TECH
LONDON
ADVOCATES
BLOCKCHAIN
LEGAL AND
REGULATORY

The Law
Society

Blockchain: Legal & Regulatory Guidance

NOTICE

This Guidance does not constitute legal advice. It is intended to provide technical guidance and suggestions as to best practice for legal practitioners when dealing with matters involving blockchain and distributed ledger technology. The authors of this Guidance accept no liability for any claim in connection with any action or inaction of any party acting in reliance on the contents herein.

CONTENTS

FOREWORD

The authors of Tech London Advocates' (TLA) Blockchain Legal and Regulatory Guidance are to be congratulated. Guidance in this area is in short supply.

As the authors acknowledge, only the UK Jurisdiction Taskforce has previously attempted any such thing, by publishing its Legal Statement on the status of Cryptoassets and Smart Contracts under English Law in November 2019. Since then, the world has been overtaken by the terrible Covid-19 pandemic, which has caused all of us to re-think the ways things are done. Tech in general, and LawTech in particular, has come into its own.

This sudden acceleration in use has only emphasised our need to understand the ways in which technology is affecting our professional lives. Lawyers face a steep learning curve. They will need to become familiar with DLT, smart legal contracts and cryptoassets – conceptually and functionally. This Guidance is an important step on that path. It explains use cases for both DLT and smart contracts, and considers their commercialisation. It considers how cryptoassets will enter the mainstream, and analyses the interaction between intellectual property and cryptoassets.

It raises significant issues as to data protection and data governance that every lawyer will face in the immediate future. It illustrates the uses and pitfalls of blockchain consortia.

Most critically, perhaps, TLA's Blockchain Legal and Regulatory Guidance suggests best practice for legal practitioners working on transactions involving smart contracts, and raises questions concerning the need for the development of on-chain dispute resolution mechanisms, which the UK Jurisdiction Taskforce is itself actively working on.

I am sure that further iterations will follow. Anne Rose and her colleagues are blazing an important trail.

The Rt Hon Sir Geoffrey Vos, Chancellor of the High Court

PRESIDENTIAL FOREWORD

Technology underpins innovation in legal services and plays a critical role in driving the post-coronavirus recovery across all sectors of the economy.

Our research indicates that the adoption of new technologies could reduce the cost of legal services to UK business users by £350 million by 2030[1], and double productivity growth in the legal sector. And since every £1 of productivity saving in the legal services sector in 2020 could generate between £3.30 and £3.50 of additional GDP for the UK by 2050, while every £1 increase in legal productivity in 2020 is estimated to result in £9.15 to £10.61 of additional capital by 2050, investing in LawTech now will lay the foundations for the UK's long-term prosperity.[2]

Lawyers are becoming quite familiar with emerging technologies like Distributed Ledger Technology, smart legal contracts and cryptoassets. The pandemic has incentivised firms of all types and sizes to embrace new technologies. As the economy recovers, we will see a further increase in LawTech adoption rates across the profession. The work of the TLA's Blockchain Legal and Regulatory Group and the work of the UK Jurisdiction Taskforce have demonstrated that English common law and jurisdiction is flexible and able to adapt to new technologies.

The report of the TLA's Blockchain Legal and Regulatory Group will provide a clear framework and much needed guidance on the use of blockchain in the legal services sector.

It is most welcome and relevant.

Simon Davis, President of The Law Society

[1] Analysis available from The Law Society on request

[2] The Law Society, 'Contribution of the UK Legal Services Sector to the UK Economy Report' (23 January 2020) <https://www.lawsociety.org.uk/topics/research/contribution-of-the-uk-legal-services-sector-to-the-uk-economy-report> Accessed 29 July 2020

INTRODUCTION

Anne Rose, Co-Lead - Blockchain Group, Mishcon de Reya LLP

Tech London Advocates

TLA was founded by Russ Shaw in 2013 *"to ensure an independent voice of* [the] *technology sector was heard"*. TLA now comprises a network of more than 9,000 tech leaders, entrepreneurs and experts in London, across the UK and in over 50 countries worldwide. Proudly independent, private sector-led and not backed by government, TLA fundamentally believes that London is one of the world's leading tech hubs.

TLA Blockchain Working Group

TLA's dedicated Blockchain working group was founded in 2018, and serves as a hub for talented multi-disciplinary DLT experts. The TLA Blockchain Legal and Regulatory Group (the **Group**) was founded as a sub-group of TLA Blockchain in May 2018 by Anne Rose (Mishcon de Reya LLP). The Group is comprised of lawyers and technologists from the UK's leading law firms, legal consulting firms and academic institutions. A list of the Group's members is provided at Annex 2.

The Group's objectives are to: (i) assist legal practitioners when they are required to advise their clients on matters related to DLT; and (ii) identify and set out areas in which further guidance is required from regulatory authorities or other bodies. In support of these objectives, the members of the Group analyse real life use case examples of DLT. They consider a variety of technical, legal and practical issues and are supported by academics and technologists, businesses and individuals, and lawyers and non-lawyers from a number of different industries. The Group has held a number of seminars, presentations and meetings to consider these issues, including presentations given by experts such as Cassius Kiani (Atlas Neue), and Professor Michael Mainelli (Z/Yen Group). A full list of experts who have addressed and fed into the Group's work is set out at Annex 3.

Guidance

I see 2020 as a breakthrough year for DLT. The disruption caused by the COVID-19 pandemic has forced governments and businesses to re-evaluate their service and business models more fundamentally than ever before. Organisations that have historically been slow to embrace change – lawyers included – are now, by necessity, making great strides to innovate and are looking to emerging technologies such as blockchain to help them do so.

The purpose of this Guidance is to set out suggested best practice for legal practitioners working on transactions involving Smart Legal Contracts and solutions to anticipated problems. In particular, the Guidance sets out some key issues for legal practitioners to be aware of when advising on DLT-related matters such as commercial applications, smart contracts, data governance, blockchain consortia, data protection and security, intellectual property, dispute resolution and cryptoassets. The Guidance also identifies some areas in which further guidance is required from regulatory authorities or other bodies.

To date, the only formal legal statement in the UK in respect of DLT-related matters focuses on addressing very specific and limited questions, with the specific objective of providing answers to critical legal questions under English law and a legally recognised reference for counsel and the judiciary. I am referring to the UK Jurisdiction Taskforce's Public Consultation[3] and subsequent Legal Statement on

[3] UKJT Consultation paper, '*The Status of Cryptoassets, DLT and Smart Contracts Under English Private lLaw*' (London: The LawTech Delivery Panel, 2019) < www.lawsociety.org.uk/news/stories/cryptoassets-dlt-and-smart-contracts-ukjt-consultation/> Accessed 28 December 2019

the status of cryptoassets and smart contracts under English private law (**Legal Statement**).[4] This Guidance does not propose to build on the Legal Statement but rather (as noted above) to look at a number of different areas of concern where there is the need for clarity and/or additional guidance from regulatory authorities or other bodies.

I hope this Guidance is useful for legal practitioners. For the avoidance of doubt, this Guidance is not intended to be prescriptive or rigid in its application. Given the current state of DLT maturity, any prescriptive approach would likely fail.

Moreover, definitions used are intended to be interpreted broadly. The multiplicity of definitions used in relation to DLT and blockchain technology remain inconsistent and this issue is complicated particularly in this space by the divergence between legal practitioners and technologists on specific definitions in a given context, a simple example being the different interpretation of the word “execute” for a lawyer and a coder. The need to “craft simple yet usable definitions of the technology” is one of the primary recommendations of The European Union Blockchain Observatory & Forum.[5] I agree with this recommendation but do not propose to provide such definitions in this Guidance. The inclusion of a glossary in the Guidance was raised in the Group and it was agreed that the focus should be on providing legal practitioners with a useful and practical resource that expresses the knowledge and ideas of its members whilst leaving space for interpretation. Consistent with the intention to avoid prescriptive or rigid application of the Guidance, and given the constantly evolving nature of the technology, the terms and definitions used are also not intended to be prescriptive. Where contributors consider specific definitions are required in a section for the purposes of interpretation, these are included at the beginning of the relevant section but apply to that section only and do not necessarily flow through the Guidance as a whole. We have provided a list of common abbreviations at page 12.

Acknowledgments

It has been an absolute pleasure to lead this Group and collaborate with so many fantastic, cognitively diverse lawyers over the past year and I strongly believe that through collaboration and the provision of legal certainty, the DLT ecosystem in the UK will flourish.

I want to thank all of those who have freely given their time to make the Guidance possible. Special thanks goes out to: Marc Piano of Harneys (Cayman Islands) whose support and encouragement throughout this entire process has been invaluable and without which this Guidance wouldn't be possible; Phil Leonard (Waterfront Solicitors LLP) for his endless enthusiasm and support; and Sian Harding (Mishcon de Reya LLP) for assisting with the final compilation of the report.

Special thanks also to all those who lead the sub-groups and have written submissions to this Guidance, including: Jonathan Emmanuel (Bird & Bird LLP); Sue McLean (Baker McKenzie LLP); Akber Datoo, (D2 Legal Technology); Adi Ben-Ari (Applied Blockchain); Rosie Burbidge (Gunnercooke LLP); John Shaw, (Blake Morgan LLP); Charlie Lyons-Rothbart (Wiggin LLP); Will Foulkes (Thrings LLP); Marc Jones (Stewarts LLP); Charlie Morgan and Natasha Blycha (Herbert Smith Freehills LLP); Craig Orr QC (One Essex Court); Heenal Vasu (Allen & Overy LLP); Laura Douglas (Clifford Chance LLP), Ceri Stoner and Jennifer Anderson (Wiggin LLP), and Tom Grogan (Mishcon de Reya LLP).

And finally, my special thanks to William McSweeney, The Law Society of England and Wales, and the dauntless early readers of this Guidance including: Cassius Kiani (Atlas Neue); Adam Rose, Nina O'Sullivan, Elena Georgiou, Shulamit Aberbach, Oliver Millichap, Laura Price, Niara Lee, Henry Farris

[4] UKJT, ‘*Legal Statement on Cryptoassets and Smart Contracts’* (London: The LawTech Delivery Panel, 2019) <https://35z8e83m1ih83drye280o9d1-wpengine.netdna-ssl.com/wp-content/uploads/2019/11/6.6056_JO_Cryptocurrencies_Statement_FINAL_WEB_111119-1.pdf> Accessed 28 December 2019

[5] The European Union Blockchain Observatory & Forum, ‘*Legal and Regulatory Framework of Blockchains and Smart Contracts’* (Thematic Report, 27 September 2019) <https://www.eublockchainforum.eu/sites/default/files/reports/report_legal_v1.0.pdf > Accessed 28 June 2020

(Mishcon de Reya LLP); Wendy Saunders, Thomas Gooch, and Elina Kyselchuk (Herbert Smith Freehills LLP); and Sam Quicke (Linklaters LLP).

COMMON ABBREVIATIONS

AML	Anti-Money Laundering
API	Application Programming Interfaces
DAO	Decentralised Autonomous Organisations
DLT	Distributed Ledger Technology
GDPR	The General Data Protection Regulation (EU) 2016/679
IoT	Internet of Things
IP	Intellectual Property
IPR	Intellectual Property Rights
SLC	Smart Legal Contract
UKJT	UK Jurisdiction Taskforce
ZKP	Zero Knowledge Proof

CHAPTER SUMMARIES

***Commercial Application*:**

Covering key considerations relevant to the conception, application and adoption of blockchain / DLT technologies by an enterprise including: public vs. private blockchains; setting up a private blockchain; and contracting for private blockchains.

This section includes a use case example in the retail and consumer sector with a private blockchain being used to track and trace goods.

Smart Contracts and ***Data Governance*:**

This section is split in two parts. Part A provides an in-depth analysis of the advantages & disadvantages of SLCs, as well as consideration of hybrid partial digitisation of contracts.

Part A then goes on to detail specific considerations for digitisation projects in the context of automating SLCs and transactions, highlighting in particular those elements of a legal contract and transaction flow that can and should be digitised. It provides, in addition, real-world examples of successful projects to date.

The impact of DAOs on the legal profession and fundamental questions relating to the legal characterisation and legal personality of DAOs is then addressed.

Part B focuses on the centrality of data governance to successful smart contract development and digitisation, particularly given the inherent automaticity of SLCs.

This section highlights the importance of implementing data governance frameworks and other key considerations when incorporating big data into digitisation projects. The detail in this section on the dimensions of data quality, how data quality can be assessed and the policies to be utilised in verifying data quality are particularly informative.

***Blockchain Consortia*:**

Blockchain consortia are collaborative ventures between groups of organisations that are designed to develop, promote, enhance or access blockchain / DLT technologies. This section provides a detailed overview of the types of blockchain consortia, the reasons for the use of blockchain consortia and a consideration of the two most widely adopted blockchain consortia models before addressing key legal risks and issues to be considered when joining or creating consortia including: investment, governance, liability, competition, IPRs, compliance and tax.

***Data Protection*:** and ***Data Security*:**

This section is split in two parts. Part A draws on expert evidence from the ICO and key actors in both the academic and private sphere to acknowledge the fundamental tensions that exist between blockchain technology and the GDPR. It focusses its analysis on questions that are particularly problematic for practitioners, namely the definition of ‘personal data’ and the impact of technological changes on the blockchain / DLT space.

The analysis of how definitions of ‘personal data’ affect the application of the GDPR underlines the importance of practitioners understanding and assessing the context in which data is stored, transferred and expressed when considering blockchain / DLT implementation. Technical measures relating to re-identification, specifically pseudonymisation and anonymisation, are also considered in light of tensions with the GDPR.

The section ends with a number of proposed questions to be addressed by data authorities.

Part B focuses on ZKPs and how these work to increase data privacy and utility whilst minimising data sharing. It sets out a number of properties and types of ZKPs and provides an illustrative use case relating to proof of age.

This section demonstrates the centrality of ZKPs to the development of blockchain / DLT technologies given that ZKPs have the potential to solve both data privacy and verifiability issues at the same time.

Other Privacy Enhancing Technologies (PETs) are addressed at the end of the section.

***Intellectual Property*:**

This section sets out a comprehensive overview of the potential impact of blockchain / DLT on the recording, protection, management and enforcement of IPRs.

This section explores multiple facets of IPRs in the context of blockchain / DLT, making critical comparisons with current case law that serve to illustrate the wide range of impacts that these technologies could have across copyright, trademark, design rights, database rights, confidential information and patents.

This section also raises interesting questions for further consideration regarding the subsistence of copyright protection in DLT architecture, cryptoassets and smart contracts as well as ancillary points on jurisdiction and exhaustion.

***Dispute Resolution*:**

This section is split in three parts. Part A looks holistically at the impact of technological change, and blockchain / DLT technologies specifically, on the legal profession in a contentious context and the challenges these present to the administration of justice and procedural fairness.

Part B provides a highly logical and practical review of the options for on-chain dispute resolution. This section provides actionable advice to practitioners seeking to understand or advise on the impact of DLT / blockchain technologies in the context of dispute resolution and the development of resolution-facilitating technology. It covers both the availability of on-chain dispute resolution mechanisms and explores specific concerns arising from questions of the scope, soundness & reliability of these mechanisms to resolve the full range of potential disputes.

Part C delivers a forensic analysis of the availability and utility of traditional off-chain dispute resolution mechanisms in the context of blockchain / DLT. It addresses legal questions that are fundamental to the efficient and effective governance of any blockchain / DLT system, namely: jurisdiction, applicability of laws and money laundering.

This section covers in detail the availability of arbitration and traditional litigation to both permissioned and permissionless systems, as well as addressing property law aspects relevant to digital assets held on blockchain / DLT systems. It goes on to address the anti-money laundering regulations applicable to blockchain / DLT technologies and digital assets from an EU & UK perspective.

***Regulation of Cryptoassets*:**

Sets out an in-depth overview of the treatment of cryptoassets from a regulatory perspective, both in the UK and worldwide, and consideration of the complicated intersection between the characterisation and treatment of cryptoassets that legal practitioners are required to evaluate from both a regulatory and legal perspective.

Adopting the FCA taxonomy, the regulatory treatment of security tokens, e-money tokens and unregulated tokens is covered in detail in addition to the relevant prudential requirements.

This section is particularly instructive in its detailed presentation of the future regulatory changes to be expected in this space and is an essential resource for assessing the global regulatory approach to cryptoassets.

***Blockchain and Tax*:**

The transformative potential of DLT extends to the tax system, where there is immense scope for disruption. DLT and blockchain technology have the potential to revolutionise how transactions are taxed and reported given the core characteristics of the technology. This section deals with three key tax issues for legal practitioners: taxation of cryptoassets and blockchain; the impact of blockchain on the in-house tax function; and the impact of blockchain on tax authorities.

KEY RECOMMENDATIONS

Commercial Application

Recommendations:

- The key recommendations of the Commercial Application section have significant crossover with other sections of the Guidance, with an emphasis on greater clarity for both developers and participants regarding: liability for lost or corrupted data, standards of data security for blockchain service providers, availability of dispute resolution mechanisms and clarity on IP ownership in the context of DLT and blockchains.

Law Society & TLA Activities:

- Further engagement with those designing, developing, procuring or deploying commercial applications of blockchain technologies to produce cross-sector guidance.

- Engagement and collaboration with data protection supervisory authorities, insurers, regulators and intellectual property offices on the contents of this report.

Data Governance

Recommendations:

- The adoption of effective data governance measures, in addition to strategic and long-term approaches to platform choice and digitisation, are central to reducing risk in digitisation projects.

- When designing smart contracts we propose the following changes to best practice be adopted:
  - data input variables should specify data governance and quality requirements; and
  - the data quality parameters should define the contract scope, including scenarios in which automated performance would not be within the expectations of the contracting parties.

- Applications of smart contracts should assist parties with their wider data governance and quality compliance obligations, for example through the provision of data lineage to back up any automated performance step by way of an audit trail. This may be particularly necessary for certain applications in regulated areas (as required by BCBS239 ("Principles for effective risk data aggregation and risk reporting") in the banking industry).

Law Society & TLA Activities:

- Produce a thought leadership series with stakeholders on the application of technology, and how technology can contribute to compliance and be effectively leveraged for data governance.

- Produce a coding and data governance toolkit to enable the procurement of blockchain technologies.

Blockchain Consortia

Recommendations:

- Blockchain consortia can be essential in order to develop and scale blockchain platforms which enable digital transformation across a sector or a group of industry stakeholders. However, as multi-party arrangements, they can be complex to set up and operate successfully. There are a number of factors that businesses will need to take into account when forming or joining a consortium and a range of issues for their legal advisers to consider. Lawyers can add significant value to a consortium project and we recommend that they get involved early in consortium discussions to ensure that the consortium is set up for success.

Law Society & TLA Activities:

- Host roundtables to discuss practical challenges with blockchain consortia creation and governance.

- Host workshops for both DLT providers and legal practitioners, enabling both parties to build understanding of, and the capability to take part in, collaborative blockchain projects.

- Develop guidance to support cross-sector blockchain consortia creation and collaboration. This guidance could include:
  - a list of common issues encountered and mitigation strategies in relation to those issues;

  - the provision of a procurement and risk tool kit which includes the main considerations to be considered when entering into a consortium, enabling SMEs and other stakeholders to follow best practice.

Data Protection & Data Security Enhancing Measures

Recommendations:

- Recital 26 of the GDPR assumes a risk-based approach to assessing whether or not information is personal data; in contrast, the Article 29 Working Party (now the European Data Protection Board) suggests that a risk-based approach is not appropriate. Further guidance is required from data protection authorities in relation to this, as well as the elements that should be taken into account when assessing whether information is personal data, particularly in relation to how such data is stored, transferred and expressed on DLT and blockchain platforms.

- In considering the steps to take to prevent identification when using blockchain technology, we note that there is at present no legal certainty for developers wishing to handle public keys in a GDPR compliant manner, and it is considered that further guidance is needed from data protection authorities in respect of this.

- In addition, we consider that some of the questions to be addressed by the ICO and other data authorities should include the following:
  - Does the use of a blockchain automatically trigger an obligation to carry out a data protection impact assessment?

  - Does the continued processing of data on blockchains satisfy the compelling legitimate ground criterion under Article 21 GDPR?

  - How should 'erasure' be interpreted for the purposes of Article 17 GDPR in the context of blockchain technologies?

    - How should Article 18 GDPR regarding the restriction of processing be interpreted in the context of blockchain technologies?

    - What is the status of anonymity solutions such as ZKP under GDPR?

    - What is the status of the on-chain hash where transactional data is stored off-chain and subsequently erased?

    - Can a data subject be a data controller in relation to personal data that relates to them, particularly in the context of a data subject operating a node on a DLT or blockchain platform?

    - How should the principle of data minimisation be interpreted in relation to blockchains?

Law Society & TLA Activities:

- Engage and collaborate with data protection supervisory authorities to develop a framework for determining the applicability of data protection regulations to DLT and blockchain platforms.

- Convene a roundtable with data protection and security stakeholders to establish a process for developing targeted guidance around the issues identified.

Intellectual Property

Recommendations:

- It would be beneficial for there to be guidance or further commentary on how existing copyright case law on "communication to the public" will be applied to DLT, and whether any liability may fall to core software developers or other interested parties given the development of accessory liability in relation to online copyright infringement.

- It has been made clear by the court that websites operating on a model similar to The Pirate Bay will be considered to commit copyright infringement due to the number of original works posted on the site (without authorisation) and the profit making nature of those sites. Greater clarity on how this decision may be applied in future to DLT would be beneficial.

- In addition:
    - Regarding database rights, we note there is no legal certainty for developers on the level of database right protection for their creations. There is a need for clarification from the court on whether, and to what extent, a database right will subsist in DLT and any DLT-based application.

    - In relation to confidential information, we note that there is currently a risk relating to whether the cryptographic security tiled in DLT is sufficiently secure to enable confidential information to be stored on-chain. Guidance on whether the cryptography used in DLT is sufficiently secure in this way would increase confidence in the technology.

    - In relation to IP subsisting in the DLT framework itself, we note that there is little guidance or commentary on which elements of DLT, such as the underlying software or design, are capable of being protected. Further commentary on whether, and to what extent, the technology and networks (including smart contracts) will be protected by each of copyright (e.g. in the software code), database right (e.g. in the ledger structure), or patent (e.g. in the block building process) would be beneficial for practitioners so that there can be an understanding amongst key stake holders as to the level of protection that may be achieved in the DLT framework itself.

    - It would be beneficial for there to be guidance on whether the distributed nature of DLT will be influenced by territoriality of IPRs, given the different jurisdictions in which various actors may be based.

Law Society & TLA Activities:

- Engage and collaborate with the Intellectual Property Office, Law Commission and UK LawTech Delivery Panel to:
    - Establish which elements in the DLT framework are capable of being protected;
    - Determine how copyright law will be applied to DLT in the areas identified;
    - Establish which protections database creators will be entitled to, and whether the protections subsist in DLT;
    - Identify the minimum-security standard for confidential information to be stored on-chain; and
    - Ascertain what influence other territories will have on IPRs, and how these rights will be enforceable given the distributed nature of DLT.

Dispute Resolution

Recommendations:

- There are at present no recognised standards or judicial treatment which might make on-chain dispute resolution mechanisms a viable alternative to traditional dispute resolution options. Guidance from the judiciary and arbitrational bodies as to the effectiveness and form of on-chain dispute resolution mechanisms would be incredibly useful in improving commercial confidence in the ability to successfully seek remedies without recourse to litigation, the costs of which would likely be increased due to the technology.

- We consider that authoritative guidance should be developed and published regarding best practice standards for digitised dispute resolution solutions, including on-chain elements where appropriate, to expedite the efficiencies and legal insights of such solutions. In particular:
    - guidance from the London Court of International Arbitration (LCIA) as to whether it envisages the need for specialist rules or whether the flexible design of the current regime is deemed to be sufficient; and
    - the potential for arbitrational bodies to endorse, or otherwise provide guidance, on current forms of on-chain dispute resolution such as Kleros, Juris, Codelegit, and Confideal.

- Parties should consider entering into a master or 'umbrella' dispute resolution agreement that codifies the agreed applicable law and dispute resolution procedure throughout the chain and allows for disputes to be joined or consolidated where appropriate, further to the Financial Markets Law Committee (FMLC) report.

- Parties should consider carefully the choice of law, depending on the quality, willingness and expertise of lawyers and the judiciary in the jurisdiction of choice. Those which have so far shown a willingness to engage constructively with DLT include England, Singapore and Switzerland.

- An international approach to, and consensus on:
    - regulating anonymous participants in DLT and blockchain networks, particularly in relation to cryptocurrencies, in order to counter their illicit use without unduly restricting technological innovation; and

    - the regulation of exchanges and custodian wallet providers, as well those participants who are currently widely unregulated such as miners and those using peer-to-peer exchanges.

Law Society & TLA Activities:

- Engage and collaborate with Government and the judiciary to discuss on-chain dispute resolution.

  Continue to monitor regulatory and legislative approaches globally to enable those using DLT to select a beneficial jurisdiction.

Regulation of Cryptoassets

Recommendations:

- Legislation and/or regulatory guidance should be provided on whether the use of cryptoassets as collateral would be deemed to be enforceable security under the laws of England and Wales.

- Legislation and/or regulatory guidance should be provided clarifying that any cryptoassets will not be considered as a commodity or fiat currency under the laws of England and Wales.

- Legislation and/or regulatory guidance should be provided clarifying which regulatory requirements apply to "hybrid" cryptoassets and cryptoassets that move between categories throughout their lifetime, particularly with respect to authorisation requirements under the Electronic Money Regulations 2011 and Financial Services and Markets Act 2000, and the registration requirements under the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017.

- Perimeter guidance should be provided with respect to the activities of acting as a "cryptoasset exchange provider" and "custodian wallet provider".

- Perimeter guidance should be provided in the context of the application of the UK financial promotion regime, outsourcing and conduct rules in respect of crypto-related services and business models.

- The PRA should set out a detailed prudential framework for cryptoassets, and as part of this, detail any additional guidance, including measures under Pillar II (i.e. discretionary supervisory measures and, potentially, additional capital charges). Moreover, it would be helpful for there to be clarification of the accounting treatment of cryptoassets to avoid queries about their prudential treatment under current EU prudential laws and regulation.

- Given that the law and regulations governing the current post-trade market infrastructure in the UK were not designed with DLT in mind, it is considered that an assessment should be undertaken of whether the UK legislative and regulatory framework for post-trade infrastructure needs to be adapted to facilitate market adoption of DLT technology (and if so, how), including, but not limited to the impact of the European Market Infrastructure Regulation, Securities Financing Transactions Regulation or the Central Securities Depositories Regulation (CSDR). As part of this assessment, it would be helpful to explore the implications of CSDR book-entry form requirements for cryptoassets and be provided with guidance on how they are to operate in practice.

- Similarly, given that the UK legislative and regulatory framework governing financial markets has not been developed with cryptoassets in mind, we recommend carrying out an assessment of the current framework, including but not limited to the Markets in Financial Instruments Regulation and the Market Abuse Regulation to identify whether there are gaps in the current framework that do not adequately address risks posed by cryptoassets, or whether other adjustments may be required (and are desirable) to facilitate the development of efficient and orderly markets in cryptoassets.

Law Society & TLA Activities:

- Further engagement between those designing, developing, procuring or deploying blockchain technologies and the FCA.

Blockchain and Tax

Recommendations:

- Alignment of the legal and tax perspectives on the nature of assets and transactions using blockchain technology.

- Current HMRC Guidance should be updated to provide clear, consistent HMRC guidelines.

- Further guidance and specific legislation is required to guide tax practitioners through the key issues in advising on the correct tax treatment of all aspects of distributed ledger transactions.

- UK government-backed cross sector working groups should be established and/or re-energised to identify areas where the taxation of blockchain technology can be addressed and progressed. Key focus areas could include:
    - transactional taxes: for example, VAT, withholding tax, stamp duties and insurance premium taxes;
    - transfer pricing: for example, codification of subjective judgments as to how profits are attributed to different parts of the business. From a technical perspective, this is theoretically possible; and
    - double taxation: could an international information exchange enable the reduction of double taxation?

- HMRC's adoption of technology: blockchain could be harnessed by tax authorities for mutual benefit, i.e. to reduce the compliance burden on tax functions and improve relations with taxpayers through the efficient capture of reliable information. Stakeholders should be consulted on a timely basis as government considers how to roll out blockchain and adopt the technology for the benefit of all. Many stakeholders would probably favour a focus on identifying where efficiencies can be made, rather than a wholesale reform of the tax system. For example, issues to be addressed should include:

  - Controlled pilot testing: this should identify where tax efficiencies could be made prior to investment by the government and also the taxpayer. This would prevent the pre-emptive roll out of government tax initiatives such as ‘Making Tax Digital’, which placed a high time and cost burden on the taxpayer.

  - Rollouts of new digital systems: i.e. how to best implement a phased introduction where the old system is steadily retired. New technology could be rolled out according to size, sector, geography or tax type, such as is already in progress amongst early adopters of digital systems, for example in Russia.

  - Mandating a new digital system: the UK Government recently estimated that there is about £6.5bn of tax uncollected due to small business errors. It is considered that approximately £600m could be collected with a digital system but only 10% would come about if companies were transferred only voluntarily to the new system. As such, mandating could be a valuable approach.[6] This benefit to the Treasury should however be balanced against the initial burden on all, but in particular small and medium sized companies (or individuals) who, without the right tools and/or knowhow, are particularly likely to struggle to cope, especially in these otherwise challenging times.

  - Ministerial ownership: cross government buy-in will be key, given that many digital solutions rely on information being shared across government departments. The ultimate aim should also be for solutions to be compatible with the international tax system and the UK’s cross border information sharing obligations.

  - Third party involvement: it seems inevitable that there will be significant reliance on third party software providers. As such, relationships need to be nurtured, and time and resources spent identifying and adapting external systems (e.g. CREST) and improving internal systems.

Law Society & TLA Blockchain Legal and Regulatory Activities:

- Further engagement between those designing, developing, procuring or deploying blockchain technologies and HMRC.

[6] Letter from David Gauke MP (then Financial Secretary to the Treasury) letter to MPs, ‘Making Tax Digital’, (8 May 2016) < https://www.parliament.uk/documents/commons-committees/treasury/FST-to-Chairman-Making-Tax-Digital-10-May-2016.pdf> Accessed 14 August 2020

SECTION 1: COMMERCIAL APPLICATION

Jonathan Emmanuel, Bird & Bird LLP

Introduction

There has been much media hype surrounding blockchain technologies, driven (in part) by the huge price rises of cryptoassets, such as Bitcoin, that exist on the Bitcoin public blockchain. However, since the peak of late 2017/early 2018, there has been a significant drop in the price of Bitcoin and other similar cryptoassets (although prices have stabilised recently) and last year Gartner announced that blockchain technologies had entered the "Trough of Disillusionment" in its Hype Cycle.

That being said, Gartner predicts that blockchain technologies will begin to climb out of this Trough of Disillusionment by 2021 (although this prediction was made prior to the COVID-19 pandemic) and other experts have predicted a "blockchain spring" as enterprises, armed with the lessons learned from previous blockchain proof of concept implementations, target more limited blockchain deployments focused on solving specific use cases and utilising private blockchains. Often these use cases relate to how data exchange between disparate parties can be more efficiently recorded and shared, which some experts have called the "internet of record".

This section analyses a potential use case in the retail and consumer sector. Firstly, however, it is important to understand why enterprises are choosing private blockchains over public blockchains or centralised databases. When we refer to "blockchains" in this section, we are referring to the network of nodes comprising a blockchain, which could be a private or public blockchain depending on the context.

Public vs private?

The cryptoassets Bitcoin and Ether are underpinned by public blockchains (the public Bitcoin blockchain and the public Ethereum blockchain, respectively). Generally speaking, these blockchains share some common features:

- **Fully decentralised:** anyone can download the blockchain software on their computer to set up a node that connects with other nodes in the network over the internet. Each node in the network is a "peer" meaning there is no one node or entity in charge of running the network. The network is run by the blockchain software or protocol.

- **Broadcast-based blockchain:** once connected, these nodes can download a copy of the blockchain, send transactions for recording on the blockchain and view all entries in the blockchain.

- **No contracts:** there are no (or very limited) formal contracts in place governing the rights and responsibilities of the participants. For example, there are no (or very limited) rules governing stakeholder participation in the blockchain.

- **Consensus mechanism:** the blockchain will have a consensus mechanism built into the blockchain software that determines when a new transaction can be recorded on the blockchain.

There are many benefits associated with these features. As the blockchain is decentralised, participants do not have to trust an always-available central authority to manage it, and the blockchain's broadcast-based nature means that there is full transparency on the data held on the blockchain.

However, there are also drawbacks. The lack of formal contracts in place makes it harder for participants to easily understand their rights and responsibilities and bring claims against entities they think have caused them to suffer loss. For example, if the blockchain goes down because of a bug in the software operating on all the nodes, what recourse do affected participants have? Moreover, the consensus mechanism ("proof of work"[7] for the Bitcoin public blockchain) is time-consuming and costly to run.

For these reasons, and in our experience, enterprises are more interested in private blockchains. Again, these blockchains share some common features:

- **Trusted intermediary:** there is one entity in charge of running the nodes that make up the private blockchain network. Depending on the use case, this could be a regulator, joint venture entity or a company limited by guarantee.

- **Control:** the trusted intermediary decides what data participants can send for recording on the blockchain and what data they can view.

- **Contracts:** there are formal contracts in place governing the development of the blockchain and participation in it, which provide stakeholders with more certainty over their rights if things go wrong.

Private vs central database?

One question to ask, however, is this: why should enterprises implement private blockchains given that the existence of a trusted intermediary reintroduces the concept of a central authority, resulting in little difference between a private blockchain and a centralised database?

Whilst there is some truth to this, there are in fact many benefits specific to blockchain technologies (compared with centralised databases) which mean that private blockchains can be useful in the right circumstances. For example:

- **Immutability:** once data has been recorded on a blockchain, it is very difficult to change it without it becoming immediately obvious to all participants and rejected by them (as necessary).

- **Digital signatures:** the use of digital signatures makes it easier for disparate parties to approve and send data for recording on a blockchain without the need to rely on a third party. This makes it easier to coordinate input from disparate parties.

- **Peer-to-peer:** as the blockchain network is peer-to-peer, it can continue to function even if some of the nodes in the network become unavailable. This makes the network more robust than networks reliant on a central database as there is no single point of failure which could result in the database being unavailable if the server hosting it is unavailable.

Setting up a private blockchain

The process of setting up a private blockchain is, generally, as follows:

- **Trusted intermediary:** the trusted intermediary downloads the blockchain software and sets up the nodes that comprise the network. It is not necessary to have only one trusted intermediary, although this is common; the process may in fact involve multiple trusted intermediaries with authority over the blockchain software, who may then subcontract out this authority to other entities. A trusted intermediary, or each of the trusted intermediaries where more than one are used, is in charge of the blockchain because it runs and operates the nodes that comprise the network, either by itself or by delegating the running of the nodes (and therefore the validation of transactions on the blockchain) to its subcontractors.

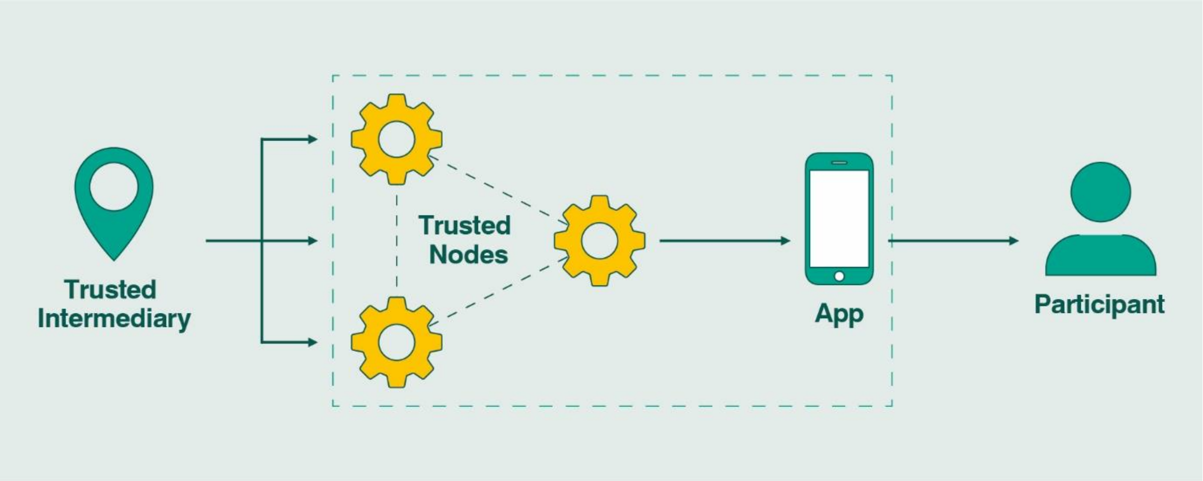
[7] See Annex 1

- **User-facing application (app):** the trusted intermediary builds an app (for example, a mobile app) that interfaces with the nodes and through which participants can access the nodes.

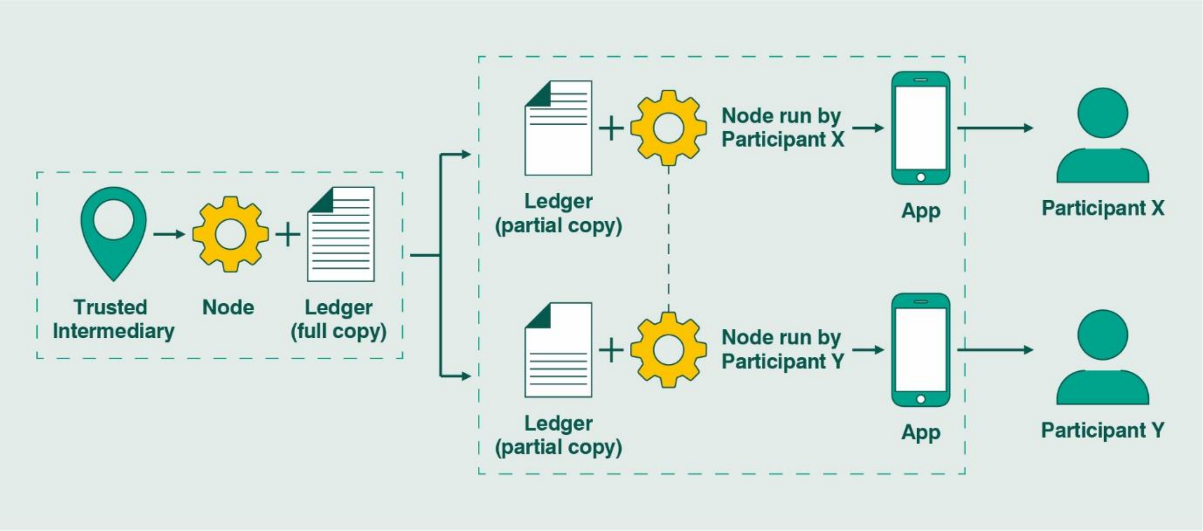
- **Participants:** the participants access the trusted intermediary's nodes via the app. Using the app, participants can send data to be recorded on the private blockchain and view the data recorded on the private blockchain.

In our experience, there are two models that are most commonly used when setting up a private blockchain:

- **Distributed ledger model:** the trusted intermediary runs all the nodes and participants access the nodes on a software-as-a-service basis.



- **Shared ledger model:** the trusted intermediary runs a node that hosts a full copy of the database. Participants can also run their own nodes that download a partial copy of the database (this copy only includes data to which the relevant participant is a counterparty).



Use case

There are a number of use cases being trialled by different enterprises. For example, in the retail and consumer sector, enterprises are using private blockchains to track and trace goods.

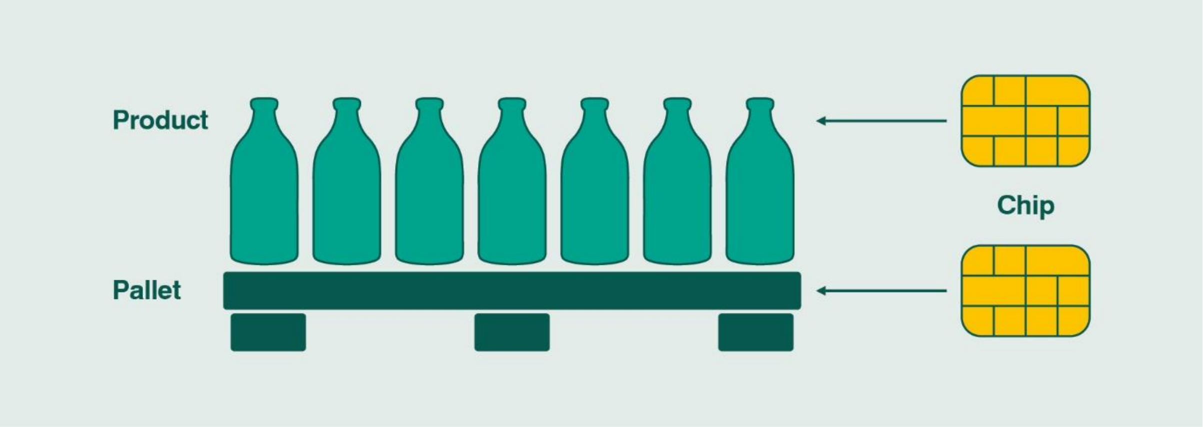
In this example, the trusted intermediary might be a food standards agency or supermarket, and the participants might be farmers, distributors or IoT devices (devices that connect to the blockchain over the internet).

It might work as follows:

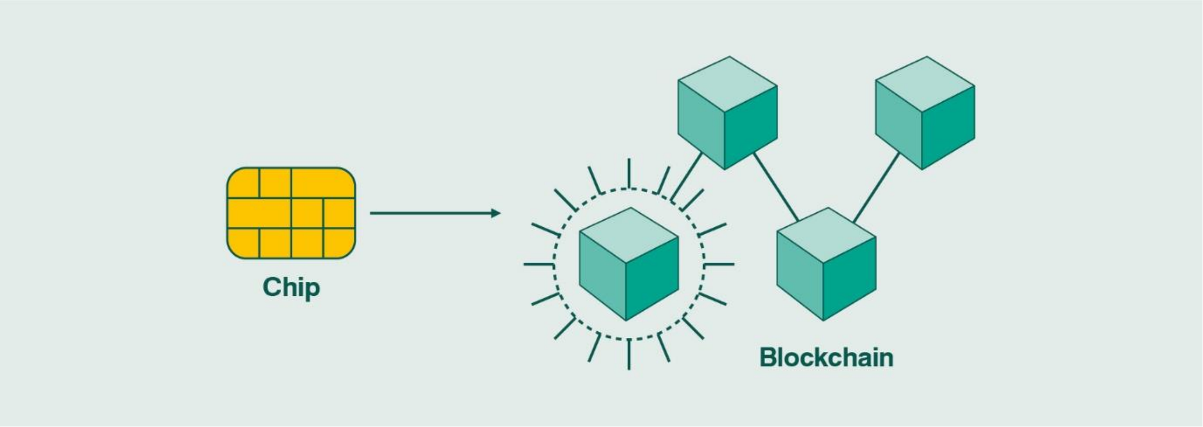
- The trusted intermediary, a supermarket, sets up a private blockchain (based on the distributed ledger model described above).

- Farmers access the private blockchain by accessing the app built by the trusted intermediary.

- Farmers prepare a pallet of goods (for example, milk bottles). Each pallet has a RFID chip / QR code (an **identifier**) and each bottle in the pallet has an identifier. Each farmer's identifiers are linked, making it easy to track and trace all of their goods. When the identifier is scanned, it shows data relevant to the pallet, for example, the farm's name, its location, and a certificate of authenticity of the goods (**Farmer's Data**). The Farmer's Data is verified by a human before the data is linked to the identifier.



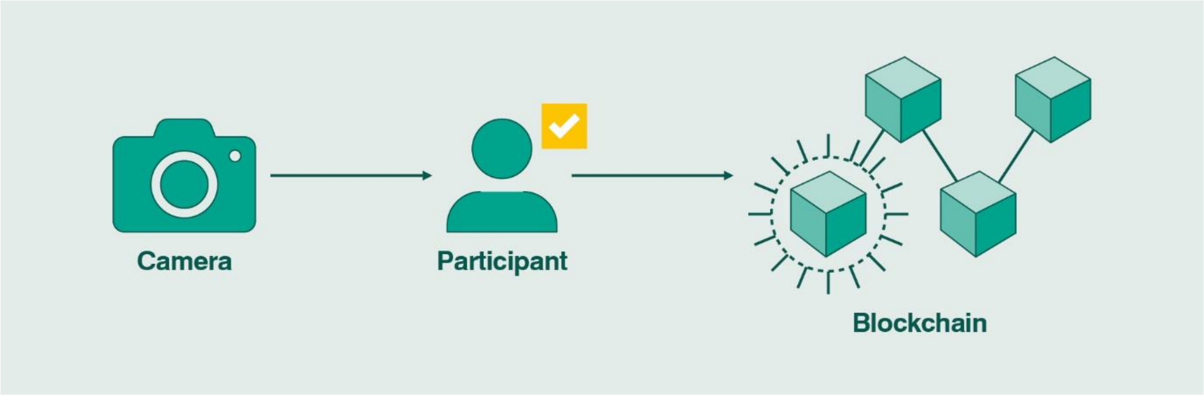
- When the goods are ready for delivery to the supermarket, the farmer accesses the app and sends the identifier (which is linked to the underlying data described above) for recording on the blockchain.



- At this point the distributor will receive a prompt to collect the goods from the relevant farm.

- The distributor will pick up the goods and then deliver them to the supermarket. The act of picking up the goods and delivering them to the supermarket (including the times at which these activities occurred) can be sent as data entries to be recorded on the blockchain.

- IoT devices can be connected to the blockchain and send data to it. For example, cameras installed at the pick-up location of the farmer's warehouse and delivery location of the supermarket's warehouse can be configured to send camera images to be recorded on the blockchain at the times the distributor confirms pick-up and delivery of the goods (as described in the point above).



- The Farmer's Data is sent by the farmer to the blockchain and is automatically recorded once the goods are ready for delivery.

- The distributor's entries to the blockchain (pick-up and delivery) will be sent to the blockchain with the camera images from the IoT devices. This bundle of data can be verified by a third party auditor and once confirmed can be recorded on the blockchain.

- The verification of certain data points by third parties helps mitigate the risk of "garbage in, garbage out" (i.e. bad data being recorded automatically on the blockchain which is assumed to be correct).

- If there is a problem with the goods, then the relevant stakeholder(s) can consult the blockchain to find out where the goods are, whether at the farmer's warehouse ready to be delivered, at the supermarket's warehouse or in transit. Since each pallet from a farm is linked, it is easier to quickly locate their whereabouts and safely and efficiently recall them in the event of a problem.

Contracting for private blockchains

As mentioned above, enterprises are likely to be attracted to private blockchains over public blockchains for a number of reasons, including because there is greater certainty of the rules governing how these blockchain networks operate. These rules will be set out in contracts.

Generally, there are two main contracts:

- **Blockchain services contract:** this is the contract between the blockchain developer and the trusted intermediary. Under this contract, the blockchain developer will licence its blockchain software and provide support services to the trusted intermediary to help it set up the network and operate it.

- **Participation contract:** this is the contract that governs access to the blockchain network, and is made between the trusted intermediary and each participant.

It is important that any commitments made by the trusted intermediary (for example, availability service levels) under the participation contract are appropriately backed off under the terms of the blockchain services contract. Other key issues that arise include liability (what happens if data is lost or corrupted), security (what security measures are being utilised by the trusted intermediary to ensure the integrity of the network), suspension and termination (the rights of the trusted intermediary to suspend or terminate access to the network) and IP (the ownership of IP in any bespoke developments – see below).

Who owns IP in the blockchain?

At a basic level, the blockchain network will constitute the back-end blockchain software and the user-facing app.

The blockchain software determines how data is recorded on the distributed database. The user-facing app is what each participant accesses to send transactions for recording onto the blockchain and will interoperate with the blockchain software via application programming interfaces (**APIs**).

The blockchain software will often be pre-existing software that is used by the blockchain developer to service multiple clients. The user-facing app will often be bespoke software developed by the blockchain developer for the trusted intermediary to solve its particular use case.

One of the key IP battlegrounds between the blockchain developer and trusted intermediary is who owns the IP in the user-facing app. Analogous to traditional software development agreements, there are commercial considerations for parties around various aspects of the IP in both the blockchain software and the user-facing app. Establishing the ownership and licence limitations of pre-existing IP and IP generated in the development of the blockchain network is fundamental and will likely be influenced to a greater or lesser degree by the level of customisation and bespoke design necessary to the creation of the app, in addition to any proposals to “white-label” the app. Further considerations around use of, and liability for, the incorporation of both third party and open source software into the development of the app should be addressed early in the development process. One potential middle-ground position is for the IP in the app to vest with the blockchain developer, but for the trusted intermediary to have a wide licence (for example, exclusive for a certain period of time) to use the IP in the app in order to use the blockchain network and also to modify the app for use with other blockchain networks (i.e. with another blockchain developer's software). For this to work, it is important that the app is developed in such a way to avoid "lock-in" with a particular blockchain developer's solution.

Conclusion

Critics of blockchains have described them as "a solution looking for a problem". There is no doubt that blockchain is not the solution for every kind of problem. However, in some specific cases, a private blockchain may be useful because the technology makes it hard to edit data once it has been recorded on the blockchain; and, by virtue of the use of digital signatures, helps to bring together disparate parties for better coordination and sharing of data. In other cases however, having a trusted central authority as the golden source of data is no bad thing, and can often be the best option. For example, people trust a government department such as HM Land Registry in the UK to run a central database for recording land and property ownership because they trust the UK government, and they trust the UK government to compensate anyone who suffers loss because of any error or omission in the central database. Sometimes centralised is better than decentralised.

SECTION 2: SMART CONTRACTS AND DATA GOVERNANCE

Anne Rose (Mishcon de Reya LLP) and Marc Piano (Harneys (Cayman Islands))

PART A: Smart Contracts

Introduction

Smart contract technology, the process of digitising legal contracts and/or transactions using any combination of Smart Legal Contracts, Smart Contract Code, Internal Models and External Models as defined below, theoretically permits any written legal contract to be digitised into self-executing code. In turn, traditional transaction flows can be digitised in whole or in parts, using tokenised representation of transactional objects where required.

Several in-house and public projects already permit digitisation of contracts and transactions at least in part. Some of these projects are explored in this report.

As at the date of this report, projects range across open and closed systems, using a combination of open source and proprietary platforms and processes. Each project and the nature of the legal contracts and transactions involved has unique requirements and objectives. Taken together with the benefits and drawbacks of automating elements of English law, each project approaches the use of smart contracts in digitising and automating legal contracts and transactions differently.

The scale, level of development and public accessibility varies for each of the projects explored. However, all experts who gave evidence on their projects demonstrated development far beyond proof of concept, and are well placed to give evidence on the issues forming the subject of this report.

Objectives of the coding sub-group

The coding sub-group has four objectives:

1. Identify the extent to which different types of existing, primarily document-based, legal transactions are and/or may in future be carried out by or through smart contracts, and/or DLT technology and/or cryptoassets (in whole or in part);

2. Identify the current and/or future role of legal professionals in such transactional processes with a focus on the technical elements;

3. Identify, using recent examples, transactional flow and parties involved from a technical perspective; and

4. Identify, using recent examples, areas of risk, opportunity, responsibility, liability and value add for legal professionals and law firms in respect of the technical elements of such transaction processes.

Experts and evidence

The group convened on four evidence telephone sessions between November 2019 and February 2020, at which expert evidence was heard from each of:

Niall Roche (Head of Distributed Systems Engineering, Mishcon de Reya LLP)

Niall Roche is the Head of Distributed Systems Engineering at Mishcon de Reya LLP and a Senior Teaching Fellow at the UCL School of Management. As a member of the UCL Centre for Blockchain

Technology (CBT), Niall has been involved in DLT projects in the real estate, construction, legal and retail supply chain.

Niall is an active member of the real estate and construction working groups of the Accord Project. This work led to his involvement in the Digital Street initiative run by HM Land Registry to create the first proof of concept residential property transaction in the UK using DLT.

Ciarán McGonagle (Assistant General Counsel, International Swaps and Derivatives Association (ISDA))

Ciarán McGonagle is responsible for ISDA's legal work on fintech, including smart contracts and distributed ledger technology. Mr. McGonagle also leads ISDA's Legal Technology Working Group, which is responsible for delivering increased standardisation and digitisation of ISDA documentation. Mr. McGonagle also supports ISDA's legal and policy work on EU financial services regulation.

Prior to joining ISDA, Mr. McGonagle spent over five years at Deutsche Bank, where he worked in the bank's legal department specialising in derivatives and structured products. He also spent some time in Deutsche Bank's Global Regulatory Management Group. He has also worked at Morgan Stanley and at Allen & Overy.

Mr. McGonagle has a law degree from Queen's University Belfast.

Akber Datoo (Founder and CEO, D2 Legal Technology (D2LT))

Akber Datoo is the founder and CEO of D2LT, a global legal consulting firm advising clients on the use of technology and data to unlock business value through legal change and operating at the intersection of FinTech and LegalTech. After graduating with first class honours in Computer Science from Cambridge University, Akber began his career as a technologist at the investment bank UBS. Through this, he saw an opportunity for digital transformation across the legal profession and decided to retrain and qualify as a lawyer, working at law firm Allen & Overy.

Akber founded D2LT in 2011, where he has overseen its international growth during the last nine years. He was appointed to the Law Society's Technology and Law Committee in 2016 and is the author of the Wiley textbook, "Legal Data – Banking & Finance", published in May 2019.

Aaron Wright (Professor, Cardozo School of Law and Co-Founder, OpenLaw)

Aaron Wright is a Co-Founder of OpenLaw, its Chief Executive Officer and a Professor at Cardozo School of Law in New York City. He is also Director of Cardozo's Blockchain Project and formerly Senior Vice President of Product/Business Development and General Counsel at Wikia.

The coding sub-group thanks each of the experts for their time and contribution, without which this report would not be possible.

Definitions

Drawing from the definitions provided by Ciarán McGonagle:

- **Smart Legal Contracts**: a written and legally enforceable contract where certain obligations may be represented by or written in code; and

- **Smart Contract Code**: code that is designed to execute certain tasks if pre-defined conditions are met. Such code may or may not be intended to give effect to legal provisions or have legal ramifications. In some cases, such code is required for the internal function of an SLC, or communication between smart contracts (whether pursuant to contractual provisions or not).

Two potential SLC models:

- **Internal Model**: the provisions that can be performed automatically are included in the legal contract, but are rewritten in a more formal representation than the current natural language form; and

- **External Model:** the coded provisions remain external to the legal contract, and represent only a mechanism for automated performance.

Digitising legal contracts and/or transactions may use any combination of SLCs, Smart Contract Code, Internal Models and External Models.

Findings

The findings of the group are divided into four parts:

1. Advantages and disadvantages of SLCs;

2. Data governance;

3. Digitisation considerations; and

4. Additional comments.

Advantages and disadvantages of Smart Legal Contracts

In summary, the advantages and disadvantages of SLCs are:

Advantages

- **Increased accuracy and potential transparency of contractual terms**: the logic and information in each contract may be visible to all participants in the blockchain network (although, where relevant, some or all contractual terms can be made confidential, visible only to the transacting parties and hidden from the wider network). This transparency combined with automatic execution facilitates an environment of trust, and removes manual errors.

- **Efficiency in automating performance**: standard-form SLCs can be written so as to permit limited negotiation of commercial and legal terms. This is particularly beneficial for high-volume contracts and transactions. Negotiated contracts and related transactions can be quickly deployed and concluded by making the assembly of contracts dependent on variables or computable logic provided by the contracting party. Tokenised value or objects can be quickly transferred with an automatically generated audit trail.

- **Less scope for misinterpretation or competing interpretations**: subject to good data governance, standardised definitions and provisions in SLCs will automatically execute in accordance with their agreed terms. Where provisions of an SLC or elements of a transaction occur off-chain, appropriate on-chain or off-chain dispute resolution mechanisms can resolve issues arising from competing interpretations more efficiently than traditional methods, the availability and applicability of on-chain and off-chain dispute resolution methods are explored in more detail at Section 6.

- **Potential evidential value of deployed contracts, electronic outputs and audit trail of tokenised representations of subject matter or value**: computer code is more definitive, precise and immediate than traditional paper-based contracts. Electronic outputs – such as documents, inter-contract activity and external outputs – together with automatic generation of an audit trail of transfers of tokens, can help to minimise disputes around fulfilment of contractual terms and ownership of title.

- **Scope for efficient dispute resolution using novel and inherent dispute resolution mechanisms**: elements of a contract or transaction in dispute may be isolated and resolved quickly and efficiently without necessarily affecting the wider contract or transaction. Importantly, a smart contract can escrow or parties can pre-authorise the transfer of funds at issue and an arbitrator can render a decision and direct payment to one or both parties, thereby decreasing the need for post-litigation enforcement proceedings.

- **Interoperability:** contractual data can be imported and exported into an SLC, which can be useful to keep track of contracts and manage risk. If deployed at scale, for example in relation to derivatives contracts where the collection, storage and dissemination of data is imperative to assessing risk, it is conceivable that a particular jurisdiction utilising SLCs would be able to have a more detailed view of the economy by analysing and aggregating contractual information in an anonymised manner.

Disadvantages

- **Over-automation:** not all elements of a legal contract that can be automated should be, such as provisions over which parties may wish to retain discretion to amend or waive from time to time. Over-automation due to poor digitisation planning or otherwise may inadvertently restrict the flexibility that is often expected and exercised over some contractual provisions, and expose parties to unintended risk.

- **Full automation is not always possible**: some terms implied by English law which require subjective assessment of the parties' intentions, or which must allow external intervention or determination, are not easily automatable. Attempts to do so may result in contracts being unenforceable or not fully reflecting the intentions of the parties. Digitisation scoping must seek to identify and address these issues.

- **Unsuitable contracts or transactions**: highly complex, one-off transactions contingent on many external parties and factors may not be suitable for automation, along with more “relational contracts”, which are assembled by the parties to memorialise an agreement to engage in commerce as opposed to precisely defining the rights and obligations of members.

- **Systems interoperability**: where there are SLCs and transactions dependent on external actors or systems, it may not be possible to fully automate or complete electronically. Proper digitisation considerations will identify and address these issues and facilitate off-platform fulfilment of relevant contractual provisions.

- **Inflexibility to amend contracts or waive provisions due to immutability**: where an automated term is expressed incorrectly, it may be that parties are unable to prevent or reverse performance, particularly given the immutability of DLT records.

- **Necessity to pre-fund accounts due to the automation of movements of value**: while SLCs have the potential to be able to automate movements of value (for example, collateral movements in the context of collateralised derivatives agreements) and so create several operational efficiencies, in order to achieve this automation it may be necessary for counterparties to pre-fund specific accounts/wallets which are linked to the smart contract code.

This may not be practical or efficient in all markets, as it may mean that any such pre-funded value would not be capable of being used by its owner while it remains in the pre-funded account.

- **The "oracle problem":** to achieve the extensive automation which SLCs could be capable of, many SLCs need to be able to rely on objective sources of external data which both parties can trust (the so-called "oracle problem"). For example, with respect to an SLC which is designed to trigger a payout in the event that one party to a contract enters into insolvency proceedings, the smart contract would need to rely on an external data point which is capable of accurately confirming that a winding-up petition (or equivalent) has indeed been filed in relation to that party. These oracles may not always be available.

Data governance

A working definition of data governance from the Data Governance Institute is "*the exercise of decision-making and authority for data-related matters*". By extension, data governance involves marshalling and unifying consistency and accuracy of data used in digitisation projects, such as defined terms, mechanical clauses, representations and warranties, covenants, standards, and rights and obligations.

Data governance forms a fundamental prerequisite of any digitisation project. Data governance failure can result in contractual uncertainty, legal or regulatory breaches, failure of automated provisions and unnecessary disputes arising.

Any digitisation project should therefore involve a data governance audit at the outset. This can include an internal glossary to ensure common standards within an organisation, an audit of any data subject to digitisation, standardisation of relevant data, and portability across documents and platforms. In particular, legal agreement terms play a crucial role in respect of smart contracts, and any data inputs and outputs need to have appropriate data governance to ensure certainty and completeness of contractual terms (which in the context of a smart contract, can often manifest themselves through data variables).

Effective data governance measures will assist in efficient contract and transaction digitisation, and reduce risk to all parties.

More information on data governance is set out in Part B of this Section.

Digitisation

Stakeholders (being transaction parties, businesses, and service providers including law firms or other intermediaries) in seeking to wholly or partially automate legal contracts and transactions undertake a form of digitisation project.

General scoping and project management considerations for digitisation projects will apply. These considerations are beyond the scope of this report, and detailed resources on the topic are already widely available.

However, the sub-group does recommend additional considerations specific to legal contract and transaction digitisation.

Choice of platform

Digitisation need not necessarily involve the development of an entirely new platform or protocol. The sub-group heard evidence from each of ISDA, Mishcon de Reya and OpenLaw, each of which utilised different approaches to digitisation. ISDA has developed an industry-standard, digitised representation of derivatives transactions and events called the ISDA Common Domain Model. Mishcon de Reya, as part of the "Digital Street" project, utilised the open source Accord Project. OpenLaw developed a protocol to allow digitisation, execution and tokenisation of any legal document.

The requirements of contractual parties and advisors for a particular contract or transaction, or series thereof, will influence the approach that is right in the particular circumstances.

We would caution that the complexity and risks inherent to a digitisation project lend to a strategic and longer-term approach in platform choice and digitisation generally. It may not be efficient, for example, to digitise a contract or transaction specific to one particular platform if the likely volume or subsequent demand for digitisation lends to development of an in-house protocol or use of a different platform in future.

Finally, choice of platform should include due diligence on use of third party protocols (whether open source or proprietary, and permissioned (private) or permissionless (public)) to assess suitability and risk relevant to the particular transaction(s) and intentions of the parties. As this technology space continues to evolve, regard should be had to development roadmaps, and continued suitability and support availability (where relevant) across the intended lifespan of the transaction and possible subsequent changes in relevant law and regulation, particularly for relatively novel protocols or offerings. Where a digitisation project includes critical reliance on third party services beyond a protocol itself – such as use of oracles – the role of those services and any recourse to responsible entities should be carefully considered. This may include analysis of sources, data and transaction flows and any standard terms of use of each third party service. Reviews of terms and service should focus in particular on any representations and warranties as to service availability, accuracy and verification (or disclaimer thereof) of data flows where input data is sourced from third parties, liability clauses, and governing law, jurisdiction and dispute resolution. Where appropriate, it may be prudent to negotiate with critical third party service providers to contract on bespoke terms.

Effective and efficient digitisation

Consideration must be given to which elements of a legal contract and transaction flow can and should be digitised, and which should not. It is not feasible to develop a set of general best practice guidelines, as these will be specific to the contracts, transactions and project objectives in each case. We can, however, provide examples of the different approaches taken from the evidence provided to the sub-group.

ISDA

ISDA's evidence focussed on the work they are doing to develop a foundation for the development of smart derivatives contracts. ISDA's approach involves distinguishing between operational aspects (i.e. mechanical elements such as delivery or payment) and non-operational aspects (relating to time, or rights and obligations) within a derivatives contract.

Whilst many elements of derivatives contracts lend to digitisation, many do not. These include elements common to many contracts, such as representations and warranties, document delivery obligations, payment obligations subject to withholding, set-off or other deductions, transfer or assignment of contractual rights, events of default and insolvency events.

In its presentation to the group, ISDA noted that: "*This complexity and potential need for human intervention in respect of certain events, such as the triggering of an Event of Default, may mean that it may never be efficient or desirable to automate certain parts of a derivatives contract, even if it were technically possible.*"

D2LT – ISDA Clause Taxonomy

D2LT's evidence detailed, inter alia, the legal agreement digitisation work it had completed for ISDA, designed to work together with the ISDA Common Domain Model. One of the issues the OTC derivatives industry faces was the huge variation in language of legacy ISDA Master Agreements between market participants. Although in some cases the language of particular clauses achieved different business outcomes, in many cases, the substance of the business outcome was identical – only the form/style of the legal drafting differed. This offered a significant impediment to efforts to automation, be it: (i) generation of new agreements; (ii) management of the contractual obligations contained within the agreements downstream (e.g. liquidity and collateral management); or (iii) use of AI and smart contract applications. Accordingly, the ISDA Master Agreement Clause Taxonomy was developed, which defines the various clauses contained within an ISDA Master Agreement, and enumerates the main business outcomes that parties negotiate within these agreements (determined with regard to twelve pre-defined design principles). Such standards are necessary to facilitate the automation of legal contractual obligations.

"Digital Street" program

Similar considerations formed part of the development of the "Digital Street" project for HM Land Registry, through the open-source Accord Project ecosystem.

The Digital Street project furthers HM Land Registry's ambition of becoming the world's leading land registry for speed, simplicity and an open approach to data through the use of blockchain technology to develop a simpler, faster and cheaper land registration process.

The program did not digitise the Standard Conditions of Sale owing to their complexity. As an alternative, the Accord Project permits digitisation of clauses that are independent of any particular distributed ledger, enabling global interoperability. The project is therefore able to digitise such clauses, as they are conducive to digitisation, while enveloping compliance with, and fulfilment of, non-digitised clauses offline pursuant to established conveyancing protocols.

The project further allows any disputes to be resolved offline, and the outcome to be recorded within the digitised transaction flow. As the project develops, the intent is to make clear to the parties which elements of the contract and transaction are fulfilled online and which will occur offline, without requiring separate processes running in parallel and fitting within the wider digitisation envelope.

OpenLaw

OpenLaw has developed an open source protocol for contract digitisation, execution, workflow management and tokenisation.

The protocol permits any legal document to be digitised according to the requirements of the parties. This approach affords flexibility for the parties to determine digitisation of contracts and transactions according to their agreed parameters for any particular transaction. However, we observe that this requires such parties and their legal counsel to have undertaken diligent digitisation scoping on a contract and transaction basis to ensure that digitised contracts and transactions are legally enforceable and commercially viable.

While OpenLaw is aimed at lawyers, for the time being they must be trained or be self-taught in the use of the mark-up language necessary to create programmable legal agreements capable of execution (e.g. basic logic actions and calculations). The solution currently utilises the Ethereum platform to manage the contract execution actions, but can be generalised to other systems and does not need to rely on a blockchain. On execution, the smart contract related evidence, if incorporated into an agreement, is recorded and managed on the Ethereum blockchain.

The solution provides contract management support and automatically saves contracts on third party cloud hosting platforms such as Dropbox, Google Drive, and Microsoft One Drive.

OpenLaw provides a public "library", but also permits parties to run their own private instance to enable peer-to-peer contracting. Parties that run an OpenLaw instance can pass contractual information between one another without the need to share that information with third parties.

Any limitations of the proprietary mark-up language were not discussed in the evidence session, but users of OpenLaw must give careful consideration to the use of the mark-up language to effect complex multi-party agreements.

Additional comments

Legal contracts and transactions best suited for smart contract digitisation are those which:

- already occur at scale, using standard-form documents and standardised transaction flow;
- operate within a range of known or knowable variables and events, each of which can be accommodated during the digitisation and automated transaction process;
- can access external third-party data (through sources known as "oracles") available in a standard and processable form from trusted sources, where required; and
- produce deliverables or outputs in forms that can be accommodated as part of the digitisation process.

Legal counsel will play a central role in digitisation of contracts or transactions as both counsel and likely project managers. They will therefore be required to fully scope any digitisation project from both a legal and project management perspective. This will involve choice of platform, extent of digitisation, anticipating any technical or legal issues which may arise, and identification and coordination of stakeholders. As an additional safeguard, a well-scoped independent code audit can assist with objective confirmation that the code-dependent constituent elements give proper effect to legal and commercial terms, identify unintended mechanics and security risks, and generally provide comfort to all relevant parties that the code implements the desired transaction according to the agreed terms that reflect the parties' intentions.

Legal counsel should always consider whether digitisation can fully allow implied terms, application of principles derived from precedent, facilitation of industry or market standards, and the flexibility to amend contracts where required due to changes in law, regulation or where contingent on external input, such as third party expert determinations.

Inadequate digitisation scoping may risk breach of contract or frustration due to unanticipated issues arising from automatic execution. This may heighten transaction risk for the parties and unnecessarily strain commercial relationships.

Legal counsel may be exposed to liability when facilitating a digitised contract or transaction where full consideration has not been given to the digitisation and transaction flow process, and unintended consequences arise. We note that there is no judicial determination on these specific points as at the date of this report. We do not offer any legal opinion on likely risk or determination on these points, however the changing risk landscape for lawyers is addressed in more detail at Section 6, Part A.

Automating transaction elements best concluded off-chain

As seen above, digitisation is not an "all or nothing" process and is not without risk. Digitisation of contracts and transactions can involve a hybrid partial digitisation and off-chain fulfilment of some contractual provisions not suitable for digitisation. For some contracts and transactions, this hybrid approach may be unavoidable to ensure contractual soundness and proper reflection of commercial intent.

This means that, where relevant, any digitisation must be able to facilitate and record off-chain compliance (or breach and any relevant remedies) as part of the digitised contract and transaction flow. This influences digitisation scoping, choice of platform, transaction flow and record generation. In some cases, the additional work required for full or partial digitisation may outweigh any time and cost efficiencies gained from digitisation, particularly for highly complex or one-off transactions.

Dispute resolution considerations

As at the date of this report, numerous on-chain dispute resolution mechanisms are available. These may have the equivalent effect of an arbitration clause in a traditional contract.

However, any digitisation must carefully consider whether these mechanisms provide sufficient scope to resolve the full range of potential disputes that may arise in a digitised contract or transaction.

The soundness and enforceability of these mechanisms has not yet been challenged or given judicial consideration. For example, mechanisms that are only able to determine digitised matters and not off-chain matters, or are contingent on pre-appointed arbitrators who are no longer available, may be open to challenge.

Reliance on any dispute resolution mechanism must also consider the ability to enforce any decisions issued through them, as well as any scope for appeal. Unlike traditional arbitration protocols, there is also no recognised set of clauses for proper incorporation, operation, appeal or enforcement.

Further, the novel nature of these mechanisms may themselves be the source of dispute, increasing legal costs and risk for both parties.

As at the date of this report, we consider that on-chain dispute resolution mechanisms lack any recognised standards or judicial treatment which might make them a viable alternative to traditional dispute resolution options. Both on-chain and off-chain dispute resolution mechanisms are addressed in more detail in Section 6.

Regulatory considerations

The Financial Action Task Force (**FATF**) is an intergovernmental organisation that develops policies to combat money laundering. The FATF Recommendations require all jurisdictions to impose specified AML/CFT requirements on financial institutions and designated non-financial businesses and progressions.

In October 2018, the FATF adopted changes to its Recommendations to explicitly clarify that they apply to financial activities involving virtual assets, also defining "virtual assets" and "virtual asset service providers".

Current FATF Guidance[8] on a risk-based approach to virtual asset activities or operations and virtual asset service providers may apply to some stakeholders, parties or counterparties where smart

[8] The Financial Action Task Force, '*Virtual Assets and Virtual Asset Service Providers, Guidance for a Risk-based Approach,* (June 2019) <https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf> Accessed 13 April 2020

contracts are used to effect legal transactions involving the transfer of virtual assets. In particular, relevant platforms and service providers may be deemed to be virtual asset service providers and fall to be regulated (for AML/CFT purposes at a minimum) by a relevant financial services regulator.

Detailed consideration of this issue is outside the scope of this report, but this issue is raised to ensure that parties and stakeholders consider any regulatory issues which may arise out of activities involving virtual assets where used to effect legal transactions by or through smart contracts involving tokenisation, and activities involving such tokens. Specific legal advice should be taken where needed.

Decentralised Autonomous Organisations and the impact they may have on the legal profession

Marc Jones (Stewarts LLP)

What is a Decentralised Autonomous Organisation (DAO)?

One of the main problems in the developing (and connected) areas of digital assets, smart contracts and DAOs is the terminology. For example, there are (with only slight exaggeration) almost as many definitions of a cryptocurrency as there are cryptocurrencies. The authors of the recent Legal Statement on Cryptocurrencies and Smart Contracts recognised the problem:

> "*Because of the great variety of systems in use and kinds of assets represented (ranging from purely notional payment tokens such as bitcoins to real-world tangible objects) it is difficult to formulate a precise definition of a cryptoasset and, given the rapid development of the technology, that would not be a useful exercise… As with cryptoassets, it is difficult, and unlikely to be useful, to try to formulate a precise definition of smart contracts and so we have again sought instead to identify what it is about them that may be legally novel or distinctive*."[9]

The same can be said for DAOs. As such, it is perhaps easier to start with the broad "idea" of a DAO. Cryptocurrencies, smart contracts and DAOs have all emerged from a philosophy that, amongst other things, seeks to replace human involvement with the automaticity and immutability of distributed ledger technology. Human involvement – error, inaction or fraud – is eliminated. A DAO is simply an extension of this idea to an organisational structure, the actions of which are automated by code, both in terms of its own governance and/or its commercial activities. It is a smart contract or network of smart contracts on an organisational scale.

At this point, a real world example will help. The original DAO, helpfully called "The DAO", was a venture capital fund. It had no board of directors and no management structure in any traditional sense. The DAO was simply code deployed on the Ethereum blockchain as a set of pre-programmed instructions. It was created by Slock.it UG, a German corporation, whose founders promoted The DAO in a variety of fora. Anyone could invest in The DAO by transferring Ether (a cryptocurrency) to The DAO. In return, investors were allocated DAO Tokens and a register of token ownership, like a share register, was maintained by The DAO. The purpose of The DAO was to invest these funds in project proposals, which were themselves in the form of smart contracts that existed on the Ethereum Blockchain. Token-holders were entitled to vote on which proposals should be funded (and indeed that was largely the extent to which Token-holders were involved) and the votes were administered by The DAO. The DAO would also calculate and administer returns on investments. So, apart from the initial contribution of Ether (which required human action), The DAO administered everything. It is in this sense that it was "autonomous".

The structure used by The DAO functions well as long as a DAO does not have to interact with the physical world. For example, The DAO could invest in proposals that were themselves smart contacts, because the entire process of investment, performance and return was governed and enforced by code.

[9] UKJT Legal Statement (n 4) paras 26 and 135

However The DAO could not, for example, have invested in opportunities that required the negotiation of complex financial terms and contracts, or the inspection of physical goods, because that would require human involvement, and would not be "autonomous". Equally, transacting in fiat currency as opposed to cryptocurrencies was not feasible because it would have involved The DAO interacting with the regular banking system, thereby exposing The DAO to, and making it in some part dependent on, human action. As such, there are at present very obvious and significant limits to the use of DAOs.

It must be noted, however, that the "autonomous" aspect of any DAO is, in any event, pretty slippery. Turning back to The DAO itself, the above outline is in fact an over-simplification of the reality. For example, The DAO had "curators", a group of individuals (humans) chosen by Slock.it who, amongst other things, had complete control over which proposals could be voted on by Token-holders, and who would carry out due diligence on proposals to ensure that the code matched the proposal. Equally, when The DAO was hacked and one-third of The DAO's Ether stolen, the only solution open to The DAO – or more accurately the Token-holders, because the DAO could not itself initiate any kind of mitigation – was to persuade a sufficient number of humans running Ethereum, The DAO's software platform, to amend the code in order to undo the hackers' action.

The legal question

So what does all this mean for the legal characterisation of DAOs? Again, as with cryptocurrencies and as the example above is intended to illustrate, the answer is going to be highly fact specific and will depend on the precise characteristics of each DAO.

Two aspects of DAOs have drawn most attention: its purported "organisational" nature, and its automaticity. In terms of determining what a DAO is, it is suggested that automaticity is a red herring. Smart contracts have that same characteristic but it is not suggested that as a result a smart contract has a separate legal personality from the contracting parties. Automaticity does (and will) give rise to very difficult issues (for example, of intention and mistake, as demonstrated recently in the Quoine litigation[10]) but legal personality is not one of them.

It is the organisational nature of DAOs that gives rise to the most significant legal and commercial issues: does a DAO interpose a separate legal entity between, putting it at its broadest, those involved with the DAO internally (e.g. developers, investors) and those who transact with the DAO externally? If so, is it with a DAO that external parties enter into legal relations? And, critically for investors in DAOs, do liabilities arising from a DAO's activities rest with the DAO (effectively providing the protection of limited liability to investors) or with investors, developers or others? Finally, answering those issues will also involve determining what the relationships(s) is (are) between those involved with a DAO internally.

In considering these points, it is helpful to refer back to the example of The DAO. Not only did Slock.it create The DAO, but its co-founders promoted it and created a website for that purpose. In that type of scenario, it is conceivable that serious defects in the code might found claims for breach of contract or negligence against the programmer by investors. The DAO might be treated as a unilateral contract (an offer made by the developer which is accepted by the investor by the transfer of funds), or the creator may be found to have assumed a duty of care to investors. Equally, anyone promoting the DAO could be at risk of claims for negligent (or fraudulent) misrepresentation. In that case, there may be no relationship between investors; each may simply have a contractual relationship with the developer, and the DAO's "governance" aspects may constitute nothing more than the automated exercise of the developer's investment and other management decisions. The precise history and features of each DAO will be critical.

[10] *B2C2 Ltd v Quoine Ptd Ltd* [2019] SGHC(I)

The same might apply to third parties. The DAO might be characterised as a service offered by the developer, and the underlying reality may be that investors provide financial backing to the developer to pursue his enterprise for profit. In that case, one can see the DAO wrapper counting for very little and liability falling on the developer. However, this avoids the more difficult issue: what if the only humans in the frame are the investors, the “token-holders”?

If it is assumed that a DAO exists with no human involvement save for its investors, what is the relationship between investors *inter se* and with third parties? The DAO's original White Paper contains the interesting statement that a DAO “*can be used by individuals working together collaboratively outside of a traditional corporate form. It can also be used by a registered corporate entity to automate formal governance rules contained in corporate bylaws or imposed by law*.”[11] In the latter case, a DAO is simply an IT solution to improve a traditional company’s governance procedures, and if that is all we were talking about, we wouldn’t be talking about it. It is the idea of a DAO as an entity “outside of a traditional corporate form” that is said to cause problems. But does it really? The short point is that a DAO by its very nature is not, cannot be, and is not designed to be a company of any kind. Companies are legal constructs; if the legal requirements necessary to constitute a particular type of company are not met, the company does not exist. A DAO's "token-holders" are simply a number of individual investors who are carrying on business in common with a view to profit. That looks very much like a general partnership. The alternative, an unincorporated association, is not an available option unless the purpose of the group is not for profit; a limited liability partnership is also not an option because it requires specific steps to be taken, for example, to register the partnership as such.

Depending on the number of investors, the bounds of a general partnership may become stretched, but in cases where the developer/promoter is not the locus of liability for acts of the DAO, there is at present no other option. That means investors in a DAO face potentially unlimited liability to third parties, and may owe fiduciary duties amongst themselves.

While the scope of legal property at common law gave the courts sufficient flexibility to include cryptocurrencies as a type of legal property, there is no such scope when it comes to limited liability. Limited liability corporations and partnerships are creatures of statute, with specific statutory requirements (e.g. registration, directors) with which DAOs do not (by definition) comply. The common law cannot create a new legal entity, and nor should it. As artificial intelligence and the internet of things develop, so too will the ability of DAOs to interact more fully and autonomously in the physical world. At some point, autonomous AI entities may have to be accorded some form of legal personality, but that is the kind of world-changing issue that legislators will have to grapple long and hard with.

[11] Christoph Jentzsch, 'Decentralized Autonomous Organization To Automate Governance' (*slock.it*, undated) <https://archive.org/stream/DecentralizedAutonomousOrganizations/WhitePaper_djvu.txt> Accessed May 2020

PART B: Data Governance Requirements – Smart Contracts

Akber Datoo (D2 Legal Technology (D2LT))

Introduction

The potential of smart contracts has attracted a lot of attention and excited many. By relying on a DLT such as a blockchain, it is possible to run code reflecting contractual arrangements between parties that is resilient, tamper-resistant and autonomous. Smart contracts extend the functionality of DLT from storing transactions to "performing computations."[12]

Indeed, it has been said that these may create contractual arrangements that are far less ambiguous than agreements written in legal prose, due to the fact that their performance is contained within the very essence of the smart contract, rather than being a separate step, as is the case with "traditional" legal contracts. However, even leaving aside the challenge that the smart contract code may not be in a human-readable form and may instead create standardised contracts that few are able to truly understand[13], the data governance challenges behind creating correctly performing smart contracts should not be underestimated, and form an area that lawyers will need to focus on very carefully.

What is a smart contract?

At a very simple level, smart contracts are coded instructions which execute on the occurrence of an event. However, there is no clear and settled meaning of what is meant by a smart contract. The idea of smart contracts was first perceived in 1994 by computer scientist and legal theorist, Nick Szabo, who defined it as "*a set of promises, specified in digital form, including protocols within which the parties perform on these promises*". However, at the time, smart contracts remained a somewhat abstract term and of limited value, as they ultimately relied on stakeholders trusting another entity to execute the smart contract. The advent of DLT and blockchain has enabled smart contracts to come back to the forefront of development and innovation, since they rely on consensus algorithms rather than trust in an intermediary. Taking a well-known example, the Bitcoin blockchain is technically a limited form of smart contract whereby each transaction includes programs to verify and validate a transaction (each being, effectively, a small smart contract).

For the purposes of this Section and as a foundation on which to base the discussion, we use the Clack et al. definition of a Smart Contract:[14]

> "*A smart contract is an automatable and enforceable contract. Automatable by computer, although some parts may require human input and control. Enforceable either by legal enforcement of rights and obligations or via tamper-proof execution of computer code*".

This definition is broad enough to encapsulate a wide spectrum of smart contracts, including both types identified by Josh Stark, namely (i) "smart code contracts" (where legal contracts or elements of legal contracts are represented and executed as software); and (ii) "smart legal contracts" (where pieces of code are designed to execute certain tasks if predefined conditions are met, with such tasks often being embedded within, and performed, on a distributed ledger).

[12] Nick Szabo, 'Smart Contracts: Building Blocks for Digital Markets' (Extropy: The Journal of Transhumanist Thought, 1996) vol 16

[13] Smart contracts are usually classified as fitting into either the "External Model" or the "Internal Model". In the case of the former, the legal contract remains in the traditional agreement form, but external to this legal contract, certain conditional logic elements of the contract are coded to occur automatically when relevant conditions (based on data inputs) are satisfied. In contrast, with the "Internal Model", certain conditional elements of the legal contract are rewritten in a formal logic representation, and this logic is executed automatically based on the data inputs to that logic.

[14] Clack et al, 'Smart Contract Templates: Foundations, Design Landscape and Research Directions' (Barclays Bank, 3 August 2016) <http://www.resnovae.org.uk/fccsuclacuk/images/article/sct2016.pdf> Accessed 19 May 2020

Smart contracts offer event-driven functionality triggered by data inputs (which may be internal or external), upon which they can modify data. External data can be supplied by "oracles" (trusted data sources that send data to smart contracts). Smart contracts can track changes in their “state” over time, and can act on the data inputs or changes in their state, resulting in the performance of contractual obligations.

The elevated role of data and data governance in smart contracts

In many ways, smart contracts are similar to today’s written contracts, in that to execute a smart contract, one must also achieve a “meeting of minds” between the parties.[15] Once this meeting of minds has been reached, the parties memorialise it, which might be triggered by digitally signed blockchain-based transactions.

A traditional legal agreement will typically contain various details of events which the parties have agreed will result in certain consequences, and typically an obligation on a party to perform some action. By way of example, it might provide that:

> “*if the rate of defaults on the underlying portfolio exceeds 2%, the protection seller shall make a payment of £1,000,000 to the protection buyer*”.

Such contractual obligations of course require a certain degree of certainty and specificity in order to ensure the “meeting of minds” required for the formation of a contract.

Smart contracts do, however, differ from traditional legal agreements through the smart contract's ability to enforce obligations through autonomous code. Promises in smart contracts, such as the example given above, are harder to terminate – especially in cases where no one single party controls a blockchain, and there may therefore not be any straightforward manner in which execution can be halted. Where transactions represent real-world business interactions between parties collaborating on a complex business process, the specific facts surrounding the operation of the business process become critical to the successful running of that business process, and accordingly, the data quality of those facts is key.

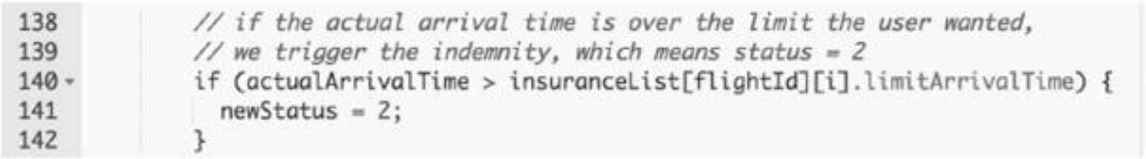
In the context of a smart contract, factual matters relevant to the contractual obligations are likely to be automatically assessed, removing the normal human assessment of the triggering event. In the example above, this would be the question of whether the rate of defaults has exceeded 2%, which may simply be an input from another system.

It is the fact that smart contracts seek to automate performance, and therefore need to automate the process of applying fact to a contract at hand, that elevates the importance of data governance from the traditional legal agreement context. A smart contract operates through Boolean logic – a form of mathematical logic that reduces its variables to "true" and "false".

AXA’s "Fizzy" application is an example of a smart contract application for flight insurance, whereby the terms of the contract between the holder of the insurance and AXA are based around insuring against a flight delay of greater than 2 hours. The smart contract operates on the Ethereum blockchain network, and it continuously checks data from oracles in real time. Once the delay exceeds 2 hours, the compensation terms are automatically triggered and given effect. Putting this into colloquial Boolean algebra, "if the plane is late by more than 2 hours, then compensation must be paid out". The key code representing this logic is shown below[16] (note that the variable limit ‘limitArrivalTime’ is defined as 2 hours elsewhere in the code).

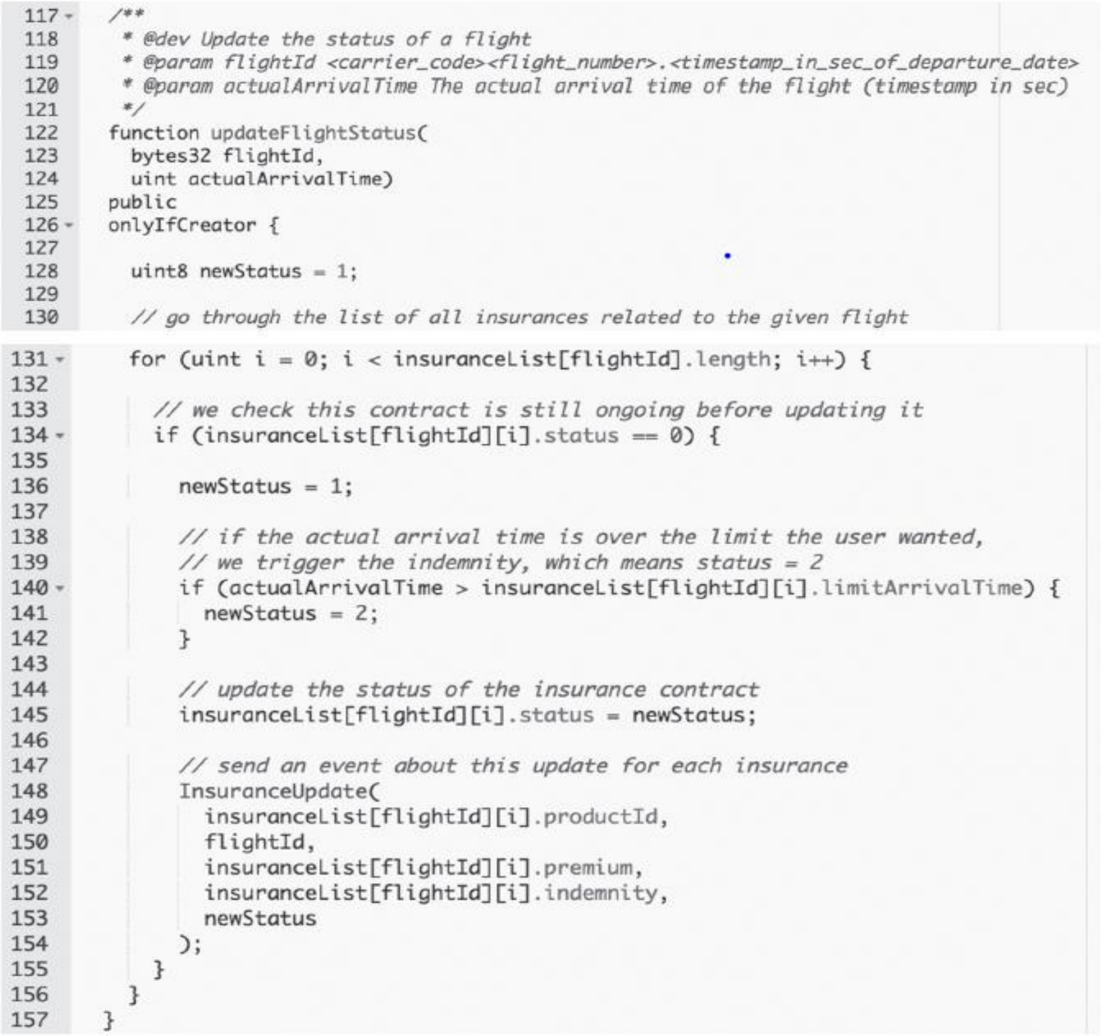
[15] Stephen J Choi and Mitu Gulati, 'Contract as Statute' (Michigan Law Review, 2006), Vol 104

[16] Akber Datoo, ‘*Legal Data for Banking: Business Optimisation and Regulatory Compliance’* (John Wiley, 2019)



```
      // if the actual arrival time is over the limit the user wanted,
      // we trigger the indemnity, which means status = 2
      if (actualArrivalTime > insuranceList[flightId][i].limitArrivalTime) {
        newStatus = 2;
      }
```

The core logic code for the Fizzy smart contract application



```
/**
 * @dev Update the status of a flight
 * @param flightId <carrier_code><flight_number>.<timestamp_in_sec_of_departure_date>
 * @param actualArrivalTime The actual arrival time of the flight (timestamp in sec)
 */
function updateFlightStatus(
  bytes32 flightId,
  uint actualArrivalTime)
public
onlyIfCreator {

  uint8 newStatus = 1;

  // go through the list of all insurances related to the given flight
  for (uint i = 0; i < insuranceList[flightId].length; i++) {

    // we check this contract is still ongoing before updating it
    if (insuranceList[flightId][i].status == 0) {

      newStatus = 1;

      // if the actual arrival time is over the limit the user wanted,
      // we trigger the indemnity, which means status = 2
      if (actualArrivalTime > insuranceList[flightId][i].limitArrivalTime) {
        newStatus = 2;
      }

      // update the status of the insurance contract
      insuranceList[flightId][i].status = newStatus;

      // send an event about this update for each insurance
      InsuranceUpdate(
        insuranceList[flightId][i].productId,
        flightId,
        insuranceList[flightId][i].premium,
        insuranceList[flightId][i].indemnity,
        newStatus
      );
    }
  }
}
```

An example of the Solidity smart contract coding language (taken from the Fizzy smart contract)

In many ways, the automated performance feature of smart contracts extends the need for "certainty and completeness of terms of a contract", to "certainty and completeness of data specification of data variables inherent in a smart contract" (be this data input or contractual state data). This can only be addressed through the governance of such data.

Data governance

The term ‘data’ is typically used to refer to facts or pieces of information that can be used for reference and analysis. A phenomenal amount of data is created, stored and processed in the ordinary course of day-to-day life and business – and its proliferation is ever increasing. These are likely to form key data inputs into the conditional logic of a smart contract. However, the quality (typically through the lens of definition, accuracy and timeliness) of such data needs to be considered as this will likely impact the functioning of a smart contract and any automated performance, noting that this is not simply a question of whether the data is accurate, but must be viewed through a variety of data quality lenses such as timeliness, consistency and precision.

As a result, smart contracts need to ensure an appropriate data governance framework is in place in relation to any data variables relevant to it. This is a formalisation of authority, control and decision making in respect of these data variables. This is unlikely to be in the complete control of the parties to a smart contract, however there ought to be a meeting of minds as to acceptance of the data governance.

In the context of data relevant to a smart contract, it is fair to assume that this will be structured rather than unstructured data (noting, of course, that this is not a binary question, but rather data will sit along a spectrum of degrees of structure, defined by the purpose of a structure and intended use of the data). In the same way that traditional contract definitions are key to their reflection of the intentions of parties and envisaged outcomes, smart contracts, due to their automated performance features, are hugely reliant on the way in which data inputs flow through their conditional logic – requiring the drafters of smart contracts to carefully consider data governance parameters that might mean the logic is no longer appropriate, or in more sophisticated contracts, to provide for alternative logic based on data quality features of the data inputs at “run-time”.

To the extent that “big data” is utilised as data in the smart contract context, there is of course likely to be a methodology developed to use such a data set in order to address any inherent "messiness" in the data. The extent of any techniques used to overcome such "messiness", needs to be assessed in the context of their use within a smart contract’s conditional logic, and the logic may need to differ based on various aspects of the governance of such data (for example, the appropriateness of certain “less-conforming” data structures as inputs).

Enterprise data management theory typically defines the following roles:

- the data trustee;
- the data steward; and
- the data custodian.

The data trustee is ultimately responsible and is the overarching "guardian" of a particular data domain, defining the scope of the data domain, tracking its status, and defining and sponsoring the strategic roadmap for the domain. They would ultimately be accountable for the data, but would typically delegate the day-to-day data governance responsibilities to data stewards and data custodians.

The data steward is a subject-matter expert who defines the data category types, allowable values and data quality requirements. Data stewardship is concerned with taking care of data assets that do not necessarily belong to the steward(s) themselves, but which represent the concerns of others.

Data custodians are also accountable for data assets, but this is from a technology perspective (rather than the business perspective in respect of the data steward), managing access rights to the data and implementing controls to ensure their integrity, security and privacy (covered in Section 4 of this Guidance).

Of course, the difficulty is that a smart contract is likely, in most cases, to operate outside of a single enterprise. Accordingly, provision must be made within the terms of the smart contract itself to ensure the data quality sought, perhaps through data governance requirements or data quality checks agreed between the smart contractual parties.

Dimensions of data quality

The dimensions of data quality that might be relevant to the data variables in a smart contract will of course vary based on the nature of the smart contract in question, and the specific business use of the specific data variable. These will typically be:

- **Accuracy:** the degree to which data correctly represents the entity it is intended to model (for example, where a default rate of a large loan portfolio is a data input, the extent to which loans which are in a potential event of default state, rather than actual event of default, are excluded from the measurement).

- **Completeness**: whether certain attributes always have an assigned value in a data set (for example, how loans without default data are treated)

- **Consistency**: ensuring data values in one data set are consistent with values in another data set (for example, where the test of whether a loan in default differs across the data set).

- **Currency**: the degree to which information is current with the world it seeks to model and represent (for example, the degree to which assumptions have been used to arrive at the data point in question).

- **Precision**: the level of detail of data elements (both in terms of, for example, the number of decimal points to which a numeric amount is detailed, to the number of data elements within a particular data attribute in the data structure that may impact the data value – often based on its intended usage).

- **Privacy**: the need for access control and usage monitoring.

- **Reasonableness**: assessment of data quality expectations (such as consistency) relevant within operational contexts.

- **Referential Integrity:** expectations of validity in respect of references from the data in one column to another in a data set.

- **Timeliness**: the time expectation for the accessibility and availability of information (for example, the precise cut-off time in respect of which loan information will be included, and whether the data source is able to guarantee timeliness of inclusion of data by the time the data is utilized within the smart contract logic).

- **Uniqueness**: the extent to which records can exist more than once within a data set.

- **Validity**: consistency with the domain of values and with other similar attribute values.

Data required to assess the data quality of a data variable and quality control policies

There are four main methodologies to be considered in assessing the data quality of a data variable within a smart contract:

1. **A data quality assessment that does not require additional data**. In this case, the data quality can be assessed by considering and analysing the value of the data variable itself. For example, “a speed of a car is within acceptable bounds if it is between 0 and 60 miles per hour”.

2. **A data quality assessment that relies on historical values of the data**. For example, the temperature of an individual taken by an IoT device is only of sufficient quality if it doesn't differ from any prior recording in the previous five minutes by more than two degrees Celsius.

3. **A data quality assessment that relies on a (single) value or feature of (possibly multiple) other variables**. For example, a property address assessed against a land register.

4. **A data quality assessment that relies on multiple other values or features of (possibly multiple) other variables.** For example, a temperature reading might be compared against prior readings of different subjects.

There are broadly five policies that can be adopted in respect of the data, allowing the verification of data quality at runtime:

1. **Accept Value**: within tolerances, even though the data quality may not be ideal, it may be accepted.

2. **Do Not Accept Value**: a breach of the agreed tolerance results in the non-acceptance of the data input. The consequence of this must be considered and agreed in the context of the contractual agreement between the parties.

3. **Log Violation**: it may be necessary to accept certain data inputs, despite some concerns regarding data quality, whilst flagging it as being of low data quality for informational purposes.

4. **Raise Event**: where a low data quality input represents a critical situation that requires an immediate action (be it by a person or system), the automated action might be to escalate and raise an event.

5. **Defer Decision**: a particular violation of a data quality threshold on an input might not be enough, in itself, to result in a definitive automated action, and the decision may simply be deferred.

SECTION 3: BLOCKCHAIN CONSORTIA

Sue McLean, Baker McKenzie LLP

Introduction

A blockchain consortium is a collaborative venture between a group of organisations that is designed to develop, promote, enhance or access blockchain technology. Several different models exist for blockchain consortia, including corporate joint ventures, contractual consortium agreements and participation agreements. Various legal risks can arise when creating and joining a consortium, including questions of contractual liability, competition law issues, intellectual property considerations and data protection concerns.

This Section is designed to help explain what a consortium is, the types of consortia in existence, and the advantages and disadvantages of the various contracting models, as well as to provide an overview of some of the key legal risks to be considered when advising clients on blockchain consortia projects.

What is a blockchain consortium?

A consortium is an association created by a group of members that is designed to promote, achieve or forward a common goal or purpose. A blockchain consortium is no different. As set out above, it is a group of various companies, organisations and/or stakeholders who come together with a common objective to collaborate in order to promote, use, develop, enhance, educate, influence or integrate blockchain technology.

Types of blockchain consortia

The participants of a blockchain consortium will differ depending on the objective. For example, some consortia are educational or promotional in nature, with a broad mandate. These types of consortia include industry working groups, collaborations or alliances and can be either not-for-profit or commercial. The aims of such consortia may be to connect stakeholders in the sector in order to educate and/or promote blockchain technology.

There are also tech-focused consortia, in which parties come together to pool resources in order to develop blockchain platforms to expand the application of blockchain technology. These consortia tend to focus on developing the technology, including standards and toolkits, rather than focusing on specific use cases. These consortia are often formed and operated by a third-party entity that then invites other parties to participate. Examples of this type of tech-focused consortia include Hyperledger, which aims to improve blockchain technology through open source collaboration, and Enterprise Ethereum Alliance, which aims to provide its members with an environment for blockchain testing and development scenarios.

There are also business-focused consortia that focus on a specific use case within a particular industry or business group. Participants tend to be a group of organisations in the same industry or cross-industry that have identified an opportunity to use blockchain to help solve a shared problem, i.e. transform or improve a particular industry or business process to increase efficiency. Examples of this type of consortia include:

- **the Digital Trade Chain**, which focuses on trade supply-chain management issues;
- **Bankchain**, which aims to implement blockchain into the banking sector; and
- **Tradelens**, which is focused on using distributed ledger technology to digitise global supply chains.

It is the rise of these types of business-focused consortia which is expected to drive blockchain adoption. A consortium is increasingly the preferred option for an enterprise-grade blockchain platform. Blockchain consortia that develop a permissioned platform may help companies obtain the benefits of decentralised technology, but with more assurance regarding compliance as the members are known and rules can be put in place to govern use of the platform.

There are also dual-focused consortia that focus on both technology and business.

Although a blockchain consortium will likely sit within one of these categories, there are different commercial drivers behind the creation of each particular consortium that will distinguish it further. These factors will influence the stakeholder community from which to draw the consortium members.

For example:

- competitive consortia bring together competitors in the same industry to drive digital transformation in the sector or address common regulatory or other challenges; and

- a leading company who commands market power and wants to drive change in its operations may create a consortium made up of members of its supply chain.

The rise of blockchain consortia

The consortium has become a popular model for the development of DLT. Over recent years, a large number of blockchain consortia have formed globally across a range of industry sectors including financial services, healthcare, energy, retail and the public sector. Indeed, in the 2019 Deloitte Blockchain Survey, 81% of those surveyed stated that they were already participating in a blockchain consortium, or were intending to join one in the next 12 months.[17]

There are a range of reasons why organisations look to form (or join) blockchain consortia. For example, membership of a consortium:

- can enable members to identify and resolve common issues relevant to the industry and/or membership group;

- may enable the promotion of blockchain adoption by leveraging network efforts. The more businesses in a sector are involved, the more likely the technology developed will meet the needs of the industry participants, end users and other stakeholders (vertical and/or horizontal) and accordingly meet the market's needs and be adopted;

- may present a low-risk effort for an organisation to obtain access to new and innovative technology, stay current on blockchain trends, defend against new threats, and initiate preparations to implement the technology;

- may present a lower-cost effort by sharing development and deployment costs amongst a group of organisations;

- can provide market players with a say in the development of new DLT platforms, enabling members to tailor blockchain technology to their specific needs, and offering them greater control and flexibility than the prevailing "contracting-as-a-service" model; and

[17] Deloitte, 'Deloitte's 2019 Global Blockchain Survey' (2019) <https://www2.deloitte.com/content/dam/Deloitte/se/Documents/risk/DI_2019-global-blockchain-survey.pdf> Accessed May 2020

- may look attractive due to "the fear of missing out". In this age of disruption, companies are afraid of being left behind and are under pressure to be (and be seen to be) innovative and ahead of the curve.

For many organisations, it will generally be cheaper and less effort to join (and help influence) an existing consortium than create a new one.

Blockchain consortia models

The consortium model is not new and various models exist for multi-party consortium projects. When developing a blockchain consortium, the members will need to consider the available models and assess which one best suits their needs.

In this section, we will focus on the contractual consortium model and the corporate joint venture (**JV**) model. These are consortia in the traditional sense, as all of the consortium members tend to have "skin in the game" and it is unlikely that any one party will exert significant control.

We will also touch upon the multi-party agreement model and the participant agreement model. These models offer some of the benefits of a consortium, but one party (say, the tech developer) takes the lead. Therefore, the other consortium members will have more limited control and influence over the development of the technology. Similarities can be drawn to cloud hosting or platform/infrastructure as-a-service arrangements, but where these are offered to a group of parties to achieve a common goal, instead of an individual user for their particular purposes.

Contractual consortium model

This model involves a contractual consortium agreement between the consortium members including the developer of the blockchain platform. Governance structures will be put in place with defined levels of membership; for example, the consortium members will expect to have a degree of control over and rights in the platform being developed. Whilst the consortium members will likely be users of the platform, there may also be additional participants/end-users who will use the platform as it is taken to market. These additional parties may be added to the consortium membership or they may remain as participants/end-users only, with their use of the platform governed by separate participation or end-user licence agreements.

This model therefore tends to assume that a tiered approach will be used to govern the consortium. End-users would have the lowest level of influence over the development of the platform and, in effect, would receive it as a service. New consortium members would be above this, as they may contribute to the development of the technology, meaning that they would have higher rights and influence. The founding consortium members are likely to be at the top of the chain. When creating the consortium governance, the founding members will need to define the rules for new members and participants/end-users.

Using this model has various advantages and disadvantages, for example:

Advantages	**Disadvantages**
The model offers more flexibility than a corporate JV, as the members and steering committee can agree to amend the consortium agreement from time to time, which can be particularly useful as the needs of the consortium change over time.	There is less certainty on funding and other contributions; this needs to be established clearly in the agreement. It can also be difficult to establish effective governance procedures,

Advantages	**Disadvantages**
	particularly if the various members and partners have different needs and goals. In particular, without a separate legal entity, thought will need to be given to how the team who is dedicated to, or otherwise charged with responsibility for, driving the efforts of the consortium will be appointed from a legal perspective. Will they be seconded in from one (or more) of the consortium members, and if so, how would this affect the governance and day-to-day dynamics of the consortium? Might they be incubated within a service provider to the consortium? Might they individually enter into an appointment agreement with all consortium members as joint customers?
The model may offer greater cost savings. Unlike a corporate JV, the creation of a separate entity is not necessary. Therefore, there are likely to be lower operational costs; in particular, each member will likely handle its own accounting and taxes resulting from their participation in the consortium.	Due to information sharing, there are potential competition law concerns with this type of agreement, particularly if a lead market player is involved. The consortium members must set up appropriate ways of working and avoid any risk of being deemed to be price-fixing, abusing their dominant market position, limiting the development of the market and so forth.
The consortium agreement can include straightforward exit provisions, which can be as simple as providing written notice to the consortium's steering committee.	As each organisation will enter into the consortium agreement, it is not separate from their respective core businesses, meaning each member could have full exposure to the consortium's risk profile.
The likely reduced barriers to entry can encourage more market leaders and key industry members to join at inception, meaning the consortium benefits from greater network effects.	Without a clear statement to the contrary, this model could run the risk of being considered a partnership under English law.

Joint venture model

The JV model involves the creation and incorporation of an independent corporate entity that will be responsible for the platform. The JV parties will be made up of the consortium members. If a tech company is involved in bringing the consortium together or otherwise involved in the consortium, they may be a party to the JV, or a service provider to the entity that is formed. The entity will be responsible for creating platform terms/participation agreements that apply to all participants/end-users. Each member of the JV will be required to invest in the development of the platform. This investment can range from financing the development itself, providing essential IP or know-how, industry knowledge, technical expertise and/or resources such as people, tangible and intangible assets.

Using a JV model offers various advantages and disadvantages, for example:

Advantages	**Disadvantages**
The risks are shared between the members of the JV and the risk will be limited to any unpaid subscription amount on the shares of the JV entity. Shares and voting rights can be tailored to reflect the contributions of the JV members.	Any imbalance in contributions could drive inequalities and tensions.
The JV entity will exist as its own legal entity that is separate from the core business of its members. This minimises the risk of exposure, as the JV entity will be responsible for its own debts, liability will be limited and the assets of the members will be separate from the assets of the JV.	The members may well have different business needs, with different goals and risk appetites. Even with a shared vision, it may be difficult to align these competing needs, and cause delays in platform development. In addition, competition law issues may arise from information sharing, and if the JV is between large industry players, there may be merger control issues to consider.
The JV entity will be the network operator and provide the platform to end-users.	Exiting the JV may be difficult and require the sale of a member's shares or a buy-out by the other members. There could be practical and commercial difficulties in achieving this, depending on the JV's articles of association. In addition, whilst the JV entity will generally own any IP rights created, consideration will need to be given to what happens to these rights if the JV is later dissolved.
The JV entity can raise outside investment, which can benefit both the JV and its members.	As this model involves forming a separate corporate entity, there are likely to be higher set-up costs and operational costs. There would also be public disclosure of information about the entity.

Of course, some consortium projects can change over time. Fnality International (which is developing systems based on DLT to enable peer-to-peer settlement among wholesale market participants) is an example of a blockchain consortium (formerly, the USC Consortium) that started as a research and development focused contractual JV that then evolved into what is now effectively a JV company. The contractual JV members gradually grew in numbers, and three of the original members (UBS, Santander, BNY Mellon) invested in Fnality International's Series A round last year, along with 12 other global financial institutions.

Developer Agreement and Participant Agreement Models

The result of initial consortium discussions or a Proof of Concept (**PoC**) may be to decide to proceed on a different basis from a consortium agreement or corporate joint venture. Where one company or tech provider is really driving the project, the parties may consider that a developer agreement or participant agreement model is more appropriate. These are not consortium agreements as such, but contractual arrangements put in place between the network operator and the end-users of the platform.

These reflect a more traditional form of contracting, in that the network operator (i.e. the consortium lead or tech provider) will tend to be responsible for the platform development and own the intellectual property in the platform and offer it to the participants. In the developer model, a range of participants would enter into a multi-party agreement between themselves and the network operator for a common purpose, but the network operator would retain the decision-making power for the platform and the other parties. In the participant model, the network operator will create a standard set of platform terms which would then be offered to a range of participants as a one-to-many solution.

Both of these models offer limited control or influence to the consortium members. The network operator is in the driving seat. These models offer members the advantage of limited financial investment, scalability, flexible membership status, low operational costs and clarity around intellectual property ownership and exit. However, these models will not be suitable where the participants want greater influence or control over the direction of the technology and its commercialisation. In addition, these models will still need governance arrangements and they will not eliminate competition law concerns that arise from information sharing. Furthermore, if the tech development requires significant funding, these models may not be suitable if the participants are not prepared to fund the investment by the network operator and it may be difficult for the network operator to attract third party funding.

Is there a preferred model?

The appropriate model will very much depend on the goals, needs and risk appetite of the consortium members. Accordingly, there is no preferred model. Whilst the contractual consortium and JV models would seem more appropriate to a multi-party venture of this kind, the developer or participant model may be more suited to the particular consortium members' needs. For example, Bankchain operates under a developer agreement, whereby its members (a community of banks) can use a blockchain platform developed by Primechain Technologies to explore and implement blockchain technologies within the banking sector, whilst Tradelens and its ecosystem of members is the result of a collaboration between Maersk GTD and IBM.

Legal risks and issues

In terms of the relevant legal documentation, many consortium discussions will start with an NDA and then may move to a pre-consortium agreement, initial heads of terms or PoC agreement. Then, if the discussions or PoC are successful, the consortium members will create a more detailed framework to govern their relationship going forward. It is at this stage that members may decide, for example, to set up an independent entity to run the platform, or enter into a commercial consortium agreement.

There are various legal issues and risks that legal advisers should bear in mind when advising clients on building and joining blockchain consortia and preparing the required contractual documentation. Because of the range of potential issues (which will depend on the particular use case and other dynamics of the particular project), it is likely that a multi-disciplinary team will be needed.

1. Creating a consortium

Topic	Issues
Members	• When creating a blockchain consortium, the potential candidates for that consortium will need to be carefully considered and evaluated against a set of requirements relevant to the needs and aims of the consortium that is being established. Only those candidates that meet the requirements for the consortium should be allowed to join. The types of matters that should be considered when evaluating a candidate include their ability to contribute, for example by way of funding, technical expertise, contacts and network, plus any reputational or regulatory risks (e.g. whether potential members have been subject to any regulatory investigation or enforcement action).
Investment and Roles and Responsibilities	• The consortium will need to identify what each member will provide in terms of financial investment (initial and ongoing phased funding) and other contributions in terms of intellectual property/know-how, industry knowledge, technical expertise and/or other resources. • The members will also need to clearly document their other roles, responsibilities and commitments as members including in terms of platform design and development, platform operation and scaling of the platform (such as their role in brand creation and promotion of the platform to new participants).
Governance	*Business Governance* • As a consortium involves a group of parties working together to achieve a common goal, the establishment of proper governance methods is key to ensure that the consortium can operate effectively and that the rights and obligations of the parties are clear. A consortium's membership can be incredibly varied, ranging from leading players in the market to smaller businesses as well as industry stakeholders and end-users. Often these members may be competitors. Accordingly, each member is very likely to have its own corporate goals and interests, several of which could compete either with those of the other members of the consortium or with the consortium itself. Governance is, therefore, a crucial issue as it will be necessary to determine how the parties are required to cooperate and will govern how such interests are to be balanced. • Given the range of parties with their own interests, consortium governance is not easy and there are well-known consortia that have reportedly run out of steam, in large part due to governance failures. It is clear that if

	consortium governance is not carefully designed, it could fail to provide the right support to ensure that the members meet their objectives to work together cooperatively to achieve their common goal. Therefore, setting up good governance is one of the most important considerations when forming a consortium and an area where legal advisers can provide a critical role. • There are a number of factors to consider when designing good governance for a blockchain consortium including: ○ **Goals, Objectives and Roadmap**: the consortium will need to establish clear shared goals and objectives, identify required deliverables, document how it will approach the platform development roadmap, prepare a sound business case and compelling value proposition; ○ **Financials***:* the consortium will need to document how budget will be set, agreed and spent, how the consortium will raise investment, design the commercial/revenue sharing model and agree the applicable fee structure; ○ **Control:** there should be clarity on how members can influence the decisions of the consortium (including members' voting rights). In the context of the consortium and JV models, it will be important to ensure that no single party can exert dominant control. After all, the purpose of a consortium is to promote collaboration. However, even in the case of the founding members there may be stark differences in contributions particularly as they relate to funding, technology and knowledge. Therefore, the consortium may need different classes of membership with different voting rights and authority levels to reflect the different contributions and level of participation between members. In addition, the creation of special voting rights or participation thresholds may be required as they relate to critical/non-routine decisions relating to the consortium; ○ **Onboarding***:* a key issue for blockchain consortia is the balancing of interests between founding members, as well as between founding members and later joiners. The members will need to identify clear criteria for membership for later participants (both in terms of qualifying criteria, obligations and rights), plus a clear onboarding mechanism; ○ **Operating model***:* the consortium will need to create and document an appropriate operating model, including all necessary committees and working groups; ○ **Dispute management***:* the consortium will need to create and document appropriate escalation and dispute resolution mechanisms;

	o **Change management***:* the consortium will need to create and document appropriate change management mechanisms and governance structures; and o **Exit***:* the consortium will need to identify clear rules for voluntary and involuntary termination of members' participation, together with appropriate off-boarding and exit transitions. *Technical Governance* • These factors are generally representative of business (off-chain) governance; i.e. the rules of engagement for participating in the consortium. However, on-chain governance (i.e. the technical and operational rulebook for how the platform operates and how members participate on the blockchain platform itself), will be just as important to establish. This technical governance will include consideration of issues such as access and permissions, protocols, consensus mechanisms (and may include tokenisation). *Flexibility* • Irrespective of the governance framework initially established by the consortium, governance may need to change over time. As blockchain is a developing technology, the consortium's governance needs may evolve as the project develops. The consortium agreement should include flexibility so that the members regularly review their governance regime and determine whether it is up-to-date and accurately represents the needs of the consortium and its members.
Liability	• It is important to clearly identify each member's roles and responsibilities as well as risk apportionment, including in terms of liability for the development and operation of the platform and for any transactions processed via the platform (including by any third parties who access the platform via a participant). Ideally, any regulatory, technological, contractual or any other form of risk should be appropriately balanced between the consortium members.
Competition	• Setting up a blockchain consortium may be subject to approval or at least scrutiny by merger control authorities. Merger control is the process of specialised regulators reviewing, usually *ex ante*, certain transactional structures that meet the applicable jurisdictional thresholds. It is designed to prevent transactions that could substantially lessen competition, and make certain that such transactions are modified appropriately in order to ensure that markets continue to operate effectively and enhance consumer welfare.

	• Furthermore, for most business-focused consortia (particularly where made up of actual or potential competitors) careful consideration should be given to competition/antitrust rules more generally to ensure compliance. In particular, information exchanges between members in relation to sensitive commercial information such as (future) pricing and other strategic information, if done without appropriate safeguards, may create competition concerns as it reduces the incentive to compete. • Excluding certain entities from participating in the consortium based on non-objective criteria may also create competition issues by foreclosing such entities from effectively competing with the rest of the consortium members. • In addition, and particularly where the consortium is technology-focused, the creation of standardised models for the industry may increase or create barriers to entry, or otherwise limit the incentives to develop new competing technologies which may in turn run afoul of competition law.
IPRs	• **Inputs:** parties will need to consider what inputs each member will provide to enable the development of the platform. These may include licences of certain IP, data, industry knowledge and materials. The members will need to consider the extent to which any such IP will need to be licensed to each other or to the JV entity (as applicable). The consortium will also need to consider any third party software or materials required (including open source licences). • **Outputs:** the formation and operation of the consortium will also lead to the creation of new IPRs (including relating to branding, design documentation, code in the platform itself). The consortium will need to determine which member(s) own the IPRs developed and how such rights can be exploited. For example, outside the context of a JV (which would in most cases hold the IP itself), whether the IP should be held by one of the parties (such as one of the founding members or the developer of the technology) and then licensed to the remaining members. Generally, parties will want to avoid joint IP ownership as this can create issues with the exploitation and enforcement of such rights. • **End User Licences**: consideration will also need to be given to the licences granted to new members and other end-users. • **Data**: a successful blockchain platform will involve the creation of rich and valuable transaction data from a range of industry participants. The parties will need to agree and clearly document who has rights in any data collected, derived or created as a result of the operation of the platform (including any insights and reference data derived from aggregated transaction data). Members will need to agree how they control the way in which that aggregated data is shared, and with whom, subject to appropriate confidentiality (and, to the extent relevant, data protection)

	requirements. They will also need to consider how any revenue produced from that data is shared amongst members. • **Exit:** the members will need to consider what the IP position will be on exit of a member or any dissolution of the consortium.
Compliance	• The members will need to consider whether operation and/or use of the platform will involve carrying out regulated activities in any in-scope jurisdictions and whether any form of authorisations or approvals will be required. In particular, it will be important to identify which parties of the consortium will need to obtain any authorisations or approvals. This may be a simpler issue where a new corporate JV entity is being set up, as the JV entity will have its own separate legal personality and will therefore be able to apply for its own authorisations/approvals. It can be a more complicated issue for the other contracting models. If by their use of the platform members are carrying out regulated services, they may need to apply for authorisations/approvals in their own name to carry out such activities legally. • Where the platform involves cryptoassets, the members will need to evaluate the nature of the cryptoasset in light of applicable financial services regulation and guidance (for example, the FCA Guidance on Cryptoassets[18]). If the cryptoasset is regulated then the members will need to identify all necessary compliance requirements (including with respect to AML/KYC). • In addition to legal requirements that relate to the particular use case itself, for many use cases which involve transactions being processed over the blockchain platform, compliance with financial crime laws (including sanctions, anti-money laundering, terrorist financing, anti-bribery and corruption, etc.) will need to be considered. Particular challenges for blockchain platforms may include ensuring appropriate compliance due diligence from a financial crime perspective in situations where details of underlying transactions are not fully visible (both in terms of the users and the types of transactions that take place). There is an increased focus from compliance regulators around the need for appropriate third party KYC/KYS due diligence (e.g. of app developers and users etc.). The risk that the platform could be used to facilitate illicit transactions (e.g. trade with sanctioned countries or involving restricted sectors or products) will also need to be considered. As such, the consortium will need to implement appropriate compliance policies, procedures and controls in the design of the platform, including making clear the rules and responsibility of members when admitting new participants. • Further, given that blockchain is a new technology and the law is playing catch-up, consortium members will need to consider how to approach, and

[18] Financial Conduct Authority, 'Guidance on Cryptoassets; Feedback and Final Guidance to CP 19/3' (Policy Statement PS19/22, July 2019) <https://www.fca.org.uk/publication/policy/ps19-22.pdf> Accessed May 2020

	who is responsible for monitoring, changes of law which may impact the platform and platform users over time.
Data Protection	• Members will need to consider whether or not the blockchain platform will involve the processing of personal data on-chain, or more likely, off-chain. This is likely to depend on the particular use case. For example, a blockchain consortium focused on building a platform for supply chain management in the food industry may not involve sharing material personal data, whereas one focused on healthcare may well do. • With respect to the platform and services, where personal data will be processed, the consortium will need to consider how to approach compliance with applicable data protection law. In particular, the members will need to: (i) identify the in-scope personal data; (ii) assess the roles of the members and future participants; (iii) document how data protection will be addressed in the consortium agreement, agreement with any relevant tech vendor(s) involved in the design or operation of the platform and any participant/end-user agreements; (iv) consider how data will be stored and shared; and (v) consider how best to ensure that the platform is designed in accordance with data privacy by design and by default principles. • For further discussion of data protection compliance in the context of blockchain projects, see Section 4.
Tax	• **Choice and location of vehicle:** if the consortium is to operate via an independent entity, consideration will need to be given to which jurisdiction (i) is best to establish tax residence; (ii) has access to the required resources; and (iii) does not disadvantage consortium members (e.g. potential for withholding taxes, size of treaty network). It may be possible to choose a legal entity that is fiscally transparent for tax purposes - this would produce outcomes similar to those under a contractual model (although this may give rise to additional complexities if the consortium operates cross-border). The choice of vehicle will also impact on whether it is the independent entity or underlying participants that have any VAT registration, and on reporting obligations in respect of the consortium's activities. • **Financing:** tax impacts should be taken into account when considering how consortium members fund the venture. • **Taxation of intercompany transactions / extraction of profit:** a contractual arrangement or the use of a fiscally transparent entity will likely result in profits being taxed at the consortium member level, in line with their current tax profiles. The use of a fiscally opaque legal entity should shift taxation on the consortium's profits to the level of the legal entity. The choice of jurisdiction for tax residence may dictate whether consortium members are subject to an additional level of taxation on receipt of distributions from the consortium. **VAT on vehicles activities and intercompany transactions:** consideration should be given to the VAT implication of any services

	supplied and income transferred between participants, as well as between participants and any independent legal entity. The consortium and any independent legal entity will need to consider whether their activities are taxable for VAT purposes, and this will depend on whether they are operating as a business and whether they are issuing cryptocurrency (which is generally exempt from VAT), or providing other services (including issuing tokens, where the VAT treatment depends on the exact attributes of the token). • **Access to losses:** if the consortium incurs losses, a contractual arrangement or the use of a fiscally transparent entity may allow consortium members more immediate access to those losses. Losses may still be accessible where incurred by a fiscally opaque legal entity, but may be subject to restrictions and are unlikely to be transferable cross border. • **Access to R&D / IP incentives:** subject to the level of tech development required to establish the blockchain platform, R&D tax incentives may be available to partially offset development costs. The choice of jurisdiction will have a bearing on the level of incentives available. There may also be favourable taxation regimes available for the IP developed by the consortium (e.g. the UK's patent box regime). • **Exit options:** on disposal of an interest in the consortium, there will likely be different tax outcomes depending on the shape of the structure. The use of a fiscally opaque entity will be more likely to result in a tax-free disposal if the consortium members' jurisdiction(s) operates a participation exemption. Pre-sale restructuring may be possible to allow optionality on potential tax outcomes. • For further discussion of tax in the context of blockchain projects, see Section 8.

2. Joining a consortium

Due Diligence	When a company is considering joining an existing consortium as a new participant, it will need to carry out appropriate due diligence on the consortium, including consideration of the following issues: • the objectives, mission and roadmap for the platform, ensuring that the consortium's plans in terms of the use case and what the members are seeking to achieve are aligned with the company's own corporate goals; • size of consortium, current market share, members, progress and rate of development. How likely is it that the consortium in question will achieve critical mass or become an industry standard?; • tech specification of the platform and related infrastructure, services and service levels, and identity and role of the network operator; • how technical/operational governance (network, protocol, data) works; • how business governance works;

	• what level of investment is required (upfront and ongoing) and whether investment and/or participation in the consortium would offer an appropriate return-on-investment; • who has built and developed the platform and any potential IP risks or issues which could impact the continued development and scaling of the platform and the company's intended use of the platform; • how the consortium has approached information sharing protocols and competition law risks; • how the consortium has approached regulatory compliance (including with respect to financial regulation and data protection) and the role of consortium members in ensuring the platform and its operation meet applicable legal requirements; • whether the proposed agreement (e.g. JV accession agreement or consortium agreement) gives appropriate levels of control, influence (e.g. voting rights) and protection to meet the new joiner's needs and reflect the company's drivers and objectives and any tax implications; • whether the consortium model creates any barriers to entry (for example, an established JV consortium is more difficult to join and may have more onerous obligations on its members than a consortium based on contract); and • whether there are any existing intra-consortium disputes or tensions. A consortium is a "team sport" and built upon cooperation. If the consortium is not working well and members are unable to cooperate effectively, it is unlikely to achieve its commercial goals. It is also advisable to conduct due diligence on the state of the market generally before proceeding with consortium membership. Blockchain is a developing technology that is quickly growing and expanding, and it is important that companies join the right consortium at the right time for their business. In particular, companies should consider the state of development of blockchain platforms for the relevant use case before joining a consortium, and consider any other potential consortia focused on the same or similar use case, including projects being developed by any key industry stakeholders. In that regard, although consortia will want to try to ensure members are focused on the success of the relevant consortium, participants will generally want to resist any form of exclusivity which could prevent them creating their own similar platform in the future, or joining a competing platform.

Conclusion

Blockchain consortia may be essential in order to develop and scale blockchain platforms which enable digital transformation across a sector or a group of industry stakeholders. However, there are a number of factors that businesses will need to take into account when forming or joining a consortium and a range of issues for their legal advisers to consider. Lawyers (both in-house counsel and external advisers) can add significant value to a consortium project and organisations are well advised to bring them in early to ensure that a consortium is set up for success.

SECTION 4: DATA PROTECTION

Anne Rose, Mishcon de Reya LLP

PART A: Data Protection

Introduction

The European Union's General Data Protection Regulation became binding on 25 May 2018 and is based, in large part, and at least in big-picture, thematic terms, on the 1995 Data Protection Directive, which it replaced.[19]

GDPR's objective is essentially two-fold. On the one hand, it establishes a framework of fundamental rights in respect of the handling of personal data, with various measures based on the right to privacy (Article 8 of the Charter of Fundamental Rights). On the other hand, it seeks to facilitate the free movement of personal data between the EU's various Member States.

The legal framework creates a number of obligations on data controllers, which are the entities determining the means and purposes of data processing. It also allocates a number of rights to data subjects – the natural persons to whom personal data relates – that can be enforced against data controllers. Blockchains, however, are distributed databases that seek to achieve decentralisation by replacing a unitary actor with many different players. The lack of consensus as to how (joint-) controllership ought to be defined, and how it impacts upon accepted (or, even contested) meanings within GDPR, hampers the allocation of responsibility and accountability. Moreover, GDPR is based on the assumption that data can be modified or erased where necessary to comply with legal requirements, such as Article 16 (personal data must be amended) and Article 17 (personal data must be erased). Blockchains, however, intentionally make the unilateral modification of data onerous (if not impossible) in order to ensure data integrity and to increase trust in the network.

The Group focused on the definition of 'personal data' under GDPR and noted that depending on context, the same data point can be personal or non-personal and therefore subject to GDPR or not. In addition, the Group considered the impact of changes in technology that could increase the tension between blockchain and GDPR, as well as the possibility that blockchain could support GDPR. The Group did not go into detail on all the various issues, as these are discussed widely elsewhere.[20]

Experts and evidence

The Group heard from a number of experts, including Peter Brown (Group Manager (Technology Policy), Technology Policy & Innovation Executive Directorate, ICO, UK); and Adi Ben-Ari, (Founder & CEO, Applied Blockchain).

Peter Brown (Group Manager (Technology Policy), Technology Policy & Innovation Executive Directorate, ICO, UK)

Peter contributes to the development and delivery of technical and information security expertise at the ICO. His role involves monitoring and researching the technological environment for new and emerging developments that may impact on information rights, providing technical advice and guidance to the ICO (particularly on technology, data breach investigations and complaints received), and producing specialist guidance at UK and European levels.

[19] Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1

[20] For example, Michèle Finck, *Blockchain Regulation and Governance in Europe* (Cambridge University Press 2018)

Prior to joining the ICO, Peter was responsible for information technology and network security at a specialist consultancy. He was responsible for implementing the company's data protection policy and procedures as part of its involvement in European projects.

Adi Ben-Ari, (Founder & CEO, Applied Blockchain)

Adi has over 20 years of enterprise software experience, more recently leading major deliveries of production blockchain solutions. Adi is widely recognised as an independent thought leader in the industry, is a noted speaker at major conferences, experienced in educating C-suite on blockchain and zero knowledge proofs, and acts as an advisor for a number of early blockchain startups.

His work has also been noted by the UK Government, where he was invited to present at Parliament and the House of Lords, and at UCL where he recently lectured on the subject. Additionally, Adi has co-invented and designed a number of patents related to blockchain as well as mobile payments. Adi holds a BSc in Computer Science and an MBA in Information Systems.

The data protection sub-group thanks each of the experts for their time and contribution, without which this report would not be possible.

Further, the Group liaised with Dr Michèle Finck, Senior Research Fellow at the Max Planck Institute for Innovation and Competition who has provided her perspective on certain elements in blockchain and the GDPR, which was produced at the request of the Panel for the Future of Science and Technology (STOA) and managed by the Scientific Foresight Unit, within the Directorate-General for Parliamentary Research Services (EPRS) of the Secretariat of the European Parliament.[21] Dr Finck has written widely on the points of tension between blockchain and GDPR – including questions of when and under which circumstances on-chain data qualifies as personal data.[22]

Anne Rose, Solicitor at the law firm, Mishcon de Reya LLP, has also considered the tensions at play between blockchain and GDPR in an interactive entertainment context.[23]

What is Personal Data?

Article 4(1) GDPR defines personal data as:

> ***"any information relating to an identified or identifiable natural person ('data subject');*** *an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person"* (**bold** for emphasis).

This underlines the fact that the concept of personal data is to be interpreted broadly, and could include anything from a picture to a post code or an IP address of a living individual.

It is also clear that an item of data may be personal data (for example, a name: Michael), or non-personal data (for example, information which was never personal in the first place: a pencil case), but there are also circumstances where it may be unclear or may even change (for example, an IP address or a hash where the linkage between the natural person and the hash has been removed – or, in simpler terms, Michael's pencil case). To assess whether data is personal, pseudonymous (personal data which

[21] Panel for the Future of Science and Technology, 'Blockchain and the General Data Protection Regulation: Can Distributed Ledgers be Squared with European Data Protection Law?*'* (European Parliamentary Research Service, July 2019) <https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf> Accessed 13 April 2020

[22] See, for example, Michèle Finck, *Blockchain Regulation and Governance in Europe* (Cambridge University Press 2018)

[23] Anne Rose, 'GDPR challenges for blockchain technology', (2019) 2 IELR 35

can no longer be attributed to a specific data subject without the use of additional information) or anonymous (data which cannot be attributed to a specific data subject, including with the application of additional information) involves considering Article 4(5) GDPR and Recital 26 GDPR:

Article 4(5) GDPR (defining pseudonymous data) provides as follows:

> *"processing of personal data in such a manner that the* ***personal data can no longer be attributed to a specific data subject without the use of additional information****, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person"* (emphasis added).

Recital 26, GDPR (which sets the background to Article 4(5)) states:

> *"…To determine whether a natural person is identifiable,* ***account should be taken of all the means reasonably likely to be used****…To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the* ***costs*** *of and the amount of* ***time required for identification****, taking into consideration the* ***available technology at the time*** *of the processing and technological developments..."* (emphasis added).

Recital 26 GDPR assumes a risk-based approach to assessing whether or not information is personal data, which the ICO has also adopted. The ICO notes that "*the risk of re-identification through data linkage is essentially unpredictable because it can never be assessed with certainty what data is already available or what data may be released in the future*".[24] In contrast, the Article 29 Working Party (now renamed as the European Data Protection Board, or EDPB) seems to suggest that a risk-based approach is not appropriate and that "*anonymisation results [only] from processing personal data in order to irreversibly prevent identification*".[25] This uncertain standard of identifiability and the elements which also need to be taken into account (costs, time required for identification and available technology) require further guidance from data protection authorities and bodies.

The Group considers this to be particularly important in times where personal data is dynamic and technical developments and advances make anonymisation (if defined as *permanent* erasure) near-impossible. Further, it is possible that anonymous data today becomes personal data in the future, once further data is generated or acquired allowing for identification by the controller or by another person. On the basis of this, it could result in the uncomfortable conclusion that personal data can only ever be pseudonymised, but never anonymised.[26]

This definitional issue needs to be constantly monitored by data controllers. As noted by the former Article 29 Working Party, "One relevant factor…for assessing *'all the means likely reasonably to be used'* to identify the persons will in fact be the purpose pursued by the data controller in the data processing."[27] The French supervisory authority (the **CNIL**) determined that the accumulation of data held by Google, which enables it to individually identify persons using personal data, is "[*the] sole objective pursued by the company is to gather a maximum of details about individualised persons in an*

[24] Information Commissioner's Office, *Anonymisation: Managing Data Protection Risk Code of Practice* (November 2012) 16 <https://ico.org. uk/media/1061/anonymisation-code.pdf> Accessed 13 April 2020. Other data protection authorities have reached different conclusions but we have not considered them here.

[25] Article 29 Working Party, Opinion 05/2014 on Anonymisation Techniques (2014) WP 216 0829/14/EN, 3 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf> Accessed 13 April 2020

[26] Michèle Finck, Frank Palas, 'They who must not be identified – distinguishing personal from non-personal data under the GDPR', (2020) 10(1) IDPL 11, 26 <https://academic.oup.com/idpl/advance-article/doi/10.1093/idpl/ipz026/5802594> Accessed 13 April 2020

[27] Article 29 Working Party, Opinion 04/2007 on the Concept of Personal Data (2007) WP 136 01248/07/EN, 16 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf> Accessed 13 April 2020

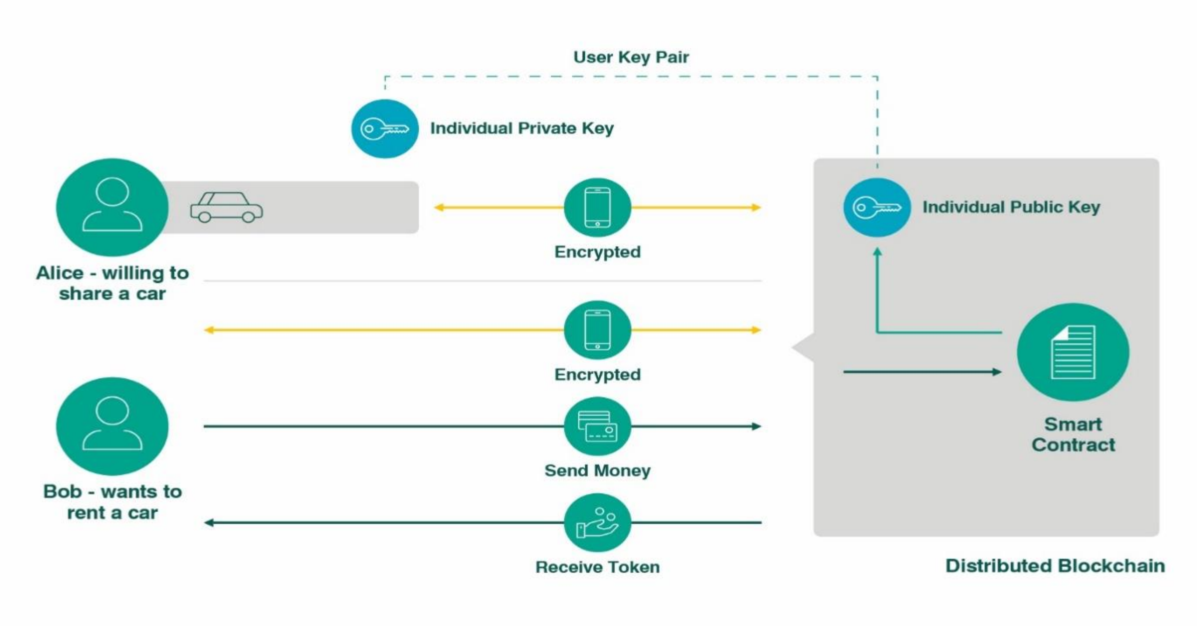
effort to boost the value of their profiles for advertising purposes".[28] In line with this reasoning, public keys or other sorts of identifiers used to identify a natural person constitute personal data.

The next section looks at various technical approaches to re-identification using a number of practical examples and considers the issues that arise.

Technical measures for re-identification – pseudonymous or anonymous?

Actors interested in using DLT and worried about GDPR compliance will seek to avoid the processing of personal data to start with. However, as noted below, this is far from straight-forward as much of the data conventionally assumed to be non-personal qualifies as personal data as a matter of fact.

Scenario:



In this scenario, Alice is willing to rent her car to Bob. In order to do this, both Alice and Bob will install an app on their personal device (e.g. a smart phone) and verify their respective digital identities (using a driver's licence or other form of ID). This will need to be verified by a third party. Once the verification process is complete, Bob will need to agree to all applicable terms and conditions in respect of price, rental duration, insurance policies and more. Once approved, Bob can proceed with verification on the smart contract. Payments will be made by reducing the balance in Bob's wallet and sending it to Alice's wallet. After payment, Bob will receive a unique car token with which to enter the car.

Is transactional data 'personal data'?

In order for the payment from Bob to Alice to work, Bob and Alice will create and manage their addresses in wallets (here, a wallet app on their smart phones). The address is a public key belonging to a private-public key pair randomly generated by a particular user. Bob will therefore transfer money from his address, 'A', to the address key of Alice, 'B', and sign the transaction with the private key responding to A. Where a blockchain uses proof of work, miners validate the transaction based on the public key A and the publicly known balance. While the transactional data is not explicitly related to a

[28] Commission Nationale de l'Informatique et des Libertés, 'Deliberation No. 2013-420' (Sanctions Committee of CNIL, 3 January 2014) < https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000028450267&fastReqId=1727095961&fastPos=1ff> Accessed 13 April 2020

natural person, it is related to an identifier (the address) which is pseudonymous data and may be classified as 'personal data' if you are able to single out the individual; by linking records to the individual and inferring information concerning the individual, the address may become personal data.[29]

Steps to take to prevent identification?

To prevent re-identification of a natural person, there are a few approaches that one can take. Though by no means exhaustive, these include:

- Use hash-based pseudonyms instead of clear-text identifiers. These are irreversible or one-way functions;
- Consider 'salting' and 'peppering' the hash to prevent re-identification. In both cases, additional data is added to the clear-text data before the hash function is applied, but the added data differs between contexts so that the resulting hashes also differ. There is, however, some argument that these methods can make the system more vulnerable, as each next validation relies on the validation of the previous hash, so if wrong once, the error could cascade through the system;
- Keep details of each party's identity off-chain to enable it to be modified and deleted;
- Consider the implementation of ring signatures and ZKP. Ring signatures hide transactions within other transactions by tying a single transaction to multiple private keys even though only one of them initiated the transaction. The signature proves that the signer has a private key corresponding to one of a specific set of public keys, without revealing which one. By using ZKP techniques, an individual (e.g. Bob) could prove to the owner of the car that he or she meets the rental requirements (e.g. a valid driver's license, insurance coverage, and bank account to cover costs) without actually passing any personal data, such as driver's license number, home address, and insurer, to the owner of the car (Alice). Where ZKP is used, the blockchain only shows that a transaction has happened, not which public key (Bob, as sender) transferred what amount to the recipient (Alice). For further details on ZKP (see Section B on Data Security Measures by Adi Ben-Ari below). This would also help with compliance with data protection principles, such as the purpose limitation and data minimisation principles.[30]

While these steps all assist in preventing transactional data being classified as 'personal data' under the GDPR, there is at present no legal certainty for developers wishing to handle public keys in a GDPR compliant matter and the Group considers that further guidance is needed from data protection authorities in respect of this.

The benefits of blockchain as a means to achieve GDPR's objective

Blockchain technologies are a data governance tool that support alternative forms of data management and distribution and provide benefits compared with other contemporary solutions. Blockchains can be designed to enable data-sharing without the need for a central trusted intermediary. They also offer transparency as to who has accessed data, and blockchain-based smart contracts can automate the sharing of data, which has the additional benefit of reducing transaction costs. These features may assist the contemporary data economy more widely, such as where they serve to support data marketplaces by facilitating the inter-institutional sharing of data. Furthermore, they could provide data

[29] Article 29 Working Party, Opinion 05/2014 (n 25) 14

[30] Under GDPR one is expected to comply with the purpose limitation which means that data is only collected for **specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes** and the data minimisation principle which means that data ought to be **'adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed' (see GDPR, Article 5(1)(b) and (c)).**

subjects with more control over the personal data that directly or indirectly relates to them. This would accord with the right of access (Article 15 GDPR) and the right to data portability (Article 20 GDPR), that provide data subjects with control over what others do with their personal data and what they can do with that personal data themselves.

Further guidance and support by regulatory authorities is required before these projects can become more mainstream.

On the basis of the Group's discussions and evidence examined, the Group believes that some of the questions to be addressed by the ICO and other data authorities should include the following:

- What does 'all means reasonably likely to be used' mean under Recital 26 GDPR? Does this require an objective or subjective approach?

- Does the use of a blockchain automatically trigger an obligation to carry out a data protection impact assessment?

- Does the continued processing of data on blockchains satisfy the compelling legitimate ground criterion under Article 21 GDPR?

- How should 'erasure' be interpreted for the purposes of Article 17 GDPR in the context of blockchain technologies?

- How should Article 18 GDPR regarding the restriction of processing be interpreted in the context of blockchain technologies?

- What is the status of anonymity solutions such as ZKP under GDPR?

- Should the anonymisation of data be evaluated from the controller's perspective, or also from the perspective of other parties?

- What is the status of the on-chain hash where transactional data is stored off-chain and subsequently erased?

- Can a data subject be a data controller in relation to personal data that relates to them?

- What is the relationship between the first and third paragraph of Article 26 GDPR? Is there a need for a nexus between responsibility and control?

- How should the principle of data minimisation be interpreted in relation to blockchains?

- Is the provision of a supplementary statement sufficient to comply with Article 16 GDPR?

Dr. Finck outlines other questions to be addressed in *Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?*[31]

[31] Michele Finck, 'Blockchain and the General Data Protection Regulation: Can Distributed Ledgers Be Squared With European Data Protection Law?' (STOA: Panel for the Future of Science and Technology, 2019) 97-98 <https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf> Accessed 28 December 2019

PART B: Data Security Enhancing Measures

Adi Ben-Ari (Applied Blockchain)

Introduction - Zero Knowledge Proofs

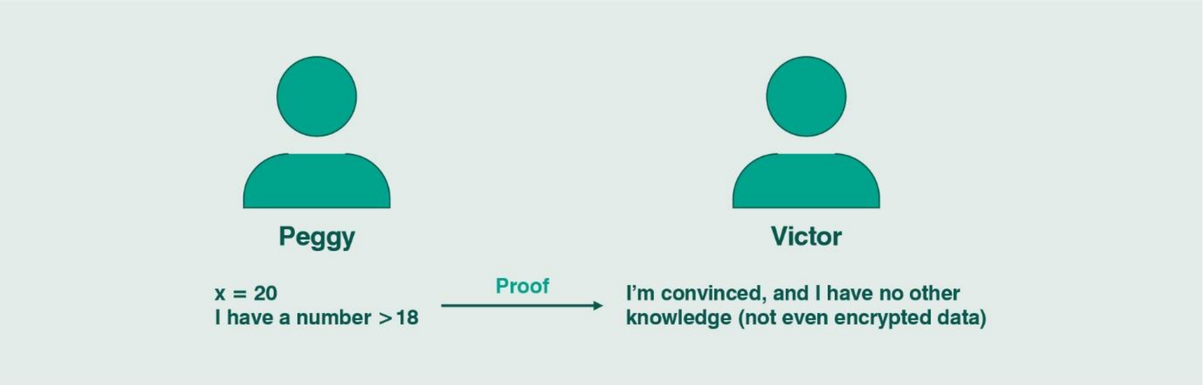
ZKPs are cryptographic outputs that can be shared and used by one party to prove to another that it is in possession of data with certain properties, without revealing anything else about that data.

In order for a cryptographic scheme to be considered a ZKP, it must demonstrate the following properties:

- **Completeness:** If the statement is true, an honest verifier will be convinced of this fact by the honest prover. That is, the algorithm must work in the sense that the party verifying the proof is satisfied that the proving party is in possession of the underlying data.
- **Soundness**: If the statement is false, no cheating prover can convince the honest verifier that it is true, except with some small probability.
- **Zero knowledge**: If the prover's statement is true, no verifier learns anything that was intended by the prover to be protected, other than the fact that the prover's statement is true.

Proof of Age example

An oft-cited example is proof of age. There are many situations in life, including in the digital world, where a person might be required to prove that they are over 18 years of age, including access to age appropriate content, purchase of goods that may only be sold to persons over 18, and signing agreements that require the consent of an adult.


Peggy
Victor
x = 20
I have a number > 18
Proof
I'm convinced, and I have no other
knowledge (not even encrypted data)

However, a person's age can constitute personal data for the purposes of data protection law, and many individuals would prefer not to share such information with a third party unless it is absolutely required. In fact, an important principle of GDPR regulation is minimisation, where data processing should only use as much data as is required to successfully accomplish a given task.

Using ZKP, an individual possessing an item of data on their device expressing their age may now generate and provide a zero-knowledge cryptographic proof that they are over 18 without revealing their actual age. This would, in theory, allow them to satisfy the requirement of a third party by proving that they are over the age of 18, while at the same time protecting their data and implementing GDPR minimisation by not revealing or sharing their actual age (or any other personal data) with the third party.

There are two potential flaws in this approach, and they illustrate how this technology should be considered in practice:

1. the prover could simply issue a statement that they are over 18, without the need for sophisticated cryptography; and
2. if the data the prover holds is incorrect, then a ZKP will be of little value to the third party verifier.

Simply issuing a statement

If a prover was to simply issue or sign a statement that they are over the age of 18, they would be making an assertion without providing any proof of that assertion. In other words, the prover could lie. This presents a risk to a third party who needs to be satisfied as to the prover's age, and often they will ask for proof in the form of a government issued document (e.g. driving license or passport). If the prover were to present such a document, they would be handing over their personal data (typically more than just their age), and be exposing themselves to the risk that their data may be used inappropriately or fraudulently, and may even be stolen or sold for commercial gain. The verifying organisation may also be non-compliant with the GDPR minimisation principle, as it is collecting more personal data than is required to satisfy the age check requirement.

Proving the information correct

If the verifier receives proof that a prover's dataset shows that they are over the age of 18, but doesn't trust the dataset itself (whether because the wrong data was mistakenly or deliberately inputted to the prover's dataset by the prover or another party), then further verification is required. In the proof of age example, the verifier would likely revert to government issued identification as a secondary verification step.

A ZKP system might therefore also include a third party signature verifying the accuracy of a prover's dataset. The verifier can then be satisfied that not only does the prover's dataset asserts that they are at least aged 18, but that such dataset (and therefore the assertion) has been signed by and verified by a third party such as a government entity. In other words, the requirement of the verifier to be satisfied that the prover is over the age of 18 is now achieved through the sharing of a cryptographic proof without receiving the precise age of the individual, nor the government documentation.

Types of Provable Knowledge

The first generation of ZKP enable proof of the following:

- **Range proofs**: a prover is in possession of a number within a range (e.g. age).
- **Location within a geofence**: a prover is located in a region (e.g. London), without revealing the prover's exact location (e.g. a specific road in a specific borough of London).
- **Set membership/non-membership**: a prover holds a value that is member or not a member of a particular set of values (e.g. AML checks on sanction lists.
- **Anonymous provenance to a cryptographic identity**: a prover owns an asset, together with properties of the asset's history, without revealing the history of the prover or historic parties.

This is not an exhaustive list, but illustrates the type of data properties that ZKP systems can prove for data in a prover's possession.

State of technology

ZKP technology is very much in its infancy and new, more secure, more efficient algorithms are regularly announced. Government entities that sanction use of cryptography algorithms for government and industry (e.g. NIST) are yet to make their official recommendations, which we look forward to in due course.

Everything described thus far in this section can be achieved without a blockchain. The added value of a blockchain-based ZKP is twofold:

1. **Immutability**. An activity can be recorded, ordered, time-stamped and then jointly secured by a group of parties, which is potentially more secure than relying on the ordering and time stamps set and stored by an individual party who may modify or even destroy records. This can improve the verifier's confidence in the integrity of a prover's dataset.

2. **Double spend prevention**. In the case of assets, blockchain-based ZKP can provide assurance to verifiers that a single copy of an asset is available to all parties, avoiding duplicate records, as well as removing the need to trust a single party to hold and manage all of the records.

These additional attributes may or may not be required for a particular use case of ZKPs.

ZKP and blockchain

One of the myths surrounding blockchains is that the data stored on them is automatically encrypted. In some blockchains (e.g. the Bitcoin blockchain) cryptography is primarily used to sign messages and ensure that historical transactions confirming asset ownership can be secured by a group. Nevertheless, the data showing the wallet holdings and transfers between wallets was publicly available.

There was a conflict between the need for transaction and data privacy on the one hand, and the need for transparency and verifiability on the other. Prior to ZKP, privacy was achieved in enterprise blockchains by separating the parties into “mini” blockchains, also known as private channels. The issue with this approach is that the number of validating parties for private activity, and therefore overall security and integrity assurance of the blockchain, is greatly reduced. These issues motivated research into advanced cryptographic techniques that would eventually lead to the first practical implementations of ZKPs.

ZKPs enable the solving of both data privacy and verifiability issues at the same time. This is because, rather than storing the assets and data openly on a blockchain, ZKPs of their existence and consistency are stored. A transaction, such as transferring an asset to a different account, will only be permitted if ZKPs are available to verify the asset ownership. A new node in the blockchain can download a copy of all of the proofs and validate the consistency and historical correctness of the data without seeing any of the actual data.

ZKP and blockchain privacy

The first practical implementation of such a blockchain was zCash, launched in late 2016. zCash implemented a ZKP called a succinct, non-interactive argument of knowledge (zkSNARK). A succinct proof reduces the volume of data required to be stored on a blockchain network (thereby improving its performance), and a non-interactive protocol allows for one time generation of proofs that are stored indefinitely on a distributed ledger which multiple parties can verify, without each verifying party requiring interaction with the prover.

There are three stages in the life of a typical ZKP. These are:

1. Circuit production

2. Proof generation

3. Proof verification

A circuit expresses the mathematical logic that the proof will implement (e.g. prove a person is over 18). This will vary depending on the use case, and there are a number of initiatives to create multi-purpose generic circuits currently in development. The circuit acts as a template for producing a certain type of proof. The circuit need only be created once, and can then be used by multiple parties to generate proofs.

A more complex area of research and development is ZKP for privacy in blockchain-based smart contracts, where there exists a much broader range of functionality that would need to be expressed privately. A number of protocols are in development for smart contracts in Ethereum (Baseline, AZTEC) and Hyperledger Fabric (ZKAT), or both (Applied Blockchain's K0).

ZKP and blockchain scalability

ZKPs offer two approaches to improving the scalability of a blockchain platform. These are:

1. Rollups

2. Flat blockchains

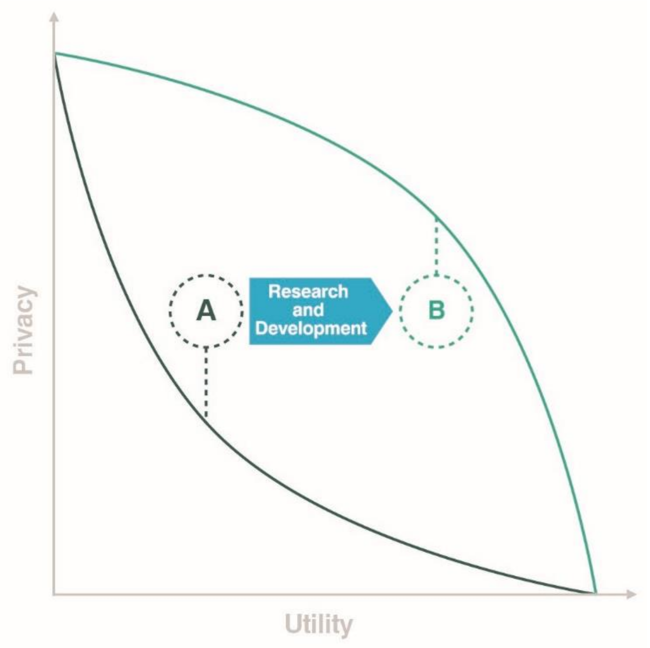
Rollups are designed to reduce the number of transactions on a blockchain by executing batches of transactions off chain, rolling these up into a proof of the outcome of the transactions, and then posting only the proof to the blockchain. This greatly reduces the load on a blockchain, as it is no longer required to execute all of the transactions on-chain.

Succinct blockchains are even more compact and never grow. Rather than maintaining a full and growing history of transactions in each node, a flat blockchain will only ever contain a single row. This single row is a ZKP of the current state of the accounts on the blockchain. Any party can verify the proof and be satisfied with the integrity of the blockchain despite the fact that they have no access to the underlying data and transactions. Each time a new block of transactions is generated, a ZKP is created to prove the changes to the blockchain taking into account the previous proof. The technique is known as recursive zkSNARKs, and the result is that transactions are compressed to the point where the blockchain hardly grows.

As has been illustrated, ZKP technology is having a profound impact on the structure and implementation of blockchains. The capabilities described in this section were not available two or three years ago, when the popular enterprise platforms in use today were designed and conceived.

Other Privacy Enhancing Technologies (PETs)

Another example of a PET is Homomorphic Encryption (HE), and the closely related Somewhat Homomorphic Encryption (SHE) and Fully Homomorphic Encryption (FHE). These cryptography schemas enable data to be encrypted in a way that allows third parties to run calculations on the encrypted data without having the ability to decrypt and see the data. This may be particularly useful where data processing is outsourced to cloud computing services, but the data is of a sensitive nature and the data owner wishes to keep the data hidden from the cloud data processor. It may also enable analytics companies to perform analytics on data that is not shared with them.



These technologies are part of a greater trend to increase data privacy by sharing less, while enabling increasing utility from privately held data. This is in direct contrast to the proliferation of data sharing in recent decades when both individuals and companies shared vast quantities of data with third parties in return for utility.

SECTION 5: INTELLECTUAL PROPERTY

Rosie Burbidge, Gunnercooke LLP; John Shaw, Blake Morgan LLP; and Charlie Lyons-Rothbart, Wiggin LLP

Introduction

DLT has a vast array of applications, particularly when it comes to IPRs. There is potential to revolutionise the way IPRs are recorded, protected and managed. Through tokenisation, automation and smart contracts, DLT could change how royalties are collected and even how licensing deals are done.[32] With these applications in mind, practitioners should consider the prospective tensions between current intellectual property law and the application of DLT.

Many of the utilities presented by DLT also have negative implications that should not be overlooked. The permanency and purported immutability of DLT has implications for copyright infringement. There may be issues with the current notice and takedown requirements for platforms that enable file sharing. Given the clear IPR registry applications, there are implications for trade mark owners. Questions arise over whether applications linked to DLT or even the underlying chains themselves can attract database rights. It is worth considering whether confidential information can be stored (and remain confidential) on a distributed ledger, given the purported escrow capabilities. Finally, it is worth reviewing the structure of DLT and whether various applications, such as smart contracts, attract IPRs, including the suitability of patent protection.

It is concluded, echoing the sentiments of Sir Geoffrey Vos in his notable 2019 speech, that it is unnecessary (and indeed undesirable) to recharacterise the well-known species of nationally and internationally statutorily recognised IPRs.[33] The following discussion shows that DLT can fit within the existing (European) Intellectual Property framework and any tensions that exist could be managed by practitioners.

Copyright infringement on the Blockchain

The reliability, transparency and automation capabilities of DLT make it an ideal technology for digital file management, sharing and transfer. The opportunities to pseudonymise users as well as the emergence of peer-to-peer decentralised applications mean that this technology will likely be utilised in order to facilitate copyright infringement, perhaps in a similar way that has been seen with the emergence of internet based file-sharing sites. Practitioners should consider the existing legal framework protecting digital copyright, given the potential for rights holders and infringers alike to enable access to original works via DLT.

File sharing

A key utility of DLT is the ability to pseudonymously share information, sometimes without the need for a third party intermediary, via a peer-to-peer network or Decentralised Application (**DApp**). DLT offers authors the opportunity to provide a licence to original works and, via a smart contract, collect royalties directly and in a transparent manner which could become automated. Use of DLT in digital rights management could revolutionise the way digital content is controlled and distributed with the allocation of tokens, such as Bitcoin or Ether in place of traditional royalty distribution. A network of smart contracts could facilitate a better distribution of value when multiple contributors are involved. Mirroring these utilities, the technology may be exploited by parties attempting to circumvent paying for access to material that is subject to copyright.

[32] Tresose, Goldenfein and Hunter, 'What Blockchain Can and Can't Do for Copyright' (2018) 28(4) AIPJ) 144

[33] Sir Geoffrey Vos, 'Cryptoassets as Property: How can English Law Boost the Confidence of Would-be Parties to Smart Legal Contracts?' (Joint Northern Chancery Bar Association and University of Liverpool Lecture, 2 May 2019)

One of the intentions of copyright law is to control unauthorised use of the work, with the aim of stimulating and protecting the fixation of original expressions. As a result, the holder of copyright enjoys exclusive rights to carry out specified actions in relation to the copyright work.[34] One exclusive right in relation to copyright works, which has become increasingly important in the digital age with the proliferation of web 2.0 and the development of the platform economy, is the right to communicate the work to the public. It is this aspect of the copyright regime that practitioners, regulators and other bodies should carefully consider when working with DLT.

DLT provides a new environment in which works can be published, and this raises the question of whether placing an original "work" on a distributed ledger would constitute a relevant communication to the public as set out in Section 20(2) of the Copyright, Designs and Patents Act 1988. It is important to note at the outset that there are two main ways in which communication to the public can take place using DLT: first, via an application which utilises DLT; and second, directly via a distributed ledger using a peer-to-peer network. Separately there are two locations to store files so that content can be accessed via DLT: on-chain and off-chain (such as via a hyperlink).

Communication and making available to the public

The act of communication is construed broadly in order to ensure a high level of protection for copyright owners and includes making their works available to the public in such a way that members of the public may access them from a place and at a time individually chosen by them. It has been held by the court that there is an act of communication when someone gives members of the public access to the work in circumstances where they would not be able to enjoy the work without that intervention.[35] This has included making a hyperlink available, even if the user does not click on it.[36] These rulings are worth considering given that users may employ DLT without storing significant amounts of transaction data on the distributed ledger itself. In fact, it may become desirable (particularly with large files) to store data in an off-chain database with a link to the distributed ledger through a hash.[37] Despite the utility of storing data off-chain, this would appear to be capable of constituting a relevant communication to the public and would not be a way to avoid infringing activity. Notably, in the Advocate General Opinion on *Ziggo* it was considered that communicating to the public also included the operation of a website, by indexing files and providing a search function which enabled users to find works protected by copyright which are offered for sharing on a peer-to-peer network.[38] In light of these decisions, it seems that operators of applications utilising DLT by posting links, indexing and providing a search function could be communicating the works to the public. This is because the links will be available to an indeterminate and fairly large number (above *de minimis*) of people.[39]

Linked to this, it is worth considering whether the party posting to the distributed ledger has actually carried out an act of communication to the public because, until the block is approved and obtains its hash, it will not appear on the ledger. The intention to communicate to the public would clearly exist, but the technical structure of DLT raises questions about whether the miners of the blocks (or the equivalent when proof of stake or other means of validation is used) should be in any way responsible, as their actions will result in the work being made available to the public. The issue of whether mining, or other means of validation, would be considered an “intervention” for the purposes of communicating to the public is one that the court may need to address, particularly with the increase in mining pools (which may become an attractive party to pursue for infringement in due course). The lack of autonomy

[34] Copyright, Designs and Patents Act 1988, ch II
[35] *Paramount Home Entertainment International Ltd v British Sky Broadcasting Ltd* [2013] EWHC 3479 (Ch) [12(7)] (Arnold J)
[36] *Warner Music UK Ltd and Sony Music Entertainment UK Ltd v Tunein Inc* [2019] EWHC 2923 (Ch) [52]
[37] Michele Finck, *Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?,* (STOA: Panel for the Future of Science and Technology, 2019) 32 <https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf> Accessed 28 December 2019
[38] Case C-610/15 *Stichting Brein v Ziggo BV and XSALL Internet BV ,* Opinion of AG Szpunar, para 54
[39] Case C-306/05 *SGAE v Rafael Hoteles SA* [2006] ECR I-11518, para 38

in relation to mining may rule out the possibility of it being considered an intervention, whereas the party posting to the distributed ledger will likely be considered to be intervening.

Another group that could be considered to be involved in communicating to the public are the DLT core software developers. It has been held that the installation of physical facilities that distribute a signal and thus make public access to works technically possible constitutes "communication".[40] [41] However, recently and in contrast, the CJEU has held that the provision of physical facilities (rental cars with radios) was not a communication to the public.[42] This decision in *SAMI* is based on the fact that the provision of a space, like the provision of a radio set, does not constitute a communication because there is no deliberate intervention. The CJEU noted that the relevant case law refers to the deliberate nature of the intervention by the user and for the user to perform a relevant "communication act", they must do so in full knowledge of the consequences of their behaviour.

These cases have particular relevance to DApps which, as in the case of BitTorrent, can be a fully anonymous decentralised application made up of a series of instant atomic interactions.[43] Whether the installation (or provision) of the file required to access a DApp or other peer-to-peer file sharing networks will constitute the "installation of physical facilities which distribute a signal" sufficient for "communication to the public" to take place will be a question for the court to consider. If this is the case, and core software developers are considered to be involved in the installation process by making it available, questions about a form of accessory liability may arise. The court has not taken this step yet, with the majority of comparable cases being against internet service providers (**ISPs**), platforms and website operators rather than developers. The recent Advocate General Opinion in the joined YouTube and Cyando cases, given its arguable divergence from previous opinions and judgments in the finding that YouTube and Cyando do not, in principle, carry out an act of "communication to the public" themselves, highlights the complexity in the area.[44]

When ruling if parties have intervened in order for a communication to the public to take place for a work that has already been subject of another communication, the court will consider whether one of two alternative further criteria has been satisfied for the act to amount to a communication to the public. The alternative criteria are: (i) whether a new technical means has been employed; or (ii) whether the communication is to a new public. This is particularly relevant to DLT as, with the majority of copyright infringement being carried out via file sharing, the original communication of the work will be accessible elsewhere on the internet.

"Technical Means"

It has been held in *ITV* that "communication to the public" covers any transmission or retransmission of the work to the public not present at the place where the communication originates by wire or wireless means and also when any retransmission of the work is made by a specific technical means different from that of the original communication.[45] Although many technologists have heralded DLT as an entirely new technology, whether the court takes this approach remains to be seen. In *Svensson,* the court treated the "internet" as a single technical means and this was noted in the useful summary on "communication to the public" provided in *TuneIn*.[46] As a DLT application will still require the internet

[40] Ibid, paras 46-47

[41] Case C-136/09, *Organismos Sillogikis Diacheirisis Dimiourgon Theatrikon kai Optikoakoustikon Ergon v Divani Akropolis Anonimi Xenodocheiaki kai Touristiki Etaireai* [2010] ECR I-00037, paras 39-41

[42] Case C-753/18, *Föreningen Svenska Tonsättares Internationella Musikbyrå u.p.a. (Stim) and Svenska Artisters och musikers, intresseorganisation ek. för. (SAMI) v Fleetmanager Sweden AB and Nordisk Biluthyrning AB* [2020] EU:C:2020:268

[43] Vitalik Buterin, 'Daos, DACs, Das and More: An Incomplete Terminology Guide', (*Ethereum Blog*, 6 May 2014) <https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide> Accessed 27 March 2020

[44] Joined cases C-682/18 *Youtube and Others* [2018] and C-683/18 *Elsevier Inc. v Cyando AG* [2018], Opinion of AG Saugmandsgaard ØE [2020]

[45] Case C-607/11, *ITV Broadcasting Ltd v TV Catchup Ltd* [2013] EU:C:2013:147 paras 23 – 26

[46] *Warner Music UK Ltd, Sony Music Entertainment UK Ltd v Tunein Inc.* [2019] EWHC 2923 (Ch) [54]

protocol network layer and will sit between the application and transport layers[47] it will be of interest to practitioners as to whether DLT is considered to be a new technical means by the court.

"New Public"

Ziggo is instructive when considering whether the users of DLT, who access copyright works, are to be considered a "new public", but (unfortunately) does not provide guidance on the issue of "technical means" in the context of the use of BitTorrent and peer-to-peer networks on the basis that the technical means were regarded to be the same. It was held in *Ziggo* that there was a communication to a new public on the basis that "*TPB* [The Pirate Bay] *could not be unaware that this platform provides access to works published without the consent of the rights holders, given that… a very large number of torrent files on the online sharing platform TPB relate to works published without the consent of the rights holders*."[48] As a result, in the context of a peer-to-peer file sharing application and even DApps it is arguable that the users of the application will be considered a "new public" where a significant number of works are shared without consent.

"*Profit Making*"

A further feature of the activity of TPB that led the court to find that there was copyright infringement was the purpose of obtaining profit.[49] It will be interesting to see how the "profit making" requirement is interpreted by the courts in relation to the activity on DLT. The use of a smart contract to access a hyperlink to a work (which had been posted without authorisation) requiring the payment in crypto to the party that posted the link would likely be sufficient to constitute infringement. In *GS Media* it was held that when there was financial gain, there was a presumption of the unlawful publication of protected works.[50]

It is worth considering the mining activity as well. Given that a transaction on the Ethereum Blockchain will require an amount of Ethereum gas money to be "paid" to the miners in order to verify the hash, a crypto profit will be made by another party (albeit minimal). The party that made the link available on the chain will not make this profit and, as a result, DLT can create the novel situation where there is profit making activity, but the mining "profit" is made by neither the uploader nor the downloader of the content.

In *GS Media* the court reasoned that when the posting of hyperlinks is carried out for profit, it can be expected that the person who posted such a link carries out the necessary checks to ensure that the work concerned is not illegally published on the website to which those hyperlinks lead; it must therefore be presumed that the posting has occurred with the full knowledge of the protected nature of that work and the possible lack of consent to publication on the internet by the copyright holder.[51] The interpretation of "posting hyperlinks for profit" might be worth consideration should it become common practice for parties to post links to works using DLT without authorisation in a not-for-personal-profit capacity.

The platform liability question is significant for the DLT industry, as various interpretational positions will determine whether or not the technology is operated within the law. It is of note that in *Ziggo*, the majority of references to TPB were not to "websites" but to "platforms". In the conclusion of the judgment of Ziggo it is held that the concept of 'communication to the public', within the meaning of Article 3(1) of Directive 2001/29, "*must be interpreted as covering, in circumstances such as those at issue in main*

[47] De Filippi & Wright, *Blockchain and the Law: The Rule of Code*, (Harvard University Press 2018) 48-49.
[48] Case C-610/15, *Stichting Brein v Ziggo BV and XSALL Internet BV* [2017] EU:C:2017:456 para 45
[49] Ibid para 46
[50] Case C-160/15, *GS Media BV v Sanoma Media Netherlands BV and Others* [2016] EU:C:2016:644 para 51
[51] Ibid [51]. It is also worth noting that in Tunein at [98] the court provides the analysis that based on European case law (with the focus on GS Media paragraph 44) that only a linker with the requisite notice of the lack of consent (governed by presumptions) will commit an infringing act in such a case.

proceedings, the making available and management, on the internet, of a sharing platform which, by means of indexation of metadata referring to protected works and the provision of a search engine, allows users of that platform to locate those works and to share them in the context of a peer-to-peer network".[52] This appears to be highly applicable to DLT. It remains to be seen which regulatory access points will be worth pursuing, particularly since, in TPB, it was the ISPs which were determined to have enabled users and operators to infringe copyright law.

Whether ISPs are the subject of further actions involving access to sites utilising DLT remains to be seen. However, there are also opportunities, perhaps, for action to be brought against the core software developers, as noted above. Finck notes that governments could impose legal obligations on core developers[53] and it is conceivable that regulations could be brought in to require core developers to disincentivise mining which promotes copyright infringement. Platform applications have seen that facilitation of copyright infringement is sufficient to raise questions of liability and so far these platforms have benefitted, to some degree, from exemptions on the basis that infringing material is taken down expeditiously. A key feature of DLT conflicts with this exemption: immutability.

Immutability

The immutable nature of DLT is a feature designed to prevent "double spending" of cryptoassets. By time-stamping and hashing blocks, entries on the ledger become immune (to a large degree) from tampering. This raises issues when infringing copies of work must be taken down at the request of the copyright holder. The DSM Directive, which contains measures designed to achieve a well-functioning marketplace for copyright, includes a 'value gap' provision in Article 17. This will be relevant to practitioners in European jurisdictions because it sets out that an online content-sharing service provider (OCSSP) will be considered to communicate to the public and also provides that it will be ineligible for safe harbour protection. This clarification of the InfoSoc Directive will mean that OCSSPs utilising DLT will not benefit from the limitation of liability "loophole" that exists in the E-Commerce Directive.

The "loophole" set out in the E-Commerce Directive allows platforms to escape liability when infringing content is made available on the platform, provided that the platform take expedient action to take down/ remove the content.[54] It is worth noting that this is true only if you assume that (i) the platform qualifies in principle for the safe harbour and (ii) there is no potential direct liability (i.e. it is not a platform that behaves like TPB). In this instance, DLT and the relevant legal framework are seemingly at odds (and parallels could be drawn with the issues surrounding the right to erasure under GDPR). However, it has been noted by Advocate General Szpunar in *Ziggo* that it may be sufficient to render access to the work impossible in order to comply with the "take down" requirement, rather than the action of actually removing that version of the work.[55]

Therefore, deletion may not in fact be necessary if individuals are unable to access the content. How this issue is interpreted will be of great interest to practitioners in the DLT space. Similar comments have been made in relation to personal data and immutability by Michele Finck[56] and it seems that her notable conclusions on how blockchain and GDPR can co-exist could be equally applicable to this aspect of the copyright regime. In *Soulier* the court emphasised the point that copyright owners, if they wish to stop communicating their work, ought to be entitled to take down a posting and prohibit future

[52] *Ziggo* (n 48) [48]
[53] Michele Finck, *Blockchain Regulation and Governance in Europe* (Cambridge University Press 2019), 52
[54] E-Commerce Directive 2000/31/EC of 8 June 2000, articles 12-14 implemented by The Electronic Commerce (EC Directive) Regulations 2002 (SI 2002/2013), regulations 17-19
[55] *Ziggo, opinion of AG Szpunar* (n 38) [51]
[56] Finck, *Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?* (n 37)

use.[57] The prohibition of future use is quite different from total deletion and so it may be perfectly possible for the immutable nature of DLT to exist within the current copyright framework.

The existing national IPR structure appears to be well suited to dealing with applications of DLT that result in copyright infringement, with various cases relating to the platform economy and peer-to-peer file sharing seemingly highly applicable. If this is substantiated in practice, there appears to be no need for bespoke legislation relating to the enforcement of IPRs on DLT, specifically with regards to copyright, and practitioners will be able to advise based on existing case law. In fact, the national (and European) copyright regime appears well suited to adapt to business (and infringement) conducted via DLT however, it remains to be seen which actors will be considered liable for infringing activity. With the CJEU perhaps moving towards a form of accessory liability in its decisions on digital copyright, the various actors in the DLT ecosystem will want to monitor decisions on copyright. Users will remain in a similar position. Operators of applications may find themselves treated in the same way as operators of websites whilst there is scope for miners and core developers to avoid liability dependent on the nature of their interventions.

Trade Mark and Design Rights

DLT has significant applications in relation to trade mark and design rights, not least as a registry for registered marks and designs, but it also, due to its structure, provides an ideal system to record evidence of use (in relation to trade marks). This application also raises prospects of infringement and similar infringement issues arise, as set out above with copyright, in relation to trade mark infringement and counterfeit products. Please note that we have not considered the registration of other IPRs in this section.

One issue that practitioners should consider is whether remedies are available to holders of registered trade mark rights where infringing articles are made available on platforms supported by DLT. Below is a consideration of relevant case law that can help to inform practitioners on the treatment of DLT by the court in trade mark infringement situations. Further issues are explored that will be of wider interest to practitioners, such as whether transactions carried out on distributed ledgers can amount to genuine use of a trade mark, and whether evidence of reputation can be linked to on-chain activity.

Platform liability for Trade Mark infringement

As with copyright, DLT poses interesting questions of liability for trade mark infringement. It is foreseeable, just as counterfeiters have utilised the platform economy, that trade mark infringement will occur via DLT, particularly given the peer-to-peer opportunities and anonymous or pseudonymous nature of transactions. This raises questions of liability for providers of DLT applications.

In the notable case *L'Oreal v eBay* it was held that eBay was not jointly liable with individual sellers for the sale of infringing or counterfeit products on its platform.[58] On a reference from the proceedings, the ECJ gave a ruling stating that an ISP may lose the benefit of this exemption from liability for intermediaries under the E-Commerce Directive (2000/31/EC) where the ISP plays an active role in the advertisement of infringing goods.[59] What constitutes an "active role" will be of interest to practitioners given that website blocking orders have been granted requiring ISPs to block access by their subscribers to certain websites advertising and selling goods that infringe the claimants' registered trade marks.

[57] Case C-301/15 *Soulier and Doke v Premier Ministre and Ministre de las Culture et de la Communication* [2016] EU:C:2016:878 para 51

[58] *L'Oreal SA v eBay International AG* [2009] EWHC 1094 (Ch)

[59] Case C-324/09 *L'Oréal SA and Others v eBay International AG and Others* [2001] I-06011

Article 11 of the IP Enforcement Directive[60] imposes an obligation on EU member states to ensure that IP rights-holders can apply for an injunction against intermediaries whose services are used by a third party to infringe an IP right. It is arguable that an application utilising DLT will be considered an intermediary, but in the case of peer-to-peer sharing and DApps, it remains open to interpretation whether a distributed ledger itself could be considered as a form of intermediary (given its decentralised structure) with responsibility falling on the core developers.

The Court of Appeal made some notable comments in *Cartier International AG v British Sky Broadcasting Ltd* regarding the threshold for making blocking orders.[61] Practitioners will note that there was no contractual relationship between the ISPs and the operators of the website, but this did not matter. The ISPs were considered essential actors in all of the communications between the consumers and the operators of the target websites. If this rationale is extended to DLT, for example where infringing or counterfeit goods are sold via a distributed ledger and it is considered an "essential actor", practitioners may see applications made to court for blocking injunctions against the DLT platform. How this could work in practice is unknown and any such action would create a novel situation.

Linking a Trade Mark to DLT

One application of DLT is the use of a citadel-key (a form of crypto-key) to identify whether a product displaying a trade mark is genuine. This could raise issues if the crypto-key is copied (in the same way that some hologram devices are copied) to give the impression that a counterfeit is genuine. The question for practitioners would be whether this would be sufficient for an action for trade mark infringement to be brought, which in turn raises questions of the tokenisation of a registered trade mark. Tokenisation involves a real world asset (such as a registered trade mark) being represented on DLT as a cryptoasset which could in turn be traded on-chain. Large-scale adoption would be needed so that on-chain activity mirrors off-chain performance, but the transfer of trade mark portfolios could benefit from a degree of automation. The use of DLT as a trade mark registry is the first step towards this.

Proof of "Genuine Use" and evidence of goodwill

It has been noted by numerous commentators that DLT has the utility to provide evidence of genuine use, by being linked either to revenue information or advertising.[62] This has a particular utility given the time stamping of blocks, searchability of entries and ease of access for brands.

Usually the focus on evidence to prove the goodwill associated with a mark relates to sales, revenue and other financial information. Social media account traffic, including followers and likes, has increasingly been used to demonstrate goodwill. It will be interesting to see if activity linked to a distributed ledger will be considered as evidence of goodwill in a similar way. This could have implications in a claim of passing off.

If such activity is sufficient to demonstrate goodwill, it will be of interest to brands with a significant number of subsidiary logos given that such brands can encounter difficulties proving goodwill in these subsidiary logos where they are predominantly used with a primary word mark.

Database rights

The underlying application of DLT is a form of database, given that it is in essence no more than a sophisticated ledger. Michele Finck provides the useful summary that it is essentially a database that is replicated across a network of computers updated through a consensus algorithm.[63] The ledger aspect

[60] Council directive 2004/48/EC of 29 April 2004 on the enforcement of intellectual property rights (2004) OJ L195/16
[61] *Cartier International AG v British Sky Broadcasting Ltd* [2016] EWCA Civ 658
[62] Rosie Burbidge, 'The Blockchain is in Fashion' (2017) 107(6) TMR 1262 - 1297
[63] Finck, *Blockchain Regulation and Governance in Europe* (n 53) 6

of DLT means that it is worth considering whether the two rights created by the Database Directive (96/9/EC)[64] (the **Database Directive**) which was implemented by the Databases Regulations 1997[65] (the **Databases Regulations**) may apply to DLT or to applications which are based on a DLT framework. The two rights are (i) a *sui generis* right (the **database right**); and (ii) copyright in databases (**database copyright**). Database copyright subsists in an original database which is dependent on the author's arrangement and selection and must constitute "the author's own intellectual creation"[66]. The database right will be of interest to practitioners, particularly given the ongoing maintenance of a distributed ledger as this can impact on extending the term of protection from which databases can benefit.

A Database

A database is defined as "*a collection of independent works, data or other materials which (a) are arranged in a systematic or methodical way and (b) are individually accessible by electronic or other means*".[67] It is worth considering whether DLT can fit within this definition before examining whether a database right or database copyright subsists. It should be noted that "database" has a wide definition, including virtually all collections of data in searchable form.[68]

- *A collection of independent works, data or other materials*

In *Bitcoin: A Peer-to-Peer Electronic Cash System*, Satoshi Nakamoto set out that an electronic coin was defined as "a chain of digital signature".[69] Such a chain of digital signatures would likely constitute a collection of data or other materials if nothing else.

- *Arranged in a systematic or methodical way*

DLTs are arranged in accordance with the hash function, with each block containing the hash of the block preceding it and succeeding it. This is likely to be considered systematic or methodical.

- *Individually accessible by electronic or other means*

DLT also contains this functionality, a key utility of DLT being its distributed and accessible nature.

It follows that a chain created in DLT is likely to fit within the definition of a Database for the purpose of the Database Regulations.

Database right

The database right subsists in a database when "*there has been a substantial investment in obtaining, verifying or presenting the contents of the database*".[70] In *William Hill* it was held that it is not the form of the data (its order, structure and "searchability") but the investment put into making the database which was the protected aspect of the database.[71] This leads to certain interpretation issues in the context of whether a database right can subsist in an entire distributed ledger (or blockchain) or even an application which utilises the ledger (or chain).

[64] Council Directive 96/9/EC of 11 March 1996 on the legal protection of databases [1996] OJ L 77/20
[65] The Copyright and Rights in Databases Regulations 1997, SI 1997/3032
[66] Copyright, Designs and Patents Act 1988, s3A(2)
[67] Ibid, s3A(1)
[68] *British Horseracing Board Limited v William Hill* [2001] RPC 31 [30]
[69] Satoshi Nakamoto. 'Bitcoin: A Peer-to-Peer Electronic Cash System', (October 2008) <https://bitcoin.org/bitcoin.pdf> Accessed 9 March 2020
[70] Databases Regulations (n 65), Regulation 13(1)
[71] *British Horseracing Board Limited v William Hill* (n 68)

Database right in DLT

Significant investment is required to develop a distributed ledger or blockchain. The creation of a DLT protocol is no small feat. Furthermore, the continued operation of a distributed ledger can require ongoing investment. The Ethereum Blockchain, for example, requires "gas money" for each transaction to be added to the chain and this cumulative "cost" to the transaction may constitute sufficient investment to benefit from the protection of a database right (even though the significant investment amount is not derived from a single source). It has been noted that court decisions often conflict on such issues as what is meant by "substantial investment".[72] It remains to be seen whether the validation procedures such as mining undertaken by nodes to verify transactions will constitute "investment" given that the definition of "investment" has previously been considered by the court to be direct financial investment.

It should be noted that in the *William Hill* case the database operated by the British Horseracing Board (BHB) containing information relating to races, horses' registration details, jockeys, fixture lists, race conditions etc. was being continuously updated and, because of this, was viewed as a single database in a constant state of revision and not a sequence of separate databases. As a result of this, William Hill's borrowing from the BHB database fell within Article 7(5) of the Database Directive on the grounds of repeated and systematic extraction and re-utilisation of part of its contents.

The ECJ has restricted the types of database in which a database right may subsist. It does not cover the resources used for the creation of materials that make up the contents of a database but rather the investment in the verification of those contents.[73] The Court of Appeal applying the ECJ decision found that "[s]*o far as BHB's database consists of the officially identified names of riders and runners, it is not within the sui generis right of Art. 7(1) of the Directive."*[74] The court rejected arguments by BHB on this point on the grounds that the provision of an official stamp of approval did not constitute the right kind of investment, making clear that it is only investment to seek out existing materials and collect them into a database that will give rise to a database right.[75] The "verification of contents" and "stamp of approval" aspect of this judgment will be of interest to practitioners given that DLT provides a stamp of approval, in the form of the hash function and mining operation, for blocks to be added to the ledger. The court, if applying *William Hill,* may consider that the addition of information to a database, including where this merely reflects an existing database elsewhere, is sufficient for there to be sui generis right within the distributed ledger.

Database right in applications

The decision in *William Hill* will also be of interest to application providers who store information on-chain given that taking the contents of a database and re-arranging them can constitute infringement. It is arguable that, without permission, applications utilising the distributed ledger in order to store information on-chain will be infringing the database right that subsists (if any) in the underlying distributed ledger. This issue could be overcome through use of a broad licence between the app developer and the blockchain developer.

Copyright in the database

The Copyright, Designs and Patents Act 1988 (**CDPA**) defines a database as a collection of independent works, data or other materials which: i) are arranged in a systematic or methodical way; and ii) are individually accessible by electronic or other means.[76] Databases can therefore be protected

[72] Simon Stokes, *Digital Copyright Law and Practice* (5th Edition, Hart Publishing 2019) 87
[73] Case C-203/02 *British Horseracing Board Ltd v William Hill* [2005] RPC. 13, para 1
[74] *British Horseracing Board Ltd v William Hill Organisation Ltd* [2005] EWCA Civ 863
[75] Stokes (n 72) 89
[76] CDPA (n 66) s.3A

by copyright as literary works in addition to tables or compilations (which are not themselves databases).[77]

The test for originality is that "*by reason of the selection or arrangement of the contents of the database the database constitutes the author's own intellectual creation*".[78]

As a result, copyright can protect the structure and arrangement of the database if this is sufficiently original. It would no doubt be considered that a distributed ledger could meet the standards of originality, however, the question remains whether it constitutes the author's own intellectual creation given the distributed nature of DLT (which itself could raise questions of joint authorship).

It has been noted by Stokes that, given the originality threshold, a database in alphabetical order is unlikely to satisfy the requirements.[79] This is significant as distributed ledgers and blockchains are organised chronologically and although there is significant sophistication in relation to how blocks are added and cryptographically secured, the manner in which they are ordered is not manifestly original (or even changeable). Although in the case of the Ethereum chain it is possible, by paying more "gas money", to have a block hashed faster and therefore “jump the queue” for a block to be added to the chain, the chain remains organised in time and date order. In *Football Dataco Ltd v Brittens Pools Ltd* the Court of Appeal referred the question on whether copyright subsisted in that database to the CJEU.[80] The CJEU made clear that a database is only protected by copyright under the Directive "*provided that the selection or arrangement of the data which it contains amounts to an original expression of the creative freedom of its author*". On this basis, there is a basis for asserting that copyright cannot easily subsist in a distributed ledger as the threshold for original expression is more difficult to meet.

Whether the selection and arrangement of the data in a distributed ledger amounts to an original expression of the creative freedom of its authors will be a question for the court. In *Forensic Telecommunications Services Ltd v West Yorkshire Police & Anor* Arnold J noted that, “*the selection and arrangement of the data did not make [the database] [the author's] own intellectual creation*".[81] The Claimants in this case exercised no literary judgment, even in the widest sense of the word, and did not devise the form of expression of the work to any material extent and so copyright in the database did not exist. If literary judgment is required to show intellectual creation, then a likely question to arise will be whether mining or other validation techniques undertaken on a distributed ledger will constitute "judgment" in any form. Given the automated nature of these validation techniques, it is questionable whether these activities would be interpreted as demonstrating any literary judgement.

Confidential information

The use of DLT as a form of escrow whereby a smart contract releases information from escrow on the fulfilment of a set input is another viable application of DLT. A valuable use of this functionality, given the cryptographic security offered by DLT, is to store and release confidential information. This raises the question of whether confidential information or trade secrets can exist on a distributed ledger and remain confidential. Answering this question is determined by whether the necessary quality of confidence is preserved through cryptography that is secure by design.

Coco v AN Clark (Engineers) Ltd sets out the three-limb test for information that is protected under the common law of confidence.[82] The three limbs are: (i) the information itself must have the necessary

[77] Ibid s.3

[78] Ibid s.3A(2)

[79] Stokes (n 72) 83

[80] *Football Dataco Ltd v Brittens Pools Ltd* [2010] EWCA Civ 1380; and Case C-604/10 *Football Dataco Ltd v Yahoo! UK Ltd* [2013] F.S.R. 1 para 94

[81] *Forensic Telecommunications Services Ltd v West Yorkshire Police & Anor* [2011] EWHC 2892 (Ch) [94]

[82] *Coco v AN Clark (Engineers) Ltd* [1968] F.S.R. 415

quality of confidence; (ii) the information must have been imparted in circumstances importing an obligation of confidence; and (iii) there must be an unauthorised use of that information to the detriment of the rights holder.

The necessary quality of confidence

One key question is whether information can retain the necessary quality of confidence whilst accessible on a distributed ledger. Once determined on the facts, the relevance of storing information on a distributed ledger to the question of communication of confidential information will be easier to establish. If it becomes clear that information stored on-chain can have the necessary quality of confidence, then it may even become possible for information to be intentionally placed on a distributed ledger so as to import the obligation of confidence. Provision of access to on-chain information, i.e. by making private key information available, could also help to determine whether there has been unauthorised access to, or use of, the information.

The decision in *Saltman Engineering Co Ltd v Campbell Engineering Co Ltd* is instructive regarding the use of potentially confidential information which is made available to the public.[83] In *Saltman* it was held that in order to have the necessary quality of confidence, the information must not be public knowledge. By comparison, the statutory definition of a trade secret is: information which is secret and not generally known or readily accessible to those who normally deal with the information, has commercial value and has been subject to reasonable steps by the owner to keep it secret.[84]

Whether decryption from a blockchain or distributed ledger is considered similar to reverse engineering "special labours", and therefore a necessary step when intending to impute confidentiality, remains open to interpretation. If *Mars v Teknowledge* is followed, then it is possible that such decryption will not be considered “special labours”.[85] In *Mars* a company acting as agents for companies that supplied coin-operated machines took steps to reverse engineer the coin sorting mechanism, which included an encryption system. It was held that because "*anyone with the skills to decrypt has access to the information*" it would not be considered confidential. However, it has been more recently held that it is not a breach of confidence to decrypt such information unless the decryption or reverse-engineering would involve a significant amount of work.[86] It is likely that a significant amount of work will be needed to decrypt a distributed ledger, particularly when salted or peppered hashes are used, due to the security by design of these techniques and the scale and sophistication of the hack that would be required.[87]

Whilst reversing the encryption used on sophisticated blockchains and distributed ledgers is difficult, it is not impossible. It is worth noting that, in situations where the encrypted version of a distributed ledger is available to the public and is capable of being decrypted, the information stored on that ledger may not yet be considered confidential. Whether uploading information to a distributed ledger is sufficient to import a duty of confidentiality (without any further communication) cannot be answered definitively in the abstract and the outcome of disputes on this issue will, as ever, be fact-specific.

Patents

The patentability of the underlying DLT infrastructure and certain applications of DLT, such as smart contracts, is an issue that requires clarification given the potential value of such patents. Applications

[83] *Saltman Engineering Co v Campbell Engineering Co* [1948] 65 R.P.C. 203
[84] The Trade Secrets (Enforcement, etc.) Regulations 2018, SI 2018 No. 597 (implementing the European Trade Secrets Directive (2016/ 244/EU) [2016]), Regulation 2
[85] *Mars UK Ltd v Teknowledge Ltd* [1999] 6 WLUK 149
[86] *Kerry Ingredients (UK) Ltd v Bakkavor Group Ltd* [2016] EWHC 2448 (Ch)
[87] Salted hashes include additional (and unique) random data to a password before hashing and then storing a ‘salt value’ with the hash, making it harder for hackers to use pre-computation techniques to crack passwords. A pepper is a secret added to an input, such as a password prior it being hashed. A pepper differs from a salt because it is secret.

for patents in relation to DLT have been made and it remains to be seen whether these are capable of withstanding challenge.

Whilst the ownership of a blockchain/DLT-related patent would seemingly run counter to the decentralised ethos of the technology itself, and would hardly be considered a step towards *lex-cryptographica*, the commercial reality is that practitioners will need to consider the applicability of the patent regime to DLT, particularly in relation to smart contracts.

It is worth noting that software which has a "technical effect" so as to control a technical process, and that is otherwise novel and inventive, is capable of being patented.[88] A computer program that enabled a computer to run faster and more reliably has been held to be patentable.[89] Whether a smart contract (which is at its core a computer protocol) enabling a transaction to be completed faster and more reliably is similarly patentable remains undetermined at present.

Issues for further consideration

Some questions on DLT that require further consideration and would benefit from further guidance are set out briefly in the Key Recommendations at the beginning of the Guidance with greater detail and context provided below. The commentary on the IP implications of DLT in this section has focussed on the numerous potential applications of the technology and the scope for infringement. There is yet to be a significant debate on the copyright protection that could exist in DLT architecture, cryptoassets and even smart contracts. Issues regarding jurisdiction and exhaustion of IPRs may also arise and these are explored briefly below.

Copyright in DLT software

There are two sets of software in which copyright may subsist in a distributed ledger. The software for the back-end ledger itself and the software configuring the user facing application. Source code and object code will be protected provided they meet the various requirements to qualify for such protection, including originality. Practitioners should familiarise themselves with the scope of protection for software, given its applicability to the various unique characteristics of DLT.

Under the CDPA, computer programs and "preparatory design material for a computer program" are protected as separate categories of copyright work.[90] However, there is no set scope for the protection of the "computer program" itself. The Software Directive (2009/24/EC) sets out that protection in accordance with the Directive shall apply to the expression in any form of a computer program. Ideas and principles which underlie any element of a computer program, including those which underlie its interfaces, are not protected by copyright under the Directive.[91]

One issue that practitioners will want to consider is the protection of the functionality provided by the software (either back-end or user facing) as various distributed ledgers and blockchains may, from a functional perspective, perform in an almost identical manner.

This principle was considered in *Navitaire* in which Pumfrey J stated (when finding no copyright infringement): "*two completely different computer programs can produce an identical result: not a result identical at some level of abstraction, but identical at any level of abstraction… even if the author of one has no access at all to the other only its results*".[92] This comment was affirmed in *Nova* in which Jacob

[88] Stokes (n 72) 136
[89] *Symbian Ltd v Comptroller General of Patents, Designs and Trademarks* [2008] EWCA Civ 1066
[90] CDPA (n 66) ss 3(1)(b) and (c)
[91] Directive 2009/24/EC of the European Parliament and of the Council on the legal protection of computer programs (Software Directive) [2009] Section 1(2),as implemented by Copyright (Computer Programs) Regulations 1992, SI 1992/3233
[92] *Navitaire Inc v EasyJet Airline Co Ltd (No.3)* [2004] EWHC 1725 (Ch)

LJ stated: "*Pumfrey J was quite right to say that merely making a program which will emulate another but which in no way involves copying the program code or any of the program's graphics is legitimate*."[93]

The approach in *Navitaire* was followed in *Nova* and in *SAS Institute Inc v World Programming Ltd.* In response to the reference on *SAS Institute,* the ECJ held that the copyright available to computer programs under the Software Directive did not protect the functionality of a computer program, its programming language or the format of data files used.[94] In the judgment in the High Court in this case it was held that it was not an infringement of copyright in a computer program to replicate the functions without actually copying its source code or design.[95] These decisions are of note to DLT developers, because when developing the underlying software, even with a unique proof of work, copyright protection may well not be available to aspects of the DLT that are considered to amount to functionality.

Stokes has noted that it is not inconceivable for the court to find that there has been copyright infringement where the architecture or structure has been copied. Such decisions have partly based on literary copyright cases, such as *Baigent v The Random House Group Ltd*[96]*,* but also on the decision in *SAS Institute.*[97] In *SAS Institute,* Arnold J referred to the "design" of a program as well as its code as potentially benefitting from protection.[98] These are relevant to DLT developers because it may be that the consensus algorithm by which a network aims to achieve distributed consensus could benefit from copyright protection in the future.

Copyright in a Cryptoasset

Whether copyright should subsist in a cryptoasset is beyond the scope of this document. However, copyright can subsist within computer code and given that an electronic coin has been defined as "a chain of digital signatures",[99] a cryptoasset can perhaps be considered at its most simple as a set of computer code and so protectable under the copyright regime.

The level of originality required to qualify as a "work" and to trigger copyright protection is, as a rule, quite low.[100] As a result, it would not be a significant leap for the court to hold that copyright can subsist in the code identifying a cryptoasset. Whether this would be desirable is a separate question.

Copyright in a smart contract

A defining characteristic of a smart contract is its immutability. The value required to action the smart contract is input and as a result the digital asset is transferred. However, a "transfer" in the conventional sense of the word does not take place. The transaction involves the transferor modifying or generating new code in order to record the details of the transfer.[101]

This modification or generation of new code will most likely involve some form of direct or even indirect copying and so it is arguable (although untested) that, on the presumption that copyright subsists in the code for a cryptoasset, if the transfer of the cryptoasset is not authorised by the owner (which is unlikely) there may be copyright infringement. This could be a useful route to pursue for claimants given the potential unavailability of other remedies where parties agree to be bound by a transaction that is immutable, unless specific remedies are written into the code or applicable contract.

[93] *Nova Productions Ltd v Mazooma Games Ltd* [2007] EWCA Civ 219
[94] Case C-406/10 *SAS Institute Inc v World Programming Ltd* [2012] EU:C:2012:259
[95] *SAS Institute Inc v World Programming Ltd* [2013] EWHC 69 (Ch) [249]
[96] *Baigent v Random House Group Ltd* [2006] FSR 44; [2008] EMLR 7
[97] Stokes (n 72) 157
[98] *SAS Institute Inc v World Programming Ltd* [2010] EWHC 1829 (Ch) [251]-[261]
[99] Nakamoto (n 69)
[100] C-683/17, Opinion of Advocate General Szpunar [2019] EU:C:2019:363 para 57; C-604/10 *Football Dataco Ltd and Others v Yahoo! UK Ltd and Others* [2012], para 33
[101] UKJT Legal Statement (n 4) 44

Jurisdictional issues

Practitioners need to be cognisant of jurisdictional issues in DLT, which will be especially relevant to the infringement of intellectual property rights. Given the distributed and decentralised nature of DLT, and the different approaches to enforcement and infringement across jurisdictions, practitioners should consider the various access points for litigation. Whether a finding of infringement in one jurisdiction will be enforceable worldwide, for example where copies of the infringing work are stored on-chain in various jurisdictions, has not yet been tested in the context of DLT. Issues of jurisdiction in relation to DLT are explored in detail in Section 6 below.

Exhaustion

Once the above issues become more settled, practitioners will then need to consider the exhaustion of such rights. Questions will arise where a digital asset is sold on a blockchain (rather than a licensed digital copy), regarding the point at which any IPRs are exhausted. As the sale of cryptoassets is likely to become more common given the properties offered by blockchain (timestamping, immutability, tracing, etc.) it may be that current exhaustion regimes are not suitable for cryptoassets.

Conclusion

There are a number of interesting issues relating to intellectual property and DLT that would benefit from further guidance, decisions and commentary. In respect of copyright, it will be interesting to see how the court treats DLT and linked applications and whether existing case law relating to communicating to the public is sufficient for the court to come to conclusions. Guidance on the issues of “technical means”, “profit making” and what constitutes a “new public” in respect of DLT could enable developers to better understand the legal landscape in which they operate. Liability issues are likely to arise when considering various types of infringement, whether in relation to copyright, trade marks, or designs, and the various access points (i.e. core software developers, miners, application operators etc.) would benefit from a greater understanding of their potential exposure and liability. The issues surrounding database rights and confidentiality appear more likely to be determinable given the applicability of the available case law, however both regimes would benefit from greater certainty, which could in turn lead to wider adoption of the technology.

Whether DLT is treated as a novel technology or whether it will be treated in such a way so as to fit within the existing framework of intellectual property law (as has been found so far in respect of other legal issues) remains to be seen. So far, there have been very few calls for bespoke legislation in the UK (although in other European jurisdictions, such as Malta, the opposite is true). This section has endeavoured to show that such legislation is perhaps unnecessary. The existing intellectual property regime in the UK and Europe has sufficient scope to adapt to this new technology, as has been demonstrated with previous technological innovation

SECTION 6: DISPUTE RESOLUTION

Will Foulkes (Thrings LLP), Natasha Blycha and Charlie Morgan (Herbert Smith Freehills LLP) and Craig Orr QC (One Essex Court)

PART A: DLT and Litigation

Will Foulkes (Thrings LLP)

Introduction

This section of the guidance focuses on the relationship between DLT (including blockchain) and litigation, and will take an in-depth look into how the traditional legal landscape will need to adapt to the ever-evolving forms of technology that both lawyers and clients are now interacting with at an ever-increasing rate. This section will discuss the following:

- The changes to the traditional risk landscape for lawyers;
- Examples of DLT and litigation;
- The role that the judiciary and magistracy will play in DLT and fair trials;
- On-chain dispute mechanisms; and
- Availability and utility of off-chain dispute resolution mechanisms.

The changes to the traditional risk landscape for lawyers

As technology evolves, the need for lawyers to evolve with it increases. The traditional risk landscape (i.e. the way in which lawyers protect themselves against litigation) is evolving into something new that lawyers will need to be alive to.

As discussed in previous chapters, most often SLCs contain both natural language and code. This code can be further categorised as arising from two broad sources: i) the code that is drafted to create rights and obligations, and ii) the body of code that builds over time produced by the running of the SLC itself. A new issue that will impact disputes in using SLCs is that most lawyers do not know how to read or write code and, on the current state of the technology, machines do not read natural language well for purposes of executing that natural language. This language impasse is a potential source for disputes, as the four walls of the legal contract may be uncertain. For example, if a client would like to contract using smart contract functionality, the code would need to be created. The lawyers involved are unlikely to be able to create the code themselves or be able to proof-check the developed code for a client to make sure it is fit for purpose. Lawyers might then be reliant on developers and programmers to be able to correctly produce or read the executed run code.

What happens when something goes wrong, and the SLC is not fit for purpose or missing a key feature? Who is to blame in this situation? Are the lawyers liable for not checking that the code is correct, given that they have a duty of care to their clients, or is the developer liable? Or is this a non-issue that will be most easily solved by well drafted boilerplate provisions as to whether and to what extent code is considered “in or out” of the legal contract, combined with the development and use of sophisticated “no code” SLC drafting tools that automate a neat digital twin of a party's intended precedent automations.

Having said this, it is likely that in the short to medium term we will see increases in programmers in or working with legal teams to develop and proof-check code, particularly as the early tranches of SLC precedents are developed. It is believed by some that law firms will evolve following the model of the investment banks, with senior legal advisors supported by a team of developers.

Of course the least sensible way to mitigate this issue is for all lawyers to learn to code themselves. This is unlikely and impractical given the significant investment of time required to be a proficient coder and the improvement in the tools being developed that do not require it. This should not stop interested lawyers who would like to act as "multilingual specialists" learning to code so as to act as useful bridge people working between development teams and lawyers.

As this area of law continues to develop, so does the client. Traditional lawyer-client relationships are changing, especially in the wake of the Covid-19 pandemic. Lawyers have had to turn to technology-focused ways of connecting with their clients (such as Zoom or Skype). Along with the change in technology, clients' legal entities are evolving. The typical client entity of a human or physical business is now developing into computer programmes and DLT platforms (as with the DAO example given in Section 2). As a result, the way that lawyers interact with their clients is changing.

Examples of DLT and litigation

The following examples provide an insight into the current examples of DLT being used to help assist in the world of litigation:

- *Disclosure*

At present, disclosure between two parties can often be a long and complex task, and the current solutions on the market rely on specific key word searching to select documents and identify issues within the respective claims. DLT can assist in making the disclosure process quicker and more cost effective.

The relevant DLT platform would be coded to identify common and potential disputes, which allows for disclosure to be partially automated. A key function of the platform is that everything that is uploaded onto the platform is then encrypted. This key benefit will provide certainty to both parties, effectively guaranteeing that there is no tampering or removal of disclosure, as once information is saved onto the distributed ledger / blockchain, it cannot be removed. DLT platforms allow both parties to complete their disclosure requirements in a safe, encrypted way, and so minimising mistrust between the parties.

- *Digital signatures*

DLT can be used to assist in litigation through the use of digital signatures. As endorsed by the LawTech panel, the use of a signature can be met through the use of a private key (similar in concept to a pin number as mentioned below). As an overview, the DLT platform assigns a member of a distributed ledger / blockchain a public and private key. A public key is like a bank account number and the private key is akin to a pin number. Each time a member engages with the distributed ledger / blockchain (for example, to record a transaction) the private key of the member is used to generate a signature for each of its transactions which are encrypted (recorded) on the distributed ledger / blockchain.

As the member has unique access to the private key, it follows that this method is a secure way of imprinting a digital signature. Digital signatures using a private key will therefore assist in litigation in a variety of ways. Firstly, wet (physical) signatures can be subject to fraud which can cause further issues during litigious proceedings. A private key digital signature cannot be replicated by another individual (unless stolen), and therefore provides for almost 100% certainty in the form of a signature. This will greatly reduce arguments of fraud or false signatures during litigation proceedings.

Secondly, the use of digital signatures may also have an increased practical importance given the long-term impact of Covid-19 on business practices. When most lawyers no longer have access to printers or scanners, the use of a digital signature (in a private key sense) may dramatically improve efficiency in respect of signing documents and submitting them to the court. As already endorsed by the LawTech panel, the use of digital signatures using the private key should be implemented by lawyers in order to improve accuracy, improve efficiency and reduce the possibility of fraudulent behaviour.

The role that the judiciary and magistracy will play in DLT and fair trials

Her Majesty's Courts and Tribunals Service (**HMCTS**) announced a programme of technological reform in 2016 pursuant to which it has invested £1 billion to reform the court and tribunal system. HMCTS recognised that technological developments were needed within the legal system to avoid being left behind in the jurisdictional technological race.

Whilst there have been physical technological upgrades (such as iPads being used in courtrooms or online portals being used to submit forms) the crux of the issue remains: are judges able to sufficiently understand the technology itself (such as smart contract codes and blockchain)? If judges and magistrates are not able to understand the technology itself, the underlying question is whether there will be a fair outcome to any case brought before the courts.

Given the current guidance issued by the LawTech Panel surrounding these types of emerging technologies, it follows that some senior members of the judiciary have sufficiently in-depth knowledge and applicable common law guidance to enable them to preside over disputes in this area. However, the dilemma remains as to whether there is a sufficient pool of technologically literate members of the judiciary and magistracy to allow equality across the board.

One way to help eradicate this dilemma is to introduce court-appointed industry experts, much in the same way that legal advisors are present in traditional court rooms, to provide technical advice and guidance to the magistracy.[102] This will allow judges to ask technical questions to the court-appointed expert to help provide certainty and equality to all. Practically, it will be a much faster option to appoint individuals that are already established experts in their technological fields.

Another possibility to ensure fairness is for the UK to implement new procedural rules surrounding technology-related litigation. A key example of a country implementing new procedural rules surrounding technology is China. China's legal system has now set up new court procedure rules that require their "internet courts" (courts set up to manage cases relating to online matters) to recognise digital data as evidence if they are verified by methods including blockchain, timestamps and digital signatures. The new rules have been implemented immediately.

China's first "internet court" in Hangzhou has now handled over 10,000 internet-related disputes. These disputes range from lending and domain names to defamation. China's system for technology-related cases may set a trend for other countries (including the UK) to follow.

[102] The Brookings Institution's Artificial Intelligence and Emerging Technology Initiative, 'How To Improve Technical Expertise For Judges In AI-Related Litigation' (7 November 2019) <https://www.brookings.edu/research/how-to-improve-technical-expertise-for-judges-in-ai-related-litigation> Accessed April 2020

PART B: Options for On-chain Dispute Resolution

Natasha Blycha and Charlie Morgan (Herbert Smith Freehills LLP)

Introduction

The use of technologies such as DLT, smart contracts and Smart and Legal Contracts, raises new legal, procedural and practical questions about the way disputes arise and how they are best resolved in an increasingly digitised world.

Broad statements as to whether these technologies are good or bad, sound or reliable, are not terribly useful. A practitioner seeking to understand or advise on the creation or impact of these technologies – as either the subject matter of a dispute in a traditional forum, or as a resolution-facilitating technology (for example via current on-chain dispute resolution mechanisms) – should instead pay regard to the specific architectural features or design of the technology mix in question. Practitioners should also ensure up-front that parties are not speaking at cross purposes, given that the area of intersection between machines and law is rife with misunderstandings as to terminology.

With this in mind, we begin this section by setting out definitions of key concepts as used below. A widely accepted definition of a smart contract is some version of computer code that, upon the occurrence of a specified condition or conditions, runs on DLT. Alternatively, we use the term SLC to describe a legally binding, digital agreement in which part or all of the agreement is intended to execute as algorithmic instructions (where this execution often takes place on a DLT platform). An SLC then is the digitised form of the instrument that lawyers traditionally draft. Equating a Smart Contract *ipso facto* with a legally enforceable digitised contract because it contains the word “contract” is technically the same as suggesting that any software program could be called a contract.

While a common definition of DLT might reference a mechanism that supports shared, inter-generationally hashed data that is simultaneously located across multiple places using a consensus method, there is also much nuance as to how DLT is designed in practice, including in respect of:

- substantive differences in public and private infrastructures (see Section 1);

- distinct consensus protocols, methods of exchanging and retaining data, anonymity features, use of public and private keys (see Section 4); and

- single or multi-channel architectures that do, or do not allow for compliance with regulatory requirements such as those under the GDPR (see Section 4).

In this context, there are a growing number of new DLT-based dispute resolution offerings that have the stated aim of digitising the traditional dispute resolution process, but in fact appear to be technically geared to ingest smart contract code rather than complex digitised legal contracts.

These ‘on-chain’ dispute resolution offerings often purport to be a form of arbitration. However, the majority do not satisfy the requirements under domestic laws (e.g. for arbitrations seated in England & Wales, the Arbitration Act 1996) or international treaties (e.g. the New York Convention 1958) to result in a valid legal decision, enforceable against a recalcitrant party in the ‘off-chain’ world.

Many of the proponents of these ‘on-chain’ dispute resolution tools argue that validity in the eyes of the law is not what matters in the world of DLT, as long as the parties’ codified agreement enables enforcement as a matter of practice. While this argument may perhaps work in respect of some subset of non-binding smart contracts, this argument cannot hold for SLCs and is a misuse of the word ‘enforcement’ as currently understood in the legal context.

This section calls for authoritative guidance to be developed and published regarding best practice standards for digitised dispute resolution solutions (including on-chain elements where appropriate), where the gateway question for any development in this regard is the ability for a solution to be interoperable with both traditional systems and other digital legal infrastructures (including legislative and contractual digital infrastructures), the facilitation of the effective performance of SLCs (including automated arbitration or other dispute resolution clauses within those SLCs), access to justice, and the satisfaction of procedural and any other jurisdictionally based regulatory requirements.

Current availability of on-chain dispute resolution mechanisms

A number of companies have developed DLT-based dispute resolution systems seeking to respond to, and capitalise upon, users' appetite for speed, efficiency and automaticity in respect of what are essentially Smart Contracts. To date, these systems have not sought to solve on-chain disputes centred on SLCs, as SLCs themselves remain a reasonably nascent technology.

These DLT 'protocols', 'libraries' and 'platforms' have largely centred around the concept of online arbitration (although that term is often misused), crowd-sourced dispute resolution and AI-powered automated resolution of disputes (or a combination of these). These three types of proposed on-chain dispute resolution (**ODR**) procedures can be explained as follows:

- **Online 'arbitration'**: solutions that are modelled on arbitration and seek to incorporate arbitration procedures within the code of a smart contract. In general, these solutions seek to give parties an option to choose arbitration before disputes arise, and their awards are claimed to be legally binding and enforceable.

- **Crowdsourcing model**: crowdsourced dispute resolution allows anonymous users/nodes on the network to vote on "winners". Those users in the majority (who chose the right "winner") are rewarded.

- **AI-powered "Bots" resolve the dispute**: predictive analytics tools generate data-driven decisions that may be subsequently executed automatically on the DLT platform. AI tools are also being offered to help predict the outcome of disputes, which the parties can then use in driving settlement strategy.

The 'on-chain' decision is intended to be executed and enforced automatically. This means that, once a decision is issued, any applicable monetary compensation can be paid into a party's digital wallet directly (without the need for consent from a 'losing' party) or, for non-monetary awards, the relevant steps can be effected within the DLT ecosystem.

Examples of 'on-chain' dispute resolution tools include code libraries which seek to mirror the usual escalation steps of a traditional dispute resolution clause. For example, the encoded provisions agreed between the parties might include an automated breach monitoring and notification function, a command to freeze the automated operation of the code, and a mechanism by which decision makers are automatically informed of the dispute and requested to assist in its resolution. From that point onwards, the resolution of the dispute might follow largely familiar processes or seek to rely on more recent dispute resolution schemes based on game theory.

Some 'on-chain' dispute resolution offerings transfer funds from the parties' digital wallets to escrow until the dispute is resolved. Decision makers are in some instances appointed from a pool of anonymous users of the DLT network who deposit a financial stake (in cryptocurrency) in order to gain a right to vote on the outcome of the dispute. Those decision makers then cast a vote from a pre-determined list of binary outcomes and those who voted along with the majority receive compensation, while those who voted in the minority forfeit their stake. Again, the final decision may be automatically executed on the DLT network, and a payment triggered for the costs of the dispute resolution service.

A third style of 'on-chain' dispute resolution offering could be described as a digitised commercial arbitration process which is intended to render a valid and binding New York Convention award. Arbitration institutions and other bodies wishing to administer disputes could register on the DLT platform and enable users of the network to refer disputes via their smart contract or SLC for resolution under their pre-established procedural rules.

Scope, soundness & reliability of current on-chain mechanisms to resolve full range of potential disputes

In this section, we explore specific concerns arising following a review of numerous currently available on-chain dispute resolution mechanisms.

- In order for DLT-based tools to give parties the necessary certainty to carry on business in a decentralised world, they must be as legally robust as they are technologically sound. The decisions rendered on a DLT-based dispute resolution platform need to be valid, effective and final in the physical world as well as being enforceable as a matter of practice in the online world. If parties are able to challenge or otherwise undermine the outcome of that DLT-based dispute resolution process (and its outcome) in courts or before an arbitral tribunal by reference to a system of law, then the tool is likely to increase, rather than decrease, the time and costs associated with finally resolving disputes.

- If parties seek to treat their relationship as being shielded from the reach of the law, they run significant risks that, at any point, a party who is dissatisfied with an outcome may seek to obtain redress before traditional judicial authorities. In that instance, if the parties have failed to anticipate that possibility and, for example, failed to specify the applicable law of their agreement and the courts with supervisory authority over the dispute resolution process, very complex legal issues (e.g. conflicts of law) are likely to arise which could result in tactical satellite litigation around the world.

- In addition, parties need to have confidence in their decision makers. In existing DLT-based dispute resolution frameworks, the choice of arbitrators is limited to those entities who are nodes on the relevant network and/or have acquired relevant tokens. In the short term at least, this may reduce the calibre and number of potential arbitrators available (as technological expertise is needed in order to become eligible). In turn, this may lead to a high risk of repeat appointment that will arguably undermine arbitrators' independence and impartiality.

- In some system architectures, it may be difficult to identify with pseudonymity the legal personality of the entity operating a particular node (a human, a 'bot' or a DAO). If parties omit to specify the applicable law, very complex conflict of law issues are likely to arise. 'On-chain' arbitration may potentially limit how the courts with supervisory authority over arbitration can 'access' the arbitrators or parties in question.

- Real-world disputes also require tribunals to deal with the unexpected. As things stand, while 'on-chain' arbitration may be a viable solution for small, straightforward and predictable disputes, it is not clear how these current solutions can be applied to more complex, multi-jurisdictional and unexpected disputes that require careful consideration of detailed evidence.

- Next, in certain platforms, the amount of cryptocurrency that a node is willing to stake often determines the likelihood of that node being selected as a decision maker under existing DLT-based ODR tools. This creates certain risks of foul play, particularly in the context of volatile cryptocurrency markets. In addition, in the design of some systems, it is difficult to identify/obtain confidently who 'sits' behind the node, including whether they are, in fact, a human or a 'bot'. Again, this presents legal and practical challenges both for the widespread adoption of these tools and the legal validity of their outcome.

- Another important consideration in some platforms reviewed is enforcement. Specifically, how to ensure that, once a decision has been rendered, the winning party is able to obtain from the other party the relief that was ordered against them. Again, 'automaticity' is appealing here (i.e. the ability for a decision to be enforced automatically, without the need for the 'losing' party's consent). Automatic enforcement could do away with the cost and lengthy delays associated with enforcement proceedings that are often required following receipt of an award or judgment. However, this potential shift in the role of a decision maker (be it characterised as an expert, arbitrator or judge) to implement directly the terms of their decision marks a shift from traditional practices and presents further legal and practical obstacles.

- Depending on the seat of arbitration, there is likely to be a minimum mandatory period during which the award is susceptible to challenge. Beyond that time, however, a court can generally still permit a challenge if deemed necessary. The ability to challenge an arbitral decision in this way may create a further obstacle for on-chain automatic enforcement, because any automatic enforcement could ultimately need to be reversed. In one way, this is no different to the existing position. However, the practical realities are quite different; in practice, enforcement proceedings take many months. The real benefit of automated execution is to avoid that process.

Digitised elements in disputes – what comes next?

Current on-chain dispute resolution platforms raise many substantive legal questions and do not appear to have the ability to resolve the full range of potential disputes arising from the use of SLCs, but may be used for technical or commercial agreed outcomes where legal veracity or enforcement is not in issue.

Certainty and consistency of outcome are needed for parties to be able to avoid and resolve disputes amicably. Going forward, it is likely that this will be achieved through traditional processes and also through the increasing use of future forms of best practice DLT (or other digital platform) mechanisms, combined with SLC data.

Notwithstanding the current limitations of available (DLT) solutions, the creation of and need for new platforms that facilitate the ingestion, digestion, arbitration and publication (and where appropriate enforcement) of both analogue and coded dispute-relevant data (particularly that generated by SLC use) is inevitable.

Best practice methods that seek to generate new efficiencies and machine-led legal insights, whilst still incorporating technical features that support cyber security, data rights, trusted and shared source(s) or ledgers of digital truth between parties (particularly in respect of past conduct), interoperability between platforms and products, as well as access to specialist digitally trained human resources when needed, are just some of the features required for new methods of digitised dispute resolution to be adoptable and enforceable in the future.

A combination of authoritative guidance and best practice standards will expedite those efficiencies and insights without the significant downsides and limitations associated with current on-chain dispute resolution mechanisms.

PART C: Availability and utility of off-chain dispute resolution mechanisms

Craig Orr QC (One Essex Court)

Introduction

This section addresses three issues that are of fundamental importance to the efficient and effective governance of any DLT system,[103] namely:

- **Jurisdiction**: where and how should disputes arising out of the system or its operation be resolved?

- **Applicable law**: which law (or laws) should be used to determine the legal rights and obligations of the system participants?

- **Money laundering**: to what extent are system participants subject to AML and anti-terrorist financing laws and regulations?

Whilst early progenitors of blockchain technology aimed at creating self-governing and state-remote networks, as epitomised by Bitcoin, experience has demonstrated the need for cryptoassets and other DLT applications to operate within traditional legal and regulatory frameworks. Hacks of cryptoasset exchanges have demonstrated the vulnerability of intermediaries providing an interface between virtual blockchain systems and the real world[104] - The DAO hack in June 2016 demonstrated the potential for smart contracts not to function as envisaged[105] - and increasing use of DLT in financial services has stoked demand for clarity and certainty about the legal status of cryptoassets, the binding nature of smart contracts and the finality of transfers and dispositions of digital assets held within DLT systems.[106] In addition, the illicit use of cryptocurrencies to facilitate money-laundering, cyber crimes and token fraud has compelled regulators to bring cryptoassets within the scope of AML and other financial and securities regulations.[107]

A vision of DLT systems operating in an entirely self-automated manner untouched by traditional law and regulation is therefore not feasible.

Jurisdiction & applicable law

Notwithstanding the automaticity of smart contracts and the disintermediated nature of DLT systems, there remains considerable scope for disputes. These may arise between participants in the system or between participants and third parties. For example:

- Coding errors or bugs may cause a smart contract to perform in an unintended way;

[103] A term used to describe any network or application using distributed ledger technology, whether private / public or permissioned / permissionless.
[104] For example, the hack of Coincheck in 2018 resulting in loss of cryptoassets with a reported value of more than $500 million.
[105] As explained by De Filippi and Wright (n 47) 200 – The DAO hack exploited vulnerability in the computer code. The DAO's smart contract failed to reflect the actual intentions of the contracting parties; because it contained a flaw, an attacker managed to drain over $50 million worth of ether in a way that other members of The Dao did not anticipate or intend.
[106] See e.g. UKJT Legal statement (n 4); and The Financial Markets Law Committee (**FMLC**) report on *Distributed Ledger Technology and Governing Law: Issues of Legal Uncertainty* (March 2018) <http://fmlc.org/wp-content/uploads/2018/05/dlt_paper.pdf>; and ISDA / Linklaters, *Smart Contracts and Distributed Ledger – A Legal Perspective* (August 2017) <https://www.linklaters.com/en/about-us/news-and-deals/news/2017/smart-contracts-and-distributed-ledger--a-legal-perspective>; and ISDA / Clifford Chance, *Private International Law Aspects of Smart Derivatives Contracts Utilising Distributed Ledger Technology* (January 2020) <https://www.cliffordchance.com/briefings/2020/01/private-international-law-aspects-of-smart-derivatives-contracts-utilizing-dlt.html> Accessed 24 May 2020
[107] This is an ongoing process: see e.g. the SEC's assertion of jurisdiction over ICOs on the ground that they constitute securities; the New York State regulation on Virtual Currencies (Title 23 Chapter I Part 200); Bermuda's Digital Asset Business Act; Malta's Virtual Financial Assets Act and the AML measures taken by UK and EU regulators discussed below.

- There may be discrepancies between coding and natural language versions of an SLC;
- A party to an SLC may want to terminate the contract, or otherwise reverse a transaction, on grounds of misrepresentation, mistake or duress;
- Subsequent changes of law or regulation (e.g. sanctions) may make performance of an SLC illegal;
- The administrator of a permissioned system may fail to perform its role (for example, by allowing new participants onto the system who do not meet the entry requirements);
- Intermediaries providing the interface between a DLT system and real world users may fail to perform their role (for example, wallet providers may fail to keep digital keys secure); and/or
- An outside party may assert a proprietary interest over digital assets held within a DLT system, for example by way of attachment or enforcement of security rights.

There clearly is scope for resolving some disputes between participants of a DLT system by encoded on-chain dispute resolution mechanisms. However, such mechanisms could not resolve disputes involving parties outside the network. It is also unlikely that on-chain dispute resolution mechanisms will displace altogether traditional off-chain dispute resolution mechanisms. It is virtually impossible to define in advance all possible ways that a particular set of rules should apply in any given situation. Indeed, the flexibility of natural language is one of its strengths in enabling written rules in a contract or other instrument to accommodate unforeseen or unexpected events.[108]

Given the pseudonymous and decentralised nature of DLT systems, potentially involving participants located in numerous jurisdictions, ascertaining which forum and law should determine disputes arising out of the operation of such systems is a matter of fundamental importance. Unless the applicable forum and law are agreed in advance by participants, they will be determined by the courts of jurisdictions seized of disputes with unpredictable and possibly unexpected and unwelcome outcomes.

Permissioned DLT systems

In a permissioned DLT system, the business or entity that establishes the system has the ability to prescribe contractual rules governing the basis on which parties shall participate in the system, including the forum in which, and law by which, disputes between participants are to be resolved. Such rules are best viewed as a form of constitution, akin to the rules of an unincorporated association under English law.[109] They should be drafted so as to make clear that they create binding legal relationships not only between each individual user (or node) on the system and the relevant administrator or operating authority (**R(O)A**),[110] but also as between the users *inter se*.

There is no difficulty in characterising the relationships between participants in a permissioned DLT system as contractual, equivalent to the relationships between members of an unincorporated association. As the UKJT noted in its *Legal statement on cryptoassets and smart contracts*, the same analysis may be applied to a DAO, which "*maps well on to the well-established concept of an unincorporated association, whereby the association itself has no legal status, but all of the members, because of their membership, are bound by the rules*": a party who transacts with a DAO "*can be taken*

[108] As noted by the ISDA / Linklaters paper (n 106) 12: "*This is perhaps the most fundamental challenge a lawyer might pose to a computer scientist regarding the merits of smart legal contracts*"; see also De Filippi (n 47) 200-201.
[109] As Brightman J said in *Re Recher's Will Trusts* [1972] Ch. 526, at 538, "*the rights and liabilities of the rules of the association will inevitably depend on some form of contract inter se, usually evidenced by a set of rules*". See further *Chitty on Contracts*, 33edn, Vol 1, para 2-118.
[110] A term adopted by the FMLC in its report (n 106) para 6.16.

to have agreed to abide by and be legally bound by its terms".[111] A similar effect can be achieved by the use of master or framework agreements, as are typically used in DLT trading and settlement systems.[112]

Choosing the appropriate forum and law to govern disputes between participants in a DLT system requires careful consideration.

Applicable forum

As regards the forum, the main points to consider are:

- Whether disputes should be referred to arbitration or the national courts of a state (and if so, which state);

- If disputes are to be referred to arbitration, the type of arbitration (ad hoc or under institutional rules), the composition of the tribunal and the seat of the arbitration; and

- Whether some form of alternative dispute resolution, such as mediation or expert determination, should be built into the dispute resolution process (possibly as a pre-condition of proceeding to arbitration or litigation).

Arbitration has several features that make it attractive as a dispute resolution process for DLT applications. Specifically:

- **Enforceability of arbitration agreements**: arbitration agreements are widely enforced under national laws and as a matter of treaty obligation pursuant to the Convention on the Recognition and Enforcement of Foreign Arbitral Awards 1958 (the **New York Convention**), which requires all contracting states to recognise written arbitration agreements.[113] A choice of arbitration as the forum to resolve participants' disputes is therefore unlikely to be overturned by a national court.

- **Enforceability of arbitral awards**: arbitral awards are generally easier to enforce on a transnational basis than judgments of a national court. Judgments of courts in EU states are enforceable throughout the EU, and some other multi-jurisdiction judgment regimes exist, but none are comparable to the wide-ranging effect of the New York Convention, which obliges all contracting states to recognise and enforce arbitral awards (subject only to limited and generally non-substantive exceptions, including that the arbitration agreement is in writing).

- **Expertise of decision makers**: arbitration offers parties the ability to select arbitrators with appropriate expertise (for example, arbitrators with an understanding of coding for a dispute about the working of a smart contract). Several arbitral organisations offer assistance with identifying arbitrators with expertise suited to particular disputes.[114] Specialist pools of arbitrators with relevant experience of DLT disputes are likely to develop over time.

- **Flexibility**: arbitration offers parties the potential to agree bespoke procedures for resolution of their dispute and enforcement of an award. Parties may, for example, agree to give an arbitral tribunal powers to insert remedial transactions into a blockchain or automatically appropriate collateral or other assets held on the blockchain in satisfaction of an award.

[111] UKJT Legal statement (n 4) para 148

[112] For example, the DLT derivative trading platforms considered in the ISDA / Clifford Chance paper (n 106)

[113] The New York Convention has been adopted by 163 states, making it one of the foundational instruments of international arbitration.

[114] Examples include the World Intellectual Property Organisation (WIPO) and the International Centre for Dispute Resolution (ICDR).

- **Finality**: with only limited exceptions pursuant to some national laws, arbitral awards generally cannot be appealed on their merits, whereas court judgments can typically be appealed, sometimes to multiple layers of appellate court.

- **Neutrality**: arbitration provides a neutral forum, not tied to any particular state, thereby avoiding problems of actual or perceived bias by national courts in favour of their own nationals.

- **Greater confidentiality**: arbitration proceedings are generally private (in the sense of not taking place in a public forum) and can usually be made more confidential by party agreement. This may be more consonant with the pseudonymous nature of many DLT systems than litigation, which typically involves public hearings.

However, arbitration is not without disadvantages, which should be recognised when considering which dispute resolution mechanism to adopt. In a DLT context, the main disadvantages include:

- **Scope for delay**: since arbitrators' powers of coercion are more limited than those of national courts, there may be greater scope for recalcitrant defendants to delay arbitration proceedings than is the case in litigation in national courts. Arbitrators may also be reluctant to sanction obstructive parties for fear of an award subsequently being challenged on due process grounds.

- **Limited powers over non-parties**: unlike national courts, arbitrators only have jurisdiction over parties to the arbitration agreement pursuant to which the arbitral tribunal is constituted. In the absence of the parties' agreement, arbitrators do not have the power to join third parties or consolidate other proceedings to the proceedings before them.[115] This could be a serious impediment in the context of disputes concerning a DLT system with multiple participants, each of whom might be affected by the outcome of a dispute between two or more participants. Proceedings could also become bifurcated if action needs to be brought against third parties outside of the system, for example to follow misappropriated digital assets. National court proceedings can accommodate the joinder of claims against additional parties, thereby avoiding bifurcation of disputes and the consequent risk of inconsistent findings by different adjudicators.

- **Limited powers to grant interim remedies**: unlike arbitrators, national courts generally have extensive powers to grant interim injunctions and orders for disclosure of information in support of legal proceedings. Some national laws, including the English Arbitration Act 1996, provide for national courts to grant equivalent remedies in support of arbitration proceedings, but these powers generally (i) do not extend to the grant of such remedies against third parties who are not bound by the relevant arbitration agreement; and (ii) require the prior consent of the arbitral tribunal or parties (except in urgent cases).[116] This can impede the tracing of misappropriated digital assets, especially given the speed with which such assets can be transferred.

- **Lack of precedent**: unlike court judgments, arbitral awards are not ordinarily reported and have no precedential status in other arbitrations. This requires each tribunal effectively to re-invent the wheel and deprives them of the benefit of decisions in preceding cases. This is potentially problematic in a developing area of law, where it makes sense for adjudicators to

[115] Some institutional arbitration rules now provide for arbitrators to join additional parties or consolidate two or more sets of arbitral proceedings. However, complications arise with the selection of arbitrators for consolidated sets of arbitral proceedings and third parties can only be joined where they agree to become subject to the arbitration before the tribunal.

[116] See e.g. s.44 of the Arbitration Act 1996; and *Cruz City 1 Mauritius Holdings v Unitech Ltd* [2014] EWHC 3704 (Comm) [46]–[51], confirming that s. 44 does not allow relief to be granted against a non-party to the arbitration agreement.

have access to decisions in previous cases. This could be remedied by arbitration agreements providing for publication of awards, possibly in anonymised form (as is permitted under ICSID arbitration rules). However, to be effective, this would need to happen on a market-wide basis.

If arbitration is chosen as the dispute resolution mechanism for a DLT application, the following (among other) points should be addressed in the arbitration agreement:

- **Writing**: it is unclear whether an encoded arbitration agreement would qualify as an agreement 'in writing' for the purposes of the New York Convention. There is considerable force in the UKJT's argument that computer code which can (i) be said to be representing or reproducing words and (ii) be made visible on a screen or printout, constitutes 'writing' as a matter of English law.[117] However, there is no established precedent to this effect and the conclusion that might be reached by courts in other countries is uncertain. It is therefore prudent to record an arbitration agreement for a DLT application in traditional written form, irrespective of whether the agreement is also reflected in code in an SLC. Otherwise there is a risk of the arbitration agreement, and any arbitral award, being denied recognition and/or enforcement.

- **Seat**: the parties should specify the seat of the arbitration, whose law will normally constitute the procedural law of the arbitration and will determine the degree of oversight and intervention by national courts in the arbitral process. In the absence of an express choice of seat, there is a risk of satellite disputes about the applicable seat and/or procedural law. Parties should choose as the seat a state that is party to the New York Convention and whose law (i) recognises (or is likely to recognise) the legality and enforceability of SLCs and (ii) limits the scope for intervention by national courts in arbitration proceedings.

- **Type of arbitration/composition of the tribunal**: parties should decide whether to adopt a set of institutional arbitral rules or devise their own arbitral procedure. They should also set out any expert or other qualifications to be required of arbitrators, bearing in mind that any limitations imposed on the choice of arbitrators will restrict the pool of potential appointees.

- **Multiple parties/joinder**: given the scope for disputes to affect all participants on a DLT system (for example, if remedial transactions are required to be created on the distributed ledger to implement an award), it is important to ensure that the arbitration agreement binds all participants or at least provides for the joinder of other participants if that is required for effective resolution of a dispute.

- **Enforcement of remedies**: consideration should be given to providing in the arbitration agreement for awards to be binding on all other participants in the system, so as to avoid the risk of conflicting decisions being rendered on common issues in different disputes (which could have a destabilising impact on the system as a whole).[118] The parties may also agree to provide arbitrators with the power automatically to enforce awards, possibly by giving binding directions to the R(O)A to appropriate collateral held within the system or to create remedial transactions on the distributed ledger.

[117] UKJT Legal Statement (n 4) para 164

[118] Similar issues have arisen in the context of commodity arbitrations involving string contracts on materially back-to-back terms. In *Stockman Interhold SA v Arricano Real Estate* [2015] EWHC 2979 (Comm), the parties to an LCIA arbitration agreed to be bound by the result in a separate UNCITRAL arbitration. Although the parties were the same in both sets of arbitral proceedings, there is no reason why the like result could not be achieved where there is not complete overlap between the parties in both sets of proceedings.

- **Confidentiality**: if confidentiality is important, the parties should expressly agree that they will keep the arbitration, together with all materials created and all documents produced in the proceedings confidential, except to the extent required for enforcement of an award.

Litigation

If litigation is chosen over arbitration, it will be important to choose the courts of a state whose law recognises (or is likely to recognise) the status of digital assets held on a DLT system and the legality and enforceability of SLCs. The following further points should also be considered:

- **Enforceability of choice of court agreements**: choice of court agreements will generally be enforced by national courts, subject in some cases to an overriding discretion not to do so where justice otherwise requires. Within the EU, member states are obliged by Article 25 of Regulation 1215/2012[119] (the **Recast Brussels Regulation**) to give effect to agreements conferring jurisdiction on the courts of a member state. States that are party to the Hague Convention on Choice of Court Agreements are similarly obliged to give effect to exclusive choice of court agreements. Whilst these regimes probably apply to agreements wholly or partly in coded form,[120] any choice of court agreement should be reduced to writing, in traditional form, to minimise the scope for dispute about the agreement's existence and enforceability.

- **The quality of the judiciary, and lawyers, in the selected state**: courts in a number of jurisdictions, including England, have shown themselves willing to embrace the resolution of disputes concerning innovative technology.[121] The Business and Property Courts in England are well-placed for this purpose. They (and other specialist courts in England) have considerable experience of dealing with cases raising complex technical issues with international elements, often involving consideration of foreign laws. Other jurisdictions that have shown willingness to engage constructively with distributed ledger technology include Singapore and Switzerland.

- **The suitability of procedural rules in the selected state**: for example, the well-developed summary judgment procedures utilised by the Business and Property Courts in England could be useful to ensure that unmeritorious claims or defences did not impede the proper functioning of DLT systems by unnecessarily interrupting the flow of transactions on the system.

Applicable law

Irrespective of whether they choose arbitration or litigation, the parties should agree upon the applicable law to govern their disputes. This law should be specified as applying to all disputes, whether arising in contract or otherwise.

[119] Council regulation (EU) 1215/2013 of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters [2012] OJ L 351/1.

[120] Article 25 of the Recast Brussels Regulation applies to agreements (a) in writing or evidenced in writing; (b) in a form which accords with practices which the parties have established between themselves; or (c) in international trade or commerce, in a form which accords with a usage of which the parties are or ought to have been aware and which in such trade or commerce is widely known to, and regularly observed by, parties to contracts of the type involved in the particular trade or commerce concerned. The Hague Convention applies (by Article 3(c)), to agreements concluded or documented in writing or by any other means of communication which renders information accessible so as to be usable for subsequent reference. Both provisions probably encompass jurisdiction agreements recorded in a smart contract on a DLT system.

[121] See e.g. the hope expressed by Sir Geoffrey Vos, the Chancellor of the High Court, that the UKJT Legal Statement "*will demonstrate the ability of the common law in general, and English law in particular, to respond consistently and flexibly to new commercial mechanisms*" (as stated in its foreword). Since publication of the UKJT Legal Statement, the English court has adopted its reasoning to find that cryptoassets constitute 'property' and hence can be the subject of proprietary claims and remedies: see *AA v Persons Unknown* [2019] EWHC 3556 (Comm).

An express choice of law will ordinarily be enforced by national courts. Parties are in general free to choose the law to govern their contract, irrespective of whether the chosen law has any apparent connection to the parties or their contract.[122] However, under Regulation 593/2008 on the law applicable to contractual obligations[123] (the **Rome I Regulation**),[124] the parties' freedom of choice is limited in the following respects:

- Where all other elements relevant to the situation at the time of the parties' choice are located in a country other than the country whose law has been chosen, then the choice of law cannot prejudice the application of mandatory laws of that other country (Art. 3(3)). This provision is unlikely to apply in the case of a DLT system, which by its nature is likely to have elements located in multiple jurisdictions.[125]

- Where all other elements relevant to the situation at the time of the parties' choice are located in one or more member states to the Rome I Regulation, then the choice of law cannot prejudice the application of mandatory provisions of EU law (Art. 3(4)). Whilst it is possible to conceive of a DLT system located and operating only within EU member states, this provision is unlikely to affect application of a chosen law once the UK has completed its withdrawal from the EU.

- Overriding mandatory provisions of the forum must be given effect (Art. 9(2)). These are defined as "*provisions the respect for which is regarded as crucial by a country for safeguarding its public interests, such as its political, social or economic organisation, to such an extent that they are applicable to any situation falling within their scope, irrespective of the law otherwise applicable to the contract*" (Art. 9(1)). As noted by Briggs, the purpose of this definition is to "*encourage a court to keep to a minimum the occasions on which a provision of the lex fori intervenes to displace pro tanto a provision of the applicable law*".[126] It is nevertheless possible that Art. 9(2) might, for example, prevent parties evading application of investor protection laws that would otherwise apply to the issue or sale of virtual tokens by choosing a different law without such protections.

- Effect may be given to overriding mandatory provisions of the law of the country where the obligations arising out of the contract have to be or have been performed, if those provisions render the performance of the contract unlawful (Art. 9(3)). Given the distributed nature of a DLT system, it will generally be difficult to identify particular countries that could be said to be the "place of performance" of obligations owed by participants (with the possible exception of the R(O)A, whose obligations might arguably fall to be performed in the place where it is domiciled or the computer servers running the platform are located).

- Article 6(2) of the Rome I Regulation provides that a choice of law made by the parties does not have the result of depriving a consumer of the protection of mandatory provisions under the law of the consumer's habitual residence. This could affect application of a chosen law in the case of DLT applications offering digital services to consumers.[127]

[122] Dicey, Morris & Collins, *The Conflict of Laws*, (15th edn, Sweet & Maxwell, 2018) 32-040 *et seq*.

[123] Council regulation (EC) 593/2008 of 17 June 2008 on the law applicable to contractual obligations (Rome I) [2008] OJ L177/6

[124] It is possible that these rules may be amended following Brexit, but the UK Government's current position is that the Rome I Regulation, as well as the Rome II Regulation (which deals with the law applicable to non-contractual obligations), will be incorporated into UK law following the end of the transition period.

[125] As noted by Adrian Briggs, *Private International Law in English Courts* (OUP, 2014) at para 7.117, "*in practice, and particularly in commercial litigation before the English courts, [Art. 3(3)] is only very rarely liable to arise for consideration*".

[126] Ibid, para 7.245.

[127] Article 8(1) of the Rome I Regulation provides that a choice of law made by the parties does not have the result of depriving an employee of the protection of mandatory provisions of the law which would be applicable in the absence of a choice of law. This provision seems unlikely to apply to commercial use of a permissioned DLT system.

None of the above limitations invalidates a choice of applicable law; they only displace that law to the extent that specified mandatory provisions might apply. They certainly do not negate the benefits of the certainty that is achieved for parties by choosing the law to govern resolution of their disputes.

Parties should ensure that the chosen law recognises (or is likely to recognise) the legality and enforceability of SLCs. English law is a good candidate, given the conclusion reached by the UKJT that smart contracts are capable of giving rise to binding legal obligations and can be analysed according to "*entirely conventional*" legal principles.[128] The work of the UKJT has already been endorsed by the English court, which found its analysis of the proprietary nature of cryptoassets to be "*an accurate statement as to the position under English law*".[129] There is a real prospect that the English courts will also endorse the UKJT's analysis of smart contracts.

Permissionless DLT systems

A permissionless DLT system requires different analysis. The participants in such systems are unlikely to have expressly assigned the application of any particular law to resolution of their disputes, in which case the applicable law will fall to be determined by the application of relevant conflict of law rules by the national courts seized of a dispute.

An English court would apply the rules of the Rome I and Rome II Regulations to ascertain the applicable law. Analysing how these provisions apply to permissionless DLT systems is not straightforward, and surprising conclusions might be reached.

As noted by Professor Dickinson in *Cryptocurrencies in Public and Private Law*, it is possible to characterise the relationships between participants in a permissionless system (such as Bitcoin) as contractual, even in the absence of any express assent by the participants to a governing set of rules, on the ground that all participants have subscribed to a joint enterprise, governed by a set of consensus rules, by joining the network. The applicable law would arguably then fall to be determined by the final (default) rule in Art. 4(4) of the Rome I Regulation, pursuant to which the applicable law comprises "*the law of the country with which [the contract] is most closely connected*". In a cryptocurrency system such as Bitcoin, the activities of miners can (without undue artificiality) be described as "*central to, and characteristic of, the operation of the cryptocurrency system*"; in which case it is possible that an English court would find that the law of China, the place where the majority of Bitcoin mining activity is reportedly centred, is the law applicable to relationships between participants.[130]

Property aspects

The above addresses issues of applicable law as between system participants. However, digital assets held on a DLT system are a species of property.[131] It is therefore necessary also to consider the proprietary aspects of holding, owning and transferring such assets, which affect not only system participants but also those outside the system. As noted by the UKJT, "*proprietary rights are recognised against the whole world, whereas other – personal – rights are recognised only against someone who has assumed a relevant legal duty*".[132]

Proprietary rights affect matters such as the finality of transfers of digitally held assets in a DLT system, perfection of security over such assets, priority as between successive transferees, effectiveness of attachments by judgment creditors and the consequences of insolvency of a system participant.

[128] UKJT Legal Statement (n 4) paras 136-148

[129] *AA v Persons Unknown* [2019] EWHC 3556 (Comm) [57] and [59] (Bryan J)

[130] Andrew Dickinson, 'Cryptocurrencies and the Conflict of Laws' in David Fox and Sarah Green, *Cryptocurrencies in Public and Private Law* (OUP, 2019) paras 5.55, 5.62-5.63 and 5.72.

[131] As noted by the UKJT in its Legal Statement (n 4) paras 15 and 86, and confirmed by Bryan J in *AA v Persons Unknown* (n 129) [61]

[132] UKJT Legal Statement (n 4) para 36

Ascertaining the law governing these issues is extremely difficult. This stems in part from the *sui generis* nature of virtual assets held on a DLT system and in part from the multiplicity of choice of law rules that might be applied to dispositions of such assets.

The common law traditionally determined the choice of law applicable to property issues by reference to the place in which the property was situated or could be claimed (*lex situs*), on the ground that this was an objective and easily ascertainable connecting factor and the courts of the *situs* had control over the property and could therefore effectively enforce judgments concerning the property.[133] A similar approach was adopted for certain intangible assets (such as shares and dematerialised securities) by ascribing to them an artificial *situs*, usually in the place where some form of control could be exercised over the asset. In the case of shares and securities, this was generally taken to be the location of the register or account in which transfer and ownership of the shares or securities was recorded.[134] However, other approaches have also been taken, for example applying the law governing the contract between assignor and assignee in the case of assignment of choses in action.[135]

A *situs* approach does not make sense in the case of an asset that is held only in virtual form on a disintermediated and distributed ledger.[136] As noted by the UKJT, there is "*very little reason to try to allocate a location to an asset which is specifically designed to have none because it is wholly decentralised*".[137] Another solution must therefore be found. Several have been suggested.

The Financial Markets Law Committee (**FMLC**) has advocated adoption of an 'elective' *situs*, whereby the proprietary effects of transactions on a DLT system should be governed by "*the system of law chosen by the network for the DLT system*".[138] On this basis, participants would be able contractually to choose the law governing all issues arising out of the disposition of assets on the system, including the proprietary effects of such dispositions on third parties. In order to ensure that an inappropriate law was not selected, such as one that was "*subject to significant undue external or private influence*" and could be used to facilitate an enforced "*mass transfer of assets in the system*", the parties' choice of law might be made subject to regulatory approval or a substantive connection might be required between the DLT enterprise and any chosen law.[139] Whilst not free of difficulty, this approach would be transparent and enable the proprietary effects of all transactions on the system to be subject to the same governing law.

Other possibilities considered, but not preferred, by the FMLC include:

- the law of the place where the R(O)A was located;
- the law of the place of primary residence of the encryption master keyholder; and
- the law of the place where the system participant who is transferring or otherwise disposing of the assets is resident, has its centre of main interest or is domiciled.

All but the last of the above options can only be used for permissioned DLT systems which have some form of centralised or intermediated control. For this and other reasons, the last option is supported by Professor Dickinson, who argues that it represents an "*incremental development of the common law's*

[133] As explained by Dicey, Morris & Collins (n 122) para 22-025.
[134] Under regulation 23 of the Financial Markets and Insolvency (Settlement Finality) Regulations 1999, where a register, account or centralised deposit system within which securities are recorded is located in a European Economic Area (EEA) state, the rights of the holders of these securities will be governed by the law of the EEA state where the register, account or centralised deposit system is located.
[135] As in Art. 14(1) of the Rome I Regulation.
[136] An exception might be DLT systems that are used to record ownership or transfer of movable tangible assets: in such a case, where arrangements on the distributed ledger reflect title in 'real' things, proprietary questions will likely be governed by traditional conflicts of laws rules that apply to the corresponding real assets: see FMLC report (n 106) para 6.3.
[137] UKJT Legal Statement (n 4) para 97.
[138] FMLC report (n 106) paras 6.5 and 7.1-7.4.
[139] Ibid para 6.9.

lex situs approach", is relatively predictable and easy to apply and aligns with the rules that apply in the case of insolvency (which only permit main insolvency proceedings to be brought in the EU member state in which the debtor has his centre of main interests).[140] This approach, however, would fragment the distributed ledger record, leading to application of different laws to transactions involving different participants, and would be difficult to apply in the case of joint transferors and chains of transactions.[141]

Given the intractable difficulty of this problem, it can only be solved by legislation; and to be effective, any solution will have to be adopted on a transnational basis, as both the UKJT and FMLC recognise.[142] The need for such international co-operation and co-ordination is clear and compelling. Otherwise uncertainty about the law governing the proprietary effects of the transfer and disposition of digital assets held on DLT systems will undermine trust and confidence in these systems and impede their adoption in the financial services industry and other sectors.

Money Laundering

The problem identified

Regulators have become increasingly concerned about the illicit use of cryptocurrencies. Their decentralised, disintermediated and pseudonymous nature makes them ideal vehicles for money-laundering, terrorist financing and other criminal activities, including ransomware attacks, ICO token frauds and transactions on the darkweb.[143] The scale of such criminal activity is difficult to quantify but it is clearly significant and could run into tens of billions of dollars.[144]

As noted by the EU's Policy Department for Economic, Scientific and Quality of Life Policies (the **EU Policy Department**) in its report on *Cryptocurrencies and blockchain* (the **EU Report**)[145], the key issue that needs to be addressed is the anonymity surrounding cryptocurrencies. This "*prevents cryptocurrency transactions from being adequately monitored, allowing shady transactions to occur outside of the regulatory perimeter and criminal organisations to use cryptocurrencies to obtain easy access to 'clean cash*'".[146] The problem is compounded by the increasing use of devices such as tumblers, mixers and private coins to enhance the anonymity of cryptoasset transactions.[147]

The lack of centralised intermediaries to use as addressees of suitable regulations makes the regulators task even more difficult. By contrast to traditional financial services where banks and other financial institutions are the target of regulation, cryptocurrencies do not (in principle) require intermediaries. There is only a need for intermediation where the cryptocurrency network intersects with the market

[140] Dickinson in Fox and Green (n 130) para 5.110

[141] Hybrid approaches are also possible. Dr Paech, the Chairman of the Expert Group on Regulatory Obstacles to Financial Innovation, favours applying a 'law of the network', comprising either the law of the jurisdiction that regulates the platform provider or the law chosen by the platform provider when establishing the network: see Philipp Paech, *The Governance of Blockchain Financial Networks* (2017) 80 MLR 1073. Like the FMLC, Dr Paech accepts that the platform provider's freedom choice may need to be restricted, to avoid forum shopping, to jurisdictions where the platform provider is incorporated or has a major operation.

[142] See FMLC report (n 106) paras 5.1-5.2; and UKJT Legal Statement (n 4) para 99. The Expert Group on Regulatory Obstacles to Financial Innovation has similarly called for a "*common approach*" in its Final Report to the European Commission, *30 Recommendations on Regulation, Innovation and Finance* (13 December 2019) - see Recommendation 8 at 58-59. <https://ec.europa.eu/info/publications/191113-report-expert-group-regulatory-obstacles-financial-innovation_en> Accessed June 2020

[143] Notable examples of this illicit activity include the WannaCry attack, which extorted ransomware payments in Bitcoin; the PlusToken ponzi scam which reportedly attracted over US$ 3 billion worth of cryptocurrency; and attempts to raise funds for Daesh via Bitcoin.

[144] EU Policy Department for Economic, Scientific and Quality of Life, *Cryptocurrencies and blockchain* (Report, July 2018) <<https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf> Accessed May 2020. This report estimated the misuse of virtual currencies then to exceed EUR 7 billion. The *2020 State of Crypto Crime Report* by Chainalysis estimates that the value of illicit cryptocurrency transactions during 2019 exceeded US$ 10 billion.

[145] Ibid.

[146] Ibid, executive summary at p. 9; and para 4.1.1.

[147] Tumblers and mixers combine unrelated transactions together, making it more difficult for a third party to trace particular cryptoassets.

outside. It is no surprise that such regulation of cryptocurrencies as has been introduced has therefore focussed on entities operating at this interface, i.e. cryptoasset exchanges and digital wallet providers. However, it is unclear whether this suffices given the extent to which users can bypass exchanges by using cryptoassets to pay directly for goods and services or transmit value on a peer-to-peer basis.

Regulators have nevertheless been wary of stifling technological innovation. The EU Report explicitly advised against 'throwing the baby out with the bathwater': "*legislative action should always be proportionate so that it addresses the illicit behaviour while at the same time not strangling technological innovation at birth*".[148] Similar sentiments have been expressed by UK and other regulators. It should also be noted that distributed ledger technology may in fact assist regulators to detect money-laundering and terrorist financing. Since a blockchain comprises an immutable record of every transaction, it provides an incorruptible audit trail which may facilitate (rather than hinder) tracing and identifying the source and use of funds.[149]

There is clearly a risk of regulatory arbitrage. Greater regulation in the UK and EU will drive illicit activity elsewhere unless corresponding regulations are implemented in other jurisdictions. The rules will only be adequate "*when they are taken at a sufficiently international level*".[150] As noted by HM Treasury in its Consultation Response on Transposition of the Fifth Money Laundering Directive, "*it is imperative that there is regulatory harmony to successfully counter the use of cryptoassets for illicit activity*".[151] The adoption by the FATF in June 2019 of Guidance which brings virtual assets and virtual service providers within the ambit of the FATF's Recommendations (with which FATF member countries are required to comply) is an encouraging step forward.[152]

The UK Rules

With effect from 10 January 2020, cryptoasset exchange providers and custodian wallet providers (**Cryptoasset Service Providers**) carrying on business in the UK have been obliged entities within the scope of the AML regime in the UK. Specifically, such Cryptoasset Service Providers:[153]

- comprise "*relevant persons*" for the purposes of the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (the **AML Regulations**); and

- are in "*the regulated sector*" for the purposes of the Proceeds of Crime Act 2002 (**POCA**).

A cryptoasset exchange provider is defined by regulation 14A(1) of the AML Regulations as a firm or sole practitioner who, by way of business, provides one or more of the following services:

- Exchanging, or arranging or making arrangements with a view to the exchange of, cryptoassets for money or money for cryptoassets;

- Exchanging, or arranging or making arrangements with a view to the exchange of, one cryptoasset for another; or

- Operating a machine that uses automated processes to exchange cryptoassets for money or money for cryptoassets.

[148] EU report (n 144) para 4.1.6

[149] Dean Armstrong, Dan Hyde and Sam Thomas, *Blockchain and Cryptocurrency: International Legal and Regulatory Challenges* (Bloomsbury Professional, 2019) paras 3.20-3.22

[150] EU Report (n 144) para 4.1.2

[151] HM Treasury, *Transposition of the Fifth Money Laundering Directive: response to the consultation* (January 2020) para 2.23.

[152] FATF Guidance (n 8)

[153] See regulation 8(2) of the AML Regulations and Schedule 9, paragraph 1(1)(v) of POCA.

A custodian wallet provider is defined by regulation 14A(1) of the AML Regulations as a firm or sole practitioner who, by way of business, provides services to safeguard, or to safeguard and administer, either of the following:

- cryptoassets on behalf of customers;
- private cryptographic keys on behalf of customers to hold, store and transfer cryptoassets.

There is no statutory definition of what comprises "carrying on business in the UK" by such businesses, but this ordinarily requires a business to have a physical presence in the UK. Guidance published by the FCA (the relevant supervisor under the AML Regulations) indicates that a Cryptoasset Service Provider will likely carry on business in the UK where it has an office in the UK or operates a cryptoasset automated teller machine in the UK.[154] However, the mere fact that a business has UK customers does not in itself mean that it will fall within the scope of the AML Regulations.

A Cryptoasset Service Provider carrying on business in the UK is subject to the same AML obligations as other obliged entities under the UK's AML regime. In particular:

- The Cryptoasset Service Provider must register with (and obtain approval from) the FCA before commencing business as a Cryptoasset Service Provider.[155] There is a transitional period for existing Cryptoasset Service Providers, i.e. those who were carrying on cryptoasset business in the UK immediately before 10 January 2020: they must register (and be approved) by 10 January 2021. Under regulation 58 of the AML regulations, an applicant will only be registered by the FCA if the FCA determines that the applicant, any officer or manager, and any beneficial owner, are fit and proper persons.

- The Cryptoasset Service Provider must carry out a risk assessment to identify and assess the risks of money laundering and terrorist financing to which its business is subject, having regard (among other things) to its customers, the countries in which it operates, its products or services and its transactions.[156]

- The Cryptoasset Service Provider must establish and maintain suitable policies, controls and procedures to mitigate and manage effectively the risks of money laundering and terrorist financing identified by its risk assessment.[157]

- The Cryptoasset Service Provider must carry out customer due diligence (**CDD**) whenever it establishes a business relationship or carries out an occasional transaction with a value in excess of EUR 1,000.[158] This requirement is at the heart of the AML regime. It requires the business to carry out KYC checks to understand who a customer is and the nature of the expected relationship with the customer. The checks must extend to the customer's beneficial owner, where relevant.

- The Cryptoasset Service Provider's obligation to know its customer applies not only when it takes on a customer, but throughout the customer relationship. By regulation 28(11) of the AML Regulations, the Cryptoasset Service Provider must conduct ongoing monitoring of its customer relationships, including by scrutinising transactions undertaken throughout the

[154] FCA, 'Cryptoassets: AML/CTF regime: Register with the FCA' (published 10 January 2020 and updated 1 July 2020) <https://www.fca.org.uk/print/cryptoassets-aml-ctf-regime/register> Accessed June 2020
[155] Regulation 56 of the AML Regulations
[156] Regulation 18 of the AML Regulations
[157] Regulation 19 of the AML Regulations
[158] Regulation 27 of the AML Regulations

course of each customer relationship to ensure that the transactions are consistent with its knowledge of the customer, the customer's business and the customer's risk profile.

- The Cryptoasset Service Provider must in certain circumstances undertake enhanced due diligence measures, including (i) when dealing with high-risk third countries;[159] (ii) where a transaction is complex or unusually large; and (iii) where the customer is a politically exposed person (**PEP**), a PEP family member or a known close associate of a PEP.[160]

- The Cryptoasset Service Provider must keep records of (i) documents and information obtained in the course of carrying out CDD, and (ii) sufficient records of all transactions that were the subject of CDD measures or ongoing monitoring to enable each such transaction to be reconstructed.[161]

- Where a Cryptoasset Service Provider is unable to carry out CDD measures as required by the AML Regulations, the Cryptoasset Service Provider must not carry out any transaction on behalf of the customer and must consider whether to make a suspicious activity report (**SAR**) to the National Crime Agency under POCA or the Terrorism Act 2000.[162]

- Under POCA and the Terrorism Act, the Cryptoasset Service Provider must submit a SAR to the National Crime Agency if at any time it knows or suspects, or has reasonable grounds for knowing or suspecting, that a customer is engaged in money laundering or the funding of terrorism.

Conclusion

The rules implemented by the UK are reasonably comprehensive in that:

- They extend to all types of cryptoasset exchanges and not only those engaged in exchanging between cryptoassets and fiat money (as in the case of the EU's Fifth AML Directive).[163] This is sensible; the rationale for the EU having excluded cryptoasset to cryptoasset exchanges is unclear and was described by the EU Policy Department as "*a blind spot*" in the fight against money laundering and terrorist financing;[164]

- The definition of 'cryptoasset' in the AML Regulations encompasses not only cryptocurrencies (such as Bitcoin) but also security and utility tokens, whereas it is unclear whether the definition of 'virtual assets' in the Fifth AML Directive extends to security and utility tokens.[165] The UK's approach achieves clarity and avoids the risk of tokens being created in such a way as to evade the regulations.

The main gap remains that identified above, namely whether it suffices only to regulate exchanges and custodian wallet providers. This omits, among other participants, miners and those using peer-to-peer exchanges. The EU Policy Department described both omissions as 'blind spots' in the fight against money laundering and terrorist financing.[166] Whilst acknowledging the practical difficulties of regulating either of these activities, it is suggested that both should be kept under review. Developments in technology or international co-operation may make regulation of either activity more feasible.

[159] These include (among other countries) Iran, Libya, the Bahamas and the US Virgin Islands.

[160] Regulations 33 and 35 of the AML Regulations

[161] Regulation 40 of the AML Regulations

[162] Regulation 31 of the AML Regulations

[163] Council Directive 2018/843 amending Directive 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing [2018] OJ L156/43 (Fifth AML Directive) Art. 1(1)(c).

[164] EU Report (n 144) para 5.3.4

[165] Fifth AML Directive (n 163) Art. 1(2)(d).

[166] EU Report (n 144) paras 5.3.3 and 5.3.5.

SECTION 7: REGULATION OF CRYPTOASSETS

Heenal Vasu, Allen & Overy LLP and Laura Douglas, Clifford Chance LLP

Introduction

There is no specific UK regulatory regime for cryptoassets, other than in relation to AML requirements for cryptoasset exchange providers and custodian wallet providers. Instead, the UK approach to regulation of cryptoassets is to consider which types of cryptoassets fall within the perimeter of the existing regulatory framework, based on a case-by-case analysis of the relevant cryptoasset's substantive characteristics. For those types of cryptoassets that do fall within the regulatory perimeter, different regulatory rules may apply depending on whether they are characterised as a deposit, transferable securities, e-money or another type of regulated financial instrument.

FCA guidance and taxonomy

This approach is reflected in the Final Guidance on Cryptoassets[167] published by the Financial Conduct Authority (**FCA**) in July 2019, which identifies the following categories of cryptoassets, divided broadly according to their regulatory treatment:

(a) Security tokens

Security tokens are cryptoassets which provide holders with rights and obligations similar to "specified investments" under the Financial Services and Markets Act 2000 (Regulated Activities) Order 2001 (**RAO**)[168], such as shares, debentures or units in a collective investment scheme. In its Final Guidance on Cryptoassets, the FCA provides a non-exhaustive list of factors that are indicative of a security token, including any contractual entitlement holders may have to share in profits or exercise control or voting rights in relation to the token issuer's activities. However, this factual analysis may not always be clear-cut and will often require the exercise of judgement to determine how similar the substantive characteristics of a cryptoasset are to a particular type of specified investment.

In addition, different types of "specified investments" are subject to different regulatory rules. For example, security tokens meeting the definition of "transferable securities" under the EU Markets in Financial Instruments Directive (**MiFID2**)[169] are in scope of prospectus rules and requirements for the securities if traded on a trading venue to be recorded in book-entry form in a central securities depository (**CSD**). Security tokens that do not meet the MiFID2 definition of transferable securities (for example because there are contractual restrictions on transfer) may nevertheless fall within the UK crowdfunding regime and related financial promotion rules for non-readily realisable securities. In other cases, security tokens may qualify as units in a collective investment scheme under section 235 FSMA and/or an alternative investment fund (**AIF**) as defined in the Alternative Investment Fund Managers Regulations 2013.[170] Again, this would attract application of specific regulatory rules such as the requirement for an AIF to be managed by an alternative investment fund manager (**AIFM**) responsible for compliance with the UK regulatory requirements applicable to AIFs and AIFMs.

Determining exactly which regulatory rules will apply to a given type of security token will be a question of fact requiring a case-by-case analysis. The definition of "transferable securities" is

[167] Financial Conduct Authority, *Guidance on Cryptoassets Feedback and Final Guidance to CP 19/3* (Policy Statement, PS19/22) <https://www.fca.org.uk/publication/policy/ps19-22.pdf> Accessed April 2020

[168] The Financial Services and Markets Act 2000 (Regulated Activities) Order 2001, SI 2001/554

[169] Council directive 2014/65/EU of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (2014) OJ L173/349

[170] The Alternative Investment Fund Managers Regulations 2013, SI 2013/1773

somewhat unclear, referring to "those classes of securities which are negotiable on the capital market" (which the FCA interprets as meaning they are capable of being traded on the capital markets), with the exception of "instruments of payment"; this last term is not clearly defined. Likewise, the test for determining whether a particular cryptoasset structure qualifies as an AIF is complex, despite the existence of case law and FCA guidance on this definition. However, given the extensive use of these terms in existing financial regulation, further clarification of these terms for the sole purpose of accommodating cryptoassets may lead to unintended consequences and so may not be desirable. Nevertheless, a general clarification of the meaning of "instruments of payment" as used in the definition of transferable securities may assist in providing greater certainty to market participants.

(b) E-money tokens

E-money tokens are cryptoassets that meet the definition of electronic money (or e-money) under the Electronic Money Regulations 2011 (**EMRs**).[171] For this purpose, e-money is defined as electronically (including magnetically) stored monetary value as represented by a claim on the issuer, which is issued on receipt of funds for the purpose of making payment transactions and is accepted as a means of payment by persons other than the issuer (subject to certain exclusions set out in the EMRs). Some aspects of this definition give rise to uncertainties, such as when a cryptoasset is considered to be "accepted as a means of payment" by a party and the fact that the term "monetary value" is not defined (although we take this to refer to fiat currency). This particular characteristic may also change during the life of a cryptoasset, meaning that it may become, or cease to qualify as, e-money at some point after issuance.

The FCA expressly acknowledges that cryptoassets may move between categories throughout their lifetime in its Final Guidance on Cryptoassets.[172] This creates particular uncertainties, as an e-money issuer generally needs to be authorised as such under the EMRs (unless it is a credit institution) whereas firms dealing in or advising on security tokens will typically need to be authorised under FSMA with relevant regulatory permissions. Different ongoing conduct of business rules will apply to different types of cryptoassets.

Similar uncertainties arise in the case of "hybrid" tokens which exhibit characteristics of more than one category of cryptoassets (such as security tokens and e-money tokens). It would therefore be helpful for the FCA to clarify how it expects firms to proceed in these cases.

(c) Unregulated tokens

Unregulated tokens include all other types of cryptoassets which are not treated as regulated financial instruments or products. In general, this means that firms carrying on activities relating to unregulated tokens fall outside the regulatory perimeter. There are however some notable exceptions to this.

(i) **Cryptocurrency derivatives**: in April 2018, the FCA published a statement indicating that cryptocurrency derivatives may be MiFID financial instruments (but that it does not consider cryptocurrencies themselves to be currencies or commodities for regulatory purposes under MiFID2). However, the FCA did not expressly indicate which categories of derivatives it considers cryptocurrency derivatives to fall under Section C of Annex I MiFID2. This is relevant for firms trying to understand which regulatory rules will apply to them, as different rules apply to different classes of derivatives under MiFID2.

[171] The Electronic Money Regulations 2011, SI 2011/99
[172] FCA Guidance (n 167)

A likely starting point is that cryptocurrency derivatives may be treated as "other derivative contracts" under Section C(10) Annex I of MiFID2. However, a case-by-case analysis would be needed to determine whether the cryptocurrency derivative meets the conditions. For example, cryptoassets representing "rights to receive services" may not count as relevant underlyings for the purposes of Section C(10) and not all physically-settled derivatives will fall within Section C(10). Alternatively, cash-settled contracts for differences relating to cryptocurrencies might fall within Section C(9) to the extent that they are regarded as "financial contracts for differences". Even for cryptoasset derivatives that do not qualify as MiFID financial instruments, consideration would also need to be given as to whether they are nevertheless specified investments falling within one of the broader categories of futures, options and contracts for differences under the RAO. Further guidance on this would be helpful.

(ii) **Cryptoasset exchange providers and custodian wallet providers**: in January 2020, the UK introduced new registration requirements for "cryptoasset exchange providers" and "custodian wallet providers" as set out in Regulation 14A of the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (**MLRs**) and FCA rules. The definition of "cryptoasset" introduced for this purpose[173] is broad, encompassing both regulated and unregulated types of cryptoassets.

There are however some uncertainties as to which businesses and activities are captured by the definitions of "cryptoasset exchange provider" and "custodian wallet provider" as set out in Regulation 14A MLRs.

The definition of "cryptoasset exchange provider" includes firms "exchanging, or arranging or making arrangements with a view to the exchange of" cryptoassets for money or money for cryptoassets or of one cryptoasset for another. HM Treasury's response to its consultation on the new rules suggests that the intention of this language is to capture firms facilitating peer-to-peer exchange services or completing, matching or authorising a transaction between two people. However, the same language of "arranging" or "making arrangements with a view" is used in Article 25 RAO and in this context, the FCA takes the view that "making arrangements with a view to transactions in investments" has a much wider scope and is not, for example, limited to arrangements in which investors participate. It is currently unclear whether the FCA will interpret Regulation 14A(1) MLRs in a similarly broad fashion. Guidance published by the Joint Money Laundering Steering Group (**JMLSG**)[174] aims to provide practical guidance on this point, but notes that various types of activities may require case-by-case analysis, bearing in mind the policy objectives of the new regime amongst other factors.

The definition of a "custodian wallet provider" refers to safeguarding, or safeguarding and administering, (i) cryptoassets; or (ii) private cryptographic keys, on behalf of customers. However, it is unclear how a custodian could hold cryptoassets for another person without holding the private cryptographic key, based on our understanding of the operation of DLT blockchains and cryptoassets. It is therefore unclear when a service provider would be deemed to safeguard (or safeguard and administer) cryptoassets, as opposed to private cryptographic keys, for its customers. We would suggest that this is an area where further guidance or clarification from HM Treasury and/or the FCA would be helpful.

It is noteworthy that stablecoins do not have their own category under the FCA taxonomy. This is because stablecoins may be structured in different ways, leading to different regulatory treatment. For example, in its Final Guidance on Cryptoassets, the FCA indicates that stablecoins could be

[173] "a cryptographically secured digital representation of value or contractual rights that uses a form of distributed ledger technology and can be transferred, stored or traded electronically"

[174] The Joint Money Laundering Steering Group Guidance – Part II: Sector 22 (June 2020 (amended July 2020)) https://jmlsg.org.uk/consultations/current-guidance/ Accessed August 2020

regulated as e-money, as units in a collective investment scheme or another type of security token, or could fall outside the UK regulatory perimeter, depending on the way they are structured, their stabilisation mechanism and other substantive characteristics. The Bank of England has also indicated that so-called "global stablecoins" could also become (and may therefore be regulated as) systemically important payment systems.[175]

As discussed further below, there are a number of global initiatives focusing on global stablecoins, including draft recommendations published by the Financial Stability Board (**FSB**) in April 2020, which highlight the need for flexible and efficient cross-border cooperation in addressing the regulatory, supervisory and oversight challenges posed by global stablecoins. In its July 2020 consultation on cryptoasset promotions,[176] HM Treasury also notes it will continue to work with the FCA and the Bank of England to consider the risks and opportunities arising from stablecoins, particularly those with the potential to be globally or systemically significant, alongside work on a review of the UK payments landscape and an evaluation of the risks and opportunities involved in the creation of a UK central bank digital currency.

The broader legal context

It is important to distinguish the regulatory characterisation and treatment of cryptoassets from legal questions such as whether cryptoassets are capable of being owned and transferred as property and whether and how a legally enforceable security interest may be taken over cryptoassets, although understanding both the legal and regulatory position will be important for firms dealing with cryptoassets.

In relation to the legal status of cryptoassets under English law, the UKJT issued a statement in November 2019 confirming that cryptoassets are capable of being owned and transferred as property under English law and that smart contracts are capable of constituting binding legal contracts. Whilst the Legal Statement itself is not binding, these questions have also been considered by the English courts, notably in the case of *AA v Persons Unknown,*[177] where Mr Justice Bryan expressly considered the Legal Statement and agreed with its conclusions, holding in this case that Bitcoin was a form of property capable of being the subject of a proprietary injunction. Nevertheless, given that this judgment relates to an interim application, it does not constitute definitive legal authority.

However, not every use of DLT will result in creation of a cryptoasset that qualifies as property under English law. An obvious example is where DLT is used for record keeping purposes only. In other cases, a cryptoasset may be a digital representation of a traditional asset (whether physical property such as real estate or art or an intangible asset such as a dematerialised security) rather than the asset itself. As well as determining the legal rights and remedies that may apply in respect of the cryptoasset, understanding whether it is itself an asset, or property, is relevant when considering whether certain regulatory rules apply, such as FCA client asset rules.

In addition, there are difficult questions about which law will apply to proprietary aspects of dealings in cryptoassets and therefore whether English law is the relevant law to decide these questions in respect of a particular cryptoasset. These conflicts of laws issues are particularly acute for native cryptoassets and decentralised, permissionless structures where it is very difficult to conclude that the cryptoasset is situated in any particular jurisdiction. In light of this, the Legal Statement indicates that the normal rules on applicable law may well not apply but that it is unclear which rules should apply instead (themes explored more fully in Section 6). A change to the law as well as international cooperation will likely be

[175] Bank of England, 'Financial Policy Summary and Record' (October 2019) <https://www.bankofengland.co.uk/financial-policy-summary-and-record/2019/october-2019> Accessed April 2020
[176] HM Treasury, 'Cryptoasset Promotions Consultation' (July 2020) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/902177/2020-07-16_-_Cryptoasset_promotions_consultation_.pdf> Accessed July 2020
[177] *AA v Persons Unknown* [2019] EWHC 3556 (Comm)

needed in order to resolve these conflicts of laws issues satisfactorily. In the meantime, firms issuing cryptoassets could seek to increase legal certainty by specifying which law should govern the proprietary aspects of dealings in the cryptoassets as part of the underlying DLT structure – although this solution may not always be practicable (or available for firms dealing with existing cryptoassets).

What are we waiting for?

Looking ahead, the UK government has been considering whether further enabling legislation or regulation of cryptoassets is required, and in particular whether the regulatory perimeter should be expanded to specifically cover all types of cryptoassets. This would require legislative change and in July 2020, HM Treasury published a consultation[178] seeking views on whether to bring the promotion of certain types of cryptoassets within scope of financial promotions regulation. Given how recently the new registration regime for cryptoasset exchange providers and custodian wallet providers has been introduced, further significant changes may be less likely, at least in the short term. However, we might expect to see more incremental changes and clarifications of the outstanding legal and regulatory uncertainties.

Licensing and conduct of business requirements

The licensing and conduct of business requirements that apply to firms dealing with cryptoassets will depend on how the relevant cryptoasset is characterised under the UK regulatory framework (in particular, whether the cryptoasset is a security token or e-money token) as well as the types of activities that the firm is carrying on in relation to the cryptoasset.

Licensing and registration

Firms carrying on regulated activities in the UK with respect to security tokens or regulated cryptocurrency derivatives will need to be authorised under FSMA with relevant regulatory permissions, just as they would when carrying on activities with respect to traditional types of securities. Issuers of e-money tokens will need to be authorised or registered as such under the EMRs (unless authorised as a credit institution) and firms dealing with e-money tokens may be carrying on regulated payment services requiring authorisation or registration under the Payment Services Regulations 2017 (**PSRs**). Carrying on these activities in the UK without the necessary authorisation or registration is a criminal offence.

Firms dealing with unregulated cryptoassets (other than cryptoasset derivatives) will not be subject to licensing requirements under FSMA, the EMRs or the PSRs. However, cryptoasset exchange providers and custodian wallet providers are required to register with the FCA under the MLRs (subject to a transition period for existing firms carrying on these activities before 10 January 2020). Whilst not a formal licensing regime, the FCA does require applicants for registration to submit detailed information about the firm and will only grant registration if it is satisfied that the firm, its beneficial owners, officers and managers are "fit and proper". Cryptoasset exchange providers and custodian wallet providers will also need to comply with the AML-related requirements of the MLRs on an ongoing basis, as will firms authorised (or registered) under FSMA, the EMRs and PSRs. The JMSLG sectoral guidance[179] relating to cryptoassets highlights various factors that give rise to money laundering and terrorist financing risks in this area (including some specific to cryptoassets, such as privacy or anonymity and the decentralised and cross-border nature of many cryptoasset systems) along with indicative practical mitigation strategies. These strategies may include blockchain analysis or tracing as well as more traditional AML risk-mitigation strategies.

[178] HM Treasury consultation (n 176)

[179] The Joint Money Laundering Steering Group Guidance – Part II: Sector 22 (June 2020 (amended July 2020)) https://jmlsg.org.uk/consultations/current-guidance/ Accessed August 2020.

Conduct of business rules

Firms that are authorised (or registered) under FSMA, the EMRs or the PSRs will be subject to ongoing conduct of business requirements in relation to their cryptoasset activities. Firms issuing security tokens that qualify as transferable securities will also be subject to prospectus rules and certain other ongoing requirements applicable to issuers of transferable securities (but will not generally require authorisation).

The statutory and regulatory rules setting out these ongoing conduct of business obligations are generally drafted in a technology-neutral manner. They do, however, embed certain assumptions about how financial markets operate that do not necessarily hold true of cryptoassets, creating challenges in interpreting and applying certain existing conduct of business rules to cryptoassets. There are also certain gaps and issues in current conduct of business rules that may require further adaptation to cater for cryptoassets, both in terms of enabling innovation and addressing risks specific to cryptoassets. We set out a number of these issues below. Some arise particularly in the case of decentralised and permissionless platforms or only to the extent that a cryptoasset is considered to be a transferable security or other MiFID financial instrument, but others have broader relevance.

- *Issues relating to custody of cryptoassets*

  As previously noted in this section, there remains uncertainty as to what services and activities, other than holding private keys for clients, may qualify as custody or safekeeping and administration of cryptoassets. Further questions arise about whether, and if so how, FCA client asset rules under CASS might apply to custody of cryptoassets. This is particularly the case where a regulated custodian safeguards a private key but cannot be said to safeguard the cryptoasset itself, or where the cryptoasset may not be considered property (or an "asset" of the client) from a legal perspective.

- *Calibration of requirements applicable to transferable securities*

  Many more regulatory requirements will also apply in respect of cryptoassets that are considered to be transferable securities under MiFID2. However, these requirements are not always drafted or calibrated in a way that caters for cryptoassets.

  In its Advice on Initial Coin Offerings and Crypto-Assets,[180] the European Securities and Markets Authority (**ESMA**) identified various requirements under MiFID2 and the related EU Markets in Financial Instruments Regulation (**MiFIR**) that would require adjustment including: pre- and post-trade transparency requirements, transaction reporting, instrument reference data reporting and record keeping requirements. This is in part because relevant concepts and thresholds have not been calibrated for cryptoassets, but also because common identifiers and classifications used in reporting have not yet been adapted for cryptoassets.

  Further issues arise where security tokens are traded on platforms that may meet the definition of a multilateral trading facility (**MTF**) (or regulated market) under MiFID2, particularly in the case of decentralised platforms, as the rules assume that there is a clearly identified and supervised platform operator. This is relevant in respect of the rules applicable to trading venues under MiFID2 and MiFIR, as well as other regulations such as the EU Market Abuse Regulation (**MAR**) and the EU Central Securities Depositories Regulation (**CSDR**).

- *Settlement of transactions in cryptoassets*

[180] European Securities and Markets Authority, *Initial Coin Offerings and Crypto-Assets* (2019) ESMA50-157-1391 <https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf> Accessed April 2020

> Greater certainty would be welcomed around the concepts of settlement and settlement finality as they apply to cryptoassets, including consideration of the role of miners and other novel actors in the settlement process. We discuss the legal framework governing post-trade market infrastructure, including the impact of CSDR on settlement of cryptoassets further below.

It is also worth considering whether there are gaps in the current conduct of business framework that do not adequately address risks posed by cryptoassets. For example, might novel types of market abuse emerge in respect of cryptoassets? Do current rules on material outsourcings adequately cover the ways in which regulated financial services firms might engage with technical service providers and others with respect of cryptoasset activities? And might the complexity of the regulatory perimeter with respect to cryptoassets allow for regulatory arbitrage whereby cryptoassets are designed to fall outside the regulatory perimeter in order to avoid the application of licensing and conduct of business rules? In this respect, we suggest that the principle of "same activity, same regulation" is a good rule of thumb, although a flexible and pragmatic approach is likely to be needed to mitigate risks and address uncertainties in the application of the current regulatory framework, whilst ensuring that any changes to the regulatory framework do not unduly stifle innovation or restrict access to new services.

UK actions to address risks arising from cryptoassets

In October 2018, the Cryptoasset Taskforce published its final report[181] assessing the potential risks and benefits of cryptoassets and outlining actions to further develop and implement the UK's policy and regulatory approach to cryptoassets. The final report identified three major areas of risk associated with cryptoassets: (i) risk of financial crime; (ii) risk to market integrity; and (iii) risk to consumers. Many of the recent developments in relation to the UK regulatory framework for cryptoassets aim to address these risks, such as the new registration regime for cryptoasset exchange providers and custodian wallet providers to address financial crime risks.

The FCA has also taken various actions to address and mitigate risks of harm to consumers and retail clients. Even before the publication of the Cryptoasset Taskforce report, the FCA issued consumer warnings about the risks of initial coin offerings,[182] cryptocurrency contracts for difference (**CFDs**)[183] and cryptoasset investment scams.[184] More recently, the FCA has introduced new conduct of business rules[185] restricting how firms can sell, market or distribute CFDs and similar products (including those that reference cryptocurrencies) to retail consumers.

The FCA has also consulted[186] on a potential ban on the sale, marketing or distribution of derivatives and exchange of traded notes referencing cryptoassets to retail clients. The outcome of this consultation is expected shortly and if such a ban is introduced, it would replace the existing rules restricting how CFDs referencing cryptocurrencies are sold to retail clients.

[181]Cryptoassets Taskforce, 'Final Report' (October 2018) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752070/cryptoassets_taskforce_final_report_final_web.pdf> Accessed April 2020. The Cryptoasset Taskforce comprises the FCA, PRA and HM Treasury.

[182] FCA, 'Initial Coin Offerings′ (12 September 2017) <https://www.fca.org.uk/news/statements/initial-coin-offerings> Accessed April 2020

[183] FCA, 'Consumer Warning About The Risks Of Investing In Cryptocurrency Cfds' (14 November 2017) <https://www.fca.org.uk/news/news-stories/consumer-warning-about-risks-investing-cryptocurrency-cfds> Accessed April 2020

[184] FCA, 'Cryptoasset Investment Scams' (First published: 27 June 2018, updated 13 March 2020) <https://www.fca.org.uk/scamsmart/cryptoasset-investment-scams> Accessed April 2020

[185] FCA, 'Restricting contract for difference products sold to retail clients' (Policy statement PS19/18, July 1019) <https://www.fca.org.uk/publication/policy/ps19-18.pdf> Accessed April 2020

[186] FCA, *CP19/22: Restricting the sale to retail clients of investment products that reference cryptoassets* (Consultation papers, First published: 3 July 2019, updated 9 April 2020) <https://www.fca.org.uk/publications/consultation-papers/cp19-22-restricting-sale-retail-clients-investment-products-reference-cryptoassets> Accessed April 2020

Prudential requirements

Neither the current UK regulatory regime, European regulatory regime nor Basel framework specify the prudential treatment for banks' exposures to cryptoassets, given the relative novelty of cryptoassets. Specifically:

- Basel III does not provide for a separate class of exposure for cryptoassets; rather, it sets out minimum requirements for the liquidity and capital treatment of "other assets".

- Article 147 of the Capital Requirements Regulation (**CRR**)[187], which provides the methodology for banks to assign their exposures to asset classes, does not provide for a cryptoassets class. Instead, it provides for a broad and inclusive definition of "other non-credit obligation assets".

Notwithstanding this, it is widely accepted that the market would greatly benefit from a clear, robust and proportionate prudential regulatory framework for cryptoassets.

Financial institutions' acquisition of cryptoassets

Presently, UK financial services laws do not prohibit financial institutions, including credit institutions, investment firms, payment institutions and e-money institutions, from gaining exposure to or holding cryptoassets.

However, cryptoassets are an immature asset class, and certain cryptoassets have exhibited a high degree of volatility (as well as presenting risks for banks such as liquidity risk, credit risk, market risk and operational risk (including fraud and cyber risks)). Therefore, if financial institutions choose to acquire cryptoassets and take them on their balance sheets, they could face significant losses. Moreover, balance sheets which contain high-risk cryptoassets may not reflect the true financial position of that particular institution.

Currently, there appear to be only a few financial institutions that have acquired cryptoassets, and their exposure to such assets remains limited. However, with the proliferation of cryptoassets and changing market conditions, this might change. The growth of cryptoassets and related services, therefore, has the potential to raise financial stability concerns and increase risks faced by financial institutions.

Global regulatory approach

The Basel Committee on Banking Supervision (**BCBS**) has historically expressed the view that if banks decide to acquire cryptoassets, they should apply a conservative prudential treatment to such exposures, especially for high-risk cryptoassets. The BCBS clearly set out its prudential expectations relating to banks' exposures to cryptoassets and related services in its 2019 statement on cryptoassets.[188] The European Banking Authority (**EBA**) has previously expressed similar views in its January 2019 report on cryptoassets.[189]

The EBA recognised that broadly, where regulated financial institutions carry out cryptoasset activities, the competent authorities hold a range of robust supervisory powers that can be applied effectively to mitigate the risks associated with those activities. However, when it comes to the existing prudential framework (including the relevant capital and liquidity requirements), the EBA noted that there is currently no specific Pillar II treatment for cryptoassets. Moreover, it suggested that it would be helpful

[187] Council Regulation No 575/2013 on prudential requirements for credit institutions and investment firms and amending Regulation [2013] No 648/2012 OJ L176 1 [147]

[188] Basel Committee on Banking Supervision, *Statement On Crypto-Assets* (BIS Website, 13 March 2019) <https://www.bis.org/publ/bcbs_nl21.htm> Accessed June 2020

[189] European Banking Authority, 'EBA Reports On Crypto-Assets' (9 January 2019) <https://eba.europa.eu/eba-reports-on-crypto-assets> Accessed April 2020

to clarify the uncertain accounting treatment of cryptoassets to avoid queries about their prudential treatment under current EU prudential laws and regulation.

Consistent with the views expressed by the ECB Crypto-Asset Task Force, the ECB and the EBA, and as part of a conservative prudential treatment, the preferred way in which to deal with the uncertainty surrounding cryptoassets is for financial institutions to deduct them from their own funds, for now. As the European Parliament recognised in its April 2020 policy paper:[190]

> *"….most crypto-assets do not constitute a credible contribution to a financial institution's own funds. On the contrary, they qualify as high-risk assets. Therefore, from a prudential perspective, it is recommendable to treat them as such."*

The ECB adds in its May 2019 Occasional Paper Series:[191]

> *"From a prudential view, crypto-assets should be deduced from CET1 as part of a conservative prudential treatment."*

UK regulator - Prudential Regulation Authority (PRA)

To date, the PRA has largely remained silent on setting out a detailed prudential framework. The PRA did, however, send a letter in June 2018 to CEOs of banks, insurance companies and designated investment firms to remind them of the relevant obligations under PRA rules, and to communicate the PRA's expectations regarding firms' exposure to cryptoassets.[192]

Broadly, the PRA's letter noted that:

- the classification of cryptoasset exposures for prudential purposes should reflect firms' comprehensive assessment of the risks involved. Although classification will depend on the precise features of the asset, cryptoassets should not be considered as currency for prudential purposes;

- where relevant, firms should set out their consideration of risks relating to crypto-exposures in their Internal Capital Adequacy Assessment Process or Own Risk and Solvency Assessment. This should include: discussion of the major drivers of risk; sensitivity analysis to assess how changes in risk drivers might affect valuations and projections, and affect the firm's capital/solvency ratios; and an assessment of risk mitigants and what capital should be held against this risk; and

- there is an expectation that firms inform their usual PRA supervisory contact of any planned cryptoasset exposure or activity on an *ad hoc* basis, together with an assessment of the risks associated with the intended exposure.

Finally, the PRA explained that discussions are ongoing, including among authorities internationally, on the prudential treatment of cryptoassets, and that the PRA will communicate any supervisory or policy updates on the prudential treatment of cryptoassets, including through Pillar II for banks if deemed necessary, in due course.

[190] Robby Houben, Alexander Snyers, 'Crypto-assets: Key developments, regulatory concerns and responses' (Research Group Business & Law, Belgium April 2020) <https://www.europarl.europa.eu/RegData/etudes/STUD/2020/648779/IPOL_STU(2020)648779_EN.pdf> Accessed April 2020

[191] European Central Bank, 'Occasional Paper Series No 223 - Crypto-Assets: Implications for financial stability, monetary policy and payments and market infrastructures' (May 2019)

[192] Letter from Sam Woods, Deputy Governor and CEO, Prudential Regulation Authority, to the CEOs of banks, insurance companies and designated investment firms (28 June 2018) <https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/letter/2018/existing-or-planned-exposure-to-crypto-assets.pdf> Accessed April 2020

What are we waiting for?

Looking ahead, the BCBS has been considering designing a prudential treatment for cryptoassets. The deadline for comments on this Discussion Paper was 13 March 2020.

The EBA is actively engaged in the work that the BCBS is currently taking forward to clarify the prudential treatment of banks' exposure to holding cryptoassets. In the meantime, competent authorities have been advised to adopt a conservative prudential approach and the EBA recommends that the European Commission take steps where possible to promote consistency in the accounting treatment of cryptoassets.

Therefore, the UK would do well to follow up on the work that is currently being undertaken by the BCBS and the EBA to ensure that a clear, robust and proportionate framework for the prudential regulation of cryptoassets is designed. In its letter of June 2018,[193] the PRA also alluded to the fact that more guidance may follow, including measures under Pillar II (i.e., discretionary supervisory measures and potentially, additional capital charges).

Considerations for UK regulator when designing the framework

Underpinning the design of a prudential regulatory framework for cryptoassets ought to be the principle of "same risk, same activity, same treatment". In other words, for those assets that perform an analogous economic function to other traditional asset classes, the existing prudential treatment for those assets should be applied (for example, for those cryptoassets that qualify as financial instruments under MiFID2 or as e-money under the EMRs, or a virtual representation of physical assets such as real estate). We would encourage the PRA not to adopt an overly cautious approach towards risk assessment, as this could in turn discourage large swathes of the banking system from taking resolute steps to advance adoption of the technology.

Guiding principles

When designing the cryptoasset prudential regulatory framework we would invite the regulator to consider the guiding principles below, alongside those already identified by the BCBS and EBA:

- First, designing a framework that distinguishes between the various different categories of cryptoassets set out above in this section.

- Second, carefully considering the 'market' risk element of holding these different types of cryptoassets and calibrating the related regulatory framework accordingly. The types of cryptoassets with low or negligible inherent value under objectively agreed principles would tend to be much more volatile and speculative (although this may stabilise over a sustained period of time). For this category the ‘market’ risk element is considerable and the UK regulator may consider that any analogy with the market risk component of the existing Basel framework would be inappropriate. On the other hand, cryptoassets with tangible and clear inherent value on inception (e.g. cryptoassets embedding rights against a specific legal entity and/or another asset) ought to be examined and assessed in precisely the same way as traditional assets (as is acknowledged by the BCBS).

- Third, assessing any ‘add-on’ operational risks resulting from: (i) the nascent nature of the technology; and (ii) the limited adoption and market experience in relation to the classification, transfer, settlement and clearing of cryptoassets. However, this ‘add-on’ ought to be fair, proportionate and dynamic, with the ability to be reduced and calibrated

[193] Ibid

over time, as adoption and market experience demonstrates the resilience associated with more conventional types of assets.

International alignment

Finally, it is important that any national effort to design a prudential regulatory framework for cryptoassets is aligned with efforts at the international level in order to ensure a level playing field across different countries and jurisdictions, given the inherent cross-border nature of the cryptoasset ecosystem.

Clearly, regulators, legislators and policy makers hold the key to removing some of the pertinent risks associated with cryptoassets by creating appropriate legal and regulatory frameworks that legitimise certain segments of market activity. It is therefore possible that some national legal and regulatory systems will move much faster than others. Two speed adoption practices present their own risks given the inherently global nature of financial markets, and therefore seeking to align efforts at the international level is preferable – though, of course, challenging.

Post-trade infrastructure requirements

In the context of post-trade, the application of blockchain technology, coupled with the tokenisation of traditional financial instruments, is expected to improve efficiency in the post-trade value chain. While this area of development is nascent, there are a number of promising pilots and use-cases being developed by market participants across the globe. However, it is widely accepted that legal and regulatory certainty is required, both at a UK and global level, to facilitate further progress and adoption of innovative technology in this area.

Current UK regime

In the UK, there presently exists a well-defined and robust legal framework that operates to govern post-trade market infrastructure. This includes:

- EU Central Securities Depositories Regulation;
- European Market Infrastructure Regulation;
- UK Financial Collateral Arrangements (No. 2) Regulations 2003 (as amended) (**FCARs**) which implement the EU Financial Collateral Directive;
- UK Financial Markets and Insolvency (Settlement Finality) Regulations 1999 (as amended) (**SFRs**) which implement the EU Settlement Finality Directive; and
- Uncertificated Securities Regulations 2001 (as amended) which support the safety and integrity of settlement of UK securities.

At a global level, the CPMI-IOSCO Principles for Financial Market Infrastructure (**PFMIs**) sit alongside the legislative framework. The PFMIs represent internationally recognised standards for the operation, management and supervision of financial market infrastructure. They have been given statutory force by section 188 of the Banking Act 2009 in relation to FMIs that are 'recognised' payment systems by the Bank of England.

Notwithstanding the comprehensive framework that exists for the current post-trade market infrastructure in the UK, these laws and regulations were not designed with DLT in mind. Therefore, the position is far from settled, and greater clarity would be welcomed. By way of illustrative examples:

- the UK SFRs define the list of participants authorised to take part in designated systems (i.e. credit institutions, investment firms, public authorities, CCPs, settlement agents, clearing houses, system operators, electronic money institutions). Yet, this list of persons does not include natural persons, and therefore does not seem fully compatible with the functioning of cryptoasset platforms that rely on retail investors' direct access; and

- the UK FCARs might also present some challenges, for example, greater certainty would be welcomed regarding how collateral that is provided without title transfer (i.e. a pledge or other form of security financial collateral as defined in the UK FCARs) can be enforced in a distributed ledger context.

Certainly, at this stage, the prudent approach would be to assume that securities laws and regulations apply to security tokens (i.e. cryptoassets issued on a distributed ledger and that qualify as transferable securities or other types of MiFID financial instruments). To that end, a further topical area that merits consideration is the implications of CSDR book-entry form requirements for cryptoassets, explored below.

Implications of CSDR book-entry form requirements for cryptoassets

Cryptoassets that are transferable securities and are traded or admitted to trading on a MiFID trading venue will be, or become, subject to requirements under CSDR in order for the securities to be recorded in book-entry form in a CSD. There are different ways in which stakeholders may seek to meet this requirement, but each presents its own practical challenges.

One approach may involve the DLT platform operator (if one exists) becoming an authorised CSD under CSDR. This also raises questions about whether the DLT platform operator may be considered a 'securities settlement system' under the Settlement Finality Directive and whether it may need to be designated as such. This would have significant regulatory and practical implications for the DLT network. For example, a securities settlement system needs to be operated by a 'system operator' which would be particularly challenging for decentralised platforms. As noted above, only certain types of firms can be participants in a designated system, which may again cause issues if a DLT platform were designated where individuals are currently members.

An alternative structure could involve recording the cryptoassets in an existing authorised CSD and for one or more of the participants in the DLT network to also participate in the relevant CSD. In this case, the settlement of transactions as between the DLT network participants outside of the CSD may qualify as settlement internalisation, which is permitted under CSDR but subject to certain reporting requirements. However, this may not always be a viable practical solution.

Global initiatives

At a European level, the European Commission, in its December 2019 consultation on an EU framework for markets in cryptoassets,[194] sought views on the amendments that may need to be made to the EU legislative framework to facilitate the process of innovation and adoption of DLT. In the post-trade context, consultees were invited to comment on whether the provisions of various EU laws are workable in a DLT context, i.e. MiFID2 post-trade requirements, EMIR, CSDR, SFD and FCD. The consultation closed on 18 March 2020, and we await the policy statement. At a global level, the Committee on Payments and Market Infrastructures (**CPMI**) has also published a Public Report[195] that outlines the

[194] European Commission, 'Consultation Document: On an EU framework for markets in crypto-assets' (2019) <https://ec.europa.eu/info/sites/info/files/business_economy_euro/banking_and_finance/documents/2019-crypto-assets-consultation-document_en.pdf> Accessed April 2020

[195] Committee on Payments and Market Infrastructures, 'Investigating the impact of global stablecoins', (G7 Working Group on Stablecoins, October 2019) <https://www.bis.org/cpmi/publ/d187.pdf> Accessed April 2020

application of the PFMIs in the context of global stablecoins (and we would welcome a similar report on the application of the PFMIs in the context of financial market infrastructure using DLT). Additionally, the FSB, in its April 2020 consultation[196], published a set of ten (10) high-level recommendations addressed to national authorities, with the objective of advancing consistent and effective regulation and supervision of global stablecoin arrangements. These recommendations, which call for proportionate regulation, supervision and oversight, and highlight the need for flexible and efficient cross-border cooperation, could lead to an extension of the regulatory perimeter in the UK to bridge any legal or regulatory gaps that exist across borders.

UK regulator: suggested approach

In order to design a proportionate and robust legal framework, it is worth the UK regulators carrying out a similar exercise to that of the European Commission, in order to assess whether the UK legal and regulatory framework for post-trade infrastructure needs to be adapted to facilitate market adoption of DLT technology (and if so, how).[197] The key guiding principle ought to be "same activity, same risk, same regulation", with the key objective being to protect end-investors and safeguard the integrity of the markets without jeopardising innovation.

[196] Financial Stability Board, Consultative Document, 'Addressing the regulatory, supervisory and oversight challenges raised by "global stablecoin" arrangements' (14 April 2020) <https://www.fsb.org/2020/04/addressing-the-regulatory-supervisory-and-oversight-challenges-raised-by-global-stablecoin-arrangements-consultative-document/> Accessed April 2020

[197] The UK may also wish to consider whether as a result of Brexit it is minded to diverge from the position under EU law in certain respects when on-shoring EU law.

SECTION 8: BLOCKCHAIN AND TAX

Ceri Stoner and Jennifer Anderson, Wiggin LLP

Introduction

Blockchain technology is often looked at from a purely commercial perspective, as a transformative way of exchanging value. What should not be overlooked however is the ability, and perhaps the inevitability, of this transformative technology to revolutionise the tax system.

The digital exchange of value throws up three key tax issues for legal tax practitioners:

- **Taxation of cryptoassets and blockchain**
- **Impact of blockchain on the in-house tax function**
- **Impact of blockchain on tax authorities**

It is crucial that these complex issues are addressed in order to establish a best practice in the tax system which overlays the technology.

As readers will know, blockchain technology is being harnessed to provide a peer-to-peer network for conducting transactions without a third-party intermediary. This is of course achieved by utilising SLCs to embed business logic into a transaction through computer code which automates the logic, i.e. if [x] happens, then [y] follows. This, however, is just the start. Blockchain also provides a neat data store for recording those transactions and a consensus mechanism for validating transactions, thereby limiting fraudulent or false transactions.

The core attributes of blockchain suggest exciting possibilities for the tax world, with the potential to disrupt how transactions are taxed and reported. The following key characteristics of blockchain seem set to shake up long established tax practices:

- **Decentralisation of Control:** transactions amongst multiple parties, who can be identified and authenticated by cryptography.

- **Security:** the digital ledger is more secure, immutable and resilient against disruption than its traditional counterpart. Fraud is less likely (albeit false information can still be entered) and easier to spot.

- **Transparency:** traceable, validated transactions.

- **Real Time Information:** any participant can keep a copy of the ledger and access data.

Taxation of Blockchain

In the UK at present there is no specific legislation or domestic tax case law on cryptoassets or the distributed ledger technology that underpins them, albeit there is some HMRC guidance available and some limited European case law (which is focused on VAT).

The UK tax treatment of any transaction involving blockchain is therefore dependent on general taxing principles. Cryptoassets are just one application of blockchain. However, whilst not all applications of blockchain involve cryptoassets, the utilisation of blockchain in this particular context has been an area of primary focus for HMRC. Consequently, this section will focus primarily on the taxation of cryptoassets.

As ever, it is a question of substance over form, and consequently the labelling of any cryptoasset or transaction in, or in relation to it will not of itself determine the tax treatment. Rather, the tax treatment will be dependent on three primary factors:

- First, the legal nature of the assets created. The categorisation of the cryptoasset for tax purposes will inevitably dictate its tax treatment – for example, whether it is deemed to be a tangible or intangible, a security or civil asset will fundamentally alter how it will be taxed.

- Second, the substance of the transaction, i.e. whether at any given moment there is a taxable event in relation to the cryptoasset and if so, categorisation of its nature. For example, is it best analysed as income or capital? Is it taxed on conversion and/or on sale? How will volatility in the value of a cryptoasset be dealt with – will it be taxable without realisation? Will losses be deductible?
    - It is worth noting that in many cases, the nature of blockchain means that each transaction stage is capable of being splintered into many more. For example, in the context of cryptocurrencies one could question exactly when code modification creates a new asset for tax purposes. Is this when there is a hard fork, i.e. a change to a protocol that invalidates earlier versions, creating a 'new' asset with similar basic code but not equivalent characteristics to the old? Could or should the definition of 'new' asset be stretched to a soft fork, a gentler change which is more analogous to an upgrade? What would be an appropriate method to assess the fair value of a cryptoasset at any stage in the process?

- Third, how the UK's existing tax framework overlays the above, taking into account the legal nature of the entities involved, whether individuals, corporate entities or other.

All of this is an area of live and lively debate. Tax professionals are on notice that HMRC are aware and seeking to deepen their understanding of blockchain technology.

HMRC Perspective on the Legal Nature of Cryptoassets

The question of how to fairly tax a cryptoasset is multi-faceted and, as indicated above, in the first instance it pivots on the definition of a cryptoasset.

HMRC do not consider a cryptoasset to be a form of money or currency. From a tax perspective, the term 'cryptoasset' is defined by HMRC[198] as "cryptographically secured digital representations of value or contractual rights that can be transferred, stored and traded electronically". This definition differs subtly but significantly from the legal analysis of a 'cryptoasset' endorsed by the UKJT of the LawTech Delivery panel, which found there to be no transfer as such but the cancellation of one asset and creation of another. The UKJT proposed in its Legal Statement[199] that the process of transfer in this context is not analogous to the delivery of a tangible object or assignment of a legal right. Whilst the Legal Statement does not have the force of law, it seems likely that it will carry weight in UK courts and tribunals. Any divergence of the legal and tax perspectives on this needs to be addressed and clarified as a matter of urgency.

On a global level, the tax treatment of cryptoassets has been further complicated to date by differing tax treatments in different jurisdictions.

The consistent application of agreed principles is required in order to avoid discrepancies and double taxation of cryptoassets and blockchain more generally. This will require a greater degree of consensus on a national and international level.

[198] HMRC, *Cryptoassests: Tax for Individuals* (Policy paper, updated December 2019) <https://www.gov.uk/government/publications/tax-on-cryptoassets/cryptoassets-for-individuals> Accessed June 2020
[199] UKJT Legal Statement (n 4)

Returning to the UK, the government's Cryptoasset Taskforce (comprised of HM Treasury, FCA and Bank of England) has recognised three types of cryptoassets since October 2018:[200]

1. **Exchange Tokens:** used as a method of payment. HMRC observes that, typically, there is no person, group or asset underpinning these, instead the value exists based on its use as a means of exchange or investment. They do not provide any rights or access to goods or services.

2. **Utility Tokens:** provide the holder with access to specific goods or services, typically on a blockchain platform. HMRC observes that the person or persons issuing the tokens normally 'commit to accepting the tokens as payment for the particular goods or services in question'.

3. **Security Tokens:** provide the holder with specific rights or interests in a business, for example in the nature of debt due by the business or a share of profits in the business.

Substance of transaction

In the view of the Cryptoasset Taskforce,[201] a transaction where a cryptoasset is given or received by way of consideration is a transaction effected for non-monetary consideration (in most cases) – a barter transaction. Cryptoassets are therefore perceived by HMRC as a means of exchange, functioning as a decentralised tool to enable the buying and selling of goods and services, or to facilitate regulated payment services.

The Cryptoasset Taskforce's final report also recognised that cryptoassets are used for direct investment, with firms and consumers gaining direct exposure by holding and trading cryptoassets, or indirect exposure by holding and trading financial instruments that reference cryptoassets.

Finally, the role of cryptoassets in supporting capital raising and/or the creation of decentralised networks through Initial Coin Offerings (**ICOs**) was also acknowledged.

It was recognised that each type of cryptoasset, i.e. exchange tokens, security tokens and utility tokens, could be used in each of the above ways.

UK Tax System

Application of the UK's Existing Tax Framework

In the absence of specific legislation, the tax treatment of cryptoassets and other blockchain based transactions will need to be worked through within the framework of the existing tax system, based upon HMRC's view of the legal nature of cryptoassets and substance of transactions. This should in theory lead to the correct: income and capital treatment; application of transfer taxes and VAT; and withholding taxes and tax credits. But for a theory to be right, it must work in practice.

HMRC guidance to date has focused on the UK tax treatment of cryptoassets and transactions in or involving cryptoassets (focussing primarily on exchange tokens in each case) both for individuals and businesses. In broad terms, HMRC advocates that the nature of the cryptoassets and the purpose for which they are held will dictate the tax treatment.

On an individual level, HMRC takes the view that since individuals tend to hold cryptoassets for personal investment purposes in the majority of cases, they will usually be liable to pay capital gains tax when

[200] Cryptoassets Taskforce report (n 181)
[201] Ibid

they ultimately dispose of their cryptoassets. Income tax and national insurance contributions (**NICs**) on cryptoassets will however arise in certain circumstances, i.e. where individuals receive the cryptoassets from:

- their employer as a form of non-cash payment;
- mining, transaction confirmation or airdrops.[202]

With this in mind, the general application of the existing tax framework is summarised below in high-level terms. This summary is based upon HMRC guidance which, for tax purposes, sets out the key considerations for advisors.

Income Tax and withholding **taxes**

Cryptoassets as non cash remuneration

Where cryptoassets are given by an employer to an employee, as non-cash remuneration, these will constitute 'money's worth' and are therefore generally subject to income tax and NICs.

In order to ascertain whether or not an employer needs to operate pay as you earn (**PAYE**), it needs to be determined whether the cryptoassets in question are Readily Convertible Assets (**RCAs**) or not. According to HMRC guidance, HMRC considers that "*exchange tokens like bitcoin can be exchanged on one or more token exchanges in order to obtain an amount of money. On that basis, it is HMRC's view that 'trading arrangements' exist [for the purposes of determining whether the tokens are Readily Convertible Assets] or are likely to come into existence at the point cryptoassets are received as employment income"*".

If not RCAs then "*the employer should treat the payment [of the cryptoassets] as being a benefit in kind and pay and report any Class 1A National Insurance contributions arising to HMRC*". The employee himself will then report and pay any income tax to HMRC that is due on the value of the cryptoasset received.

Airdrops of cryptoassets

An airdrop occurs where an individual is selected to receive an allocation of tokens or other cryptoassets automatically, for example, as part of a marketing or advertising campaign. In these circumstances, income tax may apply. If an airdrop is received in exchange for provision of services, then the cryptoassets are also likely to be liable to income tax as either miscellaneous income or receipts of an existing trade. However, this will not always be the case, for example, where cryptoassets have been received without the individual having provided anything in return or not as part of a trade or business involving cryptoassets. As such, the precise nature of the airdrop needs to be considered when assessing its tax status.

Trading in cryptoassets

HMRC guidance makes it clear that in most cases, cryptoassets will be held as investments. It considers that it is only in exceptional circumstances that it anticipates individuals will buy and sell cryptoassets with such frequency, organisation and sophistication to cause the activity to amount to a financial trade in itself.[203] To the extent that the individual is considered to be conducting a trade then income tax would apply to trading profits (or losses) in the usual way.

Capital Gains Tax

As noted above, HMRC considers that cryptoassets are typically held as personal investments and, as such, will attract capital gains tax on disposal on any gains realised. While intangible assets,

[202] HMRC policy paper on tax for individuals (n 198)

[203] Ibid

cryptoassets constitute ‘chargeable assets’ for capital gains tax purposes if they are both capable of being owned and have a value that can be realised.

Whilst further guidance would be welcome, HMRC has indicated that in the context of cryptoassets, a ‘disposal’ will include:

- selling cryptoassets for money;
- exchanging cryptoassets for a different type of cryptoasset;
- using cryptoassets to pay for goods or services; and
- giving away cryptoassets to another person.[204]

It should, however, be noted that this is a non-exclusive list.

On disposal, any consideration will be reduced by the amount already subject to income tax charged on the value of tokens received (as HMRC guidance has confirmed that section 37 Taxation of Capital Gains Act 1992 will apply in a crypto context).

In addition, HMRC guidance requires cryptoassets to be pooled under section 104 Taxation of Capital Gains Act 1992 when calculating a chargeable gain or an allowable loss for capital gains tax purposes on the basis that they fall within the sweeper provision in that section and qualify as “any other assets where they are of a nature to be dealt in without identifying the particular assets disposed of or acquired”. The application of these rules also applies in a corporate context.

Corporation Tax

As noted above, HMRC does not consider cryptoassets to be money or currency. As such, any corporation tax legislation relating exclusively to money or currency does not apply to cryptoassets.[205]

Typically, for the purposes of corporation tax, HMRC prescribes that "if the activity concerning the exchange token is not a trading activity, and is not charged to Corporation Tax in another way (such as the non-trading loan relationship or intangible fixed asset rules) then the activity will be the disposal of a capital asset and any gain that arises from the disposal would typically be charged to Corporation Tax as a chargeable gain".[206]

As provided above for capital gains tax, exchange tokens in HMRC’s eyes count as a ‘chargeable asset’ for corporation tax if they are both capable of being owned and have a value that can be realised. It follows that if a company holds exchange tokens (or, presumably, other forms of cryptoasset) as an investment, they should be liable to pay corporation tax on any gains they realise when they dispose of it.

It is worth noting that, for corporation tax purposes, the "rules for intangible fixed assets[207] have priority over the chargeable gains rules".[208] As a result, companies that account for exchange tokens as ‘intangible assets’ may be taxed under the UK’s corporation tax rules for intangible fixed assets if the token is both an ‘intangible asset’ for accounting purposes and an ‘intangible fixed asset’, i.e. created or acquired by a company for use on a continuing basis.

There are further specific exclusions for financial assets, non-commercial assets and assets that derive rights or value from certain excluded assets (such as tangible assets, rights in companies, trusts, partnerships).

[204] Ibid

[205] HMRC, *Cryptoassets: Tax For Businesses* (policy paper, updated December 2019) <https://www.gov.uk/government/publications/tax-on-cryptoassets/cryptoassets-tax-for-businesses#corporation-tax> Accessed June 2020

[206] Ibid.

[207] Corporation Tax Act 2009, Part 8

[208] HMRC policy paper on tax for businesses (n 205)

As for other assets, if a business disposes of exchange tokens (and potentially other forms of cryptoasset) for less than their allowable costs, they will have a loss. Certain ‘allowable losses’ can be set off against other income so as to reduce overall gain, however, such losses must be reported to HMRC first.[209] Also, in the same way as for other assets, businesses can also crystallise losses for exchange tokens (and potentially other forms of cryptoassets) that they still own if they become worthless or of ‘negligible value’. When reporting the loss to HMRC, a negligible value claim can also be made at the same time. This treats the exchange tokens/cryptoassets as being disposed of and re-acquired at the amount stated in the claim. As noted above for capital gains tax, exchange tokens are pooled. This means that any negligible value claim should be made in respect of the whole pool, as opposed to only the individual tokens.[210]

Transfer Taxes

The application of transfer taxes, such as stamp duty and stamp duty reserve tax, to cryptoassets themselves is assessed on a case by case basis, depending on the nature and characteristics of the cryptoasset in question.

There is some inconsistency between different HMRC guidance on the topic. However, HMRC’s view in its latest policy paper is that exchange tokens and utility tokens are unlikely to meet the definition of ‘stock or marketable securities’ or ‘chargeable securities’ for the purposes of stamp duty or stamp duty reserve tax, although a security token may, depending on its precise characteristics and transfer, be subject to either of these transfer taxes.

This leaves the question of whether cryptoassets could themselves form the consideration for purchases of ‘stock or marketable securities’ and/or ‘chargeable securities’ for the purposes of transfer taxes.

By way of best practice in this context, HMRC provides that: "*If exchange tokens are given as consideration, this would count as ‘money’s worth’ and so be chargeable for Stamp Duty Reserve Tax purposes. Tax will be due based on the pound sterling value of the exchange tokens at the relevant date.*"[211] This logic could potentially extend to all cryptoassets, depending on their specific terms.

The same is considered true if exchange tokens were given as consideration for a land transaction in which instance they would be deemed to be ‘money or money’s worth’ and therefore chargeable to stamp duty land tax.

The position in respect of stamp duty differs, however. HMRC guidance suggests that exchange tokens – and therefore by extension all cryptoassets – are not considered to meet the definition of ‘money’ in the context of stamp duty consideration. This is the logical conclusion to HMRC’s position that cryptoassets are neither money nor currency.

VAT

HMRC guidance provides that "*VAT is due in the normal way on any goods or services sold in exchange for cryptoasset exchange tokens. The value of the supply of goods or services on which VAT is due will be the pound sterling value of the exchange tokens at the point the transaction takes place.*"[212]

VAT (as applied in the UK) is the only tax that has received any judicial consideration to date in its application to transactions in or involving cryptoassets. The results of case law in relation to the application of VAT to cryptoassets[213] have been incorporated into HMRC guidance as follows:

[209] Ibid

[210] Ibid.

[211] Ibid

[212] Ibid

[213] For example, cases: C-264/14, *Skatteverket v David Hedqvist* [2015] EU:C:2015:718; and C-172/96, *Commissioners v First National Bank of Chicago* [1998] I-04387

- "exchange tokens received by miners for their exchange token mining activities will generally be outside the scope of VAT on the basis that:
    - the activity does not constitute an economic activity for VAT purposes because there is an insufficient link between any services provided and any consideration; and
    - there is no customer for the mining service.
- when exchange tokens are exchanged for goods and services, no VAT will be due on the supply of the token itself.
- charges (in whatever form) made over and above the value of the exchange tokens for arranging any transactions in exchange tokens that meet the conditions outlined in VAT Finance manual (VATFIN7200), will be exempt from VAT under Item 5, Schedule 9, Group 5 of the Value Added Tax Act 1994."[214]

It should be noted however that here 'best practice' has a temporary aspect to it since the treatments outlined above are provisional pending further developments, most notably in respect of the regulatory and EU VAT positions.

The VAT treatment of transactions in or involving cryptoassets that are not exchange tokens depends on the precise nature of the cryptoasset. It is generally anticipated that transactions in or involving security tokens may, depending on their precise characteristics, be treated in the same way as transactions in or involving shares or securities. A utility token, depending on its precise characteristics, may be more likely to be treated as a voucher for VAT purposes.

Impact of Blockchain on In-House Tax Function

This section would not be complete without briefly touching upon the potential impact of blockchain on in-house tax functions.

Compliance, in terms of reporting and disclosure, is generally one of the primary purposes of the in-house tax function. One of the greatest challenges for the modern tax function is the increasing demand for data from tax authorities across the globe, to be delivered at an ever-increasing speed. Blockchain could help organisations manage the scale and ever tightening reporting deadlines in respect of the data required.

Historically, tax functions have struggled to access the full spectrum of information they need to structure, plan and report for tax purposes across their business. As a result, it is arguable that tax functions have been consulted too late, or not at all, on issues and decisions that have tax implications. Blockchain has increased the ability of organisations to capture and collate enormous amounts of data, both internal and in respect of its customers and suppliers. Having the information shared in real-time with the tax function could propel it to a role of greater prominence, closer to the heart of the decision-making process, rather than at the periphery.

Impact of Blockchain on Tax Authorities

Finally, blockchain technology certainly has the potential to underpin a more streamlined, efficient and reliable tax system. A distributed ledger that allows anything of value to be traded securely, transparently and without the risk of tampering could be invaluable to tax authorities looking to fill the tax gap, i.e. the difference between the amount of tax that should, in theory, be paid and what is actually paid.

[214] HMRC policy paper on tax for businesses (n 205)

Blockchain technology could significantly contribute towards the efficient collection of revenue by tax authorities, i.e. maximum revenue collection for minimum cost. It is widely reported that digital collection methods are cheaper for tax authorities to operate than analogue methods. For example, an Australian government survey concluded that the same service could be provided for $1 digitally as against $16 by phone, $32 by post, or $42 in person.[215]

Ultimately, this is likely to be a question of balance, i.e. of maximising revenues without stifling growth, of lowering the collection costs for tax authorities without placing an unbearable compliance cost on the taxpayer. Tax authorities when exploring the uses of blockchain technology in the compliance sphere must endeavor to get this balance right or they risk lowering medium- or long-term tax revenues.

Blockchain technology however has the capability to deliver real-time, reliable information to a wide demographic, and the potential to create a bespoke system where both taxpayers and tax authorities have equal confidence in the veracity of the data collected. Before the introduction of digitalised tax systems, most administrations worked off taxpayers returns, and information gained from third parties (such as employers) to review accuracy. With the pre-population of information in a digitised world, the information flow is inverted.

Consequently, in time, it could lead to the earlier collection of taxes and, additionally, ultimately assist tax authorities in exchanging information between jurisdictions.

Furthermore, there are arguments that tax morale, the citizen’s opinion regarding paying their taxes, is increased by digitalisation and a correlation exists between tax morale and tax compliance. Technologists argue that from the taxpayer’s perspective, a digitalised tax system is seen as fairer, reducing scope for human error and subjectivity.

However, there are a number of barriers to the full exploitation of blockchain in a tax compliance context that need to be addressed in order to enable a successful implementation. These include:[216]

- **Digital exclusion:** this is the largest, most persistent issue and includes generational differences, varying beliefs and also temporary issues, such as natural disasters.

- **Cost and complexity:** the short-term investment costs necessary in order to adopt new technology may be prohibitive in some areas.

- **Security and privacy:** whilst the security of blockchain is often cited, any system is of course open to abuse and there will inevitably be questions as to corporate and personal privacy.

- **Legacy systems: o**lder systems (analogue and digital) contain vast amounts of vital data that should ideally be integrated and retained.

- **Future proofing:** proofing against changes in technical capabilities and standards will be crucial in order to validate the initial investment to adopt such technology in the first place and for it to remain relevant.

- **Mission creep:** as the digital goals are broken down into steps and developments in the sphere of cryptoassets continues, there is a risk that unplanned and unsustainable long-term commitments may be made.

- **Limitations of digitalisation:** in certain cases digitalisation will not be appropriate, nuances may be missed, and a digitised approach may not be capable of facilitating certain judgement calls.

[215] ICAEW Tax Faculty, 'Digitalisation of Tax: International Perspectives' (2019 edition) <https://www.icaew.com/-/media/corporate/files/technical/information-technology/thought-leadership/digital-tax.ashx> Accessed July 2020
[216] Ibid

- **Legislative basis:** it will be vital to establish a proper legal basis for the collection of data and use of data.

Existing HMRC Guidance

- HMRC Manuals: these provide limited guidance relating only to bitcoin and similar cryptocurrencies:
  - HMRC VAT Manual: VATFIN 2330[217], discussing *Hedquist*[218] and *First National Bank of Chicago*[219].
  - HMRC Capital Gains Manual: CG 12100.[220] This covers the nature of transactions, the 'pooling' rules and 'forks'.
- HMRC Policy Paper: Tax on Cryptoassets (published December 2018, superseding Revenue & Customs Brief 9/2014).[221]
- HMRC Policy Paper (19 December 2018) (Cryptoassets for individuals).[222]
- HMRC Policy Paper (Cryptoassets: tax for businesses).[223]
- HMRC Cryptoassets Taskforce: final report.[224]

[217] Available at <https://www.gov.uk/hmrc-internal-manuals/vat-finance-manual/vatfin2330> Accessed June 2020

[218] Case C-264/14 (n 213)

[219] Case C-172/96 (n 213)

[220] Available at <https://www.gov.uk/hmrc-internal-manuals/capital-gains-manual/cg12100> Accessed June 2020

[221] HMRC, 'Tax on Cryptoassets' (Policy paper, published 19 December 2018, updated December 2019) <https://www.gov.uk/government/publications/tax-on-cryptoassets#ct-it-and-cgt-treatment-of-bitcoin-and-similar-cryptocurrencies> Accessed June 2020

[222] HMRC policy paper for tax on individuals (n 198)

[223] HMRC policy paper on tax for businesses (n 205)

[224] Cryptoassets taskforce report (n 181)

ANNEX 1: OVERVIEW OF DLT

Tom Grogan, Mishcon de Reya LLP

1) Introduction

The term DLT refers to a broad umbrella of technologies that seek to store, synchronise and maintain digital records across a network of computing centres.

The concept of maintaining a ledger is certainly not a new one. The earliest ledgers date back to c.4,000BC in Mesopotamia. These ledgers were kept on clay scripts or carved into stone and were used to record and demonstrate definitive ownership, and the transfer of ownership, of crops in storage. Recording the ownership and movement of value has been a central tenet of human civilisation ever since. The form and structure of these ledgers however has evolved (and continues to evolve) with time.

The Mesopotamian example given above describes what we now call a centralised ledger (see Fig 1 below). Centralised ledgers are the definitive and only record within an ecosystem. In many circumstances, such a centralised ledger is effective and in many instances remain in use today. Centralised ledgers do however have some drawbacks. Notably, they have a single point of failure (i.e. the single ledger). If the ledger is lost, stolen or attacked (i.e. tampered with by a third party), the ecosystem and its participants (i.e. those placing reliance on the definitive nature of the ledger's record keeping) will fail. Clearly, as an ecosystem becomes more complex and its value rises, the use of a centralised ledger will become less appropriate.

As civilisation has developed, so too has the use of decentralised ledgers become more prevalent (see Fig 1 below). In modern society, we often rely on trusted intermediaries to keep and maintain common digital record repositories. These intermediaries may for example be financial institutions, which keep and maintain records relating to our finances, or social networks, which keep and maintain records of our photographs, status updates and music. Decentralised ledgers, just like their centralised cousins, are widely used today but do also have their own drawbacks. They too have points of failure which impact the wider ecosystem – see for example the damage caused when a financial service provider's IT infrastructure suffers an outage. They also rely heavily on the trustworthiness and integrity of the intermediary maintaining the decentralised ledger – if the ledger is the target of an attack, the ecosystem participants who fall victim to it may have limited recourse.

Distributed ledgers seek to avoid the drawbacks associated with centralised and decentralised ledgers by, amongst other things, removing points of failure (see Fig 1 below). Distributed ledgers see the ledger (or parts of the ledger) replicated and stored across a network of computing centres. This network of computing centres, known as nodes, work to update the ledger as new updates (i.e. transactions) arise, and propagate the updated ledger to the network. Distributed ledgers are, theoretically, infinitely scalable, and by distributing their control and maintenance, seek to mitigate against the risk of attack.

In this Annex 1, we use the term cryptoassets loosely to mean an asset of whatever kind that is represented digitally on a DLT platform. Such assets might exist purely digitally, for example a so-called cryptocurrency such as Bitcoin (BTC), or physically, for example a piece of real estate that is represented by way of tokenisation. This Annex 1 distinguishes between cryptoassets which, in line with the UKJT Legal Statement, we hold to be capable of constituting property as a matter of English private law, and records, which we typically consider to be pure data and therefore not capable of constituting property as a matter of English private law.

In this Annex 1 we also refer to wallets. Again, we use this term broadly to mean the digital device which is used to store a user's public and private keys, which are used to manage and control the user's DLT-stored records and/or cryptoassets. Please see (2) below for details regarding the purpose and functionality of public and private keys in the context of DLT systems.

DLT is a rapidly evolving area of computer science and its implementation at scale remains nascent. The limitations of this Annex 1 therefore are acknowledged and accepted. This Annex 1 does not seek to provide an exhaustive and detailed explanation of DLT. Rather, it seeks to: (i) identify and accessibly set out some of the key characteristics of DLT; (ii) explore the mechanisms by which some distributed ledgers create, amend and replicate their digital records; and (iii) provide brief, indicative examples of certain DLT.

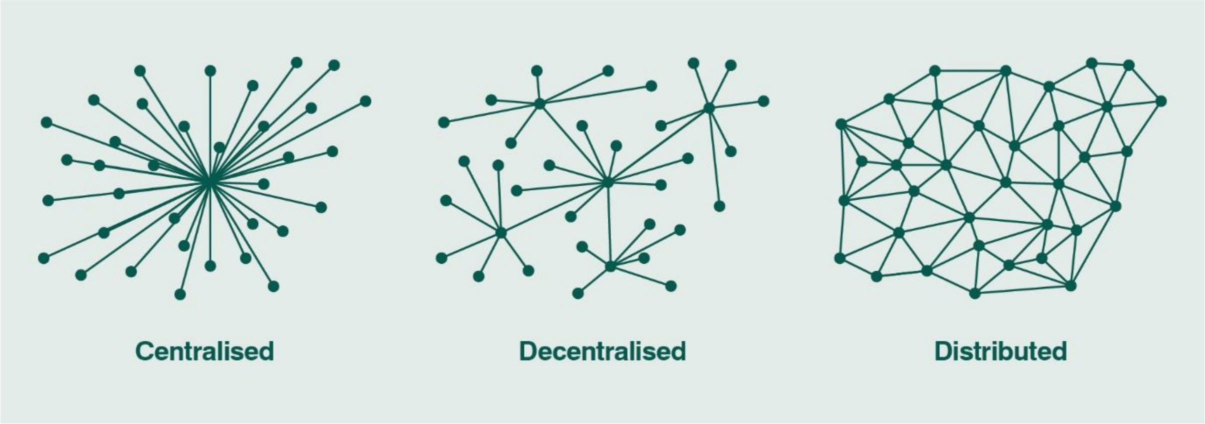


Fig 1 – Centralised, decentralised, and distributed ledgers. NB the structures of these ledgers, in particular the distributed ledger, have been simplified for illustrative purposes.

2) Key features of DLT

A series of mechanisms and computer protocols dictate how distributed ledgers work – namely, how their network participants may create, amend and synchronise records held on them. These mechanisms and computer protocols typically seek to:

- enable network participants to **exclusively** control 'their' records or cryptoassets;
- maintain a clear **chronology** of distributed ledger entries; and
- provide a mechanism by which network participants will reach a **consensus** as to new distributed ledger entries and the state of the distributed ledger from time to time, thereby ensuring a common, synchronised ledger.

These three components represent key features of DLT. Each of them are explored below in more detail.

Exclusivity

To enable network participants to exclusively control 'their' records or cryptoassets, any (indeed, at the time of writing, most) DLT implementations utilise public key cryptography.

Public key cryptography is a cryptographic system that uses two types of information (typically a fixed length string) known as keys:

- **public keys**: these may be widely disseminated and known to some or all other network participants; and

- **private keys**: these should be known only to the relevant network participant.

If a network participant wishes to send a message (or, in the case of cryptoassets, make a transaction), they would enter their message (or transaction details) together with the intended recipient's public key (or a hash of the intended recipient's public key, known as a wallet address).

The network participant who is sending the message (or transaction) then 'signs' the message (or transaction) using their private key. The recipient and the wider network is then able to verify that the message (or transaction) is genuine, by entering the public key of the network participant who sent the message (or transaction). When combined, the message (or transaction) will (provided the public key entered is indeed associated with the private key used to send the message or transaction) be decrypted.

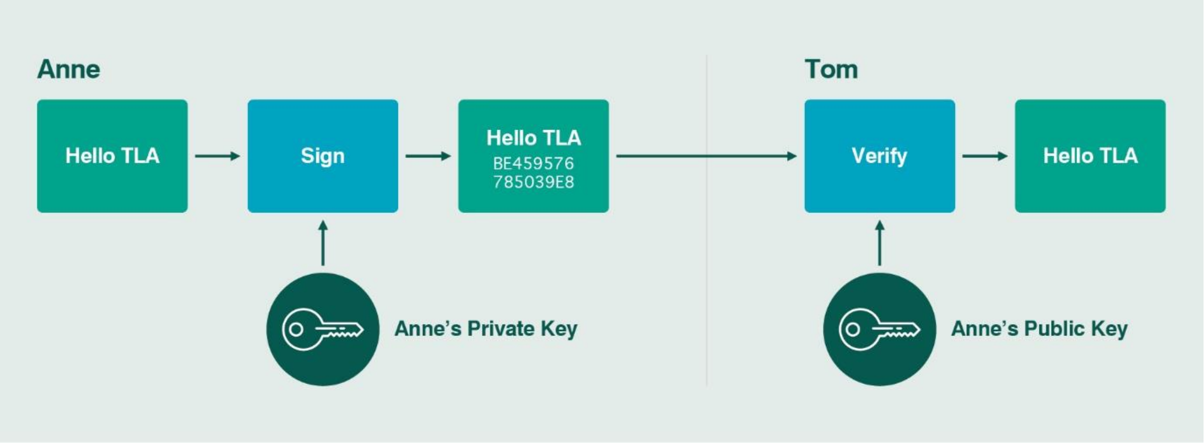


Fig 2 – Public key or asymmetrical cryptography-enabled messaging

Public key cryptography is also known as asymmetrical cryptography. This is because a message (or transaction) which was encrypted using the sender's private key, can be decrypted using the sender's public key, without revealing or compromising the security of the sender's private key.

An important conceptual point to grasp is that wallets do not contain records or cryptoassets. All that is contained in a wallet is a private key. Accordingly, when we make a new record or transaction on a distributed ledger, we do not 'send' records or cryptoassets *per se*, rather we send a message or transaction to the network's nodes, which then update their respective copies of the ledger accordingly.

DLTs therefore enable exclusive ownership of records and cryptoassets by ensuring that the right to send messages (or make transactions) on behalf of a public key relies on a private key, which is capable of being kept secret and known only to a single individual. In this way, an individual can be said to 'own' (albeit indirectly) certain cryptoassets.

Chronology

One of the key challenges that faces a distributed ledger is how to establish a clear chronology of records or transactions. As the network becomes larger and more distributed across territories and time zones, so too does the so-called Distributed Ledger Problem become more pronounced.

The Distributed Ledger Problem

Records and transactions are passed from node to node within the network, and therefore the order in which transactions reach each node can differ.

For example, say an attacker has a wallet holding 1 TLA Coins (a fictional cryptoasset used for illustrative purposes only). Exploiting the Distributed Ledger Problem, the attacker may make a purchase from a supplier of goods and send 1 TLA Coin to the supplier as payment. The attacker would then wait for confirmation that the supplier has shipped the goods. Once the attacker has received the confirmation, he or she would then send a transaction to another of his wallets for 1 TLA Coin. Due to the Distributed Ledger Problem, some nodes might receive the second transaction before the first. Those nodes would then consider the initial transaction invalid, as the transaction inputs would be marked as already spent. If sufficient nodes to satisfy the distributed ledger's consensus protocol believed the second transaction to be the 'true' transaction, the transfer of TLA Coin to the supplier would be rejected and the supplier, having already shipped the goods, would be out of pocket.

The way in which DLTs establish a clear chronology of records and transactions is typically determined by the manner in which their ledger dataset is structured. This varies from DLT to DLT – see (4) below for some high level examples of different forms of DLT.

Consensus

Each DLT node has its own view of the state of the distributed ledger at a given time. The result of this, exacerbated by the Distributed Ledger Problem set out above, is that, at any one time, there may be as many views of the present state of the ledger as there are nodes in the network.

Distributed ledgers implement clear rules to enable their constituent nodes to reconcile differences and record messages and transactions in a harmonious fashion. These rules are known as consensus protocols. There are a number of 'flavours' of consensus protocols, each with their own trade-offs that in turn impact on the distributed ledger's performance and functionality. See (3) below for some high level examples of consensus protocols.

3) Consensus protocols

There a range of different consensus protocols which might be adopted by DLTs. The following is a very high-level overview of two well-known examples: proof of work, and proof of stake.

Proof of work

Proof of work requires participating nodes (known as "miners") to prove that computational resource has been committed before a record of transactions can be accepted as part of the distributed ledger. Proof of work is perhaps the best-known example of a consensus protocol and is used by the Bitcoin (BTC) blockchain.

In order to prove their commitment of computational resource, miners 'race' to solve a computational puzzle which is designed to require a large number of computational steps without shortcuts. Once solved, the successful miner can broadcast the answer to the puzzle to the DLT's node network, which can then easily and quickly verify the answer as being correct and thus accept the new entry to the ledger. Most DLTs require a majority of nodes to verify the puzzle answer in order to accept the entry of the new records or transactions to the ledger. Typically, in DLTs that use proof of work, mechanisms are built in to reward and incentivise miner activity.

Proof of work's advantages include that it is secure (subject to a well distributed network of computing power), it deters spam (by requiring miners to expend effort in order to successfully enter new ledger entries), and it is democratic (as the same puzzle is posed to all miners). It has however been criticised for being, amongst other things, relatively slow, expensive (owing to the hardware required to give miners a reasonable prospect of success, which undermines its democratic credentials), and environmentally unfriendly (owing to the energy consumption associated with mining activity).

Proof of stake

Proof of stake requires each node that seeks to update the ledger to prove that it has a 'stake' in the system. Proof of stake is a well-known consensus protocol that it has long been suggested that the Ethereum blockchain will adopt. The Ethereum Foundation, a non-profit organisation dedicated to supporting Ethereum and other technologies, had targeted January 2020 as the date on which the Ethereum blockchain would adopt proof of stake, but this date has now passed. Though the Ethereum Foundation maintains its intention to adopt proof of stake, at the time of writing it is unclear as to when (and whether) such adoption will take place. Other well-known implementations of proof of stake include Stellar, DASH and NEO.

In order to establish a new ledger entry, competing nodes (known as validators) construct a particular type of transaction that 'locks-up' their funds in a form of deposit. Validators then take turns proposing and voting on the next ledger entry. The weight of each validator's vote is proportionate to the size of its lock-up. If the majority of validators reject a proposing validator's ledger entry, the proposing validator loses its lock-up.

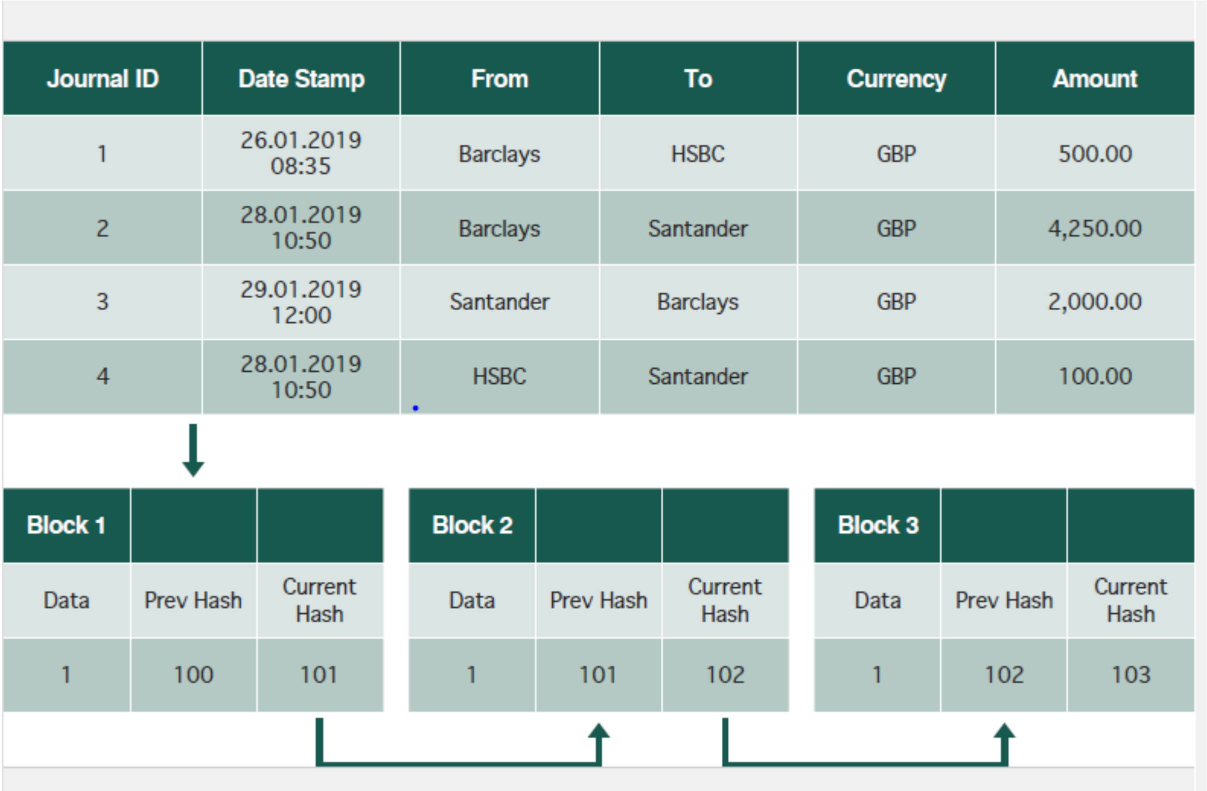
In addition to deterring validators from proposing fraudulent new entries (for fear of losing their lock-up), proof of stake DLTs also ensure that the state of their ledger is dictated by those invested in them – those investors will wish to ensure the integrity of the ledger as, if doubt is cast upon it, the value of the DLT (and in turn the investor's investment) will diminish. Other advantages of proof of stake include that it is quicker and more energy efficient than some other consensus protocols (such as proof of work). Disadvantages of proof of stake include that is more difficult to secure and can be seen as undemocratic.

4) Examples of DLT

Blockchain

The best-known example of a DLT, blockchain rose to prominence on the publication of the Bitcoin whitepaper in 2008 under the pseudonym Satoshi Nakamoto. Blockchains bundle digital records into data container structures known as blocks. These *blocks* are appended to the end of a *chain* of blocks in chronological order, hence the name.

Typically, each block in a blockchain will contain a hash of the preceding block. This ensures that a clear irrefutable chronology is established and maintained.



Journal ID	Date Stamp	From	To	Currency	Amount
1	26.01.2019 08:35	Barclays	HSBC	GBP	500.00
2	28.01.2019 10:50	Barclays	Santander	GBP	4,250.00
3	29.01.2019 12:00	Santander	Barclays	GBP	2,000.00
4	28.01.2019 10:50	HSBC	Santander	GBP	100.00

Block 1		
Data	Prev Hash	Current Hash
1	100	101

Block 2		
Data	Prev Hash	Current Hash
1	101	102

Block 3		
Data	Prev Hash	Current Hash
1	102	103

Fig 3 – Blockchain structure

Directed acyclic graphs

Directed acyclic graphs are a well-established branch of graph theory and computer science. They are graphs that travel in one direction without cycles connecting the other edges. The graph uses topological sorting, wherein each node is in a certain order. In the context of DLT however, directed acyclic graphs present an exciting alternative to blockchain database structuring.

The one directional nature of a directed acyclic graph ensures that a clear chronology can be maintained, while the impossibility of 'loops' mitigates against the risk of 'double-spend', which is often associated with distributed ledgers. The consensus protocols typically adopted by directed acyclic graph DLTs prevent against network participants validating their own transactions (save by chance) and can allow for multiple transactions to be simultaneously verified, thereby improving performance.

A well-known example of directed acyclic graphs is IOTA's Tangle.

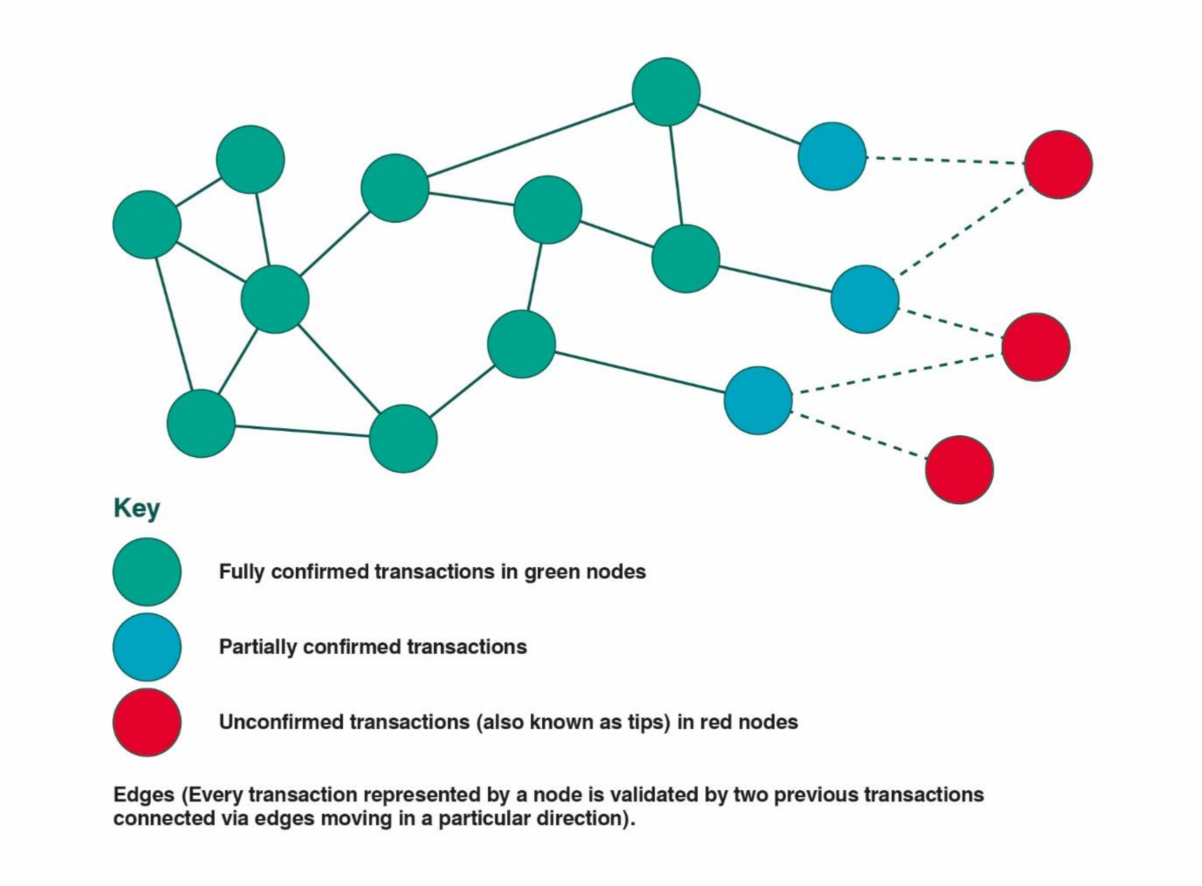

Key
Fully confirmed transactions in green nodes
Partially confirmed transactions
Unconfirmed transactions (also known as tips) in red nodes
Edges (Every transaction represented by a node is validated by two previous transactions connected via edges moving in a particular direction).

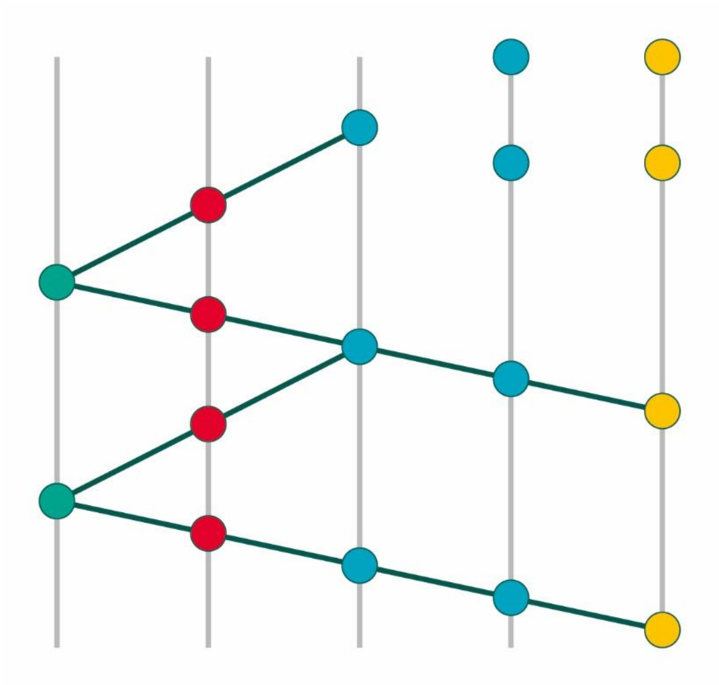
Fig 4 – Directed acyclic graph structure

Hadera Hashgraph

Hadera Hashgraph, better known simply as Hashgraph, is an alternative DLT and close cousin of the directed acyclic graph, developed by Leemon Baird in 2016.

Hashgraph is perhaps best known for its so-called 'gossip protocol', whereby every node spreads 'gossip' regarding its information (i.e. records or transactions, known in Hashgraph as 'events') and events it has heard (via the gossip protocol) from others, to two randomly chosen neighbours (which in turn further propagate the gossip alongside their own events in an aggregated fashion). Chronologies are established using timestamped events.

The advantages of Hashgraph's streamlined consensus mechanism include speed and fairness. An inherent assumption of Hashgraph is that less than a third of nodes are bad actors (i.e. those who forge, delay, replay and drop incoming and/or outgoing events) and therefore, if this is not (or cannot be reliably be proved to be) the case, security concerns may arise. Hashgraph has met some criticism for the proprietary nature of its algorithm which, unlike most public DLTs, is protected by a patent.



Hadera Hashgraph structure

ANNEX 2: MEMBERS OF TLA BLOCKCHAIN LEGAL & REGULATORY GROUP

Members

Akber Datoo, D2 Legal Technology
Alastair Monty, Macfarlanes LLP
Albert Weatherill, Norton Rose Fulbright LLP
Alex Cravero, Herbert Smith Freehills LLP
Alex Murawa, Reed Smith LLP
Alpeshi Doshi, Fintricity
Anna Donovan (Dr.), UCL
Anne Rose, Mishcon de Reya LLP
Ben Sigler, Stephenson Harwood LLP
Birgit Clark, Baker McKenzie LLP
Bret Hillis, Reed Smith LLP
Brian Gray, Brian Gray London
Byron O’Connor, Infinity Works
Callum Sommerton, Mishcon de Reya LLP
Catherine Goodman, Paul Hastings
Catherine Hammon, Osborne Clarke LLP
Ceri Stoner, Wiggin LLP
Cassius Kiani, Atlas Neue
Chantelle Gough, Hill Dickinson LLP
Charlie Cull, University of Cambridge
Charlie Morgan, Herbert Smith Freehills LLP
Charlotte Lyons-Rothbart, Wiggin LLP
Ciáran McGonagle, ISDA
Craig Orr QC, One Essex Court
Daniel Relton, Baker McKenzie LLP
Danielle Murphy, Pinsent Masons LLP
David McCahon, Barclays
David Naylor, Wiggin LLP
David Quest QC, 3 Verulam Buildings Chambers
Dean Armstrong QC, The 36 Group
Eitan Jankelewitz, Sheridans LLP
Estelle Tran, Barclays
Fleur Kitchingman, Herbert Smith Freehills LLP
Gabrielle Tanner, Wiggin LLP
Gary Maw, Irwin Mitchell LLP
Heenal Vasu, Allen & Overy LLP
Howard Womersley Smith, Reed Smith LLP
Ian McKenzie, Osborne Clarke LLP
James Klein, Shoosmiths LLP
Janet Morrison, Hubher
Jason Pugh, D2LegalTech
Jason Rozovsky, R3
Jermaine Paul Smith, Thrings LLP
John Shaw, Blake Morgan LLP
Jonathon Emmanuel, Bird & Bird LLP
Kate Parker, 5 Paper Buildings Chambers
Katie Nagy de Nagybczon, CMS Cameron McKenna Navarro Olswang LLP
Laura Douglas, Clifford Chance LLP
Marc Jones, Stewarts LLP

Marc Piano, Harneys (Cayman Islands)
Marco Dalla Vedova, Dalla Vedova Studio Legale
Martin Fanning, Dentons UKEMA LLP
Martin Hevey, Herbert Smith Freehills LLP
Mary Kyle, City of London
Matthew Farrer, The Alizeti Group
Michelle Howell, Macfarlanes LLP
Nagia Paraschou, Wiggin LLP
Nathalie Hoon, R8 Group
Niall Roche, Mishcon de Reya LLP
Paris Theodorou, Saunders Law LLP
Patrick O'Connell, Wiggin LLP
Paul Glass, Taylor Wessing LLP
Phil Leonard, Waterfront Solicitors LLP
Philip Horler, Withers & Rogers LLP
Philippa Dempster, Freeths LLP
Rachel Amos, The Senate
Richard Folsom, Kemp Little LLP
Richard Hay, Linklaters LLP
Richard Reeve-Young, Kemp Little LLP
Rob Grant, Macfarlanes LLP
Rohana Abeywardana, Hill Dickinson LLP
Rosie Burbidge, Gunnercooke LLP
Sam Quicke, Linklaters LLP
Sian Harding, Mishcon de Reya LLP
Sophie Rance, ASOS
Stephen Carter, K2 IP
Stuart Whittle, Weightmans LLP
Sue McLean, Baker McKenzie LLP
Tara Chittenden, The Law Society
Thomas Hulme, Mackrell LLP
Tom Bleasley, Radcliffe Chambers
Tom Grogan, Mishcon de Reya LLP
Victoria Thompson, Barclays
Will Foulkes, Thrings LLP
William McSweeney, The Law Society
Yasmin Tiyamiyu, SCA Ontier

ANNEX 3: SPECIALIST CONSULTEES

Aaron Wright, Professor, Cardozo School of Law and Co-Founder, OpenLaw
Adi Ben-Ari, CEO, Applied Blockchain
Cassius Kiani, Chief Product Officer, Atlas Neue
Ciaran McGonagle, ISDA
Gary Chu, General Counsel, Fnality International
Professor Michael Mainelli, Executive Chairman, Z/Yen Group
Dr Michèle Finck, Max Planck Institution for Innovation and Competition
Niall Roche, Head of Distributed Systems Engineering, Mishcon de Reya LLP
Nick West, Chief Strategy Officer, Mishcon de Reya LLP
Peter Brown, Group Manager Officer, ICO