identify the appropriate nonce value. This is an extremely challenging mathematical exercise and can, effectively, only be solved by 'brute force.'[38] That is, the miners cannot apply logic or reason to determine a valid nonce, rather they must simply continue to try number after number until the right hash (or output) is produced (it is for this reason that the proof-of-work system incurs significant central processing unit '**CPU**' usage).[39] Once a miner (or pool of miners) thinks it has identified a valid nonce the rest of the network applies the hashing algorithm to verify the nonce (acting by a majority calculated by

[37] Other mechanisms exist, such as proof-of-stake, which seek to address some of the challenges of the proof-of-work model (such as its speed and energy consumption). However, these alternative mechanisms are not without their own problems (such as the risk that in a proof-of-stake ledger multiple block histories can be voted on, the so-called 'nothing at stake' problem). Technical solutions to these issues exist but it is important to be aware of the fact that most consensus mechanisms have a number of characteristics that need to be considered to properly evaluate their risks and benefits. For a more detailed description of the nothing at stake problem see: Vitalik Buterin, 'On Stake' (5 July 2014, Ethereum Blog) <https://blog.ethereum.org/2014/07/05/stake/> accessed 2 May 2019.

[38] See: Adam Back, 'Hashcash – a Denial of Service Counter-Measure,' (1 August 2002) <www.hashcash.org/Hashcash.pdf> accessed 29 March 2019. One function of making the hash calculation so difficult is to protect against what is known as a 'sybil' attack, which is where a malicious actor creates multiple identities to obtain undue influence and control of a peer-to-peer network.

[39] The difficulty and energy required to identify the nonce can be seen from the current hash rate (the estimated number of hashes on the bitcoin network), which is 44, 078, 986 trillion hashes per second. See: <https://blockchain.info/charts/hash-rate> accessed 29 March 2019.

reference to one vote per CPU) and, if approved, seal the block. In contrast to a traditional, centralised, system there is no human intervention or discretion (that is, no single point of error) the nodes simply apply the network's consensus rules to determine whether the block has been appropriately validated. The successful miner is rewarded by the allocation of the ledger's native cryptocurrency (this is known as the 'coinbase' transaction), motivating the miner to perform the functions necessary to enable the decentralised model to function.

Explained another way, this hashing function can be understood by reference to the analogy of a combination padlock. If we give a locked combination padlock to someone (a miner) to 'solve' it will likely take them a significant amount of time to find the right code. To do so, they will have to simply try different number combinations until they find the right one. However, when they return the padlock (to the network) to confirm that they have identified the right code it is easy to verify whether they have identified the correct number; all the network has to do is apply the proposed code to see if the padlock opens.

There are three important characteristics of the proof-of-work model that combine to ensure the integrity and operation of the ledger. First, proof-of-work requires that an extremely difficult cryptographic puzzle is resolved through brute force. The difficulty (and cost) of this activity makes it, practically, difficult (if not currently impossible) for a minority of the mining pool to fraudulently amend or add a block. Secondly, and conversely, once a miner thinks it has identified a valid nonce, it is exceptionally easy for the network to verify that nonce. Recall that the same input data (block data including the nonce) will produce the same output data (or hash). Therefore all the network has to do to verify the nonce is apply the hashing algorithm to the complete input data set to confirm that a correct hash has been produced. Finally, it adopts an incentive mechanism through the allocation of bitcoin (or other relevant cryptocurrency) to the successful miner to ensure that the network continues to operate successfully.

One final point of definition is needed. The bitcoin blockchain is a permissionless ledger and, as the name suggests, it is the rules that govern whether a node can join the network that determine whether a ledger is 'permissionless' or not.[40] That is, any node can download the relevant software, join the network and participate in the mining process. In addition, blockchain is a public ledger as, similarly, any party can view and submit transactions.[41] In this way, a somewhat rudimentary but nonetheless useful analogy is to compare a permissionless ledger to the Internet whereas a permissioned ledger (discussed in the next section) is akin to an organisation's intranet.

It is the permissionless and public nature of ledgers such as blockchain that allow parties to transact with a high degree of pseudo-anonymity. Parties to the ledger do not need to reveal their personal identities or 'true names,'[42] with transactions being sent instead to their wallet address. Therefore, it should be made clear that it is technically possible (if not always easy) to identify an individual participant if their wallet is linked to their real identity. In addition, if the wallet is used for multiple

[40] Angela Walch, 'The Bitcoin Blockchain as Financial Market Infrastructure: a Consideration of Operational Risk' [2015] 18 NYU Journal of Legislation & Public Policy 837, 844.

[41] Gareth W. Peters and Efstathios Panayi, 'Understanding Modern Banking Ledgers Through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money' in Paolo Tasca, Tomaso Aste, Loriana Pelizzon and Nicolas Perony (eds) *Banking Beyond Banks and Money, a Guide to Banking Services in the Twenty First Century* (Springer International 2016), 244.

[42] An identifier such as a person's birth name that 'links many different kinds of information about a person.' See: Nick Szabo, 'Smart Contracts: Building Blocks for Digital Markets,' (1996) available at < http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html> accessed 22 July 2019.

transactions then this too can contribute to a growing understanding of the user's real identity.[43] As such, whilst claims to complete anonymity on a permissionless ledger are often over-stated, identification on a permissionless ledger is nevertheless a crucial issue, particularly when looking at regulated activities.[44]

Table 1: Advantages and Disadvantages of Permissionless and Public Ledgers

Advantages	Disadvantages
Consensus mechanism manufactures trust between unknown parties	Proof-of-work consensus mechanisms require significant computing power (alternative approaches are now being explored)
Disintermediation reduces transaction costs associated with third parties	Removes wider gatekeeping function performed by third party intermediaries
Ability to transact on a pseudonymous basis increases participants' privacy	Introduces enforcement risks (and challenges for regulated activities) as off-chain identity is difficult to verify
Network transparency enables the whole community to view the protocol, identify issues and suggest improvements	May not be suitable for transactions where transactional privacy is paramount
Decentralised network means there is no single point of failure	Requires sufficient participant incentivisation to operate the network

(ii) Permissioned (and private) ledgers

Notwithstanding the White Paper's release in 2008, until recently the impact of DLT on legal, financial and other professional services was limited.[45] Arguably, one reason for this was the common conflation at that time of bitcoin the currency with blockchain the platform. During its infancy, bitcoin became synonymous with illegal transactions conducted on the Silk Road (an online marketplace that was eventually closed by the FBI in 2013). The consequence of this public association was that, regardless of the actual distinction between the currency and the platform, a perception issue existed that inhibited the (overt) adoption and development of blockchain technology in professional services.

A second challenge that permissionless ledgers raise for commercial operations is the risk of what is known as a 51 percent or 'hash attack.'[46] As mentioned in part 1(i), the proof-of-work mechanism adopted by the blockchain ensures the proper validation of the network's blocks. However, to validate the hash, only a majority of the nodes need to agree. As such, and as recognised in the White Paper, the 'system is secure as long as honest nodes collectively control more CPU power

[43] The White Paper suggested that users create a separate wallet for each transaction to avoid transactions being associated with a common owner. See: Satoshi (n 23), 6.
[44] In contrast, some criticise the introduction of anti-money laundering and know your customer requirements to decentralised applications as being contrary to the traditional ideology of the technology.
[45] For a more detailed discussion of the reasons for this see: Donovan (n 27), 320-322.
[46] Sometimes also referred to as a 51% attack.

than any cooperating group of attacker nodes.'[47] A permissionless ledger is, therefore, exposed if a malicious miner (or pool of coordinated miners) gains control of the majority of the network's CPU. If this occurs, the group controls the validation process on the ledger and could authorise fraudulent transactions, including double-spending, which was the problem that the blockchain was designed to resolve.

The risk of a mining pool gaining control of the network in this way is not merely a theoretical one. In July 2014 the mining pool 'Ghash.io' crossed the 51% threshold on the bitcoin blockchain. Whilst Ghash.io mitigated concerns by voluntarily agreeing not to exercise their power, they also noted that a long-term solution to the issue of a hash attack (beyond voluntary commitments) had yet to be identified.[48] Indeed, in January 2019, Ethereum Classic was subject to a similar hash attack where an unknown participant managed to effectively alter transactions on the network and validate double spends. These two incidents demonstrate a fundamental risk that is inherent in the current consensus mechanisms used by some permissionless ledgers,[49] one that is considered too big to risk by those looking to develop mainstream commercial applications. As one commentator observed, 'I can tell you from personal experience that boardroom anxiety is greatly diminished the moment you tell them that [DLT applications] can be implemented in a "closed sandbox environment."[50] Indeed, for these reasons (together with privacy and compliance concerns, such as anti-money laundering ('**AML**') and know your client ('**KYC**') requirements) permissionless ledgers have, to date, been thought of as 'unworkable'[51] for financial institutions. It is for this reason that Société Générale's recent bond issue on a permissionless ledger (albeit where Société Générale was both the issuer and investor) was a novel and significant development.[52]

One solution to these challenges, and arguably the technical catalyst for more widespread DLT adoption, was the emergence of permissioned ledgers. These are closed networks that, as the name suggests, require nodes to be approved before joining the network. These ledgers are often (although not exclusively) also private, meaning that participants similarly need to be granted permission to view and submit transactions to the ledger (making these ledgers more appropriate for networks sharing sensitive data). In essence, the trust between ledger participants exists off-chain. The parties' true identities are fully known to each other (they are not pseudonymous) and an onboarding or participation agreement can be signed as a condition of joining. This agreement is a traditional off-chain contract addressing common issues that may arise with a permissionless ledger such as agreeing the applicable law and jurisdiction, the allocation of rights and liabilities together with an agreed upon dispute resolution procedure. Even if such an agreement was not entered into, the lack of anonymity on a permissioned ledger does, of course, facilitate easier interaction with traditional dispute resolution procedures and enable compliance with regulatory requirements (such as AML and KYC checks). By enabling enforcement and regulatory compliance in this way, permissioned ledgers made it possible for mainstream and regulated businesses to engage

[47] Nakamoto (n 23), 1.

[48] The full statement is available at: <https://blog.cex.io/news/official-statement-on-51-threat-and-closed-round-table-6619> accessed 29 March 2019.

[49] These are not the only incidents of hash attacks but are the most well-known, having occurred on two of the most popular ledgers. See: Alyssa Hertig 'Blockchain's Once-Feared 51% Attack is Now Becoming Regular' (coindesk, 8 June 2018) <https://www.coindesk.com/blockchain's-feared-51-attack-now-becoming-regular> accessed 29 March 2019.

[50] R Tyler Smith, 'Public and Private Blockchains: Enemies or Allies? Why the Enterprise Ethereum Alliance Will Prove the Latter' (2017) <https://medium.com/@rtylersmith/public-and-private-blockchains-enemies-or-allies-45f050c38fc0#.8lxlviw5m> accessed 21 July 2019.

[51] Michael Casey, ' A Glimpse of Banking's Future, Live on the Ethereum Blockchain' (29 April 2019, *coindesk*) available at <https://www.coindesk.com/societe-generales-work-with-public-ethereum-is-a-big-deal> accessed 20 July 2019.

[52] Ibid.

more seriously with DLT, whilst also distancing the technology from the perception issues that had arisen with the blockchain. As such, whilst permissioned ledgers are a clear departure from the open, fully transparent and borderless ideologies that underpin permissionless ledgers, they have enabled the deployment of DLTs by regulated sectors. For example, we have now witnessed the transfer of a residential freehold title on a permissioned ledger, a proof of concept deployed as part of HM Land Registry's Digital Street initiative.[53] Permissioned ledger applications are also becoming increasingly prevalent in the banking and insurance sectors, with examples including: 'we.trade' a joint venture between 12 banks (including Deutsche Bank, UBS and Santander) that is designed to increase efficiency and security in cross-border transactions; 'Insurwave' which is a marine insurance platform that is a joint venture between EY and Guardtime; and project Madrec, the collaboration between UBS, Barclays, Credit Suisse, KBC, SIX and Thomson Reuters that used permissioned DLT to facilitate compliance with MiFID II.[54]

Notwithstanding their benefits for regulated activities, permissioned ledgers do raise their own challenges. One consequence of the off-chain relationship between participants on a permissioned ledger, and the existence of a centralised authority that controls the ledger, is that the parties are not looking to the ledger technology itself to generate trust. Rather, they are utilising DLT for its other characteristics, such as the speed and efficiency of on-chain transactions. This enables permissioned ledgers to adopt much more efficient (in terms of time, energy consumption and cost) consensus mechanisms that are, knowingly, under the control of a small number of pre-approved and trusted nodes. One consequence of this return to a more centralised model is that it exposes the ledger to a similar concern (albeit in a different context) to a hash attack, namely that a single entity (or coalition) controls the verification process. However, with a permissioned ledger the participant's protection lies elsewhere, namely in the fact that the parties are known to each other and can enforce the terms of the participation agreement or other legal remedy. Therefore, in a permissioned ledger focus turns to, *inter alia,* off-chain governance and security. For example, what are reasonable procedures to introduce (or mandate) to ensure suitable data governance, reduce the risk of human error and maintain ledger accuracy? These questions are all the more relevant as many permissioned ledgers provide nodes with the ability to pause or potentially even reverse a transaction. This significant departure from the relative immutability of the permissionless ledger provides comfort to those who might be using the technology to engage in substantial financial transactions but similarly demands that systems and controls are in place to ensure that this privilege is not abused. In this way, permissioned ledgers can resemble 'traditional' off-chain databases, leading some to question (not unreasonably) whether DLT is needed in all proposed use cases.[55] Nevertheless, the automation, transparency and efficiency of these ledgers coalesce to continue to offer an attractive use case for deployment.

When considering private ledgers, it is important to be cognisant of the fact that, by their very nature, they are not subject to the same public scrutiny as their permissionless counterparts. Whilst it is this characteristic that has enabled more widespread adoption, it is also means that the ledger's code is not constantly analysed (and potentially improved) by a large DLT community in the same way that the blockchain is. In essence, one of the trade-offs for having clearly identifiable liabilities (for example, to govern any code errors)[56] is that the code does not benefit from the scrutiny of an

[53] Tombs (n 28).

[54] Michael del Castillo, 'UBS to Launch Live Ethereum Compliance Platform,' (11 December 2017, coindesk) available at <https://www.coindesk.com/ubs-launch-live-ethereum-platform-barclays-credit-suisse> accessed 22 July 2019.

[55] For a broader discussion of this question see: Karl Wüst and Arthur Gervais, 'Do you need a blockchain?' (2018) IEEE Crypto Valley Conference on Blockchain Technology 45.

[56] Something arguably lacking from blockchain. See: Walch (n 40), 874.

open source environment, thereby reducing opportunities for mistakes to be identified and remedied before a loss is incurred.[57]

One final point to note regarding permissioned ledgers is that they have introduced a new mechanism for regulated entities to engage with the relevant regulator, namely through the inclusion of a regulator node on the network. Northern Trust (an investment and wealth management firm) adopted this approach in 2017 when it used a permissioned ledger to better manage the administration of a Guernsey-domiciled fund. Northern Trust's rationale for adopting DLT was the increased efficiencies it provided, particularly concerning compliance with client instructions. However, it was the firm's engagement with the Guernsey Financial Services Commission ('**GFSC**') throughout the development and deployment of the ledger that is particularly interesting. Both the construction and operation of the ledger was undertaken in close collaboration with the GFSC and, following deployment, the GFSC has oversight of the ledger's regulator node. The regulator node provides the GFSC with access to a broad range of data, but does not increase the type of information that the Commission was entitled to under the previous system. However, it does facilitate the provision of information to the Commission in 'real-time.'[58] In November 2018, Northern Trust went on to process the first live capital call using DLT for Emerald Cleantech Fund III LP, an endeavour that was again undertaken whilst 'working in partnership with key clients and regulators.'[59]

Table 2: Advantages and Disadvantages of Permissioned and Private Ledgers

Advantages	Disadvantages
Trust exists 'off-chain,' reducing enforcement risk and allowing traditional on-boarding/accession agreements to be signed	Risk of conflict/confusion between off-chain agreements and ledger protocol
Off-chain trust enables faster, cheaper and more scalable consensus mechanisms to be adopted	Centralised control of the protocol introduces potential for single points of failure and collusion, making data and code governance crucial
Transparent to the parties allowing real time access to data, including the use of regulator nodes	Lack of public scrutiny e.g. to identify code risks and opportunities
Ability to control access facilitates ease of adoption in regulated activities	Potentially slows innovation if stakeholder group is restricted

[57] As to the inevitability of 'bugs' in the code see: Derek Bambauer, 'Ghosts in the Network' (2014) 162(5) University of Pennsylvania Law Review 1011.

[58] Michael del Castillo, 'Northern Trust Goes Live with IBM-Powered Private Equities Blockchain (coindesk, 22 February 2017) <https://www.coindesk.com/northern-trust-goes-live-ibm-powered-private-equities-blockchain/> accessed 29 March 2019.

[59] See: <https://m.northerntrust.com/news-financial-statement/press-release?c=871cebb9540c3> accessed 29 March 2019.

PART TWO: DECENTRALISED APPLICATIONS AND USE CASES

The potential impact of DLT on legal and other commercial markets is not derived from the underlying ledger technology *per se* but the decentralised applications (so-called '**dapps**') that are built on top of it. One of the most popular ledgers for building dapps (although by no means the only one) is Ethereum.[60] Ethereum's founders sought to capitalise on blockchain's value as a 'tool of distributed consensus,'[61] realising that given the right scripting language,[62] DLTs had the potential to accommodate more complex applications (and therefore relationships), beyond the unconditional transfer of funds from A to B (which is the intentional limit of the bitcoin blockchain).[63]

Three of these dapps, which are of particular relevance to legal services (and illuminate some of the key opportunities and risks for the sector), are: smart contracts, initial coin offerings and decentralised autonomous organisations. These applications traverse a number of the regulatory objectives, giving significant opportunities to enhance consumer interests but with a concomitant element of consumer risk. For example, all offer the potential to promote the public interest by increasing access to justice, enhancing competition and diversity in the legal services market and reducing transaction costs. Further, if regulatory involvement is approached in the right way, these dapps can help increase confidence in a modern regulatory system and the rule of law through the deployment of a regulatory approach that reflects (and enhances) social and technological developments. However, dapps do also raise a number of questions for legal services regulators to consider, including their implications for the professional principles (for example, in determining the level of technical knowledge that is reasonably required for a legal services provider to meet the expected standard of work).

(i) Smart contracts

Smart contracts were first introduced by Nick Szabo in 1996[64] and further developed in a second paper published the following year (although it was not until the release of the bitcoin White Paper some ten years later that the technology that made smart contracts possible came to public attention).[65] A true polymath (Szabo is a lawyer, cryptographer and computer scientist), Szabo wanted to draw upon the benefits of each of these fields to develop an architecture for commercial agreements that rendered breach of contract prohibitively expensive.[66] It is important to be clear from the outset that Szabo expressly recognised the value of the common law supporting contractual relationships and was not proposing that this be replaced. Rather, he sought to understand how best to 'apply these common law principles to the design of our on-line

[60] The Ethereum network (which is a public ledger) adopts a programming language (Solidity) that enables more complex operations to be executed in comparison to bitcoin's blockchain. Whilst the bitcoin blockchain enables the transfer of bitcoin, Ethereum is able to support the execution of conditional smart contracts, the establishment of DAOs and the creation of ICOs (each of which is explained in the main text). On the Ethereum network, miners work to earn 'gas' (which is settled in the network's currency known as Ether). The gas payment is the amount that the smart contract develop offers to the network by way of transaction fee to entice the miners to validate and execute the transaction.

[61] Ethereum White Paper (n 34).

[62] In Ethereum's case, solidity. For a more detailed discussion of the restrictions of bitcoin's scripting language see: Ethereum White Paper (n 34), 'scripting.'

[63] Ibid. As the Ethereum White Paper notes on the bitcoin blockchain, bitcoin can 'either be spent or unspent; there is no opportunity for multi-stage contracts.'

[64] Szabo (1996) (n 42).

[65] Szabo (n 2).

[66] In doing so, Szabo demonstrated the disruptive capabilities of drawing on multi-disciplinary expertise, one of the recommendations set out in part five.

relationships'[67] and reduce reliance on traditional 'enforcement traditions'[68] given that the 'digital revolution is radically changing the kinds of relationships we can have.'[69] Specifically, Szabo recognised that technological advances made the (heretofore too expensive) running of algorithms possible, with the effect that ways in which business relationships were structured could now be transformed.

Whilst multiple definitions have been offered since,[70] Szabo defined a smart contract as 'a set of promises, specified in digital form, including protocols within which the parties perform on these promises.'[71] Against this, there is a further distinction to be made between 'smart contract code' and 'smart legal contracts.' Whilst this area is subject to an ongoing and emerging debate as to taxonomy (again highlighting how opacity may give rise to risk and therefore where useful clarity could be provided),[72] this paper draws on the distinction offered by Stark.[73] That is, defining 'smart contract code' as 'code that is stored, verified and executed on a blockchain'[74] (put another way, discrete code that comprises the entire relationship between the parties and does not interact with a traditional off chain contract) and 'smart legal contracts,' which refers to the application of DLT as a complement to traditional legal contracts, or parts thereof, often as the performance mechanism for obligations set out in an off-chain agreement.

Notwithstanding these definitional challenges, it is trite to say that a smart contract is neither smart nor a contract (although this is certainly possible depending on how the relationship is designed). Rather, what a smart contract does is embed contractual provisions into software to automate performance, rendering breach practically (or economically) implausible. In short, a smart contract guarantees practical performance in accordance with the code. By way of example, if the smart contract relates to the lease of a property it may provide for the transfer of funds on a certain date and, on receipt of those funds, for the automatic release of a digital key to the property. What it does not do is preclude the operation of substantive law and exhaust any ongoing legal rights or obligations. For example, what if (unbeknownst to the parties at the time) the property in question was destroyed on the morning of completion thus frustrating performance?[75] Alternatively, in a transaction relating to the sale of goods, what if the goods were of insufficient quality? This reflects a crucial point of clarification, namely that smart contracts automate practical performance not legal finality. This fundamental distinction can often be obscured or missed, certainly (and understandably) in the minds of consumers, given the narrative of smart contracts as a means of 'guaranteeing' performance. Education to address this potential misconception is an important means of ensuring that consumers do not erroneously think they are left without legal redress once the contract has ostensibly been performed.

One clear benefit that smart contracts are designed to achieve is the reduction of 'mental' transaction costs.[76] Szabo recognised that the traditional contracting process generated not only computational transaction costs but also costs associated with anticipating (and developing mitigation strategies for) contractual breaches. Once a contract is executed, even with such *ex ante*

[67] Szabo 1996 (n 42), 1; Szabo 1997 (n 2), 1.
[68] Ibid, 3.
[69] Ibid, 1.
[70] See: Christopher Clack, Vikram Bakshi and Lee Braine, 'Smart Contract Templates: Foundations, Design Landscape and Research Directions,' (2016) <https://at iv.org/abs/1608.00771v3> accessed 29 March 2019.
[71] Szabo (1996) (n 42).
[72] Clack *et al* (n 70), 2.
[73] Cited by Clack *et al* (n 70): See: John Stark, 'Making Sense of Blockchain Smart Contracts; (coindesk 4 June 2016) <http://www.coindesk.com/making-sense-smart-contracts> accessed 29 March 2019.
[74] Stark (n 73).
[75] A similar question was considered by the court in *Taylor v Caldwell* (1863) 3 B&S 826.
[76] Szabo (1997) (n 2), 7.

planning, unforeseen circumstances almost inevitably arise leaving the parties with incomplete contracts necessitating ongoing monitoring. It is these mental transaction costs that smart contracts seek to reduce by automating performance.[77] Understanding this objective helps to identify those relationships that can benefit from smart contract technology and those that are better suited to a traditional contracting model. For example, highly repeatable contracts with little variation of performance will benefit significantly from automation. In contrast, bespoke agreements, circumstances where the parties might want to retain the ability to voluntarily breach the agreement (and pay damages)[78] or those that have significant discretionary provisions are, at this stage, unlikely to be well suited to smart contract technology. A key skill for legal services providers is to have sufficient understanding of the technology to identify these considerations, determine the risks and rewards of deploying a smart contract, the issues that might arise and the implications of this approach for their clients.

Separate to the (in)ability to revisit the terms of a smart contract, is the current limitation of the types of contractual provisions that can be automated, namely the difficulty in codifying discretionary or 'non-operational provisions.'[79] That is, codification of conditional or operational provisions of an agreement is relatively straightforward, but this task becomes increasingly difficult with non-operational or discretionary provisions.[80] For example, an obligation to pay a fixed sum on a specified date (or upon the occurrence of an unambiguous and verifiable event) does not pose any significant challenges to enshrine within a smart contract,[81] what is more difficult is automating a provision that depends upon a party exercising, for example, 'reasonable' endeavours. As a consequence, early proposals for the commercial deployment of smart contracts have adopted a hybrid structure, where a traditional contract is executed by the parties (addressing non-operational provisions such as law and jurisdiction) with the performance of operational clauses being automated via a smart contract. This hybrid architecture does immediately raise a number of questions relevant to the legal profession, some of which can be addressed by the traditional contract that the code is implementing.[82] For example, what happens if there is a discrepancy between the traditional contract and the smart contract code? Who is responsible for the code's performance? Does the code itself constitute a legally enforceable contract? What rights, if any, do third parties have with regard to the smart legal code?

Whilst most commercial parties will, at this stage, want the protection of a hybrid architecture it is certainly possible for parties to be willing to enter into an agreement that is expressed entirely (save for any implied terms) by computer code (hence the distinction set out above between smart legal contracts and smart contract code). In the event that parties execute smart contract code a number

[77] Ibid, 8.

[78] The relative merits (or otherwise) of efficient breach arguments are outside of the scope of this report. See: Charles Fried, *Contract as Promise, a Theory of Contractual Obligation* (Harvard University Press 1981).

[79] Although it is anticipated that as research emerges, the boundaries of these semantic constraints will increase. As to codifying operational and non-operational clauses see: Clack *et al* (n 70).

[80] See: ISDA and Linklaters, 'Whitepaper: Smart Contracts and Distributed Ledger – a Legal Perspective,' (August 2017). Available at: <https://www.isda.org/a/6EKDE/smart-contracts-and-distributed-ledger-a-legal-perspective.pdf> accessed 22 July 2019.

[81] This is where an 'oracle' is used. An oracle is, in effect, a data feed to the smart contract. It provides a connection to the real world to supply the off-chain data that is necessary for the smart contract to determine whether certain conditions have been met, thereby triggering execution. See for example, AXA's delayed flight insurance product 'fizzy,' which utilises smart contract technology to automate plane delay insurance payments: <https://fizzy.axa/en-gb/> accessed 19 May 2019. The smart contract engages with public databases to determine whether a particular flight was delayed, thus verifying whether or not the condition for payment has been met. The use of oracles does of course raise its own issues as to the security (and therefore reliability) of the oracle and which party is liable in the event of an oracle error.

[82] Indicating the potential content of best practice guidance that could be issued by a regulator.

of fundamental legal questions arise (although some of these questions certainly do overlap with smart legal contracts). For example, does the smart contract code constitute a contract at law? If so, how do traditional rules of interpretation apply (for example, what if 'in code' comments are made)? What if an intervening event frustrates the contract or renders it illegal? What if the code does not perform in accordance with one or both parties' expectations (see part 1(iii) for a case study on how this issue arose in the context of decentralised autonomous organisations)?

The issues that smart contracts raise are not questions that can be either fully identified or resolved in subject-matter silos. They require a detailed understanding of both the underlying technology and the relevant legal framework. As discussed in part four, a valuable role that regulators can perform is using their convening power to bring together the experts that are required to identify, and potentially resolve, some of these questions in an authoritative manner.[83] This multi-disciplinary approach is crucial to ensure that legal services providers and the developers that will be building smart contracts are able to communicate effectively so that risks of, *inter alia*, misinterpretation are reduced. This might seem like a simplistic point, but it is a vital one. Bringing together two different disciplines, with different languages and approaches, can (as Nick Szabo demonstrated) introduce innovative practices that have the potential to realise significant benefits for the public. However, these differences also risk confusion and misunderstanding. Nevertheless, whilst this risk must be addressed it should not be unduly feared. As legal services providers have traditionally had to learn to translate business strategy into legal prose, what is now required is simply a third strand of communication, namely communicating legal requirements to the relevant development team to accurately translate this into computer code. This is, of course, a reciprocal skill set. It is similarly important to ensure that computer scientists and engineers are able to recognise and appreciate fundamental legal principles that are of relevance to their work.

(ii) Initial coin offerings ('ICOs')

An initial coin offering is a mechanism for dapp developers to raise funds for their projects. The developers issue cryptoassets (ordinarily a 'token' or 'coin') in exchange for the payment of the relevant platform's native currency e.g. Ether for an ICO running on the Ethereum network. Given this objective, it is perhaps understandable that a taxonomy was adopted to reflect the similarity to initial public offerings ('**IPOs**'). However, unlike the highly regulated IPO market, ICOs initially operated outside of the regulatory perimeter exposing consumers to investment risk in a highly speculative market. As a result, ICOs quickly attracted the attention of regulators who are working to identify and clarify whether and, if so when, an ICO falls within their remit.

ICOs operate through the use of smart contracts. Investors submit funds to the smart contract that issues the relevant cryptoasset in exchange. These assets can take a variety of forms, meaning that their classification from a securities perspective has not been straightforward (see section (iii) below). For example, some tokens (generally known as utility tokens) give the holder the right to participate in the underlying protocol, product or service (such as file storage).[84] In contrast, others bear a closer resemblance to traditional equities and are hence generally classified as 'securities tokens.'[85] The risk of ICOs to consumers (and therefore the interest of regulators) is clear and significant. Whilst the regulatory classification of ICOs is being determined, anyone can establish an

[83] Of course, many have a view on how the existing legal framework will respond to these questions and, as discussed in part three, the English common law is particularly well suited to do so. However, pending formal adjudication these questions remain extant.
[84] See: filecoin.io
[85] See: Blockchain Capital's security token 'BCAP.'

ICO and sell their tokens to the general public.[86] All that is required is a website and a white paper that, whilst unregulated (or subject to uncertainty as to their classification), can make unsubstantiated claims about the prospects of the underlying business.

From 2013 (with the peak starting in 2014) to 2018, ICOs saw a significant wave of investment. Although obtaining an accurate figure is difficult (itself an indication of some of the challenges in this space), some trackers estimate that just over $10 billion was raised through ICO's in 2017 rising slightly to $11.4 billion in 2018.[87] This activity does, of course, offer potentially significant benefits to start-ups providing access to funds that may not otherwise be available. However, as set out below, these fundraising endeavours do expose consumers to significant risk (especially given the media attention that ICOs have attracted and the risk of herding behaviour by retail investors). Given this potential for investment, but concomitant risk of harm, regulators are required to achieve a difficult balance when deciding how to respond to ICOs. One initial question for financial services regulators is, of course, whether a given cryptoasset falls within their regulatory remit. Thereafter, there is the more nuanced question of whether ICOs should be treated as a new form of security, one criticism being that if ICOs are governed by the same regulatory framework as IPOs then there is little benefit in pursuing this novel form of fundraising. There is also a clear educational need in terms of consumer awareness. In this regard, the SEC adopted a novel approach by 'offering' a 'Howey Coin' to the public (the 'Howey Test' is applied in the USA to determine whether a transaction qualifies as an investment contract). When investors tried to invest in the Howey ICO they were redirected to an SEC web page warning of the dangers of the ICO market.

(iii) Decentralised autonomous organisations ('DAOs')

In his 1996 paper, Nick Szabo recognised the potential that smart contracts had to fundamentally transform collective organisation, providing the opportunity to create 'new kinds of businesses and social institutions.'[88] Ultimately, this vision was realised with the emergence of DAO's, a form of smart contract that is used for automating 'organizational governance and decision-making.'[89] In essence, a DAO is a form of digital organisation that facilitates fund raising and project investment, with investment decisions being made by the DAO token holders (defined below). Whilst 'DAO' is a generic term for all such collectives, the DAO that is most well-known, and that demonstrated a fundamental risk with this type of organisation (and DLT governance more generally), was itself entitled 'The DAO.'

The DAO ran on the Ethereum platform and was created to mitigate what its founders saw as two key problems with traditional forms of organisation. First, that people 'do not always follow the rules and [secondly] people do not always agree what the rules actually require.'[90] To achieve this goal, The DAO is comprised, in broad terms (a more detailed analysis of The DAO's architecture can be found in its white paper),[91] of three key constituents: the token holders, contractors and curators.

---

[86] Although regulators are starting to take enforcement action e.g. SEC v Kik Interactive Inc (Case No. 19-cv-5244).

[87] Daniele Pozzi, 'ICO Market 2018 vs 2017: Trends Capitalization, Localization, Industries, Success Rate,' (Coin Telegraph, 5 January 2019) <https://cointelegraph.com/news/ICO-market-2018-vs-2017-trends-capitalization-localization-industries-success-rate> accessed 4 April 2019.

[88] Szabo 1996 (n 42), 3.

[89] For a more detailed explanation of The DAO see The DAO's white paper: Christopher Jentzsch, 'Decentralized Autonomous Organization to Automate Governance' <https://download.slock.it/public/DAO/WhitePaper.pdf> accessed 29 March 2019.

[90] Ibid, 1.

[91] Ibid, 1.

Token holders invest Ether (Ethereum's cryptocurrency) in exchange for tokens in The DAO, giving them 'voting and ownership rights.'[92] The tokens, which are issued in proportion to the Ether invested and are freely transferable on the Ethereum ledger after an initial pre-determined 'creation' phase, enable token holders to vote on the projects that The DAO invests in. Thus, token holders would control, in real-time, The DAO's funds. The Contractors perform the projects that the DAO invests in. To be selected for investment, contractors submit projects for the token holders to consider and vote upon. If the project is authorised, The DAO would transfer the requisite Ether to a smart contract relating to the contractor's proposal and the contractor would then be responsible for implementing the project. It would be possible for a contractor to be another DAO, raising the possibility in the future of a network of DAOs, much like we have corporate groups and interactivity today.

To protect minority (and potentially apathetic) token holders, the final constituent in The DAO is the curator. The curator is a technical role that verifies the address of the contractor and decides whether to add the contractor to The DAO's approved list, namely the list of contractors that are entitled to receive Ether.[93] This mechanism is designed to prevent a malicious attacker with control of The DAO's tokens from voting for a project that directs The DAO's funds to themselves (or changing The DAO's governance rules for their own interest). The DAO's architecture (and indeed that of DAO's in general) raises numerous, fundamental, legal questions. For example, when issuing tokens is a DAO in fact issuing securities that fall within the regulatory perimeter of the relevant authority? As a distributed organisation, what jurisdiction governs a DAO's activities? What is the legal status of a DAO and what are the implications of this? How are the relevant constituents characterised? Specifically, are any constituents occupying a fiduciary position necessitating the imposition of duties in that capacity? If so, to whom are these duties owed?

The DAO was, initially, a huge success. A reflection of the then highly active crypto-market, The DAO raised over $150m dollars in May 2016, setting a record for the largest crowdfunding endeavour at that date. Notwithstanding this initial success, concerns were raised over the security of The DAO's protocol (as noted above, one benefit of open source code is that it is subject to public scrutiny). Proposals to resolve these issues were suggested but, on 17 June 2016, before these proposals could be voted upon, a hacker exploited a loophole in The DAO's code transferring 3,689,577 Ether (approximately $50m) from the fund into a 'child' DAO. Importantly, the child DAO was created in accordance with The DAO's original payment protocol, which included a minority token-holder protection mechanism that enabled token holders to transfer funds into a child DAO if they did not agree with a project that had been approved by the majority (the funds were then subject to a minimum holding period in the child DAO). Following the hack, developers sought to both close the loophole and identify how to respond to the loss in a way that would gain consensus of the network. Ultimately, the token holders approved a 'hard fork,'[94] which effectively created a remedial block that would transfer the funds back to The DAO and then distribute them to the token holders.

The DAO hard fork divided the network and broader DLT community, including those who had lost money in the attack. In particular, the hack exposed fundamental legal, practical and ideological questions relating to the governance of smart contract relationships as well as a tension amongst the DLT community as to its answer.[95] That is, in the event of a loophole in the transaction protocol,

[92] Ibid, 2.

[93] Ibid.

[94] That is, a modification to the ledger protocol that renders the old code invalid as the two versions are incompatible.

[95] Although the question of spirited or creative compliance is one that has been debated by the corporate community for some time. See: Doreen McBarnet, 'After Enron: Corporate Governance, Creative Compliance

is it legitimate or, to the extent this differs, lawful for a network participant to exploit that loophole for their own gain, even if this is contrary to the clear intention of the parties? Alternatively, should token holders accept the risk of an immutable ledger including any code 'errors' (investment in the DAO was clearly stated to be governed by the DAO's code, with that code taking priority over any contradictory statements made elsewhere)? Put another way, what takes precedence – the code or the expectations of the parties?

The DAO hack was an important catalyst (but by no means the first) for financial services regulators to issue guidance on the question of token classification. Notably, the SEC issued its '*Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO*'[96] (the '**DAO Report**'). The DAO Report concluded that the The DAO's tokens were securities and subject to federal securities laws, but 'in light of the facts and circumstances, the agency has decided not to bring charges in this instance.'[97] It noted that whether a cryptoasset constitutes a security depends on the facts of a particular case but was clear that this was not a determination that was made by reference to the name of the asset and that digital and cryptoassets could certainly fall within this classification. Up until this point, ICOs had been on the radar of financial services and markets regulators for some time. The DAO Report made clear what had long been suggested, namely that (certainly for the purposes of US federal securities laws) cryptoassets were capable of being subject to securities regulation and the concomitant compliance obligations that this entailed.

Since the DAO Report, the SEC has continued its activities in this space. For example, on 3 April 2019 the SEC's Strategic Hub for Innovation and Financial Technology ('**FinHub**') released its own guidance (the '**FinHub Guidance**') on cryptoasset classification.[98] The FinHub Guidance is expressed to 'assist those seeking to comply with U.S. federal securities laws'[99] and to explain in 'plain English'[100] how the *Howey*[101] test (the US test for determining whether an instrument qualifies as an investment contract for the purposes of US securities regulation) can apply to cryptoassets. The FinHub Guidance expressly states that it is 'not a rule, regulation, or statement of the [SEC] … [and it] does not replace or supersede existing case law, legal requirements, or statements or guidance from the [SEC].'[102] Further, the FinHub guidance is stated to provide additional guidance to (and does not replace) the DAO Report. The FinHub Guidance has been seen as a 'positive first step'[103] although the initial view from industry is that a number of critical areas still need to be addressed and greater specificity would have been preferred on topics such as guidance on how overseas organisations will

---

and the Uses of Corporate Social Responsibility,' in Justin O'Brien (ed) *Governing the Corporation: Regulation and Corporate Governance in an Age of Scandal and Global Markets* (John Wiley & Sons 2005) 205-222.

[96] 25 July 2017, Exchange Act Release No 81207.

[97] Ibid, 1.

[98] Securities and Exchange Commission, 'Framework for "Investment Contract" Analysis of Digital Assets,' (4 April 2019) <https://www.sec.gov/files/dlt-framework.pdf?utm_medium=email&utm_source=cio> accessed 4 April 2019.

[99] SEC Public Statement, 'Statement on "Framework for 'Investment Contract' Analysis of Digital Assets"' 3 April 2019 <https://www.sec.gov/news/public-statement/statement-framework-investment-contract-analysis-digital-assets> accessed 4 April 2019.

[100] William Hinman (US SEC Director of Corporation Finance), speaking at D. C. Fin tech Week (5 November 2018). See: Nikhilesh De, 'SEC Official Says 'Plain English' Guidance on ICOs is Coming,' (coindesk 5 November 2018) <>http://www.coindesk.com/sec-official-says-plain-english-guidance-on-icos-is-coming accessed 29 March 2019.

[101] *SEC v W. J. Howey Co.* 328 US 293 (1946).

[102] FinHub Guidance (n 98), 1 and fn 1.

[103] Nikhilesh De, 'SEC's Crypto Token Framework Falls Short of Clear and Actionable Guidance,' (coindesk 4 April 2019) <http://www.coindesk.com/secs-crypto-token-framework-falls-short-of-clear-and-actionable-guidance> accessed 4 April 2019.

be treated and the circumstances in which a token might cease to be treated as a security.[104] Early responses also demonstrate the challenge that can arise whenever a term is defined (a common issue for DLT regulation). By way of example, the FinHub Guidance seeks to define an 'active participant,' which is relevant to the latter stages of the *Howey* test, and is a definition that interviewees informed CoinDesk could 'really impact and even hinder the process in which a token project/start-up can decentralize itself.'[105]

The SEC is not the only financial services regulator that is active in this space. The FCA has, from the outset, been cognisant of the benefits and potential risks that ICO's pose. To support innovation in DLT activity, the FCA has included a number of DLT businesses in its regulatory sandbox, which allows these organisations to test their products with real consumers. Moreover, it is leading the Global Financial Innovation Network, which is comprised of 11 regulatory bodies and was established to help create a 'new framework for co-operation between financial services on innovation related topics'[106] whilst also providing a more effective and efficient way for innovative firms to interact with regulators. In terms of guidance, the FCA issued an early warning by way of a consumer notice as to the risks of ICOs.[107] Thereafter, it consulted extensively on the classification of cryptoassets for the purposes of determining whether such assets fall within their regulatory perimeter. Their recent guidance note (which is subject to consultation),[108] reaffirms the FCA's position as a technology-neutral regulator, whilst setting out clear perimeter guidance. In particular, the guidance differentiates and defines exchange tokens (ordinarily outside the regulatory perimeter), security tokens (ordinarily within the regulatory perimeter) and utility tokens (which may fall within the regulatory perimeter).[109]

(iv) Application to legal services

Currently, the take up of DLTs by the sector for the provision of legal services has been limited, with the majority of work concentrating on supporting client activity (this can be contrasted with other forms of LegalTech such as machine learning, AI and predictive analytics that have seen greater levels of adoption). As such, the immediate impact for most legal services providers is to ensure an adequate understanding of the architecture, function, risks and opportunities that DLTs represent so that they may properly advise clients operating in this space.

Nevertheless, a number of legal services providers are engaging directly with DLT services. For example, both Legal Zoom and Rocket Lawyer are looking to offer smart contract capabilities direct to consumers. As discussed in part one, on 6 March 2019 HM Land Registry tested its blockchain prototype to complete the transfer of a freehold title, potentially laying the foundations for widespread use of DLTs in conveyancing transactions. The ability to issue tokens has also introduced new ways of financing litigation with legal-tech start up 'Legaler' launching an ICO to fund its legal aid platform that intends to focus on social justice cases. One potential area of early mainstream adoption of DLTs by legal services providers is in AML and KYC compliance. DLTs offer a time-stamped record of identification, providing comfort to the service provider and increasing efficiency for consumers who can simply provide access to a DLT record, rather than obtaining certified copies of identification every time they seek professional advice. In the mid-term, it is likely that the

[104] Ibid.
[105] Ibid.
[106] FCA Press Release, 'FCA collaborates on new consultation to explore the opportunities of a Global Financial Innovation Network,' 7 August 2018 <https://www.fca.org.uk/news/press-releases/fca-collaborates-new-consultation-explore-opportunities-global-financial-innovation-network> accessed 29 March 2019.
[107] FCA, 'Consumer Warning About the Risks of Initial Coin Offerings (ICO's)' 12 September 2017.
[108] FCA Guidance on Cryptoassets (n 8).
[109] Ibid, 7.

increased use of smart contracts will necessitate a form of DLT dispute resolution (this could be on-chain or integrate with an off-chain mechanism), which will require legal foundations and support to adequately meet consumer needs.

In other fields, the practical immutability of DLTs make them valuable for recording title to (and managing rights in) intellectual property (a model adopted by Mycelia for the music industry), recording share ownership (a model adopted in the US by Delaware), issuing bonds (such as the World Bank's 'bond-i') and as a mechanism for derivatives trading (ISDA has long been active in exploring the possibilities of DLTs in the derivatives market).

To realise their potential, decentralised applications will, of course, need a robust legal foundation. Far from hindering innovation, this foundation provides the certainty that creates market confidence and facilitates investment. However, it is an important policy question to determine what form that foundation takes and when it should be engaged. Part three explores some of the international regulatory approaches that have been adopted before part four outlines key considerations for legal services regulators in this jurisdiction.

PART THREE: THE REGULATORY LANDSCAPE

This part provides a brief overview of some of the increasingly extensive regulatory activity relating to DLTs. The current pace of activity is such that it is not possible to provide an exhaustive analysis of the regulatory landscape. Rather, the report highlights five jurisdictions, which demonstrate the range of approaches that have been engaged thus far. Notwithstanding the divergent strategies that have been pursued, several broad observations can be made. First, the watchful approach to DLT regulation that the UK has adopted has, to date, been largely endorsed as an appropriate strategy (although it is likely that we have reached a regulatory tipping point in respect of crypto-assets such that regulatory intervention in this regard may well be forthcoming).[110] This strategy has facilitated responsible innovation by allowing the jurisdiction to develop an understanding of the technology, recognise the consumer risks and opportunities that it presents and thereafter identify where specific regulatory or other interventions may be required. As set out below, this provides a robust foundation for rigorous consultation and, ultimately, the introduction of initiatives that are transparent, accountable, proportionate, consistent and targeted.[111]

Secondly, there is a common industry call for international coordination and alignment.[112] DLTs do not have geographical boundaries and the emergence of disparate international regimes (as indicated from even the small sample set out in this section) risks both stifling innovation and

[110] Patrick Armstrong, European Securities and Markets Authority 'Regulation and DLT: Working to Strike the Right Balance' (22 November 2016, ESMA/2016/1613). See also: European Securities and Markets Authority, 'Report: The Distributed Ledger Technology Applied to Securities Markets,' 7 February 2017. As to crypto-assets see: House of Commons Treasury Committee, 'Crypto-Assets, Twenty-Second Report of Session 2017-19' (19 September 2018, HC 910); and Securities and Markets Stakeholder Group, 'Advice to ESMA, Own Initiative Report on Initial Coin Offerings and Crypto-Assets' (19 October 2018).

[111] Reflecting the principles of good regulation set out in the Legislative and Regulatory Reform Act 2006, s 2(3).

[112] See for example: European Securities and Markets Authority, 'Advice: Initial Coin Offerings and Cryptoassets,' 9 January 2019; European Banking Authority, 'Report with Advice for the European Commission,' 9 January 2019. Where international convergence may emerge is in the field of AML and KYC requirements. See for example: Fifth European Anti-Money Laundering Directive (EU 2018/843); and the Financial Action Task Force ('**FATF**') 'Interpretative note to FATF Recommendation 15.' The interpretative note is due to come into force in June 2019 and applies the FATF Recommendations 'International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation,' to virtual assets and virtual asset service providers.

facilitating regulatory arbitrage. Thirdly, in most jurisdictions there is a greater appetite for substantive regulatory intervention (across a spectrum of actions)[113] concerning ICO's, with smart contract regulation (if any) focussed on providing clarity as to the legal status of the agreement. Fourthly, the lack of access to traditional banking services by crypto-businesses (even in jurisdictions that have adopted favourable DLT policies) continues to pose a significant practical challenge to growth. Finally, and aligned to the fourth observation, jurisdictions that have successfully created a vibrant DLT environment have looked holistically at the DLT ecosystem (in addition to the regulatory framework), introducing a range of measures including the creation of regulatory sandboxes and support for multi-disciplinary research collaborations.

(i) United Kingdom

As a common law system, the UK has consistently demonstrated that it is well placed to respond to corporate, commercial and technological advances.[114] For example, the courts have repeatedly shown how fundamental principles of contract law are able to respond to what was, at the time, a new technology (such as the use of car park ticket machines).[115] In doing so, the jurisdiction has established a consistent and coherent framework of rules that consumers and businesses can rely upon. In this way, the common law is able to adjudicate an issue in a fair and reliable manner (providing certainty and clarity to the parties and the wider market), avoiding the difficulties that can arise from direct regulation. In particular, reliance on the common law avoids the potentially stultifying effect of legislation that (whilst likely necessary in some respects regarding DLTs) can lack the flexibility to respond to market developments, particularly in the case of rapidly developing technologies. This flexibility has enabled the UK to adopt a 'watch and wait' approach to DLT regulation, a strategy that has been welcomed by industry as it has allowed market understanding to develop whilst avoiding the risks that can arise when regulating too soon in an emerging field. Importantly, the UK has always signalled that regulation of some form will likely be forthcoming in due course, thus potentially avoiding Collingridge's Dilemma (described earlier).[116]

That is not to say the jurisdiction has been inactive, in fact far from it. Sector-specific regulators have been supporting their respective communities through the issuance of guidance notes,[117] in some cases consumer warnings[118] and, in others, educational guides.[119] Crucially, regulators have also been proactive in supporting the emerging DLT ecosystem in a number of other ways. For example, by using their convening power (exclusively or with others) to bring together stakeholders

[113] See the FCA's use of consumer warnings (FCA, 'Consumer Warning About the Risks of Initial Coin Offerings (ICO's)' 12 September 2017), reports (HM Treasury, FCA and Bank of England, 'Cryptoassets Taskforce: Final Report' October 2018) and guidance with corresponding consultation (FCA, 'Guidance on Cryptoassets' (January 2019 CP19/3).

[114] For a more detailed analysis of the value of the advantages of the English common law in supporting emerging technology see: Sir Geoffrey Vos, Joint Northern Chancery Bar Association and University of Liverpool Lecture, 'Cryptoassets as Property: How Can English Law Boost the Confidence of Would-Be Parties to Smart Legal Contracts' (2 May 2019).

[115] *Thornton v Shoe Lane Parking* [1971] 2 WLR 585.

[116] See (n 11) and accompanying text.

[117] FCA, 'Guidance on Cryptoassets,' (Consultation Paper CP19/3, (January 2019, FCA); HM Treasury, FCA and Bank of England, 'Cryptoassets Taskforce, Final Report,' (October 2018).

[118] FCA, 'Consumer Warning about the Risk of Initial Coin Offerings,' (12 September 2017, FCA Statements); FCA, 'Over £27million Reported Lost to Crypto and Forex Investment Scams' (21 May 2019, News).

[119] The Law Society, '*Horizon Scanning, Forward Thinking: Blockchain, the Legal Implications of Distributed Systems*' August 2017.

to support the emerging market,[120] operating regulatory sandboxes[121] or partnering with incubators. This breadth of support not only enables new entrants (as well as incumbents) to develop their DLT (and other LawTech) offerings but also allows regulators to better understand the likely deployment of the technology and, as a consequence, where the risks and opportunities might lie.

Following this period of observation and engagement, it is becoming clear that increasing legal certainty regarding DLT activity will provide vital support to, and confidence in, the development and deployment of the technology. In response to this need, the UK Jurisdiction Taskforce of the LawTech Delivery Panel has launched a public consultation to identify the key legal questions that arise in respect of cryptoassets, DLT and smart contracts.[122] The consultation is worthy of note not only for its substance, but also because it provides a helpful model for ensuring rigorous and multi-disciplinary engagement in this space, thereby avoiding the risks of moving precipitately and risking unintended consequences. In brief, the taskforce released a detailed (both technical and legal) consultation paper and gave stakeholders the opportunity to discuss the issues raised therein at a public town hall prior to the consultation close. Following the consultation, an 'authoritative legal statement on the status of cryptoassets and smart contracts under English private law'[123] will be prepared.

The UK has also been cognisant of the need for multi-sector and international collaboration when looking at crypto-regulation and governance. For example, in May 2019 the FCA released its 'Call for Input: Cross-Sector Sandbox'[124] citing DLT as a particular area where cross-sector collaboration could be of benefit. In the consultation, the FCA recognised that innovative technologies such as DLT drive changes that are not always sector-specific and that different regulators face common questions in meeting their objectives of harnessing innovation whilst maintaining, *inter alia*, market integrity and consumer protection. As such, the report outlines a proposal for a cross-sector regulatory sandbox to enable regulators to gather insights, gain understanding from more advanced technology markets, create a harmonised policy approach and collaborate to explore the issues that emerging technology raises.[125]

(ii) Italy

The requirements of a jurisdiction's existing legal framework can be a factor in the decision to introduce DLT specific legislation. For example, Italy introduced Law No 12/2019 (which came into force on 13 February 2019) confirming that smart contracts that comply with the corresponding technical guidelines (due to be released by the Agency for Digital Italy in May 2019) have equal footing with off-chain contracts.[126] The decree was particularly (although not exclusively) necessary due to the fact that Italian law requires contracts to be in writing and, to this end, it stipulates that the use of a smart contract has the same effect as an 'electronic time stamp' as defined in the European Regulation (no 910/2014) on electronic identification and trust services for electronic transactions ('**eIDAS**').[127]

---

[120] See for example: the UK LawTech Delivery Panel; the Law Society's Public Policy Technology and Law Commission (whilst the latter focuses on AI it addresses certain key questions that are relevant across the LawTech space); and the Law Society's Technology and Law Committee.

[121] The FCA's fifth regulatory sandbox has accepted a number of DLT related companies (as did its fourth cohort). For details of the firms that were accepted to the sandbox see: <https://www.fca.org.uk/firms/regulatory-sandbox/cohort-5> accessed 19 May 2019.

[122] UK Jurisdiction Taskforce consultation (n 7).

[123] UK Jurisdiction Taskforce consultation (n 7), 5.

[124] FCA, 'Call for Input: Cross-Sector Sandbox' (May 2019).

[125] Ibid 9.

[126] Law No 12/2019, art 8(2).

[127] Law No 12/2019, art 8(3).

Notwithstanding this potential driver for Law No 12/2019, the recognition of the legal validity of smart contracts is also part of the Italian government's move towards supporting blockchain technology. In December 2018 the Ministry of Economic Development convened an expert group to develop the country's strategy on blockchain and signed a joint declaration with Cyprus, France, Italy, Malta, Portugal and Spain agreeing to promote blockchain adoption in order to 'transform its economy.'[128]

(iii) Malta

Malta is one of a number of examples where smaller jurisdictions have moved relatively quickly to introduce DLT regulation.[129] In July 2018 Malta was one of the first jurisdictions to introduce a comprehensive statutory DLT regime, passing three statutes designed to meet its objective to become the 'blockchain island.'[130] These are: (i) the Malta Digital Innovation Authority Act 2018 (the '**MDIA Act**'); (ii) the Innovative Technology Arrangement and Services Act 2018 (the '**ITAS Act**'); and (iii) the Virtual Finances Assets Act 2018 (the '**VFA Act**'). The MDIA Act provided for the establishment of the 'Malta Digital Innovation Authority' (the '**MDIA**'), the competent authority to regulate innovative technologies (including DLT) in the jurisdiction. The MDIA Act specifies that, amongst other matters, the MDIA will be responsible for promoting consistent principles for the development of 'visions [and] skills' relating to innovative technologies and to exercise regulatory functions relating thereto. The MDIA Act offers definitions of, amongst other terms, DLT and smart contracts.

The ITAS Act addresses questions of 'legality, integrity, transparency, compliance and accountability'[131] and includes smart contracts and DAOs within the definition of innovative technologies. It provides the MDIA with authority to certify different technologies for one or more specified purposes,[132] includes a requirement that the relevant software (or parts thereof) have been reviewed by a systems auditor[133] and mandates that systems providers shall respect specified principles of best practice.[134] This aligns with Malta's DLT policy to focus on the actual technology, not just the corresponding white paper, to ensure that the underlying technology delivers on market expectations.[135]

The VFA Act is concerned with ICOs and sets out a licensing regime for those wishing to launch a coin in Malta. It mandates that all ICOs must be supported by a white paper (which must be filed with

[128] Yogita Khatri, 'Italy Announces 30 Experts to Lead National Blockchain Strategy,' (28 December 2019, *coindesk*) <https://www.coindesk.com/italy-announces-30-experts-to-lead-national-blockchain-strategy> accessed 19 May 2019.

[129] Bermuda is another such example with others including Gibraltar and Lichtenstein. As to Bermuda, see: (i) the Digital Asset Business Act (introducing a licensing regime for DLT businesses); and (ii) in July 2018 the Banks and Deposit Companies Act 1999 was amended to allow banks to accept cryptocurrency organisations (with effect from 28 February 2019, New York based Signature Bank has been accepting Bermuda-licensed crypto-companies).

[130] Rachel Wolfson, 'Silvio Schembri Explains How Malta Has Become The World's Blockchain Island,' (31 July 2018, Forbes) available at <https://www.forbes.com/sites/rachelwolfson/2018/07/31/silvio-schembri-explains-how-malta-has-become-the-worlds-blockchain-island/#20b715842cad> accessed 19 May 2019.

[131] ITAS Act, s 8(3).

[132] ITAS Act, s 7.

[133] ITAS Act, s 8(4)(b).

[134] ITAS Act, s 11.

[135] STA Law Firm, 'ICOs and ICO Regulations in Malta,' (25 April 2019) available at: <http://www.mondaq.com/x/800132/fin+tech/ICOs+And+ICO+Regulations+In+Malta> accessed 19 May 2019.

the Malta Financial Services Authority),[136] and sets out minimum disclosure requirements for the white paper.[137] The Act imposes a civil liability to pay damages to any investor that suffers a loss as a direct consequence of reliance on untrue statements contained in the white paper.[138]

(iv) Singapore

Singapore is often cited as a blockchain friendly jurisdiction and, until early 2019, much like the UK had not introduced DLT specific regulation. Instead, and in common with the FCA's approach, the Monetary Authority of Singapore ('**MAS**') issued guidance providing clarity as to token requirements, engaged with the banking sector to assist DLT based businesses in securing traditional banking services and supported research projects looking at the use of DLT for clearing and settling of payments and securities.[139] Recently, the Singapore International Commercial Court provided some clarity as to the status of cryptoassets, holding that cryptocurrencies could be treated as property that may be held on trust.[140] The Singapore Government has been proactive in supporting the development of DLT and LawTech through, for example, the creation of a blockchain accelerator[141] and establishing the Future Law Innovation Practice.[142]

Against this background, in January 2019 the Singapore Parliament passed the Payment Services Act 2019, which is due to come into force later this year and expands the remit of the MAS to include digital payment token services. The Act sets out a designation regime and licensing regime, the latter of which provides the MAS with authority to regulate a range of payment services including digital payment token dealing and exchanges (commonly known as cryptocurrency dealing or exchange services).[143] The Act requires providers of such services to comply with all relevant AML and counter-terrorism financing requirements. Importantly, the Act also gives the MAS powers to ensure the interoperability of payment solutions.

(v) United States of America

The USA has been increasingly active in DLT and crypto-regulation, both at a state and federal level. The federal system does, of course, mean that policy decisions have to navigate the relationship between federal and state regulation,[144] whilst state activity has varied significantly in terms of underlying policy objectives and regulatory design (although see the efforts of the Blockchain Promotion Act discussed below, which is intended to introduce at least definitional coherence across legislative activity). To support state legislative activity, in December 2018 the Chamber of Digital

[136] VFA Act, s 3(1).
[137] VFA Act, s 4 and schedule 1.
[138] VFA Act, s 10.
[139] For example, the MAS supported 'Project Ubin,' which is an industry collaboration exploring the use of DLT in the financial services and payment sector. See: < http://www.mas.gov.sg/Singapore-Financial-Centre/Smart-Financial-Centre/Project-Ubin.aspx> accessed 19 May 2019.
[140] *B2C2 Ltd v Quoine Pte Ltd* [2019] SGHC(I) 03.
[141] https://tribeaccelerator.co
[142] https://www.flip.org.sg
[143] Mr Ong Ye Kung, 'Payment Services Bill,' (Second Reading Speech on behalf of Mr Tharman Shanmugaratnam, 14 January 2019) available at: <http://www.mas.gov.sg/News-and-Publications/Speeches-and-Monetary-Policy-Statements/Speeches/2019/Payment-Services-Bill.aspx> accessed 19 May 2019.
[144] The Uniform Law Commission ('**ULC**') recently announced that states should refrain from adopting its model Act for virtual currency businesses (the Uniform Regulation for Virtual Currency Businesses Act and Supplemental Act) whilst it identifies the impact that the technology has on the Uniform Commercial Code ('**UCC**'). The ULC's Joint Study Committee on the UCC and Emerging Technologies will instead review the UCC to determine whether amendments are needed to accommodate emerging technologies including DLT.

Commerce (a blockchain trade association) issued the 'Legislator's Toolkit for Blockchain Technology,' setting out its own legislative proposals.[145]

To understand the range of State responses, it is helpful to start by considering New York's BitLicense regime, which came into force in 2015 and was one of the first state level DLT licensing (or other regulatory) initiatives. Arguably, the BitLicense was not well received by the DLT community, which found it to be unduly costly and burdensome, with several DLT businesses leaving the state in response.[146] To date, only 18 businesses have secured a license. Changes to the BitLicense are expected and in December 2018 New York, in common with other states,[147] launched a multi-disciplinary cryptocurrency taskforce with the mandate of reporting (by December 2020) on how the state can best regulate and utilise the technology.[148]

In contrast to New York's initial regulatory approach, several states have sought to establish themselves as supporting DLT activity. In 2017, Delaware (known as the incorporation state) made a small amendment to its general corporate law, affirming that corporations were able to maintain their stock ledgers on DLT.[149] Similarly, Tennessee made minor amendments to its existing framework to confirm that records on a blockchain are considered to be electronic records and that a contract will not be invalidated simply because it utilises smart contract technology. As to the purpose of these changes, Rep Jason Powell was clear that Tennessee Bill 1507 'shows that our state is supportive of blockchain … and we'll do what we can to encourage and promote businesses who are already in this space or are interested in it to set up shop here or continue to thrive.'[150]

One state that has implemented a holistic and wide reaching approach to regulation is Wyoming, which has at the date of writing enacted a suite of 13 pro-DLT statutes that address issues from tax, access to banking facilities and the classification of cryptoassets. These are supported by an educational website, which claims that 'attracting the growing Blockchain ecosystem could be a huge win for the citizens of Wyoming.'[151] As a consequence, the co-founder of the Wyoming Blockchain Taskforce has called Wyoming the 'Delaware of digital asset law.'[152] It is not possible to provide a full review of such extensive legislative treatment here. However, key provisions include clarification as to the classification of digital assets under the Uniform Commercial Code (namely that digital assets constitute intangible personal property),[153] authorisation of a 'new type of state-chartered depository institution to provide basic banking services to blockchain and other businesses'[154] and the exemption of utility tokens from state securities law.[155]

---

[145] The toolkit is available at: <https://digitalchamber.org/state-legislators-toolkit/?utm_source=Public+Mailing+List&utm_campaign=55a55e02b1-EMAIL_CAMPAIGN_2019_06_12_03_55&utm_medium=email&utm_term=0_e6622a916a-55a55e02b1-344818093> accessed 3 July 2019.

[146] Daniel Roberts, 'Behind the "Exodus" of Bitcoin Startups from New York,' (14 August 2014, Fortune).

[147] See for example the Connecticut Senate Bill 443, establishing the Connecticut Blockchain Working Group.

[148] Assembly Bill A8783B.

[149] Delaware Senate Bill 69, amending the Delaware General Corporation Law, ss 219, 224 and 232.

[150] See: Adrianne Jeffries, 'Blockchain laws tend to be hasty, unnecessary and extremely thirsty,' (29 March 2018, The Verge) <https://www.theverge.com/2018/3/29/17176596/blockchain-bitcoin-cryptocurrency-state-law-legislation> accessed 2 May 2019.

[151] http://wyomingblockchain.io

[152] Caitlin Long, 'What do Wyoming's 13 New Blockchain Laws Mean?' (4 March 2019, Forbes) available <https://www.forbes.com/sites/caitlinlong/2019/03/04/what-do-wyomings-new-blockchain-laws-mean/#18a18a635fde> accessed 19 May 2019.

[153] Bill No SFO125.

[154] Long (n 152); Bill No HB0074.

[155] Bill No HB0070.

Arguably in recognition of the challenges that may emerge with increasing state activity, at a federal level, the Blockchain Promotion Act has been introduced to Congress for a second time. The bill seeks to, *inter alia*, 'direct the Secretary of Commerce to establish a working group to recommend a definition of blockchain technology'[156] thereby avoiding (or at least curtailing) the proliferation of 'blockchain' definitions across states,[157] whilst assisting with the DLT scalability challenge.[158] A second bill, the Token Taxonomy Act, seeks to provide greater clarity as to the legal status of cryptocurrencies in the US and, if passed, will place specified cryptocurrency activities outside the remit of the Securities and Exchange Commission. The intention of the legislation is clear, Representative Warren Davidson (who reintroduced the bill) stated that it 'would send a powerful message...[that] the U.S. is the best destination for blockchain technology.'[159] Indeed, it appears that DLTs are increasingly becoming the focus of federal attention. On 24 May 2019 seven members of Congress wrote to the Director of the US National Economic Council requesting that the Administration convene a forum on blockchain technology, citing the potentially transformative impact of DLT and suggesting that 'more can be done … to coordinate support for this technology in the United States.'[160] The letter went on to observe that to retain its 'standing as a world leader in technological innovation' it was crucial for the USA to engage a wide range of stakeholders (including policy makers, academics and the private sector) to promote research and development in this field.

Outside of legislative activity, the SEC (like other regulators)[161] has been active both in issuing guidance notes and in applying existing securities regulations to a number of 'crypto' businesses.[162] For example in *SEC v Shavers* (2013), Trevor Shavers was found to have been running, in effect, a Ponzi scheme, offering and selling investments in breach of the anti-fraud and registration provisions of existing securities laws. In *USA v Zaslavskiy*[163] (which ultimately concluded with a guilty plea) a federal judge ruled that ICOs are capable of falling within securities laws, providing some guidance on how the *Howey* test might apply when the proposed 'security' was a token (or other cryptoasset) issued pursuant to an ICO.

The *Zaslavskiy* decision was not surprising given that it came after the SEC's DAO Report[164] that, as noted in part 2(iii), concluded that DAO tokens were securities for the purposes of the Securities Act

[156] H.R. 1361 – Blockchain Promotion Act of 2019.

[157] Press Release, 'Matsui, Guthrie, Young, Markey Introduce the Blockchain Promotion Act of 2019' (26 February 2019) <https://matsui.house.gov/news/documentsingle.aspx?DocumentID=1838> accessed 19 May 2019.

[158] Jeff John Roberts, 'Congress is Pushing a Blockchain Bill. Does it Defeat the Point of Decentralised Tech?' (9 April 2019, Fortune) <http://fortune.com/2019/04/09/blockchain-promotion-act/> accessed 19 May 2019.

[159] Nikhilesh De, 'Lawmakers Reintroduce Bill to Exempt Crypto Tokens From US Securities Law,' (9 April 2019, *coindesk*) <https://www.coindesk.com/lawmakers-reintroduce-bill-to-exempt-tokens-from-us-securities-laws> accessed 19 May 2019.

[160] Letter dated 24 May 2019 to the Honorable Lawrence Kudlow, signed by US Representatives Trey Hollingsworth, Darren Soto, Bill Foster, Tom Emmer, Ted Budd, Josh Gottheimer and Davis Schweikert. Available at: <https://digitalchamber.org/wp-content/uploads/2019/05/5282019Blockchain_LettertoNEC.pdf> accessed 30 May 2019.

[161] See: FinCEN, 'Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies,' (9 May 2019). Available at <https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20CVC%20Guidance%20FINAL.pdf?mc_cid=282e0509fa&mc_eid=8f941c7c9b> accessed 19 May 2019.

[162] A list of all digital asset/ICO enforcement actions is available on the SEC's website: https://www.sec.gov/spotlight/cybersecurity-enforcement-actions

[163] 17 CR 647 (2018).

[164] See: (n 96).

1933 and Securities Exchange Act 1934.[165] However, it is of note that not all ICOs will fall within the definition, on 3 April 2019 the SEC issued a no-action letter in respect of the TurnKey Jet ICO, concluding that their tokens were not securities.[166] Since then, the SEC has continued to focus on the crypto-market by releasing further guidance on the classification of tokens,[167] issuing several subpoenas to crypto-businesses and specifying digital assets as one of the SEC's Examination Priorities for 2019.[168]

This report can only provide a high level overview of a sample of DLT regulatory activity. However, the perennial question when looking at any new area of regulatory focus is whether there is a trend towards a race to the top, or the bottom, in terms of regulatory substance and design.[169] That is, are jurisdictions mainly concerned to protect standards, or are they adopting a lenient legislative approach (risking a reduction in standards) in the interests of attracting and retaining economic activity and investment? Given that this is such a novel area of policy focus, it is not possible to offer an absolute answer at this juncture. However, it is clear that, save for a few notable exceptions,[170] most jurisdictions are regulating with a view to creating a supportive environment for DLT businesses and attempting to provide clarity as to the status of DLT activity and the applicability of existing regulatory frameworks. Nevertheless, regulatory activity to date does also demonstrate the challenge of moving early in this space. For example: (i) the problem of defining nascent technology; (ii) developing robust principles that will remain effective as the technology and its applications develop; (iii) properly identifying where existing legal provisions apply and where genuine gaps (requiring regulatory responses) may be required; and (iv) demonstrating how quickly a patchwork of global provisions can emerge, creating a potentially confusing regulatory framework for a borderless technology.

PART FOUR: CONSIDERATIONS FOR REGULATORS

For legal services providers looking to develop a strategic response to DLT, some of the regulatory objectives can seem to stand in conflict with one another (and indeed that tension may exist within any one objective). For example, it is in the public interest[171] to promote innovation in legal services and products (which also increases competition in the market).[172] However, it is also necessary to ensure that consumers are adequately protected against the risk of financial loss (see The DAO example discussed in part two) or misunderstanding as to their legal rights following the execution of a smart contract, which could also lead to a lack of confidence in the legal system.[173] Similarly, it is anachronistic to many consumers that they can access an inordinate range of products and services via their smart phones yet most contracts (and any disputes relating thereto) necessitate lengthy, costly and largely paper-based processes.

---

[165] DAO Report (n 96), 1.

[166] See: FinHub Guidance (n 98).

[167] Securities and Exchange Commission, 'Framework for "Investment Contracts" Analysis of Digital Assets,' (SEC). Available at: <https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets> accessed 19 May 2019.

[168] U.S. Securities and Exchange Commission, *2019 Examination Priorities Office of Compliance Inspections and Examinations*,' 11.

[169] A phenomenon noted by: Berle and Means, *The Modern Corporation and Private Property* (1932 Transaction Publishers) 206 and cited with approval by Mr Justice Brandeis in *Louis K. Liggett Co. v Lee* 288 US 517.

[170] See for example China's ban on initial coin offerings and cryptocurrency exchanges.

[171] Legal Services Act 2007, s 1(1)(a).

[172] Legal Services Act 2007, s 1(1)(e).

[173] Legal Services Act 2007, s 1(1)(g). See part two for a discussion of the potential lack of consumer clarity as to the distinction between automated performance of a smart contract and any ongoing legal right or remedy.

As set out in part three, the flexibility of the UK's common law system means that the jurisdiction is well placed to respond to innovative technology such as DLT without the immediate need for specific regulation. The purpose of this observation is not to suggest that there isn't a place for DLT regulation. Undoubtedly this will likely be considered in the near future to remove impediments to innovation and provide clarity where needed (for example with regard to the classification of cryptoassets).[174] Rather, it is to advocate a cautious approach to intervention at a sector-specific level whilst demonstrating that existing, principles-based approaches to governance (such as the professional principles)[175] are well suited to responding to new and novel developments. Moreover, to best achieve the difficult balance between supporting innovation and ensuring consumer protection, a range of responses across a broad continuum of activities is likely to be the most efficient and effective strategy. By adopting a multi-faceted approach (and process) to DLT governance (as suggested below), regulators are better able to encourage innovation amongst stakeholders, identify innovative governance solutions and increase the likelihood of managing some of the perceived conflicts between the regulatory objectives

(i) Stakeholder engagement, research and consultation

To mitigate the risks of regulating too early and in a manner that doesn't fully address the technological, commercial or legal challenges that may arise, it is, of course, crucial to ensure that any action is predicated on a robust understanding the technology in question. This enables stakeholders to fully present their concerns whilst enabling regulators to identify the regulatory issues that may arise. Whilst this might seem to be a trite suggestion, it is fundamental in the DLT space that a very detailed understanding of DLT and dapps is established, as nuances in development and deployment can have a significant impact on the appropriate (and applicable) regulatory framework and response.

Sector specific regulators are in an important and influential position to support this research by utilising their convening power to bring together multi-disciplinary stakeholder groups. It is vital that a broad spectrum of expertise is engaged, including policy makers, profession-specific regulators, lawyers, developers and consumers, to examine the functionality of the technology and the risks and opportunities that this gives rise to. In this way, true impediments to innovation can be identified together with any risks to consumers, legal institutions and the rule of law that may need to be addressed. Not only does this interaction help to design a better regulatory response, but it also increases the transparency and legitimacy of that response by engaging the relevant stakeholder community throughout the regulatory process.[176]

The benefit of this interaction does, of course, apply in both directions. Just as lawyers need to understand the characteristics of the technology, developers need to appreciate the application and function of a legal framework to the development of DLT products and services, together with the rule of law implications that may arise. We are at a pertinent time to embed this collaboration across the sector. Technical solutions are continually being developed to address challenges with DLT development. For example, identity management,[177] interoperability[178] and standards that facilitate the use of a range of coding languages to develop dapps, which reduces an important barrier to developing DLT applications (namely the need to be proficient in native scripting languages such as Ethereum's Solidity).[179] It is critical that these technical responses are established

[174] Vos (n 114).
[175] Legal Services Act 2007, s 1(3).
[176] See Bekkers and Edwards (n 12).
[177] See Microsoft's DID development.
[178] https://cosmos.network
[179] For example, by facilitating the use of Web Assembly for DLTs.

with an understanding of, and alongside, the applicable legal framework to facilitate a holistic and streamlined approach to DLT development.

There are a variety of ways in which regulators can provide this support. We have already seen sector-specific regulators engage with industry through their partnership with incubators,[180] providing strategic leadership and support to foster innovation in LawTech[181] and producing important research outputs for the community to consider. Regulator support for these initiatives is crucial to ensure that collaborative engagement not only enhances our understanding of the potential for new technologies but that this understanding helps to inform policy decisions where necessary. Further, regulators can engage with members to identify key areas of concern, providing the basis for future research and consultation projects. In turn, this collaborative approach does of course also have the oblique consequence of enhancing the education and understanding of each stakeholder group (as they continue to work together and share insights from their respective disciplines).

(ii) Education and training

Ensuring that all participants within the sector have access to the appropriate education and training in DLT (and related issues) should be at the core of any regulator's response. DLT, like many disruptive technologies, is subject to significant media and public attention, which is not always accurate and can be subject to hyperbole and supposition. For the profession to respond in a meaningful and legitimate manner, and in accordance with professional obligations, it is crucial that those interacting with DLT (be it to advise clients, develop products or make procurement decisions) fully understand the technology and its interplay with legal, professional and regulatory requirements.

Regulators can offer an important source of reliable and authoritative information in a market that is becoming increasingly crowded. As the previous section outlined, regulatory bodies are in a position to convene the necessary participants to develop appropriate educational programmes (technical, policy and legal), whilst providing guidance as to the application of the professional principles when working with DLT. A regulator can also offer significant comfort to the profession in two ways. First, they can provide insight into how front line regulators might interpret professional obligations (and compliance therewith) in the context of DLTs. Secondly, they can provide guidance as to what would constitute a reasonable state of knowledge for lawyers (broadly defined) working in the field. There has been significant debate as to whether lawyers should now learn to code (and vice versa), which could act as a potential barrier to those who are interested in working in this space but who are not formally trained in the relevant domain. Regulators could help to encourage engagement with DLT by making clear the scope of knowledge that is expected, such as the ability to identify legal risks and clearly communicate legal objectives and concerns to clients, developers and regulatory bodies.

There are three pertinent points to consider when developing an education programme. First, there is arguably a lacuna between the perception and reality of general digital skills (aside from DLT) across the profession. Therefore, any educational programme may helpfully include content addressing fundamental digital skills and principles, before then addressing more advanced matters such as DLT. When creating DLT specific curricula, these should of course address not only the legal questions that the technology gives rise to but also its implications for professional ethics as well as common relevant practical issues (such as the need for off-chain governance and the challenge of scalability and interoperability). Secondly, the manner of delivery needs to be structured to reach the widest audience and in a format that can be readily updated as industry knowledge increases.

[180] See for example the Law Society's partnership with the Barclays' LawTech Eagle Lab.
[181] See: the UK LawTech Delivery Panel.

For example, a mixture of digital and in-person delivery, incorporating regular opportunities for feedback, should be used. This feedback component is also relevant to research collaborations (considered in the previous section) to ensure that as new challenges and opportunities are identified, these are incorporated into training and education programmes as appropriate. Finally, sector-specific regulators should consider supporting the development of education programmes that introduce developers to core legal principles (as well as developing programmes informing their members of technical issues).

(iii) Standards and best practice

The architecture of DLTs is such that the adoption of standards and best practice provides an important mechanism for protecting against technical risks and developing consensus as to deployment. As set out in part one, once a smart contract has been deployed, its performance is automated meaning that any error in the code (or applicable data) can be embedded and escalated. Therefore, there is an important need for entities adopting this technology to develop appropriate off-chain systems and controls to ensure that (amongst other matters) suitable data governance, data privacy and compliance procedures are implemented. At this stage, these off-chain governance frameworks are not appropriate for direct regulation but are one area where regulators can provide useful guidance and support.[182] Here we can see the continuum of recommendations described in this part. By supporting research and collaboration, regulators can identify what systems and controls might be necessary thereby facilitating the development of standards and promoting best practice where it is appropriate to do so.[183]

It is of note that a number of standards-setting agencies are looking at the question of DLT and smart contracts. For example, the European Committee for Standardisation (CEN) and the European Committee for Electrotechnical Standardisation (CENELEC) created a joint working group to identify European needs in respect of DLTs.[184] The findings of the group were set out in a white paper released in October 2018, which the group intends to update periodically in line with industry and market developments.[185]

In addition, the European Commission has launched several initiatives designed to support the development of a common approach to DLT across the EU, one of which is the establishment of the International Association of Trusted Blockchain Applications ('**INATBA**').[186] Although INATBA is an EC initiative, it convenes a broad range of global stakeholders to support the development and deployment of DLT guidelines, specifications and standards across a range of sectors.[187] One of

[182] See for example the Ministry of Justice guidance that was released in respect of the Bribery Act 2010.

[183] In this regard, we are seeing a number of initiatives emerge to drive increased standardisation (both platform neutral and platform specific). See for example: BSI PAS on Smart Legal Contracts; BSI ISO technical committee (TC/307) on Blockchain and Distributed Ledger Technology (ISO); Ethereum Enterprise Alliance.

[184] For more detail on this collaboration see: < https://www.cencenelec.eu/news/brief_news/pages/tn-2018-085.aspx> accessed 19 May 2019.

[185] These needs were mapped against the work of the International Standards Organisation, Technical Committee 307 looking at Blockchain and DLTs.

[186] Other initiatives include: (i) the European Blockchain Partnership (developed to establish a European Blockchain Services Infrastructure to deliver cross-border digital public services); (ii) the EU Blockchain Observatory and Forum (designed to, *inter alia*, map and analyse blockchain initiatives and promote DLT education); (iii) the Horizon Prize on Blockchains for Social Good; and (iv) providing funding for blockchain activities. Further details of these initiatives can be found at: <https://ec.europa.eu/digital-single-market/en/blockchain-technologies> accessed 19 May 2019.

[187] Roberto Viola, 'Meeting the Global Blockchain Challenge,' (3 April 2019, European Commission Digital Single Market Blog) < https://ec.europa.eu/digital-single-market/en/blogposts/meeting-global-blockchain-challenge> accessed 19 May 2019.

INATBA's stated aims is to 'contribute to the convergence of regulatory approaches'[188] to DLT as well as to provide a forum for DLT developers and users to interact with regulators. Aligned with this, platform specific consortia are also aware of the need to generate the certainty that will drive investment in the industry. The Ethereum Enterprise Alliance has launched the Token Taxonomy Initiative, the aim of which is to develop a clear token definition and framework that 'educates and clearly defines a token … establishes a common set of terms … creates a Token Classification Hierarchy … and decomposes tokens into parts [to] drive reuse and innovation.'[189]

(iv) Direct regulation

As indicated throughout this report, technology-specific regulation does need to be approached with caution. As a jurisdiction, regulators such as the FCA have consistently adopted a technology-neutral approach, choosing to support innovation through other means, such as the use of regulatory sandboxes and the provision of guidance to provide clarity as to the application of the regulatory perimeter to, for example, ICOs. Whilst regulatory intervention may be necessary to remove impediments to reform or provide clarity as to the characterisation of DLT activities (such as the classification of tokens), at this stage more wide-reaching legislation risks unintended consequences. Rather, the implementation of a proactive programme of research, engagement and education will be both efficient and effective in identifying opportunities and risks, thereby enabling an appropriate and measured response to be developed in line with the better regulation principles. If regulation is deemed necessary, and in keeping with the approach adopted by this jurisdiction to date, regard should be had to technology-neutral intervention where possible (recognising that in some instances this may not be appropriate).

CONCLUSION

DLT offers a significant opportunity to the UK to innovate, increase opportunities and choice to its citizens and retain its position as the jurisdiction of choice. However, it does raise a number of questions for regulators as to the timing, substance and design of any intervention. Ensuring that any such regulatory response is correct is crucial to meeting regulatory objectives and professional principles, thereby supporting innovation, increasing diversity within the profession and protecting the public interest.

Looking more broadly at the needs of industry, the UK is an important venue for developing a robust legal framework that offers certainty, security and reliability. As a jurisdiction, it benefits from a common law system, an independent and technologically aware judiciary and is a global leader in terms of legal and engineering talent (amongst others). The legal services market makes a substantial and direct contribution to the UK's economy but is also a key enabler of other commercial activity and investment, including the development of innovative technologies such as DLT. This report provides an introduction to that technology and identifies some of the key considerations that oversight and front line regulators may wish to consider when determining how best to respond to DLT in accordance with their own obligations. The nature of DLT is such that these insights will necessarily need to be kept under continuous review. However, the key themes throughout this report, of education and research predicated on meaningful multi-disciplinary collaboration, are likely to remain constant as mechanisms to ensure the effectiveness and legitimacy of any future activity.

[188] https://inatba.org

[189] Ethereum Enterprise Alliance, 'Token Taxonomy Initiative' (2019), 2. Available: < https://entethalliance.org/wp-content/uploads/2019/04/EEA-The-Token-Economy-v11-1.pdf> accessed 19 May 2019.

Key points to note:

- DLTs offer significant potential for the sector. This potential can be realised by identifying and, where relevant, removing barriers to growth and providing certainty as to fundamental questions such as the classification of cryptoassets and the likely application of existing legal principles.

- Legal services regulators can provide important support to the market through education and training initiatives as well as the development of best practice and other guidance materials.

- Regulators have considerable convening power that can be engaged to facilitate multi-disciplinary collaborations that help to: (i) identify obstacles to innovation; (ii) advance the knowledge of the sector; and (iii) embed fundamental legal principles into the design and development stage of DLT projects.

- To help meet the perennial challenge of supporting innovation in the market whilst protecting consumer interests, regulators should consider a continuum of options including: (i) research and consultation; (ii) education and training; and (iii) the development of standards and other guidance.

- DLT is a rapidly developing market and regulators should undertake regular reviews of their strategic response. As part of this review, regulators should be cognisant of other activities in this space to avoid a proliferation of duplicative activities. Rather, a coordination of efforts, where appropriate, will help to escalate understanding and reduce the risk of a piecemeal regulatory landscape.