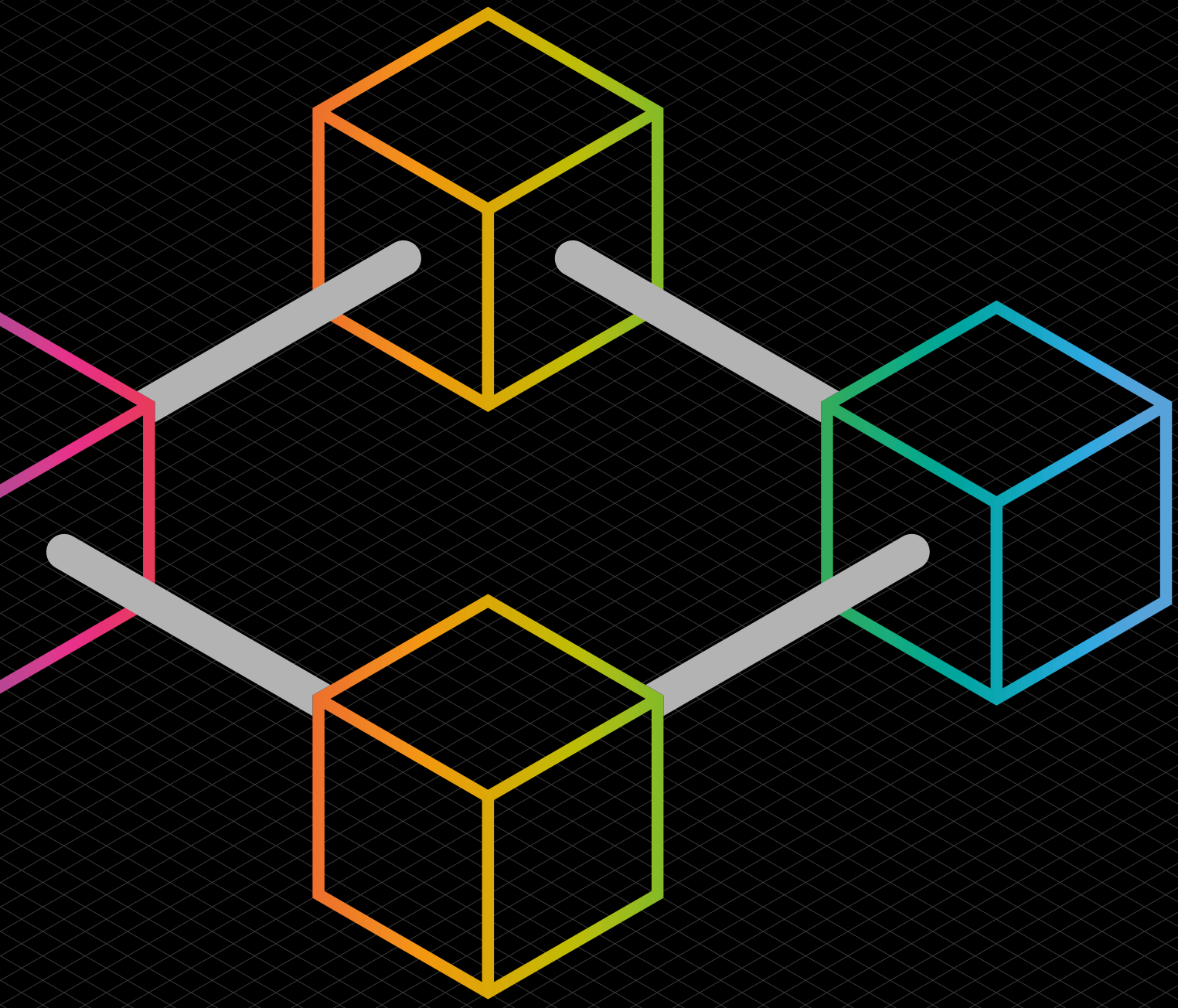
The Law Society

TECH LONDON ADVOCATES
BLOCKCHAIN LEGAL AND REGULATORY

Blockchain: Legal & Regulatory Guidance

Second Edition



Notice

This guidance does not constitute legal advice in any jurisdiction. 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

PART 2:
IMPACTS ON THE WIDER LANDSCAPE

Foreword

Once again, the authors of Tech London Advocates' (TLA) new Blockchain Legal and Regulatory Guidance are to be congratulated.

The Guidance has been massively expanded and updated since its first publication. It is now a comprehensive guide to the legal and regulatory considerations that everyone in the on-chain space needs to understand.

I believe that three major developments are imminent. They will mean that every lawyer will require familiarity with the blockchain, smart legal contracts and cryptoassets – both conceptually and functionally. Those developments are: first, the launch of central bank digital currencies that will put cryptoassets into mainstream use. Secondly, the widespread adoption of digital transferable documentation, and thirdly the transition from analogue programmes, such as Word, to smart machine readable documents.

This Guidance will put lawyers in a far better position to understand how DLT and smart legal contracts are being, and will soon, be deployed in use cases across the financial and industrial sectors. More importantly, it puts English law front and centre as the legal foundation for the blockchain.

TLA's Blockchain Legal and Regulatory Guidance suggests best practice for legal practitioners working in the new technologies. It builds on the UK Jurisdiction Taskforce Legal Statement on Cryptoassets and Smart Contracts published 2 years ago. Anne Rose and her colleagues light the path for lawyers determined to stay ahead of the game.

The Rt Hon Sir Geoffrey Vos, Master of the Rolls

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. It is also central to establishing the UK as an agile, innovative, and digital destination for business.

Our members play a fundamental role in economic growth, stability and attracting business to the UK. In fact, 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,[A] and double productivity growth in the legal sector. 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.[B]

The pandemic has incentivised businesses 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. For the benefits of technology to be unlocked, the awareness and capabilities of lawyers should be built. Distributed Ledger Technology, smart legal contracts and cryptoassets will likely form the infrastructure of the digital economy and basis for future transactions, which lawyers will continue to advise on.

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 the jurisdiction of England and Wales is flexible and able to adapt to new technologies and new types of assets.

The second edition of the Blockchain Legal and Regulatory Group provides an updated framework and much needed guidance on the use of blockchain in the legal services sector.

I. Stephanie Boyce, President of The Law Society

A Analysis available from The Law Society on request
B 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

The Guidance

Welcome to this revised and expanded second edition, which updates the 2020 guidance.

Over the past 18 months commercial and technological developments, accelerated by COVID-19, have seen a proliferation in the use and evolution of distributed ledger technology (DLT) such as blockchain. Alongside well-known cryptoassets such as the cryptocurrency Bitcoin, DLTs increasingly offer opportunities to build new platforms, products and protocols, from non-fungible tokens (NFTs) and stablecoins to increasing research and experimentation around Central Bank Digital Currencies (CBDCs) and a growth in decentralised finance (DeFi). And new regulations and legislation are being introduced to catch up and keep pace.

At the same time, lawyers are increasingly assuming the role of 'project managers', working with various technological experts and specialists. They need to be aware not only of how network technology and other code-based technologies operate, but how these technologies impact on the wider areas of litigation, including how decentralisation and smart contracts are changing the very way financial, property and legal services are carried out.

As the complexity of DLT grows so does the need for lawyers to understand it. This guidance aims to provide a useful stepping-stone in this process, and we hope it will be useful not only to lawyers but to all those working in this landscape, including technologists and academics.

Who wrote this guidance?

The Tech London Advocates (TLA) Blockchain Legal and Regulatory Group (the Group) was founded in 2019 by Anne Rose (Mishcon de Reya LLP) as a sub-group of TLA's dedicated Blockchain Working Group. TLA was founded in 2013 by Russ Shaw to give an independent voice to the technology sector and comprises a network of more than 10,000 tech leaders, entrepreneurs and experts in London, across the UK and in over 50 countries worldwide.

The Group comprises lawyers and technologists from the UK's leading law firms, legal consulting firms and academic institutions, and its 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. We 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. A list of the Group's members is provided at Annex 1.

The 2020 guidance was informed by seminars and meetings held by the Group, including presentations by experts such as Cassius Kiani (Atlas Neue), and Professor Michael Mainelli (Z/Yen Group). For this 2022 guidance, we have been pleased to hear from experts including the Law Commissioner for Commercial and Common law Professor Sarah Green, and Alessandro Palombo, CEO of Jur. A full list of experts who have addressed and fed into the Group's work is set out at Annex 2.

What does the guidance cover?

This guidance covers a wide range of key issues for legal practitioners to be aware of when advising on DLT-related matters. To help offer a route through this increasingly complex landscape, it is divided into two parts.

Part 1 – Developing technologies, covers the growing types and uses of DLTs and specifically cryptoassets, which will increasingly underpin advice and litigations – this includes how DLTs work, public and private blockchains, types of cryptoassets and tokens including NFTs and social tokens.

Part 2 – Impacts on the wider landscape, covers how DLT is changing the way services including law is practiced and implications for areas of litigation: smart contracts, data and governance, blockchain consortia, data protection, intellectual property rights, dispute resolution, competition, tax and ESG.

Throughout the guidance consideration is given to the relevant regulation of cryptoassets and likely future changes both to legislation and regulations, as well as making recommendations where further guidance is required from regulatory authorities or other bodies.

Following this introduction are **section summaries** followed by **key recommendations**.

Terminology

The terminology used around DLT and blockchain can be inconsistent and the need to "craft simple yet usable definitions of the technology" is one of the primary recommendations of The European Union Blockchain Observatory & Forum[1]. This is further complicated by the fact that specific words have different interpretations when used by legal practitioners and technologists – for example the different meanings of the word "execute" for a lawyer and for a coder. Work is ongoing to ameliorate some of these issues: Christopher D Clack, for example, refers to the methodology of Computable Contracts "where a single artefact is both the contract (understandable by lawyers who are not programmers) and the code (understandable by computers)."[2]

For the avoidance of doubt, this guidance is not intended to be prescriptive or rigid in its application, and definitions used are intended to be interpreted broadly. The provision of a list of common abbreviations is intended as a useful resource that expresses the knowledge and ideas of the Group whilst leaving space for interpretation. Similarly, terms and definitions used are also not intended to be prescriptive.

The Changing Landscape Of DLT and Blockchain

What are the likely trends for DLTs?

Throughout 2022 we expect to see a greater focus in three areas in particular.

First, the growth in NFTs and digital collectibles (such as MeeBits) will only increase. When NFTs first became technically possible in 2017, when Ethereum added a new standard, ERC-721, to its platform, one of the first uses was a game called CryptoKitties, which allowed users to trade and sell virtual kittens. As a result of the digital shift, accelerated by COVID-19 and an increased interest in DLT, NFTs and digital collectibles become more mainstream and present a fundamental change to the way consumers buy and sell digital assets.

Second, we expect to see further development, testing and gradual deployment of CBDC. Although DLT is not inherent to CBDCs, DLT offers several benefits for CBDCs including smart contract programmability, interoperability, transparent audit trails and confidentiality. At the time of writing, the Bank of England and HM Treasury have joined to create a CBDC Taskforce to coordinate the exploration of a potential UK CBDC. A CBDC would be a new form of digital money issued by the Bank of England for use by households (retail application) and businesses (interbank/wholesale application). It would, for now, exist alongside cash and bank deposits, rather than replacing them.

1 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

2 Christopher D Clack 'Languages for Smart and Computable Contracts' (8 April 2021, page 31) <https://arxiv.org/ftp/arxiv/papers/2104/2104.03764.pdf> Accessed 3 November 2021

Third, as sustainability becomes an increasingly urgent priority for organisations and regulators, we expect to see a transition to, or uptake of, more energy efficient models such as proof-of-stake (PoS), rather than proof-of-work (PoW), and more organisations turning to carbon credits secured on a distributed ledger. In 2021, Alogrand paved the way to be the first fully carbon neutral blockchain. In the near future more platforms are likely to do the same.

Recent and forthcoming changes to guidance

The UK has taken several steps to embrace DLT and other novel digital technologies. In November 2019 the UK Jurisdiction Taskforce published its Legal Statement on the status of crypto assets and smart contracts under English private law (Legal Statement).[3] The Legal Statement 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. Second, in September 2020, we published our guidance looking 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.

Since we published the first edition, there have been a number of developments: the Law Commission of England and Wales has published a consultation paper on Digital Assets: Electronic Trade Documents and published two calls for evidence on: (i) smart contracts,[4] and (ii) digital assets.[5] Further to the calls for evidence, the Law Commission published its advice to the Government on smart contracts on 25 November 2021[6] and an interim update on digital assets; which noted that the consultation paper in respect of digital assets won't be published till mid 2022.[7] In addition, the UKJT published its Digital Dispute Resolution Rules (the Rules), following consultation with legal and industry stakeholders.[8] I was extremely pleased to have been part of this sub-committee to produce the Rules. The importance of these Rules cannot be overstated. Disputes and access to resolution is time consuming and costly, often prohibitively so. In conjunction with a tech-enabled online dispute resolution platform, the Rules aim to provide SMEs and others with a speedy, cheap and easily accessible solution to settle disputes arising out of novel digital technologies.

Beyond England and Wales, we see the emergence and implementation across jurisdictions of legal and regulatory frameworks specifically governing certain virtual assets, businesses and operations. Derived from general principles and recommendations published by global standard-setting bodies, such as the Financial Action Task Force (the FATF) and the Financial Stability Board (the FSB), we can expect accelerated recognition and regulation of this sector during 2022 and beyond. The result is a complex and often jurisdiction-specific legal, regulatory and tax framework potentially applicable across a broad spectrum of client requirements, from structuring and governance to contracts and transactions. This guidance now includes a very high-level overview of some of the key global regulatory frameworks together with suggested skillsets and approaches for legal practitioners at a practical level, to assist with developing frameworks for training and continuing professional development.

3 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
4 https://www.lawcom.gov.uk/project/smart-contracts/.Accessed 28 October 2021
5 https://www.lawcom.gov.uk/project/digital-assets/. Accessed 28 October 2021
6 https://www.lawcom.gov.uk/project/smart-contracts/. Accessed 28 November 2021
7 https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2021/11/Digital-Assets-Interim-Update-Paper-FINAL.pdf. Accessed 28 November 2021.
8 https://35z8e83m1ih83drye280o9d1-wpengine.netdna-ssl.com/wp-content/uploads/2021/04/Lawtech_DDRR_Final.pdf Accessed 10 August 2021

Due to the rapid changing nature of the space, we intend to release an update to this 2022 guidance during the course of the year on Degov, the metaverse/virtual worlds and smart contracts (particularly following the publication of the Law Commission of England and Wales' 'Smart legal contracts Advice to Government' on the use of smart contracts)[9]. We also intend to draft an Annex of a more technical nature in conjunction with this update outlining some of the characteristics and key legal and practical issues to consider when deploying various token standards.

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

9 https://www.lawcom.gov.uk/project/smart-contracts/. Accessed 28 November 2021

Acknowledgements

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

Special thanks goes out to: Marc Piano (Harney Westwood & Riegels LLP (Cayman Islands)) and Tom Grogan (MdRxTECH) whose support and encouragement through this entire process has been invaluable and without which this guidance wouldn't be possible; and Max Nicolaides, Oliver Millichap and Lamide Danmola (Mishcon de Reya LLP) for assisting with the final compilation of this 2022 guidance.

Special thanks also to all those who have written submissions to this guidance, including: Jonathan Emmanuel (Bird & Bird LLP); Laura Douglas (Clifford Chance LLP); Martin Dowdall (Allen & Overy LLP); Marc Piano (Harney Westwood & Riegels LLP (Cayman Islands)); Albert Weatherill (Norton Rose Fulbright LLP); Ciarán McGonagle (International Swaps and Derivatives Association, Inc. (ISDA)); Mary Kyle (City of London Corporation); Thomas Hulme (Brecher LLP); Tom Rhodes (Freshfields Bruckhaus Deringer LLP); Adrian Brown (Harney Westwood & Riegels LLP (Cayman Islands)); Joey Garica (Isolas LLP (Gibraltar)); Omri Bouton (Sheridans); Will Foulkes and Gareth Malna (Stephenson Law LLP); Niki Stephens and Sian Harding (Mishcon de Reya LLP), Nick White and Matthew Blakebrough (Charles Russell Speechlys LLP); Akber Datoo, (D2 Legal Technology); Sue McLean (Baker McKenzie LLP); Adi Ben-Ari (Applied Blockchain); Rosie Burbidge (Gunnercooke LLP); John Shaw, (Foot Anstey LLP); Charlie Lyons-Rothbart (Taylor Vinters LLP); Charlie Morgan and Natasha Blycha (Herbert Smith Freehills LLP); Craig Orr QC (One Essex Court); Brendan McGurk and Will Perry and Antonia Fitzpatrick (Monckton Chambers); Ceri Stoner and Jennifer Anderson (Wiggin LLP); Marc Jones (Stewarts LLP); Nicola Higgs, Stuart Davis, Paul Davies and Charlotte Collins (Latham & Watkins LLP), and Tom Grogan (MDRxTECH).

Finally, my special thanks to Sarah Jarvis (Placeworks) for her eagle eye, time and expertise in reviewing and editing this new guidance.

Common Abbreviations

AML	Anti-Money Laundering
API	Application Programming Interfaces
BCBS	Basel Committee on Banking Supervision
CBDC	Central Bank Digital Currency
DAO	Decentralised Autonomous Organisations
DEFI	Decentralised Finance
DLT	Distributed Ledger Technology
EMR	Electronic Money Regulations
ESG	Environmental, Social & Governance
EU GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.
FATF	Financial Actions Task Force
ICO	Initial Coin Offering
IoT	Internet of Things
IP	Intellectual Property
IPR	Intellectual Property Rights
NFT	Non-fungible token
PET	Privacy Enhancing Technology
PRA	Prudential Regulatory Authority
RAO	Regulated Authorities Order
SLC	Smart Legal Contract
UK GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act of 2018 and as amended by Schedule 1 to the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (SI 2019/419).
UKJT	UK Jurisdiction Taskforce

Section Summaries

An overview of DLT:
This overview of distributed leger technology (DLT) is included for readers who may not be familiar with the way it works. It shows how the use of ledgers has evolved over time, identifies some of the main characteristics of DLT, explores the mechanisms by which some distributed ledgers create, amend and replicate their digital records, and provides brief examples of different types of DLT – showing how blockchain, although the best know example, is not the only one that might be encountered.

Commercial Application:
Covering key considerations relevant to the conception, application and adoption of DLT/ blockchain 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 financial services sector with a private blockchain being used to better track and record information relating to trade finance arrangements.

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.

Types of Cryptoassets:
This section looks at different types of cryptoassets, including CBDCs and stablecoins, together with an overview of the adoption of the Financial Action Task Force recommendations in respect of Virtual Asset Service Providers (VASPs) and developments in the DeFi space.

DeFi:
This section provides an overview of the adoption of the FATF recommendations in respect of VASPs and the approaches to registration regimes from a compliance perspective and licensing regimes bringing the activity within the scope of prudential supervision. It covers the interpretation issues relating to what constitutes a Virtual Asset Service, and touches on some of the cross border issues the categorisation of a service in one jurisdiction can create when the platform services individuals in a separate jurisdiction.

The section also covers the development of the DeFi space, and the sensitivities around the classification of this activity in the UK and around the world. As well as the categorisation of the concept of ‘decentralisation’ the section aims to identify DeFi specific risks and approaches that may be taken to address primary compliance risks.

NFTs:
This section is split into two parts. In Part A we look at some practical and legal issues with regards ownership rights and intellectual property issues related to NFTS. In Part B we do a deep dive to look at whether an NFT could ever be fall within the remit of a financial regulatory asset and in part C we consider if the mechanics by which the NFTs are issued or sold and/or any aspect of the ecosystems in which the NFTs may be utilised might constitute “gambling” and require the provider of such facilities to hold a gambling licence issued by the Gambling Commission of Great Britain.

Social Tokens:
An introduction to the three main types of social token: (1) personal tokens; (2) community tokens; & (3) social platform tokens. Includes a brief look at social token terms and conditions, smart contracts and regulatory issues.

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 UK 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 UK 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 UK 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.

Competition:
This section begins with an introduction which emphasises the competitive benefits of blockchain, in particular the promotion of consumer welfare. It then considers potential competition harms arising in the blockchain context. Finally, it addresses enforcement issues for competition regulators. Three overarching conclusions emerge from the analysis:

— Competition concerns arising in the blockchain context can be effectively analysed under the existing analytical framework for competition harms.

— The types of competition law harms that will arise in this context are likely to depend on two main factors: (a) the extent of transparency / data sharing within the blockchain and (b) the extent to which power is concentrated in the hands of the blockchain owner(s). Although the underlying technology may be the same, there is no one-size-fits all approach to evaluating anticompetitive conduct involving blockchain.

— Perhaps the greatest challenge blockchains present for competition lawyers and regulators is enforcement. As with the likely competition law harms, enforcement challenges will depend on the blockchain's degree of transparency and concentration of power.

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; impact of blockchain on the in-house tax function; and impact of blockchain on tax authorities.

Blockchain and ESG:
As the popularity of virtual assets has grown, attention has started to focus on the industry's environmental, social, and governance (ESG) performance. This section examines the rise of ESG considerations amongst corporates, financial institutions and investors, and how this affects their interactions with cryptocurrency firms. It looks at the various ESG-related concerns and questions associated with cryptocurrency businesses and some of the challenges these businesses may need to overcome as ESG matters take on greater significance.

Key Recommendations

Commercial application
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.

Regulation of cryptoassets
— The UK has an opportunity to develop an effective and proportionate regulatory regime for cryptoassets. However, the UK must act quickly to clarify its policy approach and introduce new rules where relevant in order to give the market certainty and facilitate the development of efficient and orderly markets in cryptoassets in the UK.

— The UK should confirm how it intends to expand the current UK regulatory perimeter following recent HM Treasury consultations on the UK regulatory approach to cryptoassets and stablecoins and on cryptoasset promotions.

— Any new rules expanding the regulatory perimeter for cryptoassets should adopt the principle of "same activity, same risk, same regulation". Care should be taken with cryptoasset definitions and taxonomies in particular to ensure any extension to the regulatory perimeter is based on granular characteristics of cryptoassets and other uses of DLT (e.g. as a pure record-keeping tool) are not inadvertently captured. The territorial scope of the regime and potential interaction and overlap with other jurisdictions' rules must also be carefully considered given the cross-border nature of the cryptoasset market. The overseas persons exclusion (OPE) should be extended to relevant cryptoasset-related activities.

— The UK should also confirm whether it intends to extend other aspects of the UK regulatory regime such as market abuse requirements to cryptoassets and how it intends to adjust other aspects of the existing regulatory framework applicable to regulated cryptoassets such as security tokens to facilitate the development of efficient and orderly markets in cryptoassets.

— To aid certainty, legislation and/or regulatory guidance should also 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 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.

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

— 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 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, 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 provide guidance on how they are to operate in practice, and explore whether decentralised structures may act as financial market infrastructures.

— 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. Clarity on this latter point is important particularly following El Salvador's adoption of Bitcoin as legal tender in 2021.

Types of cryptoassets, NFTs and Social Tokens

— The key recommendations of a few types of cryptoassets have significant cross over with other section of the guidance. We recommend that an analysis should be done at the outset of any project to consider a number of legal, technical and commercial issues to ensure compliance with (among other things) UK consumer law, advertising guidance and financial and gambling regulations.

DeFi

— To ensure consistency with the activity captured under the FATF definition of a Virtual Asset Service provider through a relevant gap analysis assessment.

— To provide as much clarity and certainty as possible in respect of decentralised operations being categorised as Cryptoasset Service Providers, or operating outside of the scope of such definition.

— The development of standards for the regulation of such systems or infrastrucutre, and the development of new standards for compliant DeFi operations.

— To provide clarity and guidance around the requirements for centralised and regulated counterparts to access decentralised infrastructure under their relevant permissions.

— To ensure alignment around the categorisation of DeFi platforms with the transposition of the Travel Rule.

Smart contracts and data governance

— 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.

- Smart contracts need to be adequately tested with data sets prior to production use, including assessing the ability to appropriately deal with data quality issues.

— 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).

— We intend to release an update to this 2022 Guidance on smart contracts during the course of the year following findings from the Law Commission of England and Wales' call for evidence on the use of smart contracts[10].

Blockchain consortia

— 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.

Data protection

— Recital 26 of the UK 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 UK 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 UK GDPR?
- How should 'erasure' be interpreted for the purposes of Article 17 UK GDPR in the context of blockchain technologies?
- How should Article 18 UK 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 UK GDPR?
- What is the status of the on-chain hash where transactional data is stored off-chain and subsequently erased?

10 Smart contracts | Law Commission. Accessed 2 November 2021

- 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?

Intellectual property

— 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.

Dispute resolution

— 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.

Competition

— The current legal competition law framework is adequate to address blockchain-based abuses and as such there are no recommendations for legislative change.

Blockchain and tax

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

— HMRC's new Cryptoassets Manual (launched in March 2021) brings together and builds on previous guidance, but there remain some critical gaps in coverage and areas where greater clarity and detail is required in order to provide and clear, consistent HMRC guidelines.

— Tax policy and evasion is a critical part of the overall regulatory framework. Further guidance and specific legislation are required to guide tax practitioners through the key issues in advising on the correct tax treatment of all aspects of distributed ledger transactions.

  The UK's approach should continue to be developed and informed by the international landscape. In particular, the EU's DAC 8 and OECD's reports and proposals on the tax treatments and emerging tax policy issues.

— HMRC 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 and government to consider how to roll out blockchain and adopt the technology for maximum benefit generally. For example, issues to be addressed should include:

- Rollouts of new digital systems: i.e. 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 in Russia.

- Mandating a new digital system: The UK Government estimates 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, albeit small companies (or individuals) without the right tools and/or knowhow, will likely struggle to cope.

- Ministerial ownership: Cross government buy-in is likely to be key, on the basis that many digital solutions rely on information being shared across government departments.

- Third party involvement: It is inevitable that there will be heavy reliance on third party software providers. As such, relationships need to be nurtured and time and resources spent perfecting systems, whether external (e.g. CREST) or internal.

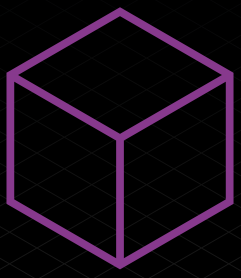
- Controlled pilot testing: To identify where tax efficiencies could be made prior to investment by the government and also the taxpayer. This would prevent the pre-

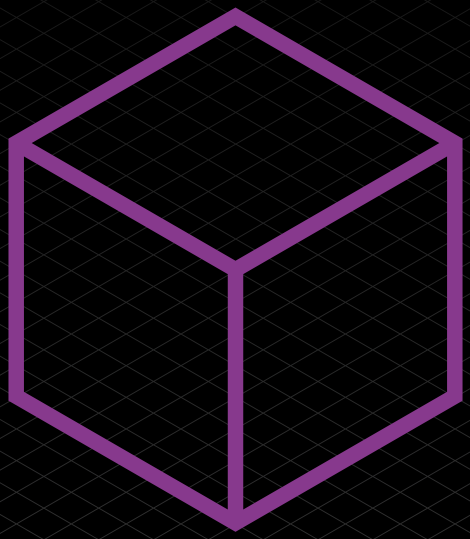
- emptive roll out of government tax initiatives such as 'Making Tax Digital', which placed a high time and cost burden on the taxpayer. Most tax practitioners would probably favour a focus on identifying where efficiencies can be made, rather than a wholesale reform of the tax system.

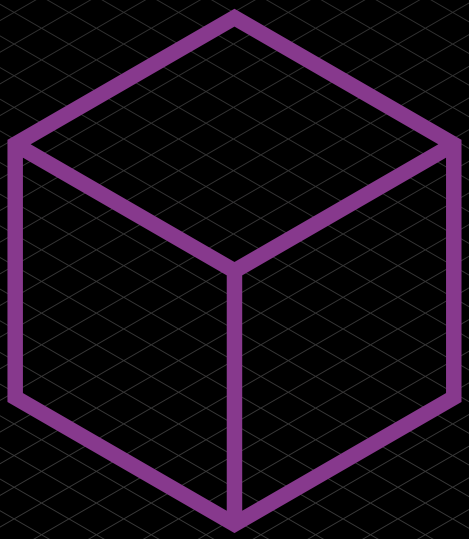
Blockchain and ESG

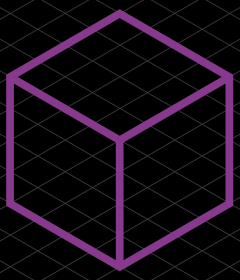
— Market participants should consider carefully the ESG impact of their cryptocurrency activities and consider, when selecting protocols / service providers, what those protocols / service providers are doing to address the ESG impact of this asset class.

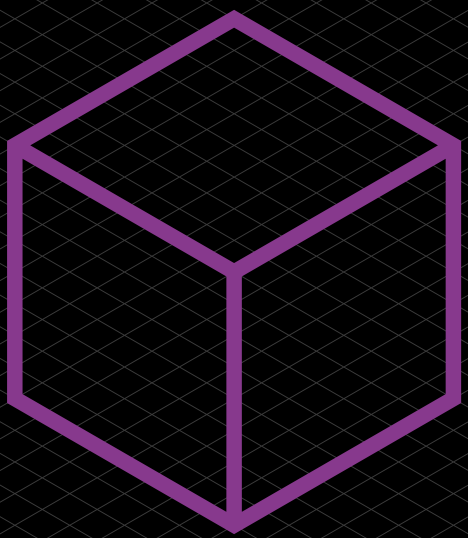
1





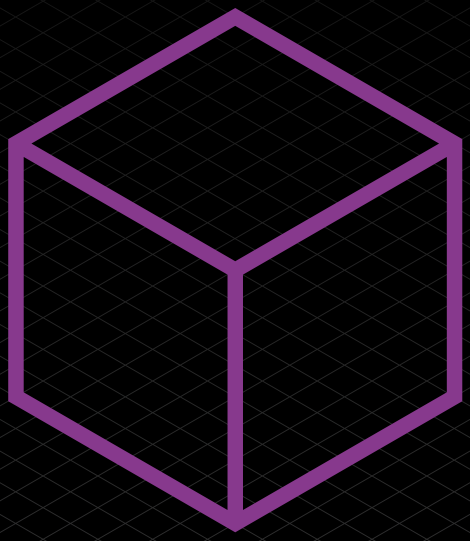


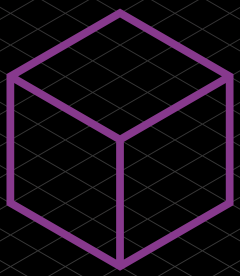


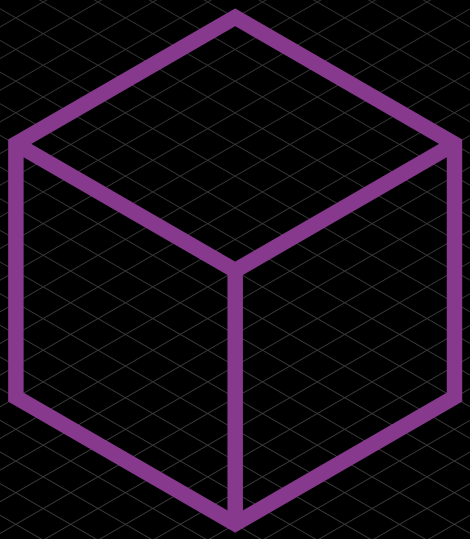


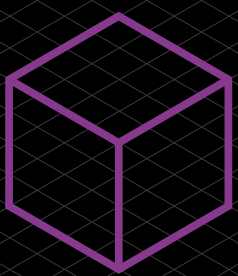
Part 1: Developing Technologies

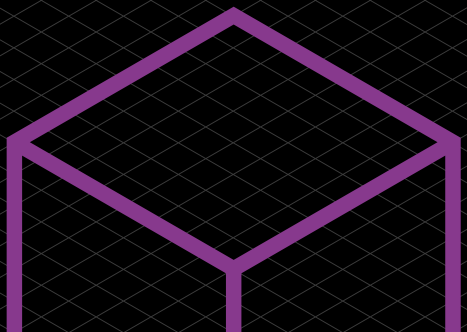
Section 1 An Overview of DLT











Section 1: An Overview of DLT

Tom Grogan, MDRxTECH

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.

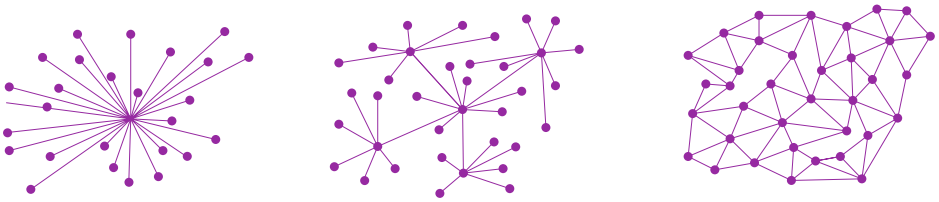
The idea of maintaining a ledger is not a new one. The earliest ledgers date back to c.4,000BC in Mesopotamia. They were kept on clay scripts or carved into stone and were used to record and demonstrate definitive ownership, and the transfer of ownership, of crops in storage. Recording the ownership 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 describes what we now call a centralised ledger (see Fig 1 below) the definitive and only record within an ecosystem. In many circumstances, such centralised ledgers are effective, and in many instances they remain in use today. Centralised ledgers do however have some drawbacks, notably that 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 (those placing reliance on the definitive nature of the ledger's record keeping) will fail. 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 have decentralised ledgers become more prevalent (see Fig 1). 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 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). 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.

Fig 1 – Centralised, decentralised, and distributed ledgers. Note that the structures of these ledgers, in particular the distributed ledger, have been simplified for illustrative purposes.



Centralised Decentralised Distributed

In this guidance 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. (In line with terminology used by the Financial Action Force (FATF), cryptoassets are occasionally also referred to as 'virtual assets'). This guidance 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.

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 Fig 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 the limitations of this section are acknowledged. It does not seek to provide an exhaustive and detailed explanation of DLT, rather, it seeks to:

1. set out the main features of DLT;
2. explain consensus protocols; and
3. give brief examples of DLT types.

1. Main 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:

i. enable network participants to exclusively control 'their' records or cryptoassets;
ii. maintain a clear chronology of distributed ledger entries; and
iii. 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 is explored below in more detail.

<u>i. Exclusivity</u>

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:

a. public keys: these may be widely disseminated and known to some or all other network participants; and

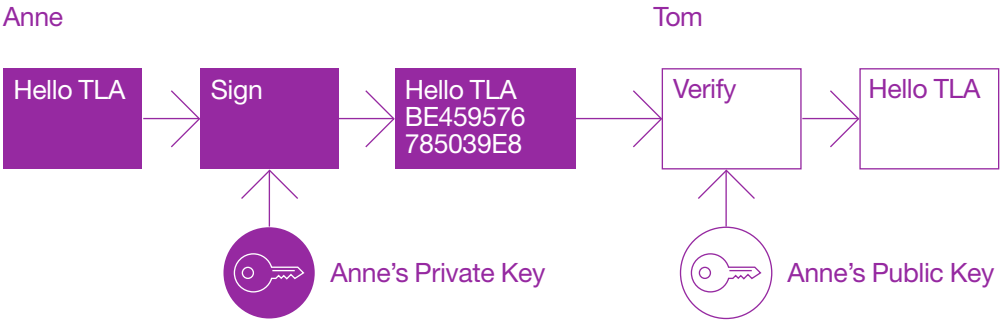
b. private keys: these should be known only to the relevant network participant.

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.

ii. Chronology

One of the main 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 the so-called 'Distributed Ledger Problem' becomes 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.

iii. 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.

2. 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.

i. 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).

ii. 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.

3. Examples of DLT

i. Blockchain
ii. Directed acyclic graph
iii. Hedera Hashgraph

i. Blockchain

The best-known example of a DLT, blockchain rose to prominence on the publication of the Bitcoin white paper 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.

Fig 3 – Blockchain structure

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

ii. Directed acyclic graphs

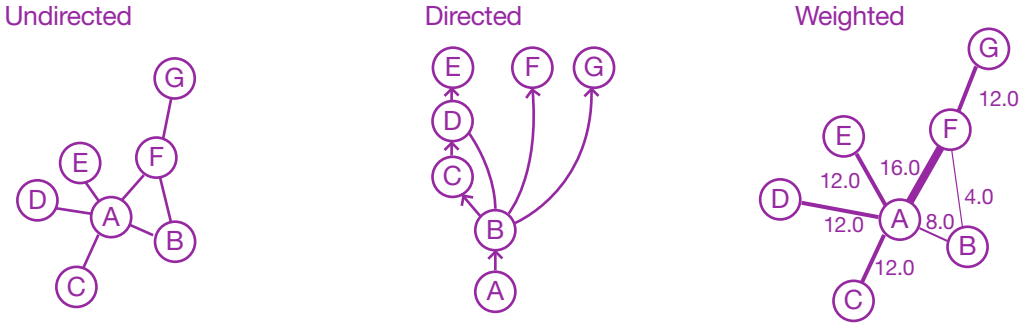
Directed acyclic graphs (DAGs) are a well-established branch of graph theory and computer science. They are graphs that travel in one direction without cycles connecting the other edges. The graph uses topological sorting, wherein each node is in a certain order. In the context of DLT however, directed 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.

In graph theory, vertices or nodes represent entities in the network. In a distributed network, each computational centre is a node. Edges convey information about the relationship or link between nodes. In a distributed network, such relationships or links might include communications between computational centres.

Depending on the relationship between the nodes, several types of graphs emerge:

Fig 4 – Forms of acyclic graphs



— **Undirected:** An edge connects all nodes. The Facebook social media platform is an example of an undirected graph: when two users connect as Friends, both parties follow each other.
— **Directed:** The edge displays the directionality of the relationship from one node to another. The Twitter social media platform is an example of a directed graph: a user might connect with another user by Following them, without receiving a Follow back.
— **Weighted:** The edge sizes represent the strength of a relationship. Many corporate CRM tools are examples of weighted graphs, by making connections between users based on the strength of interpersonal relationships.

Specifically, DAGs are directed graphs because it is possible to infer the direction of how one node relates to another. In the case of DLT, DAGs' nodes or vertices represent or hold the information of transactions or events, while edges indicate the ordering of the transactions. DAGs application as a DLT presents the benefit of processing several transactions or events simultaneously while allowing the consensus to decide the proper order of the transactions.

iii. Hedera Hashgraph

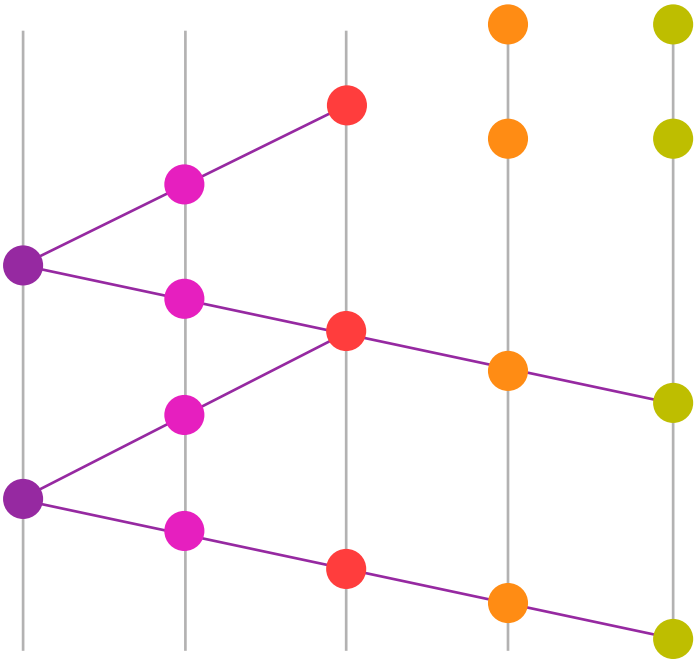
Hedera Hashgraph, better known simply as Hashgraph, is an alternative DLT and close cousin of the directed acyclic graph, developed by Leemon Baird in 2016.

Heshgraph 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)

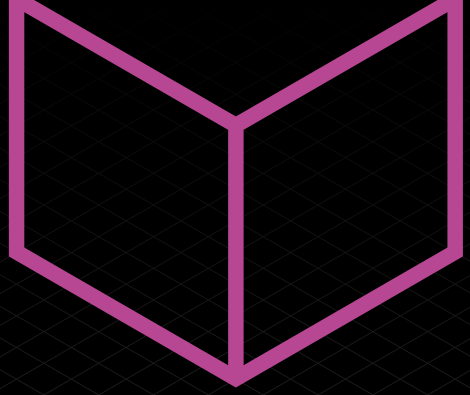
from others, to two randomly chosen neighbours (which in turn further propagate the gossip alongside their own events in an aggregated fashion). Chronologies are established using timestamped events.

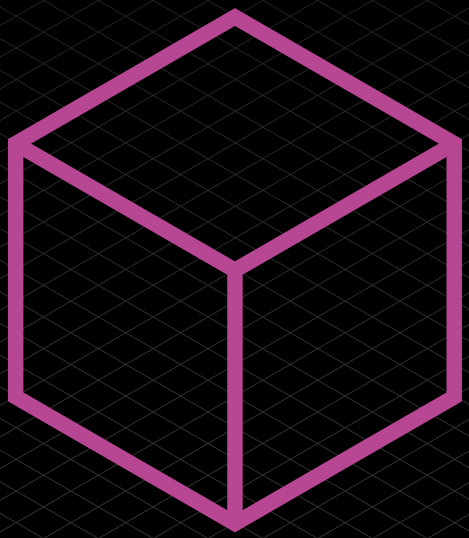
The advantages of Hashgraph's streamlined consensus mechanism include speed and fairness. An inherent assumption of Hashgraph is that fewer than a third of nodes are bad actors (i.e. those who forge, delay, replay and drop incoming and/or outgoing events) and therefore, if this is not (or cannot be reliably be proved to be) the case, security concerns may arise.

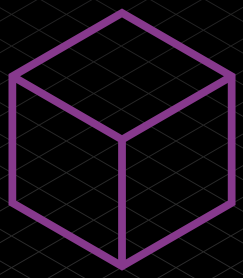
Fig 5 Hedera Hashgraph structure

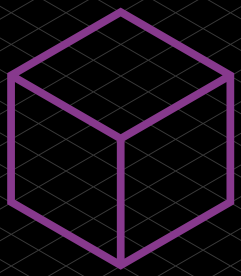


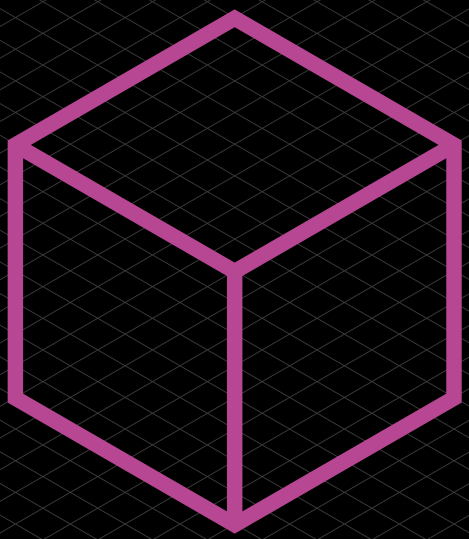
2

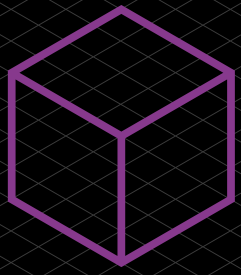






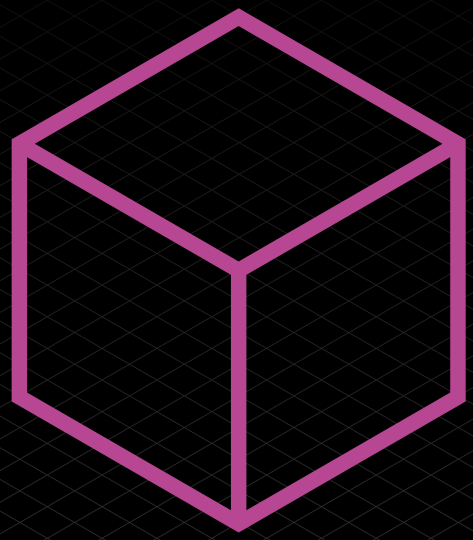


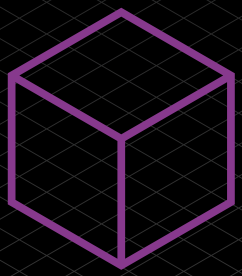


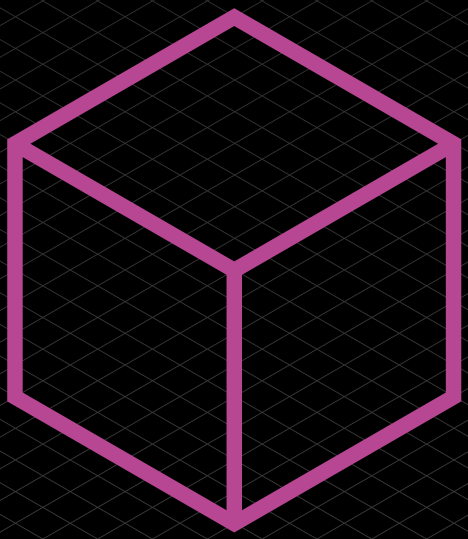


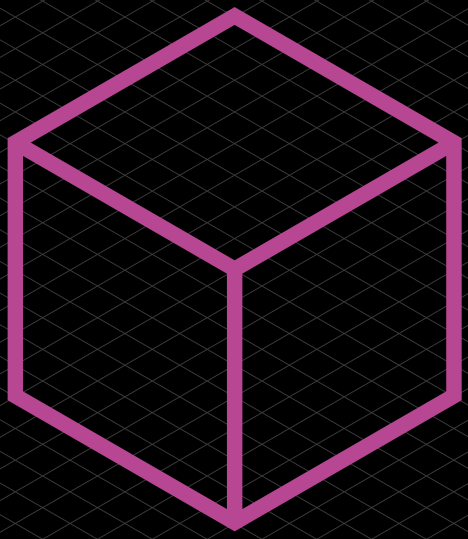
Part 1: Developing Technologies

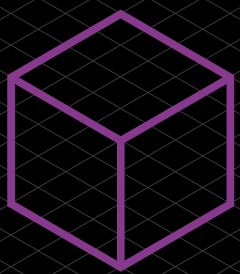
Section 2 Commercial Application











Section 2: Commercial Application

Jonathan Emmanuel, Bird & Bird LLP

Introduction

Since the publication of the first edition of this guidance the media hype surrounding blockchain technologies has continued with ideas such as "metaverse", "DeFi" and "NFTs" attracting considerable attention. Yet increasingly the evidence is that business is catching up; the ecosystem has changed. Venture capital backers are growing more comfortable with investment in the technology, as evidenced by the huge cryptocurrency-focused fund created by Andreessen Horowitz's venture capital firm ($2.2 billion), blockchain-focused software companies like ConsenSys have rapidly expanded to scale-up and beyond, and real-life use cases are now being deployed by clients in a variety of sectors. All this shows that the technology is more than just a fad.

This section analyses a live use case in the financial services sector. The most successful use cases still tend to relate to taking advantage of blockchain technology to allow for the better sharing and recording of data (sometimes with the assistance of smart contracts) between disparate parties.. When we refer to blockchain 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. First, therefore, it is important to understand why enterprises are choosing private blockchains over public blockchains or centralised databases. Public vs private?

Bitcoin and Ether are examples of cryptoassets 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"[11] for the Bitcoin public blockchain) is time-consuming and costly to run.

11 See Section 1

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.

The preference for private blockchains is not absolute though. For example, one use case for blockchain technologies, discussed in Section 5, is non-fungible tokens (NFTs). When it comes to selling NFTs for example, it is very common for the relevant entity to use public blockchain networks such as Ethereum to enable the creation of the NFTs, which are then made available for sale by customers via interoperable marketplaces like OpenSea.

Private vs central database?
One question to ask is 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:

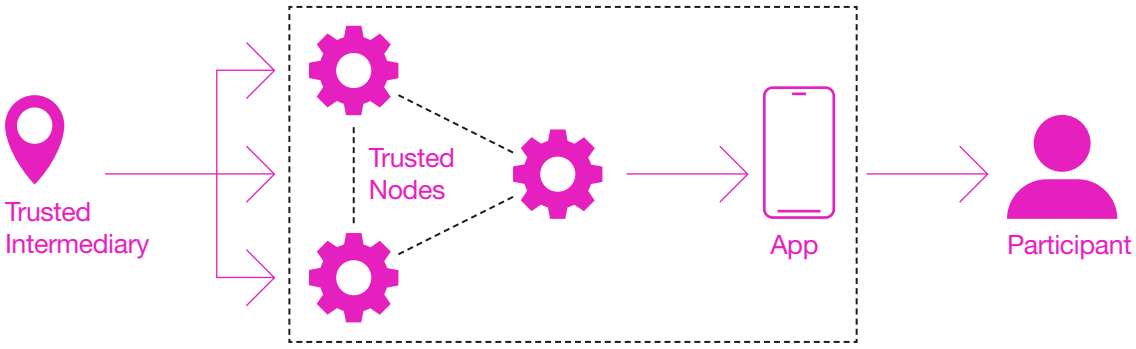
— **Trusted intermediary:** the trusted intermediary downloads the blockchain software and sets up the nodes that comprise the network. It is not necessary to have only one trusted intermediary, although this is common; the process may in fact involve multiple trusted intermediaries with authority over 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 is 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.

— **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.

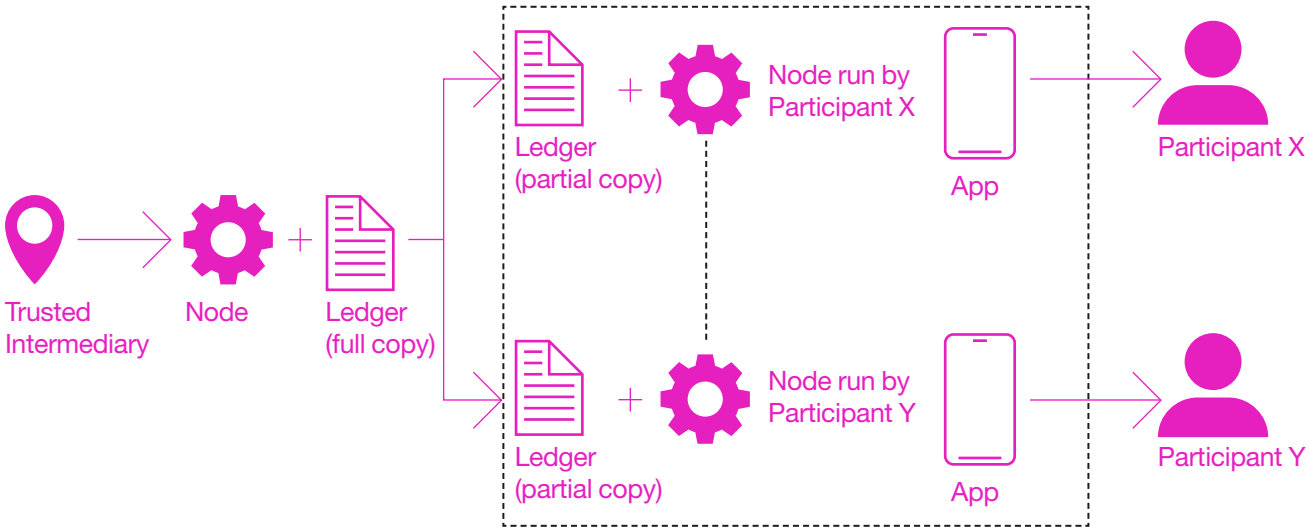
— **Participants:** the participants access the trusted intermediary's nodes via the app. Using the app, participants can send data to be recorded on the private blockchain and view the data recorded on the private blockchain.

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

One of the most common use cases relates to the better sharing and recording of data in the context of trade finance projects through the use of blockchain technologies and smart contracts. Trade finance often operates in cross-border sale of goods arrangements. In these arrangements, there are normally four key stakeholders involved: the seller, the buyer, the seller's bank and the buyer's bank. These arrangements raise some concerns for the seller and the buyer. The seller wants to sell the goods to the buyer but is concerned that the buyer takes receipt of the goods but then never pays for them, so incurring considerable costs trying to enforce a claim for payment against the buyer. The buyer is concerned that if he pays for the goods before they are delivered then the seller may never deliver them. In order to mitigate against these concerns, the seller will require a buyer to pre-pay for the goods it has shipped and the buyer will pre-pay for them subject to obtaining proof that the goods have been shipped, so are in transit, such as a bill of lading.

It works as follows:

— The seller and the buyer sign the sale of goods contract.

— The buyer's bank issues a letter of credit guaranteeing payment of the goods to the seller's bank subject to certain conditions being met such as the bill of lading being provided by a certain date.

— The goods are then shipped, and the seller sends the buyer the bill of lading and then the buyer sends this to its bank who makes the payment subject to the terms of the letter of credit.

The challenge with this arrangement is that there are a number of different documents (e.g. the sale of goods contract, the bill of lading, the letter of credit) being shared in a number of different formats (e.g. by post, fax or electronic mail) by disparate parties who do not necessarily trust each other. Documents can be lost or arrive late (in which case the buyer's bank may refuse to make payment pursuant to the letter of credit) or be easily forged (e.g. forging a bill of lading to give the impression the goods have been shipped).

As a result, these stakeholders often expend a lot of time and money dealing with managing the documentation and disputes. As an alternative, these stakeholders are now looking at technologies like blockchain to streamline the process, taking advantage of the benefits of the technology: once data is recorded to the blockchain it can't easily be changed and smart contracts (deployed to the blockchain) can help automate certain steps in order to make the process more efficient.

It might work as follows:

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

— The buyer, the seller and their banks access the private blockchain by accessing the app built by the trusted intermediary.

— The buyer sends the letter of credit for recording to the blockchain. The letter of credit refers to a smart contract which the parties to the letter of credit agree will implement certain obligations relating to letter of credit, in accordance with its terms.

— The smart contract is created and (once approved by the parties to the letter of credit) is deployed to the blockchain. The smart contract works on a simple if/then conditional: if the seller sends and records a bill of lading to the blockchain on or before the agreed date specified in the letter of credit and this is approved by the relevant consensus protocol on or before such agreed date, then the smart contract issues an instruction to the buyer's bank to send payment for the relevant goods to the seller's bank.

— The seller sends the bill of lading for recording to the blockchain (and if it is recorded on time then the buyer's bank is automatically instructed by the smart contract to pay the seller's bank).

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 bilateral 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 contracts:** these are the contracts that govern access to the blockchain network and are made between the trusted intermediary and each participant. Often, they comprise a bilateral technology agreement and a multilateral rulebook. The technology agreement governs the use of the blockchain technologies in order to enable the participant to send data for recording on the blockchain. It will deal with the usual types of issues you would expect to face when drafting or negotiating cloud services agreements: licence conditions, implementation, liabilities and indemnities (including in relation to loss or corruption of data), security, service levels, suspension and termination rights, access to data on termination or expiry and IP (see more on this in Section 9). The rule book is the set of terms between the trusted intermediary and each participant and between each participant. It will sit alongside the technology agreement and focuses on principles such as membership and eligibility criteria, the process for implementing changes to the rule book terms, general representations and warranties (e.g. not to use the blockchain network for any "prohibited purpose") and the process for how transactions are agreed to be validated and recorded to the blockchain.

It is important that any commitments made by the trusted intermediary (for example, availability service levels) under the technology agreement are appropriately backed off under the terms of the blockchain services contract.

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.

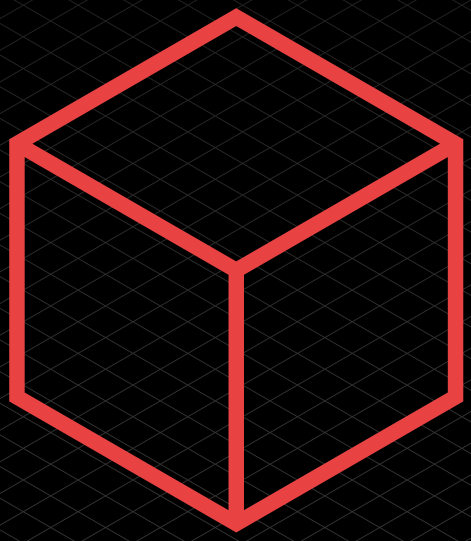
One of the key IP battlegrounds between the blockchain developer and trusted intermediary is who owns the IP in the user-facing app. Analogous to traditional software development agreements, there are commercial considerations for parties around various aspects of the IP in both the blockchain software 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

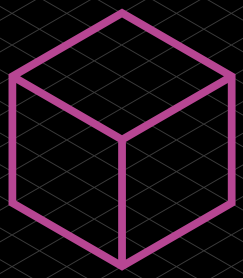
incorporation of both third party and open source software into the development of the app should be addressed early in the development process. One potential middle-ground position is for the IP in the app to vest with the blockchain developer, but for the trusted intermediary to have a wide licence (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.

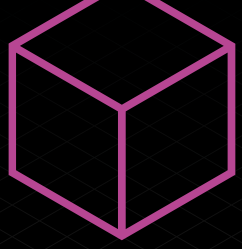
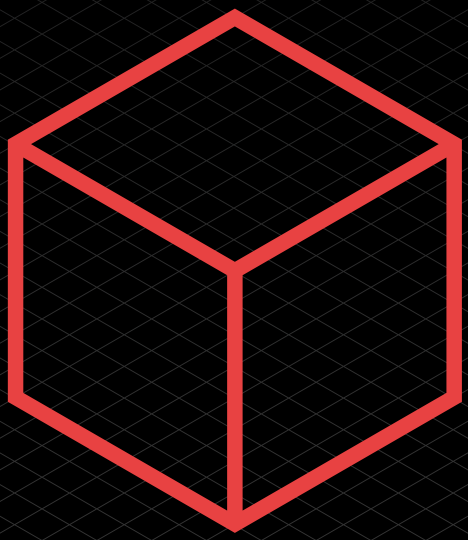
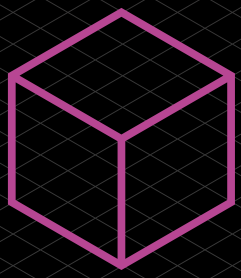
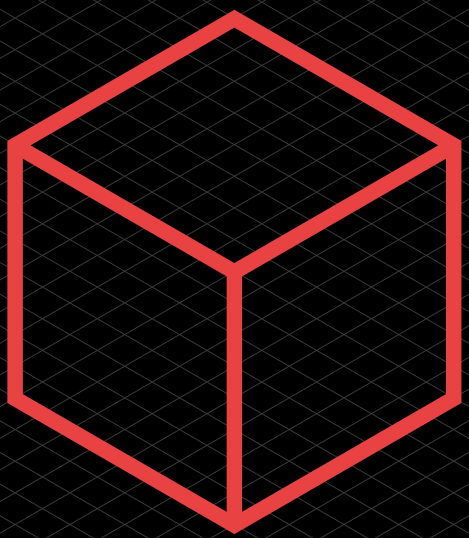
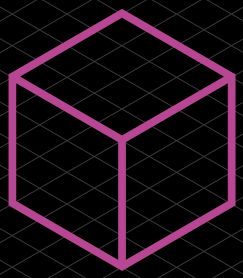
3





Part 1: Developing Technologies

Section 3 Regulation of Cryptoassets

Section 3: Regulation of Cryptoassets

Laura Douglas (Clifford Chance LLP) and Martin Dowdall (Allen & Overy LLP)

Introduction

At present, there is no specific UK regulatory regime for cryptoassets, other than in relation to anti-money laundering (AML) requirements for cryptoasset exchange providers and custodian wallet providers. Instead, the UK's 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.

PART A

FCA guidance and taxonomy

This approach is reflected in the Final Guidance on Cryptoassets[12] published by the 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)[13], 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)[14] 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 of the Financial Services and Markets Act 2000 (FSMA) and/or an alternative investment fund (AIF) as defined in the Alternative Investment Fund Managers Regulations 2013.[15] 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 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

12 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 October 2021
13 The Financial Services and Markets Act 2000 (Regulated Activities) Order 2001, SI 2001/554
14 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
15 The Alternative Investment Fund Managers Regulations 2013, SI 2013/1773

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).[16] 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 (2019).[17] 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.

   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

16 The Electronic Money Regulations 2011, SI 2011/99
17 FCA Guidance (n 167)

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.

i. **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[18] 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)[19] 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 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. However, in January 2021, HM Treasury published a consultation on the UK

18 "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"
19 The Joint Money Laundering Steering Group Guidance – Part II: Sector 22 (June 2020 (amended July 2020)) <https://jmlsg.org.uk/consultations/current-guidance/> Accessed October 2021

regulatory approach to cryptoassets and stablecoins[20], proposing that the UK regulatory perimeter should be expanded to capture stablecoins as regulated financial instruments, as discussed further below.

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.[21] 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.

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 cryptoas tions have also been considered by the English courts, notably in the case of AA v Persons Unknown,[22] 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.

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 10). A change to the law as well as international cooperation will likely be 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).

20 HM Treasury, 'UK regulatory approach to cryptoassets and stablecoins: Consultation and call for evidence' (January 2021) < https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/950206/HM_Treasury_Cryptoasset_and_Stablecoin_consultation.pdf> Accessed October 2021

21 Bank of England, 'Financial Policy Summary and Record' (October 2019) <https://www.bankofengland.co.uk/financial-policy-summary-and-record/2019/october-2019> Accessed October 2021

22 AA v Persons Unknown [2019] EWHC 3556 (Comm)

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 stablecoins and certain other types of unregulated cryptoassets. This would require legislative change and in July 2020, HM Treasury published a consultation[23] seeking views on whether to bring the promotion of certain types of cryptoassets within scope of financial promotions regulation. The outcome of this consultation has not been published at time of writing.

In January 2021, HM Treasury also published a consultation paper on the UK regulatory approach to cryptoassets and stablecoins[24], proposing that the UK regulatory perimeter should be expanded to capture stablecoins as regulated financial instruments. The outcome of this consultation has not yet been published at time of writing, and so the UK's approach to regulation of stablecoins remains unclear. We recommend that HM Treasury publishes its policy approach following the consultation quickly, in order to provide greater certainty to the market and support the use of stablecoins in the UK.

We consider that any resulting expansion in the UK regulatory perimeter should adopt the principle of "same activity, same risk, same regulation". Care should be taken as to how any new rules may interact with existing regulatory frameworks (such as e-money regulation) and overlaps addressed. Linked to this, it is also important to ensure that definitions and taxonomies are carefully calibrated based on the substantive characteristics of the relevant cryptoassets both to avoid unhelpful overlaps between regimes and also to ensure uses of DLT as a pure record-keeping tool are not inadvertently captured. In this respect, we consider the definition of cryptoasset used in the MLRs is rather too broad for use in a potential new licensing regime and could helpfully be clarified.

PART B

It is also necessary to consider carefully the territorial scope of any new licensing regime for firms dealing in or providing services relating to relevant types of cryptoassets, particularly in light of the cross-border nature of many cryptoasset structures. In particular, clear rules or guidance on when activities will be considered carried on in the UK would be welcomed to provide certainty to market participants, coupled with appropriate carve-outs from licensing requirements for overseas firms carrying on activities on a cross-border basis, for example, via extension of the overseas persons exclusion (OPE) to relevant cryptoasset-related activities. This will be important to avoid duplication and overlaps with other jurisdictions' rules, in line with the UK's broader policy and approach to the territorial scope of financial services regulatory regimes.

Licensing and conduct of business requirements
The licensing and conduct of business requirements that apply to firms dealing with cryptoassets depend on how the relevant cryptoasset is characterised under the current 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

23 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 October 2021
24 HM Treasury, ' UK regulatory approach to cryptoassets and stablecoins: Consultation and call for evidence (January 2021) < https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/950206/HM_Treasury_Cryptoasset_and_Stablecoin_consultation.pdf> Accessed October 2021

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[25] 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 structures) along with indicative practical mitigation strategies. These strategies may include blockchain analysis or tracing as well as more traditional AML risk-mitigation strategies.

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 Client Assets Sourcebook (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.

25 The Joint Money Laundering Steering Group Guidance – Part II: Sector 22 (June 2020 (amended July 2020)) <https://jmlsg.org.uk/consultations/current-guidance/> Accessed October 2021.

In its Advice on Initial Coin Offerings and Crypto-Assets,[26] 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*
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 risk, 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. HM Treasury has started to explore some of these questions in its consultation paper on the UK regulatory approach to cryptoassets and stablecoins[27], and the FCA's Regulatory Sandbox provides some much-needed flexibility and regulatory support for fintechs to test innovative solutions.

Again, clarity on the UK's expected policy approach on these questions will be beneficial for the development of efficient and orderly markets in cryptoassets in the UK. We note that similar issues are covered, for example in the EU's proposed Markets in Crypto Assets Regulation (MiCA) and so it will be important to understand the extent to which the UK may to adopt a similar approach to MiCA on issues such as extension of market abuse requirements to certain types of cryptoassets and if not, what approach the UK does intend to take to these issues.

26 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 October 2021
27 HM Treasury, ' UK regulatory approach to cryptoassets and stablecoins: Consultation and call for evidence (January 2021) < https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/950206/HM_Treasury_Cryptoasset_and_Stablecoin_consultation.pdf> Accessed October 2021

UK actions to address risks arising from cryptoassets

In October 2018, the Cryptoasset Taskforce published its final report[28] 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, and recent HM Treasury consultations on the UK regulatory approach to cryptoassets and stablecoins, and on cryptoasset promotions.

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,[29] cryptocurrency contracts for difference (CFDs)[30] and cryptoasset investment scams.[31] More recently, the FCA has introduced new conduct of business rules[32] restricting how firms can sell, market or distribute CFDs and similar products (including those that reference cryptocurrencies) to retail consumers.

On 6 January 2021 the FCA also introduced a ban[33] on the sale, marketing or distribution of derivatives and exchange of traded notes referencing cryptoassets to retail clients.

Prudential requirements

Neither the current UK regulatory regime, European regulatory regime nor Basel framework – standards of the Basel Committee on Banking Supervision (BCBS) – 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) [34], 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.

28 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.
29 FCA, 'Initial Coin Offerings' (12 September 2017) <https://www.fca.org.uk/news/statements/initial-coin-offerings> Accessed October 2021
30 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 October 2021
31 FCA, 'Cryptoasset Investment Scams' (First published: 27 June 2018, updated 13 March 2020) <https://www.fca.org.uk/scamsmart/cryptoasset-investment-scams> Accessed October 2021
32 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 October 2021
33 FCA, PS20/10: Prohibiting the sale to retail clients of investment products that reference cryptoassets < https://www.fca.org.uk/publication/policy/ps20-10.pdf> Accessed October 2021
34 Council Regulation No 575/2013 of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012 (2013) OJ L176 1 [147]

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 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 set out preliminary proposals for the prudential treatment of banks' cryptoasset exposures in its June 2021 consultation paper[35].

The BCBS proposals divides cryptoassets into two broad categories:

Group 1 being those cryptoassets that fulfil certain classification conditions and are eligible for treatment under the existing Basel Framework (with some modifications and additional guidance). Group 1 is further divided into:

i. Group 1a – tokenised traditional assets; and

ii. Group 1b – cryptoassets with stabilisation mechanisms[36]; and

Group 2 being cryptoassets that do not fall within Group 1, such as Bitcoin.
The BCBS proposes that cryptoassets in Group 1a be subject to capital requirements at least equivalent to those of traditional assets (with further consideration for capital add-ons). In relation to cryptoassets falling within Group 1b, the BCBS proposes new guidance on the application of current rules to capture risks relating to stabilisation mechanisms (with further consideration for capital add-ons). The BCBS notes that it is not possible to set out the capital treatment for all structures and instead provides illustrative examples in its consultation.

As regards cryptoassets in Group 2, the BCBS proposes a conservative prudential treatment based on an absolute 1250% risk weight applied to the maximum of long and short positions (i.e. without giving effect to netting of long and short positions).

The consultation closed for comments on 10 September 2021.

The European Banking Authority (EBA) has previously expressed similar views in its January 2019 report on cryptoassets. [37]

35 Basel Committee on Banking Supervision, Consultative Documents, Prudential treatment of cryptoasset exposures (Bank of International Settlement website, June 2021) <https://www.bis.org/bcbs/publ/d519.pdf>
36 The consultation provides further clarification on the scope of group 1b: "cryptoassets which may not confer the same level of legal rights as ownership of a traditional asset, but may seek to link the value of a cryptoasset to the value of a traditional asset or a pool of traditional assets through a stabilisation mechanism. Cryptoassets under this category must be redeemable for underlying traditional asset(s)", Section 2.2
37

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 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 [38] "most cryptoassets 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 also issued an opinion on its proposed amendments to MiCA in February 2021.[39] These proposals aim to grant greater powers to the ECB, including the ability to set prudential requirements for certain stablecoin issuers.

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.[40]

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.

38 Robby Houben, Alexander, 'Crypto-assets: Key developments, regulatory' (Research Group Business & Law, Belgium April 2020) <https://www.europarl.europa.eu/RegData/etudes/STUD/2020/648779/IPOL_STU(2020)648779_EN.pdf>
39 Opinion of the European Central Bank of 19 February 2021 on a proposal for a regulation on Markets in Crypto-assets, and amending Directive (EU) 2019/1937 (CON/2021/4) (2021/C 152/01)
<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021AB0004&from=EN>
40 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>

What are we waiting for?
Looking ahead, we are awaiting a subsequent consultation from the BCBS on the prudential treatment of banks' cryptoasset exposures following its preliminary proposals in June 2021.

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 the PRA's letter of June 2018, [41] 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 over time, as adoption and market experience demonstrates the resilience associated with more conventional types of assets.

41 PRA Dear CEO Letter <https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/letter/2018/existing-or-planned-exposure-to-crypto-assets.pdf>

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 policymakers can remove 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.

As part of its consultation published in January 2021 (as described above), HMT has called for feedback on (amongst other things) the potential advantages and disadvantages of the adoption of DLT technology by financial market infrastructures (FMIs), views on the extent to which UK regulation or legislation is fit for purpose in terms of the adoption of DLT in wholesale markets and FMIs in the UK, the wider industry incentives or obstacles to the adoption of DLT in wholesale markets and FMIs in the UK, and whether common standards would help drive the uptake of DLT or other new technology in financial markets[42].

As part of its Payments Landscape Review, HMT has noted that, in relation to digital payments: "It is the government's view that other firms have the potential to become systemically important firms in payment chains and may warrant Bank of England supervision. The bar for systemic importance and Bank of England supervision would remain high, as it is for payment systems at present."[43] HMT further notes that it will "look to ensure consistency, in the spirit of 'same risk, same regulatory outcome', between regulation applied to stablecoins and comparable payments activities".[44]

42 HM Treasury, ' UK regulatory approach to cryptoassets and stablecoins: Consultation and call for evidence (January 2021) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/950206/HM_Treasury_Cryptoasset_and_Stablecoin_consultation.pdf> Accessed October 2021, p 33

43 HM Treasury, 'Payments Landscape Review: Response to the Call for Evidence', section 2.39

44 ibid section 2.41.

Further detail on these proposals would be welcome particularly as regards any adaptation of existing legislation to DLT and stablecoin based systems.

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. 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 DLT 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 the Central Securities Depositories Regulation (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 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, [45] 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[46] that outlines the 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[47], published a set of 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.

The CPMI Board of the International Organization of Securities Commissions (IOSCO) has published a consultation on the application of the Principles for Financial Markets Infrastructure (PFMIs) to stablecoin arrangements.[48] The view of IOSCO and CPMI is that the arrangements for the transferring of coins between users is comparable to the transfer function performed by other types of FMIs such as traditional payment systems. Therefore, a stablecoin arrangement performing a transfer function can be considered to be an FMI for the purpose of applying the PFMIs. To the extent that a stablecoin arrangement is determined by regulators to be of systemic importance, IOSCO and CPMI would expect it to observe all relevant principles in the PFMIs. Given their novel features, some adaptation of the PFMIs may be necessary and care should be taken not to unduly stifle innovation.

The extension of the PFMIs to stablecoin arrangements would provide greater legal certainty for its participants. This may in turn lead to greater market confidence in such systems thereby facilitating the further development of such systems and related products and services.

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, 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. 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.

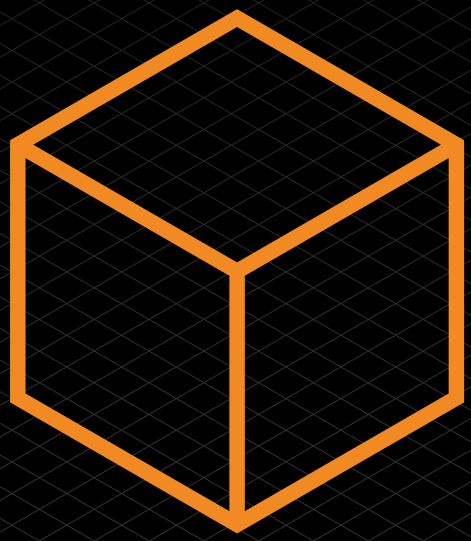
45 European Commission, Consultation Document: On an EU framework for markets in crypto-assets (Consultation Document) <https://ec.europa.eu/info/sites/info/files/business_economy_euro/banking_and_finance/documents/2019-crypto-assets-consultation-document_en.pdf>

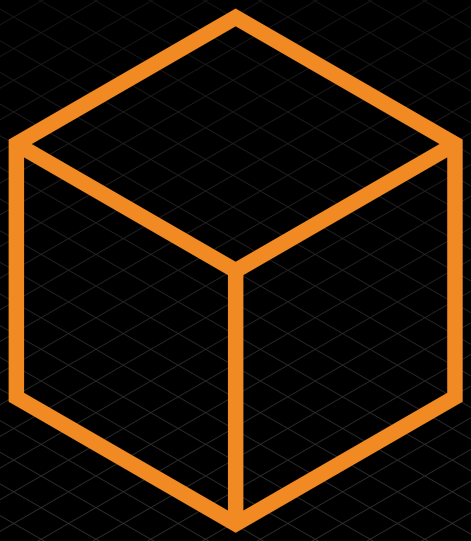
46 Committee on Payments and Market Infrastructures, ‘Investigating the impact of global stablecoins’, (Report, G7 Working Group on Stablecoins, October 2019) <https://www.bis.org/cpmi/publ/d187.pdf>

47 Financial Stability Board, Consultative Document, ‘Addressing the regulatory, supervisory and oversight challenges’ (14 April 2020) raised by “global stablecoin” arrangements

48 Committee on Payments and Market Infrastructures Board of the International Organization of Securities Commissions Consultative report ‘Application of the Principles for Financial Market Infrastructures to stablecoin arrangements <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD685.pdf>

4

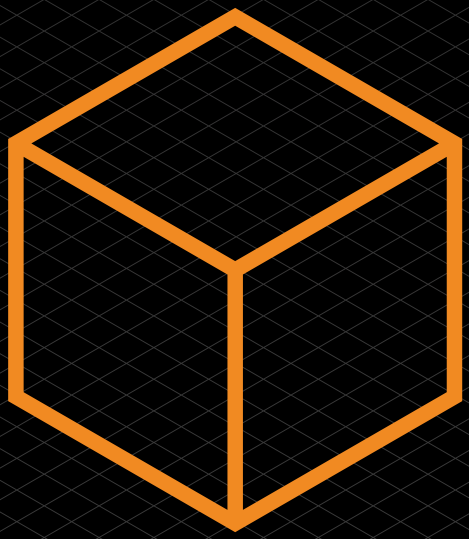




Part 1: Developing Technologies

Section 4 Types of Cryptoassets and DeFi



Section 4: Types of Cryptoassets and DeFi

Marc Piano (Harney Westwood& Riegels LLP (Cayman Islands)) and Joey Garcia (Isolas LLP (Gibraltar))

Introduction

This section looks at different types of cryptoassets: in Part A: Central Bank Digital Currencies (CBDCs) and Part B: Stablecoins. In Part C this section considers developments in the Decentralised Finance (DeFi) space and the adoption of the Financial Action Task Force (FATF) recommendations in respect of Virtual Asset Service Providers (VASPs).

PART A: Central Bank Digital Currencies

Marc Piano, Harney Westwood & Riegels LLP (Cayman Islands). The author is grateful for comments received from Albert Weatherill (Norton Rose Fulbright LLP); Ciarán McGonagle (International Swaps and Derivatives Association, Inc. (ISDA)); Mary Kyle (City of London Corporation); Thomas Hulme (Brecher LLP); Tom Rhodes (Freshfields Bruckhaus Deringer LLP); and Adrian Brown (Harney Westwood & Riegels LLP (Cayman Islands)).

This section looks at CBDCs and new forms of private money as general concepts, considers their potential distinction from other forms of virtual assets, and legal issues for legal practitioners to consider.

What is 'money'?

Briefly, 'money' is that which can serve as a store of value, a unit of account and a medium of exchange.

In most economies, money takes the form of a fiat currency. This is money backed by a government and declared to be "legal tender" (which means that it can be used to settle debts or financial obligations). For example, under section 1(2) of the Currency and Bank Notes Act 1954 (CBNA), all bank notes issued by the Bank of England constitute legal tender in England and Wales. Under section 2(1A) of the Coinage Act 1971, gold coins are legal tender for payment of any amount, nickel and silver coins in denominations of more than 10 pence are legal tender for any amount not exceeding GBP10, such coins in denominations of less than 10 pence are legal tender for any amount not exceeding GBP5, and bronze coins are legal tender for any amount not exceeding 20 pence.

The two forms of money in the UK are central bank money and private money. The Bank of England provides a brief overview of these in its 2021 discussion paper on new forms of digital money.

Central bank money represents liabilities of the central bank. For the public, this takes the form of cash (bank notes and coins). Under section 1(3) of the CBNA, bank notes may be exchanged at the Bank of England for bank notes of lower denominations. For commercial banks, this takes the form of central bank reserves. How these work is beyond the scope of this guidance.

Private money is commercial bank money, i.e. people's money deposited at commercial banks and loans created by commercial banks. The Bank of England notes that: "Around 95% of the funds households and businesses hold that are typically used to make payments are now held as commercial bank deposits rather than cash."[49]

What are CBDCs?

The Bank of International Settlements (BIS) defined CBDCs in its 2018 paper on the topic (CPMI-MC (2018)) as: "potentially a new form of digital central bank money that can be distinguished from reserves or settlement balances held by commercial banks at central banks"[50].

49 BOE June 2021 Discussion Paper, section 1.1
50 Bank of International Settlements, March 2018, p 1 <https://www.bis.org/cpmi/publ/d174.pdf>

As set out in the BIS 2020 Report[51], CBDCs may be wholesale-only or general purpose.

Wholesale-only: As with electronic central bank deposits, wholesale digital token CBDCs would only be accessible by pre-defined users (i.e. qualifying financial institutions) and may (but is not required to) be combined with the use of distributed ledger technology, with the aim of enhancing settlement efficiency for a range of transactions including but not limited to retail payments, transfers, cross-border payments, and transactions involving securities and derivatives. Such wholesale-only CBDCs could also be used as a backing or settlement asset for other payment or stablecoin services, such as payment services or stablecoins (including synthetic CBDCs discussed below) offered by the relevant institution.

General purpose: these may be token-based or account-based. These operations are described in the Consensys white paper[52]:

> *"In a token-based system, the CBDC is created as a token with a specific denomination. The transfer of a token from one party to another does not require reconciling two databases, but is rather the near-immediate transfer of ownership, very much like handing over banknotes from one person to another.*
>
> *"In an account-based system, the central bank would hold accounts for users of the CBDC, and would handle the debit and credits between users itself."*

A token-based CBDC would likely require relevant accounts and their controllers to be verified and permissioned in order to receive and transact with CBDC tokens, together with some form of reporting and record-keeping system of transactions occurring in that account. Unlike bank notes where ownership is determined by possession, ownership of CBDC accounts and held tokens is likely to be determined by control of the private key to the account or its equivalent.

A general purpose CBDC, whether token-based or account-based, requires an infrastructure comprising the issuing central bank, operator(s) of the system infrastructure, participating payment service providers (PSPs) and banks, who may be responsible for creating and permissioning relevant accounts for CBDC tokens and reporting and record-keeping requirements as mentioned above. The BIS 2020 Report notes there could be overlaps in roles, such as the issuing central bank operating the system infrastructure[53].

In its March 2020 discussion paper (the BoE March 2020 Discussion Paper), the Bank of England (the BoE) considers the potential impact of "disintermediation" through the introduction of CBDCs (i.e. the conversion of deposits held at commercial banks to CBDCs and the consequential reduction in the banking sector's balance sheet) as part of a wider range of complex policy and practical factors, noting that: "If disintermediation were to occur on a large scale, that would either imply a large fall in lending or would require banks to seek to borrow significantly more from the Bank of England. This could have profound implications for the structure of the banking system and the [BoE's] balance sheet."[54]

In short, CBDCs could reduce the role of commercial banks in the financial system, and managing the demand for CBDCs over bank deposits is a critical CBDC design factor.

What is the status of development and implementation of CBDCs?
As of May 2021, around 80% of central banks globally were exploring use cases

51 Bank of International Settlements, 2020 <https://www.bis.org/publ/othp33.pdf>
52 Consensys AG, January 2020, pp 17-18 <https://cdn2.hubspot.net/hubfs/4795067/ConsenSys-CBDC-White-Paper.pdf>
53 BIS 2020 Report, p 4
54 Bank of England, 12 March 2020, Chapter 5.2 <https://www.bankofengland.co.uk/-/media/boe/files/paper/2020/central-bank-digital-currency-opportunities-challenges-and-design.pdf?la=en&hash=A71920A2FFB6511E43F787019C549262049CC7A8#page=42>

involving CBDCs, with 40% already testing proof-of-concept programmes[55]. The Eastern Caribbean Central Bank (the monetary authority for Anguilla, Antigua and Barbuda, Commonwealth of Dominica, Grenada, Montserrat, St Kitts and Nevis, Saint Lucia, and St Vincent and the Grenadines) introduced its CBDC, DCash, on 31 March 2021 for public use[56].

The People's Bank of China has been researching its Digital Currency Electronic Payment (DC/EP) (DCEP) since 2014 and conducting small-scale trials in several cities, most recently in October 2020[57]. The PBOC intends to conduct a large-scale trial at the Winter Olympics in Beijing in February 2022[58].

The United Kingdom published terms of reference[59] for an HM Treasury and BoE CBDC taskforce in April 2021 to ensure a strategic approach to, and to promote close coordination between, the UK authorities as they explore CBDC, in line with their statutory objectives. In late September 2021, HM Treasury and the BoE announced the membership of the CBDC Engagement and Technology Forums to help progress the taskforce, which consists of senior stakeholders from industry, civil society and academia responsible for gathering strategic input on policy considerations and functional requirements pertaining to CBDCs[60]. CBDCs are also considered by the BoE as part of the BoE June 2021 Discussion Paper.

Design and operation of CBDCs will vary by central bank requirements, but a key consideration acknowledged by both the BIS and BoE is CBDC compliance with relevant anti-money laundering and countering the financing of terrorism frameworks. Research and discussions are ongoing around the use of CBDCs in cross-border payments, and this is considered briefly in more detail below.

What are "new forms of private money"?
The Bank of England defines "private money" in the BoE June 2021 Discussion Paper as mainly taking the form of deposits in commercial banks "that is, claims on commercial banks held by the public. This 'commercial bank money' is created when commercial banks make loans."[61]

The BIS 2020 Report notes that:

> *"Central banks support commercial bank money in various ways, by: (i) allowing commercial banks to settle interbank payments using central bank money; (ii) enabling convertibility between commercial and central bank money through banknote provision; and (iii) offering contingent liquidity through the lender of last resort function. Importantly, while cash and reserves are a liability of the central bank, commercial bank deposits are not."*

The key point to note is that private money, and any tokenised forms of private money, are not to be considered as CBDCs, as they are not issued by central banks. More likely, tokenised forms of private money will be deemed to be stablecoins and regulated accordingly (see Part B).

The BIS 2020 Report also considers "synthetic CBDC", under which PSPs issue liabilities matched by funds held at the central bank. Although these PSPs would act as intermediaries between the relevant central bank and end user, the BIS does not consider such liabilities as CBDCs, as the end user does not hold a claim against the central bank, only against the PSP[62].

55 Coinbase, 19 May 2021 <https://www.coindesk.com/about-80-of-central-banks-are-exploring-cbdc-use-cases-bison-trail-report-says/>
56 Eastern Caribbean Central Bank <https://www.dcashec.com/about>
57 Jiaying Jiang Karman Lucero, Stanford Law School, 6 April 2021 <https://law.stanford.edu/2021/04/06/background-and-implications-of-chinas-central-bank-digital-currency-e-cny/>
58 CBDC Insider, 6 August 2021 <https://cbdcinsider.com/2021/08/06/china-ramps-up-cbdc-pilot-plans-ahead-of-2022-winter-olympics/>
59 HM Treasury, April 2021 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1022969/Final_CBDC_Taskforce_ToR_update.pdf>
60 Bank of England, 29 September 2021 <https://edu.bankofengland.co.uk/news/2021/september/membership-of-cbdc-engagement-and-technology-forums>
61 BoE June 2021 Discussion Paper, section 1.1
62 BIS 2020 Report, p 4

Such arrangements, whether offered by qualifying financial institutions or other non-central bank entities (such as large technology companies), may constitute stablecoins, discussed in Part B, and may be subject to one or more legal and regulatory regimes in the relevant jurisdiction.

What are the properties of CBDCs?
For the purposes of this guidance, the key distinctions between CBDCs and other forms of virtual assets are that CBDCs are unlikely to be treated the same as other form of virtual assets for legal and regulatory purposes, because: (i) conceptually and by their intended function, they are, or are intended to be, representations of fiat currency; and (ii) practically, they are centrally issued and controlled by the issuing central bank instead of banks and other third parties (and such non-CBDC issuances are likely to be deemed be stablecoins for legal and regulatory purposes).

The BoE March 2020 Discussion Paper[63] notes that whilst distributed ledger technology may offer potentially useful innovations, there is no presumption that CBDCs inherently require DLT.

CBDCs are "programmable money". This means that the behaviour of CBDC accounts or tokens – alone, or in combination with smart contracts or third-party data oracles – can be programmed with instructions beyond those required merely to facilitate or restrict CBDC movement between accounts. The July 2021 white paper on the People's Bank of China's (PBOC) CBDC project notes that this can include functionality enabled through deployment of smart contracts that do not impair the CBDC's monetary function[64]. Such instructions could include limits on holdings, expiration dates, automated inflation or deflation rates, recipient or transaction restrictions and direct implementation of other forms of public or monetary policy.

The main design properties are: (a) account-based or token-based CBDCs; (b) direct pass-through (remuneration) of central bank interest rate adjustments on CBDC accounts, which can include negative rates; (c) structuring and tiering of remuneration (if any); and (d) soft and/or hard limits on CBDC holdings. Both the BIS and BoE consider the arguments for and against these structuring considerations in CPMI-MC (2018) and the BoE March 2020 Discussion Paper.

The "programmable money" element of CBDCs can theoretically facilitate policy implementation at a more granular level. For example, BNY Mellon notes that "the CBDC wallet application can be programmed in a way such that funds contained within can only be spent in designated areas and also have a certain expiry date — an exercise almost impossible to implement with physical notes and coins".[65] We would note that this approach may require some form of location-based geographical and spending restrictions, and/or linking a CBDC wallet to a holder's verified residential address or other form of digital identity, to be effective. The PBOC has already experimented with CBDC expiration dates.[66] Theoretically, this means that CBDCs could be programmed to encourage or discourage use in certain types of transactions, in alignment with national policy and behavioural objectives.

Can CBDCs be used for cross-border payments?
Central banks are designing CBDCs pursuant to domestic mandates and public policy objectives. These influence a range of design, structuring and operational considerations. CBDC interoperability will be a key element that determines whether CBDCs are suitable or even technically capable of facilitating cross-border payments.

63 BoE March 2020 Discussion Paper, Chapter 6
64 Working Group on E-CNY Research and Development of the People's Bank of China, July 2021, Section 3.2.7 <http://www.pbc.gov.cn/en/3688110/3688172/4157443/4293696/2021071614584691871.pdf>
65 Geoff Yu (BNY Mellon), Aerial View, November 2020 <https://www.bnymellon.com/content/dam/bnymellon/documents/pdf/aerial-view/china-and-the-dawn-of-digital-currency.pdf.coredownload.pdf>
66 Enrique Dans, Forbes, 7 April 2021 <https://www.forbes.com/sites/enriquedans/2021/04/07/chinas-digital-currency-is-about-to-disrupt-money/?sh=6c42e2ca1665>

The BIS published a dedicated paper on this topic in March 2021 (the BIS mCBDC Paper), introducing the concept of "multi-CBDC arrangements" (mCBDC) [67]. This paper acknowledges that improving cross-border payments efficiency acts as an important motivation for CBDC research and sets out three conceptual models of mCBDC interoperability to facilitate CBDCs being used in cross-border payments:

— developing common international standards, allowing compatible CBDC exchange between national CBDC systems;

— linking multiple CBDC systems through a shared technical interface or a common clearing mechanism (which may be decentralised); and

— integrating multiple CBDCs into a single mCBDC.

The BIS mCBDC Paper concludes by encouraging central banks to collaborate in CBDC development to identify unintended barriers, and to aid efficiency in enabling CBDC conversion as part of enabling CBDC cross-border payments. BIS's position is that this approach is preferable to widespread use of private global currencies but acknowledges the importance of safety in the CBDC design process. Development in this area is ongoing and this guidance will be updated as CBDC design models are finalised and tested.

Will CBDCs replace cash and existing banking and payment infrastructure?
CBDCs do not automatically imply either retail accessibility and use, nor replacement of existing cash, banking and payment infrastructures. The BIS 2020 Report emphasises as a foundational principle that CBDCs should complement existing central bank money and co-exist with robust private money to support public policy objectives. On cash, the BIS 2020 Report states: "Central banks should continue providing and supporting cash for as long as there is sufficient public demand for it."[68]

This position appears to be reinforced at the level of government policy. For example, the G7 document, Public Policy Principles for Retail Central Bank Digital Currencies (the G7 PPP), published in October 2021, is explicit in both Principle 9 on digital economy and innovation[69] and Principle 10 on financial inclusion[70] that CBDCs will coexist alongside cash.

Nonetheless, the possibility that CBDCs may eventually replace cash has been hypothesised, together with possible implementation mechanics. In a blog article dated 5 February 2019[71], the International Monetary Foundation describes a process by which a cash economy could transition to CBDCs through the use of negative interest rates. This involves separating the monetary base into cash and CBDCs, then applying a negative interest rate policy on cash as against conversion into CBDCs. Combined with dual acceptance of cash and CBDCs as a means of payment, this could incentivise a relatively gradual transition to CBDCs by making them a preferable form of money to cash. The BoE also notes the possibility of CBDCs replacing cash in the BoE June 2021 Discussion Paper: "In principle, a CBDC could be used, in conjunction with a policy of restricting the use of cash. If the interest rate on the CBDC could go negative, this could soften the effective lower bound on interest rates and lower the welfare loss associated with the opportunity cost of holding cash."[72] The BoE goes on to note that: "In practice, however, the UK authorities remain committed to ensuring access to cash to those that need it."

This important caveat is consistent with the stated policy positions set out in the G7 PPP: that as at the date of this guidance CBDCs will not replace cash, at least not

67 Papers No 115, Bank of International Settlements, March 2021 <https://www.bis.org/publ/bppdf/bispap115.pdf>
68 BIS 2020 Report, section 3.1
69 G7, October 2021, p 12
70 G7 PPP, p 13 <https://www.mof.go.jp/english/policy/international_policy/convention/g7/g7_20211013_2.pdf>
71 Ruchir Agarwal and Signe Krogstrup, IMFBlog, 5 February 2019 <https://blogs.imf.org/2019/02/05/cashing-in-how-to-make-negative-interest-rates-work/>
72 BoE June 2021 Discussion Paper, section 4.5

among the G7, and there are currently no indications that this position is likely to change for the foreseeable future.

Hypothetically, if CBDCs were to replace cash in whole or in part, their programmable nature could have a profound impact across and between society, human behaviour, economic activity, monetary and public policy and the relationship between governments, central banks, financial institutions, businesses and citizens. Discussion of these elements is well outside the scope of this guidance. Even if governments were to adjust any current publicly-stated policy positions and encourage a transition from cash to CBDCs, there is a confluence of as yet unresolved considerations around cross-border payments, compliance with anti-money laundering and data protection laws, responsibility and accountability for provisioning CBDC account access, and a lack of widespread infrastructure and acceptance. Together, these factors are likely to heavily influence CBDC design factors and mean that any envisaged transition from cash to CBDCs is unlikely to proceed at pace or at an international scale in the short to medium term.

CBDCs distinguished from other forms of virtual assets and practical legal considerations

As noted above, CBDCs are, or are representations of, fiat money and constitute legal tender. This means that CBDCs are likely to be explicitly or implicitly excluded from relevant local laws and regulations governing other forms of virtual assets and/or VASPs so that CBDCs can achieve their intended purpose.

For example, the FATF, the global standard-setting body for anti-money laundering and countering the financing of terrorism standards, explicitly acknowledges this position in its draft updated guidance on a risk-based approach to virtual assets and VASPs (considered separately, later in this section) (the Draft Updated FATF Guidance)[73], as does the Financial Stability Board (FSB) in its final report and high-level recommendations on "Global Stablecoin Arrangements" (the FSB Stablecoins Report)[74], considered in more detail in Part B, below.

Legal practitioners should be aware of the distinctive treatment of CBDCs as against other forms of virtual assets for legal and regulatory purposes. Although recognised as fiat currency and legal tender by the relevant government, the design and implementation of CBDCs and their use in transactions may give rise to additional analysis, advice and transactional considerations, such as cross-border acceptance, compliance with local anti-money laundering and countering the financing of terrorism laws, additional representations and warranties around relevant properties for account-based CBDCs, acceptability of relevant CBDCs as a means of payment in cross-border transactions and settlement and completion mechanics.

This section of this guidance will be updated and expanded on in future, as the development and implementation of CBDCs progresses.

Conclusion

CBDCs constitute a new form of "programmable money". Although they are "virtual assets", being assets that are virtual, their intended function lends to their exclusion from the operation of laws and regulations intended to cover other forms of virtual assets. The stated public policy of a number of governments, combined with a range of discrete and sometimes overlapping design, implementation and compliance considerations, do not lend to any indication that CBDCs, when introduced, are or are likely to replace cash in the short to medium term. Legal practitioners should be aware of CBDCs as a concept, their likely distinction from other forms of virtual assets for legal and regulatory purposes, and development of coordinated policies around cross-border acceptance of CBDCs, which will be relevant should clients seek adoption or acceptance of CBDCs in relevant transactions as a range of legal and regulatory issues are concomitant with such intentions.

73 Financial Action Task Force, March 2021, paragraph 16 <https://www.fatf-gafi.org/media/fatf/documents/recommendations/March%202021%20-%20VA%20Guidance%20update%20-%20Sixth%20draft%20-%20Public%20consultation.pdf>

74 Financial Stability Board, October 2020, Glossary definition of "digital asset", p 5 <https://www.fsb.org/wp-content/uploads/P131020-3.pdf>

PART B: Stablecoins

Marc Piano, Harney Westwood & Riegels LLP (Cayman Islands). The author is grateful for comments received from Albert Weatherill (Norton Rose Fulbright LLP); Ciarán McGonagle (International Swaps and Derivatives Association, Inc. (ISDA)); Mary Kyle (City of London Corporation); Thomas Hulme (Brecher LLP); Tom Rhodes (Freshfields Bruckhaus Deringer LLP); and Adrian Brown (Harney Westwood & Riegels LLP (Cayman Islands)).

This section provides a high-level overview of stablecoins and considerations for legal practitioners.

What is a stablecoin?

There is no consensus definition of a stablecoin. This guidance adopts the definition of a stablecoin as used by the FSB in the FSB Stablecoin Report (the FSB Stablecoin Report) as "a cryptoasset that aims to maintain a stable value relative to a specified asset, or a pool or basket of assets".[75]

This definition encompasses a range of stablecoins, broadly divided two categories: i. asset-backed stablecoins and ii. algorithm-based stablecoins. Distinguishing features between stablecoin models include design, operation and associated contractual rights. Some stablecoins may operate as a hybrid, being asset-backed as well as utilising an algorithmic stabilisation mechanism.

i. Asset-backed stablecoins

Asset-backed stablecoins represent value by reference to an underlying reserve which may consist of one or more fiat currencies, precious metals, securities such as bonds, other virtual assets or a portfolio of several assets.

Examples of asset-backed stablecoins include:

— Fiat-backed stablecoins, such as Tether (USDT, backed by the US Dollar), EURS (backed by the Euro), USD Coin (USDC, backed by the US Dollar);

— Commodity-backed stablecoins, such as Digix (DGX, backed by physical gold), Tiberius Coin (TCX, backed by a basket of precious metals) and SwissRealCoin (SRC, backed by a portfolio of Swiss commercial real estate); and

— Virtual asset-backed stablecoins, such as MakerDAO (DAI, backed by other virtual assets collateralised in smart contracts) and Synthetix (SNX, which can be backed by other virtual assets, but can also be backed by fiat currency).

ii. Algorithmic stablecoins

Algorithmic stablecoins are not linked (or wholly linked) to underlying reserve assets. Instead, such stablecoins deploy an algorithm or protocol which acts as the "central bank", increasing or decreasing supply in accordance with the rules of the algorithm, which may be by reference to relevant third party data feeds (known as oracles), and the rules of which may be changed by the applicable (usually decentralised) governance process. The algorithm rules may reference a peg of market supply of the relevant stablecoin itself, or a peg based on one or more other virtual assets which are not themselves held in reserve. If demand increases or decreases, then the algorithm calculates the increase or decrease of token supply to maintain a stable market value.

Examples of algorithmic stablecoins include Basis (BAC, which uses an automated stability mechanism to maintain supply to keep the token's value relative to the US Dollar) and Frax (FRAX, which uses underlying partial collateralisation together with a base stabilisation mechanism, whilst also allowing additional fractional stability though further policy changes that do not affect the pegging of the FRAX token as determined by the base stabilisation mechanism).

75 Financial Stability Board, October 2020, Glossary definition of "stablecoin", p 5 <https://www.fsb.org/wp-content/uploads/P131020-3.pdf>

As at the date of this guidance, algorithmic stablecoins have relatively little adoption in the market. Fiat-backed stablecoins are the primary form of stablecoin in use.

Whether or not a cryptoasset constitutes a stablecoin will be determined by regulation, regardless of the underlying technological or economic characteristics of the asset regardless of intended use, referenced assets, price determination and/or algorithmic adjustments, and whether fully centralised, partially-distributed or highly-distributed.

Absent a common definition, both the FSB Stablecoins Report and the International Organization of Securities Commissions (IOSCO) report[76] (the IOSCO Stablecoins Report) broadly agree on three underlying properties that distinguish stablecoins from other forms of cryptoassets:

— a stablisation mechanism to stabilise the price of the stablecoin, compared to other non-stabilised cryptoassets;

— the technology used/the programmed functions and activities, such as governance, issuance, transfer, redemption and destruction (i.e. if distributed ledger technology is used, it is more likely to use a permissioned rather than permissionless protocol so that eligibility and participation criteria can be determined and controlled); and

— the eligibility criteria for participation, which in part may depend on the level of centralisation and control over the stablecoin's lifecycle and operability.

As noted in this guidance's section on CBDCs, virtual assets issued by central banks will be a form of central bank money and thus fiat currency, and are therefore likely to be explicitly excluded from categorisation as a cryptoasset under relevant laws and regulations to enable them to operate as intended and to reflect their nature as a form or representation of fiat currency. This treatment of CBDCs should be distinguished from stablecoins issued by commercial banks or other third parties (such as large technology companies) and intended as a means for payment that are linked to either that bank's or third party's own deposits or that bank's claim against central bank deposits; such stablecoins will constitute cryptoassets and not CBDCs as they are not issued by central banks. The potential legal and regulatory treatment of stablecoins is considered below.

What is the purpose of a stablecoin?
Fundamentally, stablecoins purport to offer price stability relative to the often extreme price volatility and fluctuation commonly seen in other forms of virtual assets such as cryptocurrencies. Many stablecoins are intended to function as a form of money by meeting the traditional criteria of money as[77] offering a store of value, unit of account and medium of exchange. This does not presume that all stablecoins are intended to function as a form of money – the intended purpose and actual use depends in each case on the relevant arrangements, such as where a stablecoin is created as a representation of collateralised cryptoassets (which may include cryptocurrencies) used to secure a loan. Further, although a stablecoin may be created and offered as a form of money, its utility depends on acceptance as a means of payment between parties – as stablecoins do not constitute fiat currency they do not have the benefit of recognition as legal tender and are not required to be accepted as a means of payment.

In the BoE June 2021 Discussion Paper[78] (the BoE June 2021 Discussion Paper), the BoE noted the potential for stablecoins to be issued by commercial banks to facilitate payments by retail customers. Stablecoins may also be issued by private

76 "Global Stablecoin initiatives – Public Report" The Board of the IOSCO, March 2020, p 5
77 "International Monetary Fund, Finance & Development, September 2012 <https://www.imf.org/external/pubs/ft/fandd/2012/09/basics.htm>
78 Bank of England, 7 June 2021, section 5 <https://www.bankofengland.co.uk/paper/2021/new-forms-of-digital-money>

non-bank third parties backed against that third party's own assets, such as the Facebook Diem project.

Stablecoins may be created for a variety of purposes, including on a standalone basis for development of use cases by third parties, as a means of payment for products or services offered by the issuer or ecosystem participants, as a payment rail for a payment services ecosystem, to act as a benchmark (possibly by reference to the relevant underlying assets, in which case they may be subject to relevant financial services regulation around benchmarks), or to act as a form of money within the relevant ecosystem, wider protocol on which the stablecoin operates, or sector (if cross-chain compatible).

Another function of stablecoins is to credit yield generation in DeFi protocols. This involves the relevant smart contract (or network of smart contracts) in that protocol receiving cryptoassets from a transferor (i.e. such assets are "staked" and otherwise unavailable for use by the original transferor) and putting them to work – such as allowing the transferred cryptoassets to be used as collateral for borrowing or lending out – with the yield such cryptoassets generate being credited in a stablecoin held by the user of the protocol. This approach allows protocol participants to take the benefit of the yield earned on the underlying transferred cryptoassets directly into another asset that can be used as a means of payment or otherwise sold or traded.

A common feature also seen in many DeFi protocols is the liquidity pool token (LP tokens). This is a token representing a pro rata share of assets transferred to a liquidity pool and carries the right to receive the yield generated by the underlying cryptoassets staked in the liquidity pool, and the holder has the benefit of such right from holding the LP Token. LP Tokens can themselves be staked in other liquidity pools to generate additional yield. Although LP Tokens are not intended to function as a means of payment in and of themselves, their design, representation of an underlying basket of assets and redemption mechanics could lead them to fall under the definition of a stablecoin in some legal and regulatory frameworks and this element needs careful consideration by lawmakers, drafters and legal practitioners when advising clients on relevant projects, operations or transactions.

Legal and regulatory landscape, development and considerations
Stablecoins whether as standalone projects or as part of a wider business line or operation (whether cryptoasset-specific or not) present complex legal and regulatory challenges requiring consideration due to their potential range of properties and purposes. Given the rapid development and adoption of some stablecoins by some financial institutions and large non-financial institutions (such as Facebook's Diem project), global regulatory standards and local implementation continues to develop as at the date of publication of this guidance.

Legal analysis and advice in this area may need to encompass one or more regulatory frameworks, accommodate potential regulatory overlap and will require fact-specific analysis.

Regulatory development
Financial stability
A key acknowledgement across many of the reports by global supervisory bodies concerning stablecoins is their potential to become systemically important and may, therefore, present systemic risk. This is a welcome acknowledgement that stablecoins may play a critical role in financial services and payment services in particular, and shows that supervisory bodies are factoring the rapid evolution of the design, deployment and adoption of stablecoins into regulatory development within their area of oversight.

Application of CPMI-IOSCO PFMI

The transfer function of a stablecoin (which in practice is a feature of the vast majority of stablecoins) is already deemed by IOSCO to be a financial markets infrastructure (FMI) function[79]. FMI is defined as "a multilateral system among participating institutions, including the operator of the system, used for the purposes of clearing, settling, or recording payments, securities, derivatives, or other financial transactions". A stablecoin participant facilitating the stablecoin transfer function will be subject to the CPMI-IOSCO Principles for Financial Market Infrastructures (PFMI)[80]. A detailed consideration of the PFMI themselves is outside the scope of this guidance.

FSB Stablecoin Report

The FSB Stablecoin Report sets out 10 high-level recommendations around regulatory, supervisory and oversight requirements for stablecoins from a financial stability perspective. The recommendations call for "regulation, supervision and oversight that is proportionate to the risks, and [which] stress the value of flexible, efficient, inclusive, and multi-sectoral cross-border cooperation, coordination, and information-sharing arrangements among authorities that take into account the evolving nature of GSC arrangements and the risks they may pose over time".[81]

A key expectation communicated by the FSB is that: "[Stablecoin] arrangements are expected to adhere to all applicable regulatory standards and address risks to financial stability before commencing operation, and to adapt to new regulatory requirements as necessary."[82]

Although the FSB does not anticipate that every stablecoin inherently poses systemic risks, it does consider that "such instruments may have the potential to pose systemic risks to the financial system and significant risks to the real economy, including through the substitution of domestic currencies".[83]

All 10 recommendations are worth reading in full, as the FSB Stablecoin Report is the work product of a G20 mandate to the FSB to examine regulatory issues raised by stablecoin arrangements and to advise on multilateral responses. This means that the recommendations are likely to be incorporated into each jurisdiction's regulatory framework and/or inform regulatory treatment of stablecoins and stablecoin-related projects.

In October 2021, the FSB published a progress report on the implementation of the recommendations (the FSB Update Report)[84]. The report noted that "while the current generation so-called stablecoins are not being used for mainstream payments on a significant scale, vulnerabilities in this space have continued to grow over the course of 2020-21"[85] and that "jurisdictions have taken or are considering different approaches towards implementing" the 10 recommendations arising out of the original FSB Stablecoin Report. Overall, implementation remains at an early stage, and given this combined with the rapid evolution of the stablecoin landscape, the FSB appears concerned that "differing regulatory classifications and approaches to stablecoins at jurisdictional level could give rise to the risk of regulatory arbitrage and harmful market fragmentation"[86].

The UK government regulatory approach to cryptoassets and stablecoins

On 7 January 2021, Her Majesty's Treasury (HMT) published a consultation document encouraging feedback on the government's approach to cryptoasset

79 "Consultative report – Application of the Principles for Financial Market Infrastructures to stablecoin arrangements", Committee on Payments and Market Infrastructures, Board of the International Organization of Securities Commissions, October 2021, section 1.3.3
80 Technical Committee of IOSCO, Committee on Payment and Settlement Systems, Bank of International Settlements, April 2012 <https://www.bis.org/cpmi/publ/d101a.pdf>
81 FSB Stablecoin Report, p 2
82 FSB Stablecoin Report, p 2
83 FSB Stablecoin Report, p 7
84 Arrangements – Progress Report on the implementation of the FSB High-Level Recommendations", Financial Stability Board, 7 October 2021 <https://www.fsb.org/wp-content/uploads/P071021.pdf>
85 FSB Update Report, Executive Summary, p 1
86 FSB Update Report, section 2 (Progress in implementation at jurisdictional level), p 12

regulation, with a focus on stablecoins (the HMT Consultation)[87]. This is a comprehensive consultation document and worth reviewing for an indication of policy thinking and potential direction of travel in other jurisdictions. The consultation period ran from 7 January 2021 to 21 March 2021, and as at the date of this guidance HMT is analysing feedback and will publish the outcome to such feedback.

The UK government intends to apply the principle of "same risk, same regulatory outcome" in developing regulations governing stablecoins[88] and will maintain an agile approach to reflect international discussions and the rapid development of stablecoins within a framework of objectives and broader considerations set by HMT and the UK Parliament[89]. This means defining "the scope of the regulatory perimeter and the objectives and principles applicable under that new regime" instead of prescriptive legislation or regulation[90].

The UK government intends to introduce a regulatory regime for stablecoins used as a means of payment, to cover firms issuing stablecoins and firms providing services in relation to them either directly or indirectly to consumers[91]. As noted above, this may exclude LP tokens from such a regulatory regime, but draft text is not yet available.

More generally, the UK government intends that "tokens which could be reliably used for retail or wholesale transactions are subject to minimum requirements and protections as part of a UK authorisation regime"[92], which would clearly include stablecoins.

High level requirements of any authorisation regime are set out in section 3.23 of the HMT Consultation, and include capital and liquidity requirements, accounting and audit requirements, reserve asset maintenance and management, and orderly failure and insolvency requirements among other requirements. As discussed in the next few paragraphs, the UK government considers that a systemic stable token arrangement "could be assessed for Bank of England regulation in the same way that current payment systems and service providers are (i.e. when potential disruption could lead to financial stability risks"[93], extending this criteria to stablecoins performing a retail or wholesale payment system function[94]. A stablecoin arrangement with "significant potential" to be systemic at launch would need to be captured from launch by such regulation[95], echoing the FSB Report.

The concept of systemic risk can extend to other participants in stablecoin arrangements, such as wallet providers where wallets are used at scale, meaning they may also be caught within a future regulatory framework[96].

Seeking to capture stablecoin arrangements including issuers or participants that are not based in operating from the UK, the UK government is considering whether "firms actively marketing to UK consumers should be required to have a UK establishment and be authorised in the UK", with options ranging from UK presence and authorisation, through to conducting activity in the UK and determining whether UK authorisation is requirement, or no location requirements[97]. This may also extend to location requirements for systemic stablecoin arrangements[98]. This approach may also be considered by governments and regulators in other jurisdictions, giving rise to the possibility of stablecoin issuers and other participants in stablecoin arrangements requiring multiple authorisations, although some

87 "HMT, 7 January 2021 <https://www.gov.uk/government/consultations/uk-regulatory-approach-to-cryptoassets-and-stablecoins-consultation-and-call-for-evidence>
88 HMT Consultation, section 2.1
89 HMT Consultation, section 2.3
90 HMT Consultation, section 2.5
91 HMT Consultation, section 3.9
92 HMT Consultation, section 3.16
93 HMT Consultation, section 3.31
94 HMT Consultation, section 3.32
95 HMT Consultation, section 3.32
96 HMT Consultation, section 3.36
97 HMT Consultation, section 3.38
98 HMT Consultation, section 3.39

regulatory regimes may recognise authorisation or its equivalent in other jurisdictions operating a suitable or equivalent regime. Legal practitioners should be aware of the development of regulatory regimes when advising clients and the possibility of full licensing requirements or treatment of licensees in other jurisdictions on either an exemption or "lighter touch" basis.

General considerations

Constituent components of stablecoin arrangements may be subject to different regulatory treatment depending on its role within the Stablecoin ecosystem, whether the stablecoins themselves are systemically important or not.

For example, the BoE June 2021 Discussion Paper (which sets out helpful legislative development context in Box H) expects that: "Payment chains that use stablecoins should be regulated to standards equivalent to those applied to traditional payment chains. Firms in stablecoin-based systemic payment chains that are critical to their functioning should be regulated accordingly."[99] The BoE also notes that the need to consider different regulatory regimes for systemic and non-systemic stablecoin arrangements, which could include "clarity of regulatory expectations for industry, the need for minimum standards across all stablecoins used for payments, impacts on competition and innovation, and how to ensure a smooth transition between future regimes for non-systemic and systemic stablecoins", including managing any "cliff-edge" effects between regimes if a stablecoin grew to be systemic over time[100].

On stablecoins themselves, the BoE's position is that: "Where stablecoins are used in systemic payment chains as money-like instruments they should meet standards equivalent to those expected of commercial bank money in relation to stability of value, robustness of legal claim and the ability to redeem at par in fiat."[101] This BoE June 2021 Discussion Paper considers different regulatory models for meeting the Financial Policy Committee expectations[102], noting that some stablecoin issuers already operate under electronic money regulations (which may need enhancements)[103].

As with the FSB Stablecoin Report, the BoE envisages a proportionate and risk-based approach and aims to implement any regulatory models so that users can substitute between different forms of money without consequence for their level of protection[104].

BCBS proposed capital requirements

As a brief comment, it is also worth noting the BCBS's Consultative Document on the prudential treatment of cryptoasset exposures (the Basel Consultation Document)[105] in relation to stablecoin. In short, this proposes new guidance on the application of current rules to stablecoin holdings by applicable financial institutions (i.e. banks) to capture the risks relating to stablisation mechanisms (with further consideration for capital add-ons). The Basel Consultation Document proposes that stablecoins are not eligible forms of collateral in themselves for the purposes of recognition as credit risk mitigation, as "the process of redemption adds counterparty risk that is not present in a direct exposure to a traditional asset"[106]. This relates to stablecoin holdings, rather than stablecoins issued by the relevant financial institution. On the latter form of stablecoins, the Basel Consultation Document proposes that exposure to "Group 2" cryptoassets (i.e. those not falling to be classified under Group 1a (tokenised traditional assets) or Group 1b (stablecoins)

99 BoE June 2021 Discussion Paper, section 5.1
100 BoE June 2021 Discussion Paper, section 5.3.5
101 BoE June 2021 Discussion Paper, section 5.2
102 "Bank of England, December 2019 <https://www.bankofengland.co.uk/financial-stability-report/2019/december-2019> These expectations are that: "Payment chains that use stablecoins should be regulated to standards equivalent to those applied to traditional payment chains. Firms in stablecoin-based systemic payment chains that are critical to their functioning should be regulated accordingly." and "Where stablecoins are used in systemic payment chains as money-like instruments they should meet standards equivalent to those expected of commercial bank money in relation to stability of value, robustness of legal claim and the ability to redeem at par in fiat."
103 BOE June 2021 Discussion paper, sections 5.3.1 and 5.3.5
104 BOE June 2021 Discussion Paper, section 5.3.5
105 Basel Committee on Banking Supervision, Bank of International Settlements, June 2021 <https://www.bis.org/bcbs/publ/d519.pdf>
106 Basel Consultation Document, section 2.1, p 13

will be subject to a conservative prudential treatment based on a 1250% risk weight applied to the maximum of long and short position of each type of cryptoasset. The intention is for the capital to be "sufficient to absorb a full write-off of the cryptoasset exposures without exposing depositors and other senior creditors of the banks to a loss"[107]. At a minimum, this approach requires banks to hold risk-based capital at least equal in value to their Group 2 cryptoasset exposures, with additional risk-based capital holding requirements where such exposure includes short positions. This approach may inform the design and reserve decisions of banks seeking to issue their own stablecoins backed by one or more virtual assets held other than in a 1:1 reserve ratio.

Local law

As indicated above, regulators and international bodies are working to identify the risks posted by stablecoins and develop principles for stablecoin-specific regulatory regimes. However, even where regulatory regimes dedicated to Stablecoins have not yet been implemented, stablecoin arrangements may be subject to existing law and regulation.

As noted below, this will include existing financial services regulation. Some stablecoins will meet the definition of "electronic money" and need to be regulated under relevant financial services legislation (such as the Electronic Money Regulations 2017 and the Payment Services Regulation in the UK) (see 5.3.4 of the BoE June 2021 Discussion Paper). Some stablecoin models could be structured as bank deposits, in which case the issuers would need to be regulated as banks (see article 5 of the Regulated Activities Order 2001 for the UK, and recently published news articles on this possible approach in the United States of America[108]). These will be concerns for legal practitioners advising clients forming or involved in a stablecoin arrangement. As noted below, payment services regulation is also a relevant consideration.

It may be advisable to consult regulators, such as the FCA in the UK, if there is doubt as to whether a regulated activity is being carried out. Regulators are likely to scrutinise cryptoasset arrangements closely, so open and constructive cooperation would be advisable.

Counterparties to potential Stablecoin transactions will need to understand (and legal practitioners may need to advise on) matters such as:

— whether the stablecoin holder has a legal claim against an issuer or any other party by which they can redeem the stablecoin for fiat currency or some other asset

— the party against whom a stablecoin holder may claim

— the assets backing the stablecoin

— what happens if the stablecoin issuer or the person against whom a claim may be enforced fails, and which claims take priority in an insolvency situation

— data protection, anti-money laundering and legal and regulatory obligations of participants in stablecoin arrangements

— the role of other entities or participants in a stablecoin arrangement and the associated risks, e.g. is the client taking credit risk on the entity that holds the backing assets (if any)? What protections and procedures are in place to ensure there are no operational failures, e.g. errors in the ledger recording ownership?

107 Basel Consultation Document, section 3, p 18
108 Wall Street Journal, 1 October 2021, <https://www.wsj.com/articles/biden-administration-seeks-to-regulate-stablecoin-issuers-as-banks-11633103156?mod=latest_headlines>

Regard should be had to the stabilisation mechanism, properties and ecosystem participant role to determine whether existing banking, electronic money or payment/money transmission laws or other financial services regulation may apply in connection with the stablecoin arrangements and relevant activities.

Further, if the underlying assets constitute securities, the relevant stablecoin may be subject to local securities laws. The stablecoin arrangement may also constitute a money market or other form of collective investment vehicle (as noted in the IOSCO Stablecoins Report[109]), in which case the arrangement may be subject to regulation under local collective investment vehicle laws.

A business offering infrastructure or services connected with stablecoins may also be subject to local financial services regulation. As noted in the BoE June 2021 Discussion Paper[110]: "If stablecoins are used to facilitate retail payments, regulation of payment services and critical payment system infrastructure would need to apply to ensure consumer protection and the overall resilience of the network of systems involved." The position will vary by jurisdiction, but legal practitioners should consider whether a client's stablecoin-related operations fall under relevant financial services regulation in the same way that they might if such operations related to fiat currency.

Anti-Money Laundering (AML)/Combating the Financing of Terrorism (CFT)
The FATF reported to the G20 on stablecoins from an AML/CFT risk perspective in June 2020[111] and its treatment of stablecoins forms part of the draft Updated FATF Guidance, first published in March 2021 and finalised and published on 28 October 2021. The FATF is explicit that "the FATF Standards[112] apply to so-called stablecoins and their service providers either as VAs and VASPs or as traditional financial assets and their service providers. They should never be outside the scope of AML/CFT controls."[113]

Careful analysis must be undertaken for each participant in a stablecoin arrangement or stablecoin issuer to determine whether they constitute a "virtual asset service provider" subject to AML/CFT regulation under local AML/CFT laws. As a stablecoin is unlikely to be considered as legal tender under local law, its issuer may be subject to the FATF Standards as they apply to virtual assets and VASPs. At a minimum, this may require some form of registration with the local responsible supervisory body. This may impact transaction sequencing and timings – for example, a stablecoin issuer may need to be registered or licensed by the relevant local authority prior to commencing operations.

Parallel regulatory systems and regulatory overlap
Stablecoin arrangements and intermediaries may be subject to multiple regulatory regimes, and oversight by multiple regulatory or supervisory bodies, depending on the properties of the Stablecoin, role of the participants or intermediaries, and whether the stablecoin arrangements are deemed to be, or likely to be, systemically important.

Conclusion
Stablecoins are the subject of significant ongoing policy, legal and regulatory analysis by governments and the global regulatory community. As policy and regulation evolves and is adopted globally or implemented locally as appropriate, legal practitioners should closely monitor reports, guidance and statements from relevant authorities to understand the policy and regulatory direction of travel and advise clients accordingly.

109 IOSCO Stablecoins Report, pp 7-8
110 BoE June 2021 Discussion Paper, section 5
111 FATF, June 2020 <https://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-FATF-Report-G20-So-Called-Stablecoins.pdf>
112 The Financial Action Task Force < https://www.fatf-gafi.org/publications/fatfrecommendations/?hf=10&b=0&s=desc(fatf_releasedate)>
113 Draft Updated FATF Guidance, Box 1

The nature of stablecoins and the activities of related service providers means that participants in this area may be subject to regulatory oversight from more than one supervisory body and under more than one regulatory framework. This means participants require complex yet comprehensive analysis and advice from legal advisors with a deep and current understanding of the sector in particular and the legal and regulatory matrix in general. In the absence of bespoke and jurisdiction-specific stablecoin regulations, a client's obligations under existing laws and regulations and preparation for compliance with potential future regulatory frameworks should be carefully considered when advising on stablecoin issuance, offering stablecoins within jurisdictions or their acceptance as a means of payment, particularly if there is a cross-border element to the transaction.

PART C: DeFi

Joey Garcia, Isolas LLP (Gibraltar)

Introduction

Part C considers global trends in the regulatory environment for Virtual Asset Service Providers (VASPs) and the interplay with developing concepts of Decentralised Finance (DeFi).

Global Regulatory (VASP) Standards

The Financial Action Task Force (FATF) Interpretative Note to Recommendation 15 (INR. 15) on New Technologies published in June 2019 has been widely recognised and acknowledged as a significant step in the development of standards in the virtual assets space. These updates were also welcomed by the United Nations Security Council in Resolution 2462 of March 2018[114], which called on Member States to assess and address the risks associated with virtual assets, and encouraged Member States to apply risk-based anti-money laundering and counter-terrorist financing regulations to VASPs and identify effective systems to conduct risk-based monitoring or supervision of VASPs.

The Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers aimed to ensure that countries apply the same, or if not higher standards of AML/CFT to VASP related activity as is applied to other regulated financial services industries. In essence, to apply a full range of AML/CFT preventative measures to an industry which was largely not subject to effective regulation, supervision or AML/CFT controls, while at the same time providing a wide global and cross-border payments infrastructure for the transfers of value in an unregulated context.

While the focus of the FATF Recommendations was around the strengthening of standards to clarify the application of AML and CFT requirements on virtual assets and VASPs, the requirements have been on the basis of "licensing or registering" such providers and subjecting them to supervision or monitoring without defining such standards. As a global and intergovernmental organisation which sets international standards that aim to prevent money laundering and terrorist financing, the FATF is not a regulatory authority or organisation and as such, the standards for such licensing or registration were not, and will not be defined by the FATF. Section 80 of the original Recommendations[115] included references to authorities imposing conditions that should allow for "sufficient supervisory hold" and which could "potentially include, depending on the size and nature of the VASP activities, requiring a resident executive director, substantive management presence, or specific financial requirements". The updated 2021 Guidelines[116] refer to new "Considerations for licensing and registering VASPs" but the licensing and registration criteria are defined as criteria which "give national supervisors confidence that the concerned VASPs will be able to comply with their AML/CFT obligations". The updated Recommendations also note that jurisdictions "should

114 https://undocs.org/en/S/RES/2462(2019)
115 https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf
116 Section 131 to 140 <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets-2021.html>

encourage a culture of compliance with all of a jurisdictions' applicable legal and regulatory requirements. These may address a range of policy objectives, including those related to investor and consumer protection, market integrity, prudential requirements, and/or national and economic interesting, in addition to AML/CFT."

At present, there are dramatically different approaches being taken globally in respect of VASP regulation or registration and substantially different 'standards' of licensing, registration or regulation while maintaining the notable requirement for countries not to rely on any self-regulatory body for the purposes of supervision or monitoring. Many jurisdictions have aimed to capture VASP related activity within the scope of AML requirements and a registration process, while others have sought to bring the activity, or are aiming to bring the activity within the scope or prudential supervision with substantially different requirements.

To provide more specific detail, the second 12-month review of the revised FATF standards on virtual assets and VASPs covered the state of implementation by the public sector through the global network of the FATF. Of 128 jurisdictions which provided responses to the assessment on a self-assessment basis, and not subject to independent review or to an official FATF assessment, only 58 reported that they had necessary legislation to implement R15/INR/15, with 35 reporting that their regime was operational[117]. Only a minority of jurisdictions had conducted examinations, and even fewer were reported to have imposed any enforcement actions. 32 jurisdictions reported that they had not yet decided what approach to take for VASPs and therefore do not have an AML/CFT regime in place and have not commenced a legislative/regulatory process. Similarly of the 52 jurisdictions which reported that they had established regulatory regimes permitting VASPs, 31 had established only registration regimes and only 17 licensing regimes.

This creates specific considerations from a regulatory arbitrage perspective as operators in the space are in many circumstances highly mobile, or at times partially decentralised work forces aiming to establish principle operations in a secure environment from a legal and regulatory perspective. While some operators and businesses target the highest standards available, others clearly target jurisdictions where there are gaps in the activity captured within the scope of licensing or registration requirements, or where authorities have not developed the experience or knowledge to actively monitor such activity.

VASP 'activity': global interpretation and implementations

While the standards for VASP registration or licensing are extremely wide and varied around the world, there are similar considerations in respect of the 'activity' captured. In the second 12-month review by the FATF, concluded in June 2021, of the 52 jurisdictions having established registration or licensing regimes, 15 noted that they had not covered all VASPs defined in line with the FATF definition. However, even these definitions, as set out below, are subject to broad questions of interpretation and enforcement.

For the purposes of a general summary, the FATF definitions of a VASP are as follows:

— "Virtual asset service provider means any natural or legal person who is not covered elsewhere under the Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person:
  — exchange between virtual assets and fiat currencies;
  — exchange between one or more forms of virtual assets;
  — transfer of virtual assets;

117 https://www.fatf-gafi.org/publications/fatfrecommendations/documents/second-12-month-review-virtual-assets-vasps.html#:~:text=Paris%2C%205%20July%202021%20%E2%80%93%20The,and%20virtual%20asset%20service%20providers.&text=The%20report%20finds%20that%20many,implementing%20the%20revised%20FATF%20Standards.

— safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and
— participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset."

These definitions did create some issues for countries which had sought to regulate VASP activity prior to the publication of these Guidelines in June 2019. One of these is Singapore, a hub of activity in the Asia region, which transposed the amendments to the Payment Services Act in January 2019. This did not capture custodian wallet providers, but steps are being taken to expand the definitions there for consistency with the FATF definitions. Similarly, from an EU perspective the 5th Anti Money Laundering Directive which brought a platform used to exchange fiat currencies and virtual currencies within the definition of an obliged entity but did not capture an exchange between different forms of virtual assets within scope.

This is in fact a very wide global issue from the perspective of regulatory consistency. The following are a few global examples of the approaches being taken:

In Nicaragua, the Regulation of Financial Technology Payment Service Providers (Resolution CD-BCN-XLIV-1-20 approved on September 23, 2020) defines "Financial Technology Payment Service Providers" as: "Legal entities authorized by the BCN, engaged in providing payment services with digital wallets, mobile points of sale, electronic money, virtual currencies, electronic trading and exchange of currencies and/or funds transfers." The activities subject to registration there related to the management of virtual platforms on which virtual assets are traded and to provide such virtual assets (suppliers).

In Vietnam, ranked first in the world in terms of adoption rates of individuals and users within Vietnam by the Global Chainalysis Adoption Index[118], there is as yet no legal definition of a crypto currency or virtual asset although the State Bank of Vietnam has publicly announced a pilot project to form part of the strategy towards the development of a digital economy[119].

In the Philippines, the Bangko Sentral ng Pilipinas (BSP) issued circular 944 in 2017 establishing itself as arguably the first to formally regulate digital currency services, by capturing digital currency exchanges as remittance and transfer companies. They have since issued Circular 1108 in January 2021[120] and changed the scope of virtual assets regulation within the Philippines. The definition of a Virtual Asset Service Provider is now aligned with the FATF VASP definition but excludes the 5th limb of the FATF definition being the "participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset". This is because such activity and any activity relating to an Initial Coin Offering (ICO) falls under the regulatory purview of the Securities and Exchange Commission in the Philippines[121].

In Thailand, the Digital Asset Management Act BE 2561 was enacted in May 2018 and the Securities and Exchange Commission (SEC Thailand) was granted authority to regulate the space under separate categories: a Digital Asset Exchange, Digital Asset Broker, Digital Asset Dealer, ICO portal, and a Digital Asset Investment Advisory categorisation[122]. Restrictions are also in place in Thailand and the SEC approved new rules in June 2021 to prohibit regulated digital asset exchanges from providing services in relation to utility tokens and certain categories of cryptocurrencies[123]. This included meme tokens, fan tokens, non-fungible tokens (NFT) and digital tokens issued by digital asset exchanges or related persons. This restriction was introduced largely on the basis that they involve significant risk and are designed for speculative purposes creating significant market risk. The listing of any asset on any regulated platform is also subject to consent by the SEC.

118 https://blog.chainalysis.com/reports/2021-global-crypto-adoption-index
119 https://www.vietnam-briefing.com/news/vietnam-establishes-research-group-study-regulations-cryptocurrencies-
120 https://www.bsp.gov.ph/Regulations/Issuances/2021/1108.pdf
121 https://www.bsp.gov.ph/Media_and_Research/Primers%20Faqs/FAQs_VASP.pdf
122 https://www.sec.or.th/EN/Pages/Shortcut/DigitalAsset.aspx#AUDIT
123 https://www.sec.or.th/EN/Pages/News_Detail.aspx?SECID=8994

In Indonesia, the Minister of Trade Regulation 99 of 2018 formally permitted the trading of cryptoassets in Indonesia as futures contracts, and brought such activity within the scope of the Commodity Futures Trading Supervisory Authority ("Bappebti"). Bappebti Regulation No5 of 2019 provided a regulatory framework for the operation of physical cryptoasset futures market. This essentially means that the trading activity may be regulated but its application or use as a payment instrument is prohibited in the jurisdiction. Generally speaking, the activities falling within the scope of regulation are defined as Cryptoasset Exchanges, Cryptoasset Clearing Agencies, Cryptoasset Traders, Cryptoasset Clients, and Cryptoasset Storage Providers, all subject to separate requirements under local law.

In the UK the registration requirements for VASP related activity is captured by the activity defined under Regulation 14A of the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLRs). In summary this captured cryptoasset exchange providers (both fiat to crypto and crypto to crypto) and custodian wallet providers. Whether these definitions are consistent with the FATF definitions, particularly in respect of concept of "safekeeping" and instruments enabling "control" of virtual assets or smart contracts to which the business is not a party, is beyond the scope of this section but analysis against the FATF VASP definitions, accompanying guidance and international consistency on the way that these activities are legislated for, is a relevant consideration.

Cross-border considerations, VASP activity and virtual asset categorisations
The examples from the jurisdictions above are provided only to demonstrate some of the issues in the international approaches and consensus around the regulation of the space. It also provides some high-level consideration factors for advisors in the space. There are a number of jurisdictions that make the use of any form of virtual currency for any form of 'payment transaction', completely illegal. There are other countries where there are legislated for 'approved' cryptoassets that may be traded on a regulated market[124] as well as specific approval criteria. Authorities in other jurisdictions also take very different approaches as to when they deem licensed 'activity' to be conducted in that country. While many large and global operators in the space rely on principles of reverse solicitation, and to not actively soliciting business from certain countries, many do not consider these rules on a jurisdiction by jurisdiction international basis and the intricate details relevant for certain countries around the world are sensitive and should be considered when being serviced from the UK.

Also, importantly, the categorisation of a 'virtual asset' under local law may at times bring the activity within the scope of existing regulatory perimeters. The most obvious example of this is the USA where FinCEN issued interpretative guidance in 2013[125] to clarify the applicability of the regulations implementing the Bank Secrecy Act to persons creating, obtaining, distributing, exchanging, accepting or transmitting virtual currencies, and bringing such activity within the scope of money services businesses. However, there are many examples of this and virtual asset classifications around the world are generally not consistent with the Final Guidance on Cryptoassets[126] issued by the Financial Conduct Authority in July 2019 and registered firms in the UK will also need to consider the implications of the categorisation of an unregulated token in the UK in other jurisdictions where such assets may be acquired and used through the UK platform. The asset or indeed the service categorised in respect of the transaction hosted or serviced in the UK, may be treated differently at its destination or originating address, and this is something that may need to be considered.

124 Bappebti also recently enacted Regulation No.7 of 2020 defining this list in Indonesia. <http://bappebti.go.id/resources/docs/peraturan/sk_kep_kepala_bappebti/sk_kep_kepala_bappebti_2020_12_01_i6tg8tfb_id.pdf>
125 https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf
126 https://www.fca.org.uk/publication/policy/ps19-22.pdf

The Regulated VASP and the evolution of DeFi
The context of VASP activity and the legislation of the FATF VASP definitions into local law, and how such activity has been defined is also particularly relevant in the context of the global DeFi developments.

DeFi is a very broad term for financial services which are disintermediated, with no centralised point of authority or single point of failure as they are built on the decentralised infrastructure of blockchain technology. There are many types of business models and structures, or decentralised applications (DApps), which aim to replace traditional forms of intermediation. The strongest proponents of DeFi often make underlying arguments relating to the concepts of financial inclusion and allowing access to such services to any person with access to a computer and an internet connection. The design of DeFi services are typically built on programmable and open architecture and are non-custodial by design so that assets issues or managed cannot be accessed, altered or moved by any party other than the account holder. The applications are also typically trust-less in the sense that there is no 'trust' required in any central counterparty or intermediary as the trust is in the logic of the rules determined by the logic and rules of the DeFi protocol in question. The design of DeFi infrastructure is for direct participation on a peer-to-peer or peer to platform systems, and all features and functionality are coded and once executed are immutable on the underlying blockchain in a tamper-resistant and transparent form. The lack or a centralised counterpart or responsible entity also creates new frontiers to the possibilities of efficient regulatory control or standards from a consumer protection perspective.

How relevant are DeFi developments to authorities and policy makers in the UK?
In the case of many DeFi initiatives, protocols, applications and developments, some jurisdictions are aiming to determine whether such activity is 'decentralised' in more than name only, or how the risks in the developing application of decentralised exchanges, and protocols can be identified, managed, monitored or mitigated. The UK position is interesting in the context of the DeFi Adoption Index, published by the blockchain analytics group Chainalysis.[127] The adoption index was calculated by reference to three component metrics:

1. on-chain cryptocurrency value received by DeFi platforms weighted by PPP per capita;

2. total retail value received by DeFi platforms; and

3. individual deposits to DeFi platforms weighted by PPP per capita.

The UK was ranked 4th in the world under these metrics. It is ranked 3rd in the world behind the USA and China in terms of the value sent to DeFi in retail transactions and web visits to DeFi platforms. Of similar interest is the fact that the region of Central, Northern and Western Europe accounts for 25% of the global value of cryptocurrency value received, turning this into the world's largest cryptocurrency economy. Within this, the UK is by some way the largest contributor to that regional metric, accounting for around $170 billion of the value received during the period of July 2020 to June 2021. This is referenced under this section as 49% of this value is made up of value sent to DeFi protocols.

This is consistent with the DeFi trends around the world where Uniswap now accounts as the largest cryptocurrency service by transaction volume in the USA, outperforming Coinbase.com which is followed closely by another Dex, the dYdX exchange.

127 https://blog.chainalysis.com/reports/2021-global-defi-adoption-index

Decentralisation as a concept
The DeFi space has seen exponential growth since the first edition of this guidance, but the fundamental question of when a DeFi-based operation falls within the scope of registration or licensing requirements or outside of the wider scope of the VASP categorisation or definition is currently one of interpretation.

Unfortunately, there are many blockchain-based services that pursue the idea of decentralisation on the understanding that this automatically brings the activity within the concept of a 'software service' and not a virtual asset based service, or financial service, and outside of the scope of any form of regulation. One of the clearest examples of this was the Etherdelta decentralised exchange (Dex) which was the most popular order book exchange service a few years ago. The US judgement is a matter of public record[128] and cites various factors that distinguish Etherdelta from a real peer-to-peer trading platform. In summary, these included the fact that:

1. The EtherDelta defendant, Mr. Zachary Coburn, maintained a list of 'official token listings' that were available for trading, and would request certain information from that issuer, performing his own due diligence before the 'listing' could take place. This was despite the fact that any token that was ERC20 compliant could 'function' on the platform.

2. Orders on EtherDelta did not change the state of the Ethereum blockchain (so no 'gas fee' was applied on any trade). All orders were stored on EtherDelta's order book which was maintained on a centralised server maintained by EtherDelta (and not on the Ethereum Blockchain).

3. Mr Coburn would keep users appraised of key events, announcements on the platform's operations and deal with user questions directly. Similarly, public forums allowed for users and EtherDelta representatives to post questions and answers.

4. Perhaps critically, EtherDelta did not charge fees to the maker of a contract in order to incentivise orders to be placed but did charge a 0.3% fee of a transactions trade volume which was identified as the 'fee account'.

Although there is no 'test' for decentralisation as a legal concept, the FATF have noted that a peer-to-peer trading platform or peer-to-peer provider can be captured within the definition of a VASP but will not always be captured. If a Dex is seen to "conduct or facilitate" the activity as a business, on behalf of another person, it may be seen to be providing the services of an exchange and being itself categorised as an exchange or VASP. The reality is that there are a number of factors that should be considered before a determination may be made on the specific facts of that arrangement or service.

DeFi regulatory approaches, interpretations and approaches
In the UK the MLR's wording includes the definition of a cryptoasset exchange provider as a firm or sole practitioner who by way of business provides services relating to exchanging or arranging or making arrangements with a view to the exchange of one cryptoasset for another. The Joint Money Laundering Steering Group (JMLSG) have issued guidance[129] which refers to the broad definition and potentially including activities relating to a dedicated peer-to-peer platform. The guidance also refers to bids and offers traded at an outside venue through individual wallets or other wallets not hosted by the forum or a connected firm may not be captured. However, it is clearly noted that that such business models will be considered on a case by case basis and there is no binary test as to when such activity will or will not be caught by the requirements for registration. Software developers and providers are noted as being more likely to fall outside of the scope of the definition if they derive no income or benefit from consequent transactions.

The interpretation around "arranging or making arrangements" is of course not exclusive to the UK. At an EU level the proposed Markets in Cryto-Assets Regulation

128 https://www.sec.gov/litigation/admin/2018/34-84553.pdf
129 Section 22: <https://secureservercdn.net/160.153.138.163/a3a.8f7.myftpupload.com/wp-content/uploads/2020/07/JMLSG-Guidance_Part-II_-July-2020.pdf>

(MiCAR) defines the "operation of a trading platform for cryptoassets" as a Crypto Asset Service, making the business a Crypto Asset Service Provider (CASP). This activity is defined as managing a platform "within which multiple third-party buying and selling interests for cryptoassets can interact in a manner that results in a contract". The execution of orders for cryptoassets on behalf of third party, and the reception and transmission of orders for cryptoassets are also defined CASP activities and could also have DeFi touch points and regulatory triggers subject to the interpretation of those provisions in Member States. Similarly, in other jurisdictions around the world, there is common use and reference to the word "facilitation" of trading activity. One example of this is Thailand where a Digital Asset Exchange is defined as a "center or a network established for the purposes of trading or exchanging digital assets, which operates by matching orders or arranging for the counterparty, or providing the system or facilitating a person who wished to trade or exchange digital assets to be able to enter into an agreement or match the others…".

Of course, one key question is whether bringing all such activity within the scope of existing VASP, or financial services regulation is possible and enforceable. Who or what is the counterpart to such an action? Should the developer of the code be made responsible for the activity conducted on any protocol as this is wholly inconsistent with other technical infrastructures currently in operation around the world. Should the question of the 'controller' of any smart contract on which activity is conducted maintain a level of responsibility and accountability? The current updated version of the FATF guidelines[130] points towards "creators, owners and operators or some other persons who maintain control or sufficient influence in the DeFi arrangements" falling under the FATF definition of a VASP where they are providing or actively facilitating VASP services. Of course, how these guidelines are considered and transposed into local law in different countries still remains to be seen. A relevant issue is that the most commonly cited reasons for the lack of implementation of the 2019 FATF guidelines across the respondent jurisdictions included an "apparent lack of VASPs based in their jurisdiction" and a "lack of expertise and understanding" regarding virtual assets and VASPs, as well as resource constraints and restrictions arising from the COVID-19 pandemic. This of course related to the guidelines relating to (primarily) centralised exchanges and custodians/wallet providers. The extent to which authorities are prepared to consider the intricate complexities of DeFi infrastructure and activity from a regulatory perspective will be a relevant factor in the transposition of these recommendations.

DeFi risks and new approaches

It also remains to be seen whether relevant authorities will adopt the use of the technology available to address the relevant DeFi related risks. These risks are well reported[131] and involve new forms of financial risk due to the transactional behaviour of users of the service, specific counterparty risk to the underlying code, as well as liquidity and market risk. There are also technical and operational risks, and some of these have historically led to DeFi rug pulls where developers effectively abandon a project by exploiting smart contract vulnerabilities and draining assets from liquidity pools, or altering smart contracts containing project vault business logic, and draining funds. However, critically there are significant legal compliance risks relating not only to the regulatory risk of the platform, but also to financial crime. While many DeFi projects propose to be motivated by the idealistic concepts of financial inclusion they are also used for illicit purposes. Some analytics and compliance companies such as Coinfirm[132] provide DeFi/DEX liquidity pool risk assessments and these reports show quite clearly the exposure to potentially material AML, CFT and sanctions risk indicator breaches. The liquidity pools of larger unregulated DEX platforms will often show direct links, through the wallet addresses used to interact with the DEX, of mixers and tumblers, hacks, terrorist financing, ransomware, darknet and deep web touch points, as well as sanctions breaches.

130 Section 67: <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets-2021.html>
131 World Economic Forum: (DeFI) Policy-Maker toolkit: <https://www.weforum.org/whitepapers/decentralized-finance-defi-policy-maker-toolkit>
132 Coinfirm – Blockchain Analytics

Different approaches may be taken to address such risks including the development of compliance oracle systems which restrict such transactions from being able to execute on any decentralised platform. Digital Identifiers (DIDs) are also a developing new form of identifier that enables verifiable digital identity, including KYC verification and wallet address white listing processes to allow only such verified individuals to interact with a decentralised platform. There are also proof of kyc broadcasts (with no personal data) capable of being broadcast to public blockchain so that the proof of KYC is published on-chain and access to the underlying data is available only through specific nodes with the relevant authority attached.

While this section will not be able to consider each of these solutions in detail, what is clear is that the application and use of the technology may also be used to address many of the compliance related risks which are the primary focus for most authorities at present.

Similarly, authorities will need to consider the management of risk through the centralised access points to DeFi infrastructure and the (centralised) CeFi<>DeFi bridges which are being developed to allow users of regulated platforms access to the underlying benefits of these systems and services.

Conclusion

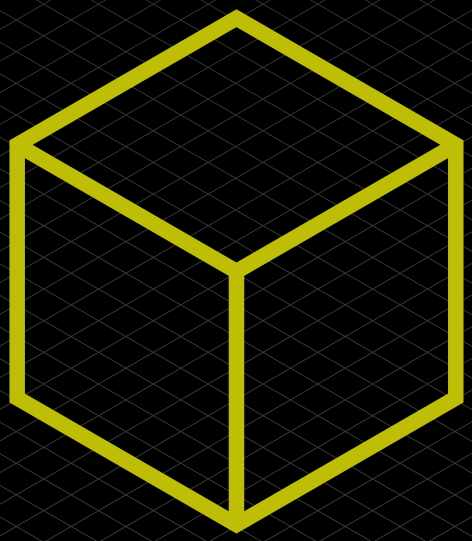
The standards of VASP regulation and frameworks being developed are evolving around the globe. Arguably there are gaps to be addressed in terms of providing a regulated ecosystem with which users are able to interact and use in a secure and reliable way. Many registration regimes are aimed at complying with FATF recommendations from a purely compliance basis and arguably not aimed at identifying some of the core underlying issues. These may relate to the integrity of the markets being developed, and applying appropriate market abuse standards, client asset protection and segregation, capital adequacy and insurance, or even listing and transaction monitoring requirements. Different jurisdictions are accelerating such developments and the questions for any financial centre aiming to provide a solid legal foundation for such platforms and developing businesses should be considered.

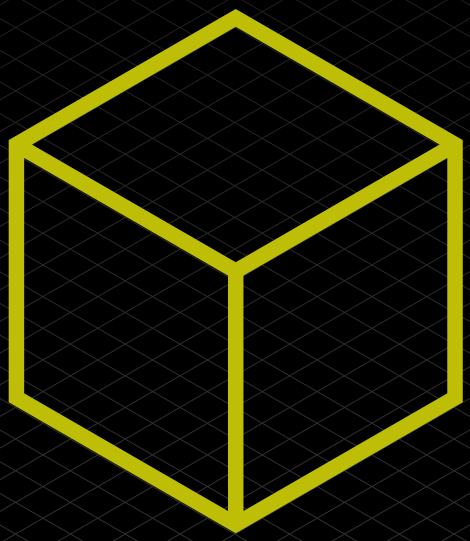
Similarly, the pace of the development of the technology, and in particular the DeFi space is accelerating at a faster pace than most authorities are able to monitor and develop. Providing clarity and certainty around such developments is key and exploring mechanisms and standards to address new risks in new digital ecosystems is also important. The application of new technology and innovative development arguably requires a level of innovation to take place at a policy and regulatory perspective on at least a research basis.

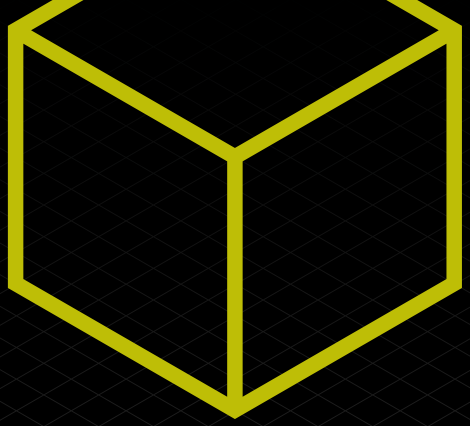
The DeFi question, and categorisation within the scope or outside of the scope of a VASP related activity also has implications beyond the interpretation of FATF Recommendations. The commonly referred to “Travel Rule” defined under Recommendation 16 has been transposed into legislation in many countries in different ways. While some jurisdictions capture all transactions from an originating VASP wallet address to any beneficiary address (whether a VASP or unhosted wallet), others have sought to comply with the FATF recommendations through both threshold limits, and exemptions for transactions with un-hosted (non-VASP) destination beneficiary addresses, or by introducing “risk scoring” requirements for destination addresses with which originator and beneficiary details may not be shared. Whether a DeFi-related operation constitutes a VASP or a cryptoasset service provider in the UK or not, may in and of itself already have implications for jurisdictions which have transposed the Travel Rule requirements in this way. Whether there is a requirement for such information to be shared or not, will also need to be considered depending on the categorisation of the underlying address as a VASP, cryptoasset service provider or neither. At present under the proposed provisions specific to cryptoasset firms in the UK, an originating provider is not expected to send information to an unhosted wallet[133]. However, whether a non-custodied wallet, relating to a DeFi platform constitutes a cryptoasset firm is potentially not yet completely clear.

133 Amendments to the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 Statutory instrument 2022. Consultation. Section 6.27: <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1004603/210720_SI_Consultation_Document_final.pdf>

5

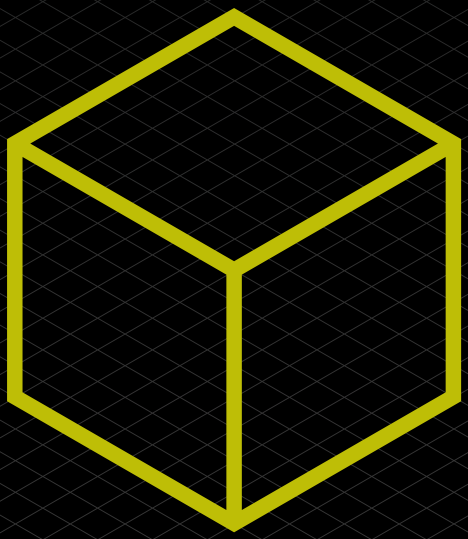


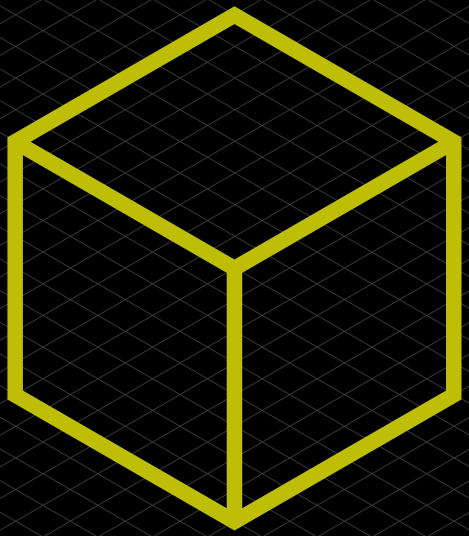




Part 1: Developing Technologies

Section 5 Non-fungible tokens





Section 5: Non-fungible tokens

Omri Bouton (Sheridans), Will Foulkes, Gareth Malna (Stephenson Law LLP), Anne Rose, Niki Stephens and Sian Harding (Mishcon de Reya LLP)

Introduction

Omri Bouton (Sheridans), Will Foulkes, (Stephenson Law LLP) and Anne Rose (Mishcon de Reya LLP)

A non-fungible token (NFT) is a unique, non-divisible token, often linked to an object (e.g. a collectable, digital art or in-game asset) which uses blockchain technology to record ownership and validate authenticity. Fungible tokens, such as Bitcoin, are not unique and therefore do not qualify as an NFT. NFTs utilise token standards supported by blockchains such as Ethereum, Algorand and Solana.

Currently used predominantly for digital collectables, digital art and, more recently, interactive entertainment, NFTs leverage the inherent characteristics of DLT to introduce scarcity and enable demonstrable exclusive ownership to digital information assets.

In Part A we look at some practical and legal issues with regards ownership rights and intellectual property issues related to NFTs. In Part B we consider whether an NFT could fall within the remit of the UK's financial regulatory regime and in Part C we consider if the mechanics by which the NFTs are issued or sold and/or any aspect of the ecosystems in which the NFTs may be utilised might constitute "gambling" and require the provider of such facilities to hold a gambling licence issued by the Gambling Commission of Great Britain.

Non-Fungibility

To understand NFTs it is important first to understand the difference between fungible and non-fungible items.

According to the Cambridge Dictionary (https://dictionary.cambridge.org/dictionary/english/fungible), a fungible item can be defined as "something such as a currency, share, or goods, that can easily be exchanged for others of the same value and type". Fiat money, and cryptoassets used similarly to or in lieu of fiat money (for example Bitcoin, Ethereum etc) fall under this category.

Conversely, non-fungible items are not easily exchangeable for other items of the same value and type. Non-fungible items, as well as the value associated with it, are unique. A painting or sculpture is an example of a non-fungible item.

NFTs versus associated assets

It is important at the outset to properly conceptualise an NFT. NFTs are cryptoassets, which in turn are merely database entries on a distributed ledger, created and recorded according to the properties of the underlying rules (token standard). They contain metadata that defines their object by providing details regarding them. This typically includes, amongst other things: the name of the NFT; the smart contract address which manages the ownership and transferability of the NFT; and an associated asset (an Associated Asset).

The Associated Asset contained in the NFT metadata is typically a url which points to the asset that is associated with the NFT, e.g. the artwork, digital collectible, music or video asset. The metadata itself does not usually contain this asset, for reasons explored below.

PART A: Ownership and storage

Omri Bouton (Sheridans), Will Foulkes (Stephenson Law) and Anne Rose (Mishcon de Reya LLP)

Ownership

It is often unclear what rights the purchase of an NFT gives to the purchaser. NFT holders do not generally enjoy full rights over the particular assets (such as digital images) that are associated with their NFTs.

By way of example, the image above represents one of ten thousand LarvaLabs' CryptoPunks - specifically CryptoPunk #6013. Each of the ten thousand tokens forming part of the CryptoPunks collection is represented by a distinct CryptoPunk having different attributes (from the particular species, such as apes, aliens and humans, to hairstyle and accessories).

However, the holder of this particular CryptoPunk is not entitled to the intellectual property rights (IPR) in the image that it is associated with and used for the purposes of representing and identifying the relevant NFT; what the holder has is a claim to the NFT itself: the token. (For more on IPR see Section 10.)

Anybody can download a copy of the file or link relating to whatever asset the NFT is tokenising, but only the NFT owner holds the contract stating their ownership rights. The NFT declares you as the official owner.

Transferring the IPR in the Associated Asset to the NFT holder is possible but requires formal assignment (i.e. it must be in writing and signed by the assignor). With regards to the IPR in the NFT itself, as an NFT is purely metadata it is not protected as the NFT is neither the actual original work nor a copy of the work, but only a tokenised version of it, which does not incorporate the full work into the blockchain, but contains only a URL linked to it. The idea that an NFT holder is the de facto "owner" of the Associated Asset, absent an explicit contractual matrix assigning the relevant IPR, is a common current misconception around NFTs.

As best practice, we recommend defining the rights vesting on the holders of their NFTs (and incorporating them in dedicated public-facing terms) so as to avoid market confusion and reputational harm to any project.

Management of rights in distributed (and semi-immutable) file storage systems

As mentioned above, NFT metadata usually incorporates a url pointing towards an Associated Asset. To facilitate prompt identification, the Associated Asset is normally accessed and displayed as a representation of the NFT associated with it, through the platform used to access the NFT (for example, one of the dedicated marketplaces through which NFTs are exchanged).

While the Associated Asset is not normally stored on-chain, due to data storage limitations and other impractical aspects, it is common practice for the creators/issuers of the NFTs (Issuers) to store it on other forms of decentralised and distributed file storage systems (DFSS) – for example, the InterPlanetary File System better known as IPFS.

While storing Associated Assets on DFSS is attractive to the holders, as it provides trustless access to any such Associated Assets, it does represent a risk on the part of the Issuer, particularly where the Associated Asset does not belong to the Issuer.

Because of the semi-immutable character of distributed and decentralised solutions, it can be very difficult, if not virtually impossible, to take down Associated Assets once uploaded onto a DFSS. Therefore, it is important for legal advisors to ensure that the scope of the legal authority by which the Issuer uploads the Associated Assets onto DFSS is explicit, which mitigates this particular risk in light of the specific characteristics of each type of DFSS.

PART B: Interaction of NFTs with the financial services regulatory landscape in the UK

Gareth Malna (Stephenson Law)

NFTs and FATF

The regulatory treatment of NFTs is potentially relatively broad.

As discussed previously, FATF publishes standards for regulation and supervision of financial intermediaries. With regard to NFTs, in its 'Updated Guidance for a Risk Based Approach: Virtual Assets and Virtual Asset Service Providers'[134] published on 21 October 2021, FATF states at paragraph 53:

> *"[NFTs], depending on their characteristics, are generally not considered to be VAs under the FATF definition. However, it is important to consider the nature of the NFT and its function in practice and not what terminology or marketing terms are used. This is because the FATF Standards may cover them, regardless of the terminology. Some NFTs that on their face do not appear to constitute VAs may fall under the VA definition if they are to be used for payment or investment purposes in practice. Other NFTs are digital representations of other financial assets already covered by the FATF Standards. Such assets are therefore excluded from the FATF definition of VA, but would be covered by the FATF Standards as that type of financial asset. Given that the VA space is rapidly evolving, the functional approach is particularly relevant in the context of NFTs and other similar digital assets. Countries should therefore consider the application of the FATF Standards to NFTs on a case-by-case basis."*

In October 2018, FATF required that virtual asset service providers (VASPs) be regulated for anti-money laundering and countering the financing of terrorism purposes, that they be licensed or registered, and subject to effective systems for monitoring or supervision. There is a risk, therefore, that in the future NFT platforms may be subject to regulation as VASPs under relevant local laws implementing the FATF standards as they apply to VASPs. This analysis will be fact-specific and involves consideration of the types of NFTs the platform deals in and whether they are offered or intended to be investments (as opposed to, say, collectibles which appeal to fans or collectors). Legal practitioners should consider local regulatory requirements as they may apply to NFT ecosystem participants (such as those operating an NFT drop or exchange platform, Issuers or other activities involving promotion of NFTs in a jurisdiction).

UK-specific regulation

There are also situations in which the rights attributable to an NFT will cause that NFT to become regulated under the UK regime.

Despite there being no NFT- or crypto-specific regulations in the UK, NFTs have, broadly, four main touch points with the existing UK regulatory regime as implemented by the FCA and PRA. They are:

1. under the Financial Services and Markets Act 2000 (Regulated Activities) Order 2001 (RAO) if tokens amount to "specified investments";
2. under the Markets in Financial Instruments Directive (MiFID) if the tokens amount to 'financial instruments';
3. under the Electronic Money Regulations 2011 (EMRs) if the tokens amount to e-money; and

134 https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf

4. within the scope of the Payment Services Regulations 2017 (PSRs).

In lieu of NFT- or crypto-specific legislation and regulations, participants in the NFT arena are required to assess their project against the above regimes utilising guidance provided by the FCA in its policy statement 'Guidance on Cryptoassets: Feedback and Final Guidance to CP 19/3', PS19/22.

In PS19/22 the FCA sets out an overlapping framework under which the various types of crypto-product in the market are to be categorised as either "regulated tokens" or "unregulated tokens". In this context, regulated tokens include:

— security tokens, which are tokens that amount to specified investments (except e-money) under the RAO. This includes those tokens that amount to "financial instruments under MiFID"; and
— e-money tokens, which meet the definition of e-money under the EMRs.

As the name and description implies, regulated tokens fall within the regulatory perimeter and firms carrying on regulated activities in relation to those tokens will need to comply with the relevant regulatory regime, including seeking authorisation to carry on those regulated activities.

All tokens that do not fit into the two types of regulated token are considered to be unregulated tokens for which there is no interaction with the UK regulatory regime. This category includes 'utility tokens', cryptocurrencies and other types of payment tokens which can be used primarily as a means of exchange.

In that way, NFTs are governed in the same way as their token forebearers such as bitcoin, ETH and other altcoins.

The exercise is to consider whether each token is one of the types of regulated token by reason of it falling within the RAO, MiFID, or the EMRs. It will be a separate exercise to consider whether those tokens could also amount to the provision of payment services under the PSRs.

1. Specified investments under the RAO

For a token to amount to a specified investment, it must meet the definition of any of the 25 (at the time of writing) defined investment types specified in the RAO. Many of these, including regulated mortgage contracts, funeral plan contracts, consumer hire agreements and the like can be dismissed out of hand. But there is some analysis to be done against other specified investments such as shares, options, futures, contracts for difference etc on a case by case basis.

Where, for instance, an NFT represents a fractionalised ownership of assets, it is possible that the NFT could, as a matter of fact, amount to the representation of "shares or stocks in the share capital of any body corporate (wherever incorporated) and any unincorporated body constituted under the law of a country or territory outside the United Kingdom", thereby satisfying the definition of "shares" under article 76 RAO.

Similarly, an NFT representing fractionalised ownership of an underlying asset could amount to a kind of derivative in the event that it is either an option, future or contract for difference as defined under the RAO. That is, the NFT either:

a. grants the holder a right to acquire or dispose of:
    i. a security or contractually based investment
    ii. currency of the United Kingdom or any other country or territory
    iii. palladium, platinum, gold or silver
    iv. an option to acquire or dispose of an investment of the kind specified in (a), (b) or (c)
    v. subject to certain stipulation sin reg 83(4), an option to acquire or dispose of an option to which paragraphs 5, 6,7 or 10 of Section C of Annex I to the MiFID read with Articles 5, 6, 7 and 8 of the Commission Regulation applies, (thereby making it an option u nder Art 83 RAO);

b. is a right under a contract for the sale of a commodity or property of any other description under which delivery is to be made at a future date and at a price agreed on when the contract is made (thereby making it a future under Art 84 RAO); or

c. subject to certain exclusions, rights under:
   i. a contract for differences, or
   i. any other contract the purpose or pretended purpose of which is to secure a profit or avoid a loss by reference to fluctuations in
      — the value or price of property of any description; or
      — an index or other factor designed for that purpose in the contract

   (thereby making it a contract for differences under Art 85 RAO).

In the event that the rights underlying the NFT cause that NFT to meet the definition of a specified investment, then it will also be necessary to consider whether the issuer or holder (or any other party involved in the NFT project) is carrying on a regulated activity under the RAO.

Regulated Activities Under the RAO

Under s19 of the Financial Services and Markets Act 2000 (FSMA), "no person may carry on a regulated activity in the United Kingdom, or purport to do so unless he is (a) an authorised person, or (b) an exempt person". This is known as the general prohibition.

Per s22 FSMA: "An activity is a regulated activity for the purposes of this Act if it is an activity of a specified kind which is carried on by way of business and (a) relates to an investment of a specified kind, or (b) in the case of an activity of a kind which is also specified for the purposes of this paragraph, is carried on in relation to property of any kind."

On that basis, if the rights attaching to an NFT cause it to be identifiable as a specified investment (pursuant to s22(a) FSMA), then it is important to understand whether the activity being performed in relation to that NFT is itself one of the types specific in the RAO.

The most relevant specified activities include, but are not necessarily limited to, "dealing in investments as principal" (art 14 RAO), "dealing in investments as agent" (art 21), "arranging (bringing about) deals in investments" and "making arrangements with a view to a person who participates in the arrangements buying, selling, subscribing for or underwriting investments" (art 25), "safeguarding and administering investments" (art 40), and "establishing a collective investment scheme" (art 51).

The article 25 activities are particularly broad, and it is necessary to work through them and the relevant exclusions carefully in order to reach the correct conclusion in each case. Failing to properly carry out this analysis could cause the persons engaging in the activities to be in breach of the general prohibition, which carries both civil and criminal penalties. Specifically, under s23 FSMA: "A person who contravenes the general prohibition is guilty of an offence and liable – (a) on summary conviction, to imprisonment for a term not exceeding six months or a fine not exceeding the statutory maximum, or both; (b) on conviction on indictment, to imprisonment for a term not exceeding two years or a fine, or both."

2. MiFID activities

MiFID activities are broadly aligned with FSMA and the RAO in the UK and, therefore, if an NFT meets the definition of a financial instrument under MiFID then it will also fall within the UK's regulatory regime, and the General Prohibition, described above.

Under MiFID, financial instruments include those things set out in Section C, Annex I of Directive 2014/65/EU, including transferable securities, money-market instruments, units in collective investment undertakings and any of the seven specific definitions of derivative contracts, which are:

i. Options, futures, swaps, forward rate agreements and any other derivative contracts relating to securities, currencies, interest rates or yields, emission allowances or other derivatives instruments, financial indices or financial measures which may be settled physically or in cash;
ii. Options, futures, swaps, forwards and any other derivative contracts relating to commodities that must be settled in cash or may be settled in cash at the option of one of the parties other than by reason of default or other termination event;
iii. Options, futures, swaps, and any other derivative contract relating to commodities that can be physically settled provided that they are traded on a regulated market, a MTF, or an OTF, except for wholesale energy products traded on an OTF that must be physically settled;
iv. Options, futures, swaps, forwards and any other derivative contracts relating to commodities, that can be physically settled not otherwise mentioned in point 6 of this Section and not being for commercial purposes, which have the characteristics of other derivative financial instruments;
v. Derivative instruments for the transfer of credit risk;
vi. Financial contracts for differences:
vii. Options, futures, swaps, forward rate agreements and any other derivative contracts relating to climatic variables, freight rates or inflation rates or other official economic statistics that must be settled in cash or may be settled in cash at the option of one of the parties other than by reason of default or other termination event, as well as any other derivative contracts relating to assets, rights, obligations, indices and measures not otherwise mentioned in this Section, which have the characteristics of other derivative financial instruments, having regard to whether, inter alia, they are traded on a regulated market, OTF, or an MTF.

If an NFT has rights in an underlying asset which looks and feels like any of these definitions then a full analysis should be undertaken to see whether any of the following MiFID activities (set out in Section A, Annex I of Directive 2014/65/EU) are being carried on in relation to that NFT:

i. Reception and transmission of orders in relation to one or more financial instruments;
ii. Execution of orders on behalf of clients;
iii. Dealing on own account;
iv. Portfolio management;
v. Investment advice;
vi. Underwriting of financial instruments and/or placing of financial instruments on a firm commitment basis
vii. Placing of financial instruments without a firm commitment basis;
viii. Operation of an MTF;
ix. Operation of an OTF.

If a MiFID activity is being carried on in relation to a financial instrument then it will be necessary to obtain authorisation in the relevant jurisdictions to carry on that activity. In the UK that will also mean obtaining authorisation for the relevant FSMA activity.

3. Electronic Money Regulations (EMRs)
Where a token meets the definition of electronic money in the EMRs then the FCA will consider that token to be an e-money token and, therefore, a regulated token. The definition of electronic money is:

electronically stored monetary value that represents a claim on the issuer
issued on receipt of funds for the purpose of making payment transactions
accepted by a person other than the issuer
not excluded by regulation 3 of the EMRs

Regulation 3 excludes:

a. monetary value stored on instruments that can be used to acquire goods or services only—
   (i) in or on the electronic money issuer's premises; or
   (ii) under a commercial agreement with the electronic money issuer, either within a limited network of service providers or for a limited range of goods or services;

b. monetary value that is used to make payment transactions executed by means of any telecommunication, digital or IT device, where the goods or services purchased are delivered to and are to be used through a telecommunication, digital or IT device, provided that the telecommunication, digital or IT operator does not act only as an intermediary between the payment service user and the supplier of the goods and services.

As with the activities under FSMA and MiFID, it is an offence to issue electronic money in the UK without being appropriately authorised.

Unlike under FSMA or MiFID, if the amount of e-money issued per month will on average amount to less than 5m then it will be possible to apply to become a Small Electronic Money Institution with the FCA, which means a lighter touch regulatory regime is imposed on the firm than on a firm subject to full authorisation as an Electronic Money Institution (EMI).

4. Payment Service Regulations
The final category of regulated activity potentially engaged by NFTs is payment services as regulated by the PSRs. A payment service is any of the following when carried out as a regular occupation or business activity:

a. services enabling cash to be placed on a payment account and all of the operations required for operating a payment account;

b. services enabling cash withdrawals from a payment account and all of the operations required for operating a payment account;

c. the execution of payment transactions, including transfers of funds on a payment account with the user's payment service provider or with another payment service provider—
   i. execution of direct debits, including one-off direct debits;
   ii. execution of payment transactions through a payment card or a similar device;
   iii. execution of credit transfers, including standing orders;

d. the execution of payment transactions where the funds are covered by a credit line for a payment service user—
   i. execution of direct debits, including one-off direct debits;
   ii. execution of payment transactions through a payment card or a similar device;
   iii. execution of credit transfers, including standing orders;

e. issuing payment instruments or acquiring payment transactions;

f. money remittance;

g. payment initiation services;

h. account information services.

The provision of payment services in the UK will also require the business to obtain authorisation from the FCA. As with the EMRs, businesses with an average payment transactions turnover that does not exceed 3 million per month and which do not provide account information services (AIS) or payment initiation services (PIS) can register with the FCA as small Payment Institutions (small Pis) rather than seek full authorisation.

The analysis to be carried on then is to assess whether the issuance or holding of the NFT amounts to the provision of one of the payment services, the most likely of which would be as a money remittance tool depending on the underlying utility of the token in question.

NFTs and anti-money laundering legislation
For any business engaging in activities with NFTs it is also important to note that the existing anti-money laundering requirements may apply to their activities, separate to the recently published FATF guidance considered above, which may affect interpretation or application of existing anti-money laundering requirements in future.

Businesses who carry on cryptoasset activity in the UK need to register with the FCA before conducting that business. They must also be compliant with the Money Laundering, Terrorist Financing and Transfer of Funds (Information of the Payer) Regulations 2017 (MLRs). For the purposes of the MLRs, cryptoasset activities means, per regulation 14A MLRs:

"(1) a firm or sole practitioner who by way of business provides one or more of the following services, including where the firm or sole practitioner does so as creator or issuer of any of the cryptoassets involved, when providing such services.

1. exchanging, or arranging or making arrangements with a view to the exchange of, cryptoassets for money or money for cryptoassets,
2. exchanging, or arranging or making arrangements with a view to the exchange of, one cryptoasset for another, or
3. operating a machine which utilises automated processes to exchange cryptoassets for money or money for cryptoassets.

"(2) a firm or sole practitioner who by way of business provides services to safeguard, or to safeguard and administer

1. cryptoassets on behalf of its customers, or
2. private cryptographic keys on behalf of its customers in order to hold, store and transfer cryptoassets, when providing such services."

In this context, a cryptoasset means "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".

As drafted, it is unlikely that the MLRs would capture an NFT artist or project utilising a centralised NFT exchange such as OpenSea but would instead capture the exchange or wallet providers themselves. However, legal practitioners should monitor and apply the interpretation and application of the FATF guidance referred to above which may change the position in future.

PART C: NFTs and the regulation of gambling in Great Britain

Niki Stephens and Sian Harding (Mishcon de Reya LLP)

Introduction

The definition of "gambling" under the Gambling Act 2005[135] (the primary piece of legislation governing gambling in Great Britain[136]) (the Act[137]) is relatively broad and the provision of facilities for gambling to persons in Great Britain without a licence, or an applicable exemption, is a criminal offence. As such, whilst the creation, issue and sale of NFTs would not typically amount to the provision of facilities for gambling, it is important for issuers of NFTs to consider if the mechanics by which the NFTs are issued or sold and/or any aspect of the ecosystem in which the NFTs may be utilised (for example, if the NFTs may be used to participate in tournaments, contests or other games) might constitute "gambling" and require the provider of such facilities to hold a gambling licence issued by the Gambling Commission of Great Britain (the Commission).

"Facilities for gambling" – an overview

The pivotal concept in the Act is that of providing facilities for gambling, which is broadly defined in section 5 of the Act. The provision of facilities for gambling otherwise than in accordance with the terms of a licence (or an applicable exemption) is a criminal offence under section 33 of the Act. Importantly, this applies to anyone who provides facilities for gambling which are used by persons in Great Britain, irrespective of whether the provider of the facilities is based in the Great Britain or elsewhere. It also applies to the provider of the facilities if they use relevant equipment that is located in Great Britain, even if the facilities are not used in Great Britain.

"Gambling", as defined in section 3 of the Act, means:

a. gaming (within the meaning of section 6 of the Act);
b. betting (within the meaning of section 9 of the Act); and
c. participating in a lottery (within the meaning of section 14 and subject to section 15 of the Act).

Meanwhile, section 339 of the Act provides that participating in a competition or other arrangement under which a person may win a prize is not gambling for the purposes of the Act (and therefore not regulated or licensable) unless it falls within the definitions of gaming, betting, or participating in a lottery under the Act.

Any analysis of a business that issues NFTs and/or that proposes to encourage consumer engagement by 'gamifying' the use of NFTs to ascertain whether it falls within the scope of the Act (and therefore may require a licence or adaption to seek to avoid the need for a licence) must therefore consider whether the activity falls within the definitions of gaming, betting and participating in a lottery.

1. Gaming

"Gaming" is defined in section 6 of the Act as follows:

"6 Gaming & game of chance

1. In this Act "gaming" means playing a game of chance for a prize.

2. In this Act "game of chance"—
   includes—
   (i) a game that involves both an element of chance and an element of skill,
   (ii) a game that involves an element of chance that can be eliminated by superlative skill, and
   (iii) a game that is presented as involving an element of chance, but does not include a sport.

135 As amended by the Gambling (Licensing and Advertising) Act 2014
136 For the purposes of this section, Great Britain means England, Scotland and Wales and excludes Northern Ireland.
137 The Gambling Act 2005 is currently being reviewed by the UK government. A white paper is expected to be issued towards the end of 2021/first quarter of 2022, which may result in legal and/or regulatory changes.

3. For the purposes of this Act a person plays a game of chance if he participates in a game of chance—
(a) whether or not there are other participants in the game, and
(b) whether or not a computer generates images or data taken to represent the actions of other participants in the game.

4. For the purposes of this Act a person plays a game of chance for a prize—
(a) if he plays a game of chance and thereby acquires a chance of winning a prize, and
(b) whether or not he risks losing anything at the game.

5. In this Act "prize" in relation to gaming (except in the context of a gaming machine)—
(a) means money or money's worth, and
(b) includes both a prize provided by a person organising gaming and winnings of money staked.

[…] "

The Act does not define a "game". However, it is clear from the wording of section 6 of the Act that a game may be multi- or single-player, that there is no requirement for participants to pay to play and that a prize of money or money's worth is a necessary element. The relevant leading cases[138] also indicate that the participant must do some act, or exercise some decision-making process; a player cannot be passive.

Whether a game is a "game of chance" will be a question of fact in each case. The definition in the Act is broad and, on the face of it, any game involving an element of chance, including one in which the chance may be eliminated by superlative skill, and even games that do not involve chance but are presented as involving an element of chance, may constitute a game of chance. The leading case[139] in this area established that "the only circumstance where chance should not be taken to make a game of skill and chance a game of chance is where the element of chance is such that it should on ordinary principles be ignored – that is to say where it is so insignificant as not to matter". The example given by the Court of Appeal in the relevant case was a game in which chance is used only to determine who starts the game (for example, chess).

It is noteworthy that the Commission has since suggested[140] that random or chance elements can exist within a game to test the skill of the player without necessarily meaning that the game is a game of chance (which we suggest is a (marginally) more generous analysis than that adopted by the Court of Appeal in R v Kelly). However, limited reliance should be placed on this because, ultimately, it is for the courts to determine the meaning of the statutory provisions and, for the time being, Kelly provides the leading authority.

In relation to the meaning of a "prize" it is worth noting that the Commission has indicated[141] that, where in-game items or currencies can be converted into cash or exchanged for items of value, they will be considered money or money's worth for the purposes of the Act. As such, it is likely that the award of an NFT would constitute a prize for the purposes of section 6 of the Act.

138 DPP v Regional Pool Promotions Ltd [1964] 2 Q.B. 244 and Adcock v Wilson [1969] 2 A.C. 326 (both of which in fact relate to the definition of "game" contained under the Betting and Gaming Act 1960) and IFX Investment Co. and others v HMRC [2016] EWCA Civ 436 (which relates to the Gaming Act 1968).
139 R v Kelly [2008] EWCA Crim 137 (NB Kelly concerned the provisions of the Gaming Act 1968, but the relevant provisions are considered sufficiently similar to those in the Act that it remains a key authority.)
140 In its advice note on "skill with prizes" machines, published in July 2010. This advice note seems to accept that, where a random element is present for the purpose of testing the skill or knowledge of a player, that element may not cause a game to be a "game of chance" for the purposes of the Act, provided that the random element does not prevent a suitably skilful player from being able to win.
141 In its 'Virtual currencies, esports and social casino gaming - position paper', published in March 2017 <https://assets.ctfassets.net/j16ev64qyf6l/4A644HlpG1g2ymq11HdPOT/ca6272c45f1b2874d09eabe39515a527/Virtual-currencies-eSports-and-social-casino-gaming.pdf>

2. Betting

"Betting" is defined in section 9 and section 11 of the Act as follows:

"9 Betting: general

1. In this Act "betting" means making or accepting a bet on—
   (a) the outcome of a race, competition or other event or process,
   (b) the likelihood of anything occurring or not occurring, or
   (c) whether anything is or is not true.

2. A transaction that relates to the outcome of a race, competition or other event or process may be a bet within the meaning of subsection (1) despite the facts that—
   (a) the race, competition, event or process has already occurred or been completed, and
   (b) one party to the transaction knows the outcome.

3. A transaction that relates to the likelihood of anything occurring or not occurring may be a bet within the meaning of subsection (1) despite the facts that—
   (a) the thing has already occurred or failed to occur, and
   (b) one party to the transaction knows that the thing has already occurred or failed to occur."

The word "bet" is not itself defined in the Act but is generally understood to involve an arrangement between two or more people who hazard something of value (money or money's worth) on the outcome of an uncertain matter. As such, if an arrangement involves participants risking/hazarding one or more NFTs on the outcome of an uncertain event, the arrangement may constitute betting.

Section 11 of the Act extends the definition of "betting" for the purposes of section 9 to cover certain types of prize competition:

"11 Betting: prize competitions

1. For the purposes of section 9(1) a person makes a bet (despite the fact that he does not deposit a stake in the normal way of betting) if—

   (a) he participates in an arrangement in the course of which participants are required to guess any of the matters specified in section 9(1)(a) to (c),
   (b) he is required to pay to participate, and
   (c) if his guess is accurate, or more accurate than other guesses, he is to—
      (i) win a prize, or
      (ii) enter a class among whom one or more prizes are to be allocated

   (whether or not wholly by chance).

2. In subsection (1) a reference to guessing includes a reference to predicting using skill or judgment…."

This section of the Act was included to cover certain types of prize competitions including fantasy leagues. Note that to be caught, players must be required to guess or predict (using skill or judgement) the outcome of a race, competition, or other event or process (or the likelihood of something occurring, or whether or not something is true). The following (non-binding, but persuasive) narrative was also included in the explanatory notes to the Act:

> "The definition [in Section 11 of the Act] is intended to exclude prize competitions (such as prize crosswords) where the elements of prediction and wagering are not both present".

If the product in question appears to fall within the definition of betting in section 9 of the Act, it will then also be necessary to consider whether it falls within the definition of pool betting, which is defined as follows:

"12 Pool betting
(1) For the purposes of this Act betting is pool betting if made on terms that all or part of winnings—

(a) shall be determined by reference to the aggregate of stakes paid or agreed to be paid by the persons betting,
(b) shall be divided among the winners, or
(c) shall or may be something other than money.

If the product meets the definition in section 12 of the Act, it will be treated as pool betting rather than general betting under section 9. Of particular interest in the fact that betting will be pool betting if all or part of the winnings shall or may be something other than money. This is likely therefore to include the award of NFTs as winnings in relation to arrangements that also meets the definition of betting under section 9 or 11 of the Act.

For completeness, it is also necessary to consider whether the provider of the facilities in question could be said to be a betting intermediary, in which case they will be providing facilities for betting. A betting intermediary is defined in section 13 of the Act as "a person who provides a service designed to facilitate the making or acceptance of bets between others". The definition is primarily intended to apply to betting exchanges, where the intermediary facilitates the making of bets between two people, where one wishes to lay odds and the other wishes to back them. In such circumstances, the intermediary usually takes no risk; instead making its profit from commission (usually charged to the person who wins the bet).

3. Participating in a lottery
Under section 14 of the Act, an arrangement is a simple lottery if:

— persons are required to pay in order to participate in the arrangement;
— in the course of the arrangement one or more prizes are allocated to one or more members of a class; and
— the prizes are allocated by a process which relies wholly on chance.

A complex lottery is defined similarly, save that the prizes are allocated by a series of processes and the first of those processes relies wholly on chance.

If there is no requirement for participants to pay to enter then the arrangements will not constitute a lottery. Schedule 2 of the Act makes provision about the circumstances in which an arrangement is or is not to be treated for the purposes of section 14 as requiring payment to participate and, for example, provides that paying includes paying money, transferring money's worth and paying for goods or services at a price or rate which reflects the opportunity to participate in the arrangement. As such, if a person is required to transfer an NFT in order to participate in an arrangement where a prize is allocated to a winner by a process which relies wholly on chance, then that arrangement is likely to constitute a lottery.

Note that a process which requires persons to exercise skill or judgment or to display knowledge will be treated as relying wholly on chance if (i) the requirement cannot reasonably be expected to prevent a significant proportion of persons who wish to participate in the arrangement from doing so; and (ii) the requirement cannot reasonably be expected to prevent a significant proportion of persons who participate in the arrangement of which the process forms part from receiving a prize[142].

It is also worth noting that a "prize" in relation to lotteries includes any money, articles or services whether or not described as a prize and whether or not consisting wholly or partly of money paid, or articles or services provided, by the members of

142 Section 14(5) of the Act

the class among whom the prize is allocated. As such, it is likely, for example, that the award of an NFT would constitute a prize for the purposes of section 14.

Finally, it is important to note that the operation of lotteries is generally limited to raising funds for charitable causes and there are relatively limited exemptions that apply to lotteries run by private clubs, resident lotteries and workplace lotteries or for fundraising at commercial or charity events (and in each case, the lottery will be subject to specific regulations that restrict the terms on which such lotteries may be operated).

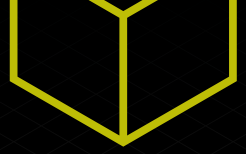
Conclusion

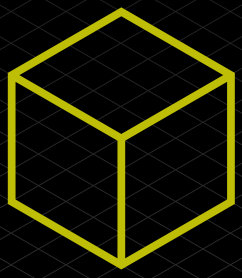
Any business that issues NFTs and/or that proposes to encourage consumer engagement by 'gamifying' the use of NFTs should consider seeking specialist advice in order to understand whether it requires a licence issued by the Commission. As set out above, the "provision of facilities for gambling" under the Act is broadly defined, and sometimes the smallest of changes to a business model or product can bring it within, or take it out of, the scope of the Act. Seeking specialist advice at an early stage has the benefit of helping to identify any elements that might be problematic and provides an opportunity for adjustments to be made, particularly if the intention is for the business to remain outside the scope of the Act.

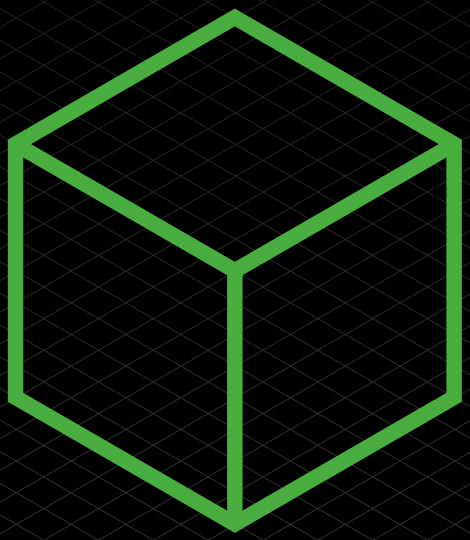
Regulators, including the Commission, are likely to be sensitive to novel business models and products, especially where those involve digital assets, particularly in the wake of Football Index.[143] Seeking specialist advice at an early stage also has the benefit of readying the business for any potential interest and enquiries by the Commission.

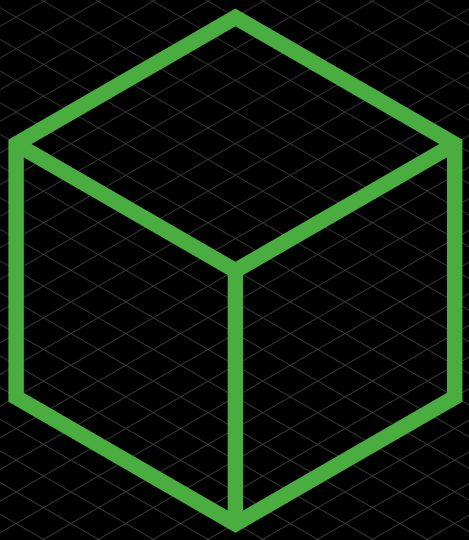
143 Football Index was a gambling platform operated by BetIndex Limited pursuant to a licence issued by the Commission, which enabled users to buy and sell "shares" in footballers. In March 2021, BetIndex entered administration and its licence was suspended, causing significant losses to consumers. Government subsequently commissioned an independent report into the regulation of BetIndex. The report was critical of both the Commission and the Financial Conduct Authority and made a series of recommendations for improvements to ensure better, more effective, regulation of novel products.

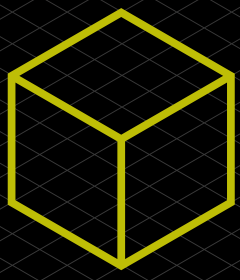
6

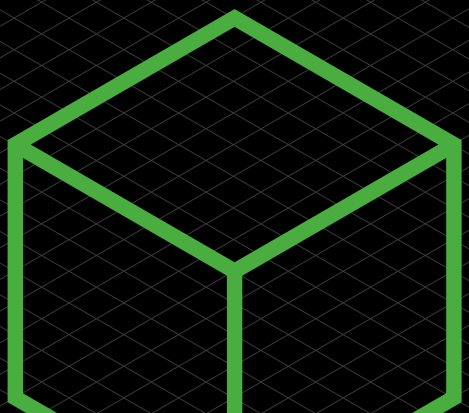






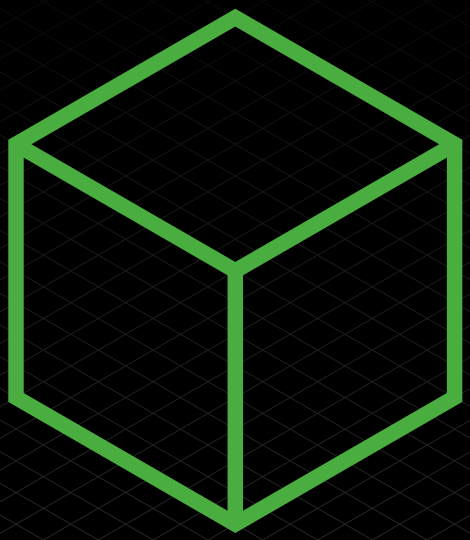
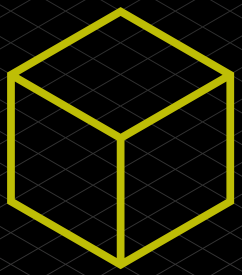
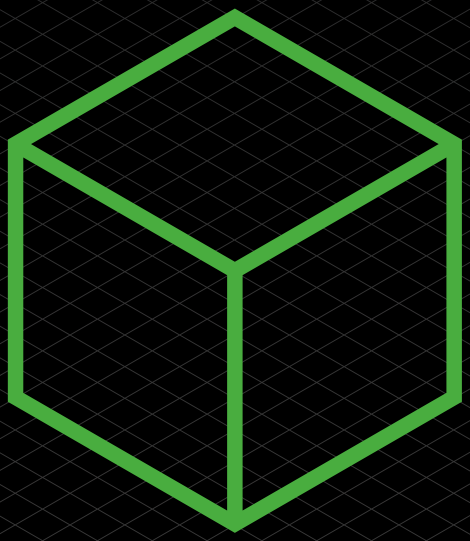
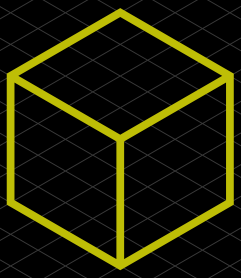
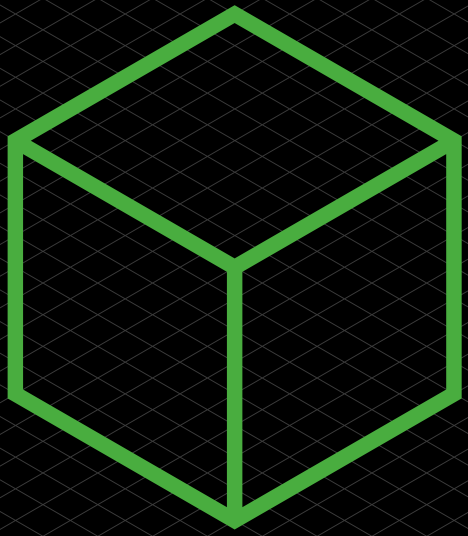
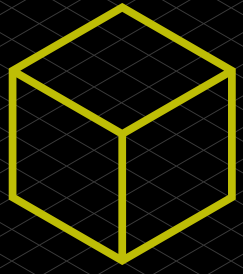






Part 1: Developing Technologies

Section 6 Social Tokens

Section 6: Social Tokens

Nick White and Matthew Blakebrough (Charles Russell Speechlys LLP)

What are social tokens?

Social tokens (also known as community tokens) are one of the latest innovations in the crypto space and have grown significantly in recent years. They are essentially a new form of cryptocurrency that is linked to a company, organisation or a person.

The social token definition covers tokens created by companies, organisations and people across a broad range of sectors, including:

— art;
— content;
— culture;
— design;
— gaming;
— music; and
— sport.

The direct rewards for owning social tokens are generally determined by the token designer or issuer. They vary significantly across the different sectors but can include benefits such as early access to new content, "money can't buy" experiences, discounts, governance rights and influence on decision making. Token ownership also carries with it other, indirect, benefits such as status within a community and growth in value.

Are there different types of social token?

There are three main classifications of social tokens:

1. personal tokens;
2. community tokens; and
3. social platform tokens.

Personal tokens

Personal tokens, also known as "creator tokens", are issued and controlled by a primary individual. The creators are often high-profile celebrities, entrepreneurs or artists. Personal tokens generally allow the holders to redeem them against services provided by their creators.

An example of a personal token is the "RAC" token issued by the musician RAC (André Allen Anjos), the DJ and Grammy award-winning artist. The token allows fans to access various perks and exclusive content.

Community tokens

Community tokens are issued and controlled by a group which is often managed by a Decentralised Autonomous Organisation (DAO). (For more on DAOs see Section 7.) These tokens generally have all the benefits of personal tokens with added governance rights of the DAO, together with influence and prestige in a niche community. Benefits may also include the right to revenue from assets owned or rented by the community or payments for services provided by the community.

One example of a community token is the "Whale" token. The Whale community is a DAO and is backed by rare and valuable NFTs primarily across the blockchain, gaming, digital art and virtual real estate sectors. It is therefore a community token backed by unique digital assets; or put another way, fungible assets backed by non-fungible ones. The token offers its owners the chance to rent NFTs from the Whale "vault", buy exclusive NFTs, participate in liquidity mining, purchase exclusive digital products and engage in DAO decision making.

Social platform tokens

Social platform tokens represent control over a platform that facilitates social token issuance and exchange. Token holders can often engage in the governance of the social platform and use the tokens to pay for transaction fees on the platform.

Additionally, because the tokens have a money's worth value, they can be held as investments by those speculating that the value will increase. Some tokens can also be staked whereby the token is deployed to validate transactions in a proof-of-stake blockchain. Staking generates rewards for the token holder.

The "Rally" token is one of the main social platform tokens on the market and is the governance token of the Rally network, which backs all "Creator Coins". Creator Coins allow individuals and businesses to receive payment for services and are essentially an individual type of cryptocurrency.

One of the best-known examples of a platform token in the sports sector is the Socios.com fan engagement platform and its "Chiliz" token. Socios allows holders of the Chiliz token to purchase fan tokens related to their favourite football team. The team related tokens are minted and exchanged on a permissioned sidechain to the main Chiliz blockchain and allow holders to engage in official sports team polls (thereby influencing club decision making) and unlock exclusive club rewards. A sidechain is used because it is less intensive in computational terms than the main Ethereum network and also enables Socios to reduce and manage the cost of gas on that network.

Social tokens terms and conditions

Unlike many of the older cryptocurrencies like Bitcoin, social tokens and related platforms generally have an identifiable individual or entity behind them which means it is more likely there will be a set of terms and conditions and/or a white paper governing the use of the platform and the token(s).

The terms and conditions currently in the market tend to exclude liability as far as possible for the token issuer. Participants or token holders should expect to see numerous unfavourable terms including extensive disclaimers for various types of risk (from hacking to lack of liquidity in the market) and uncapped indemnity provisions in favour of the token issuer.

Choice of governing law and jurisdiction is likely to be driven by where the individual, entity or platform is based. HX Entertainment Ltd (the entity behind the Chiliz social platform token) for example is a company registered in Malta and as such the Chiliz token terms and conditions are governed by Maltese Law. Rally Network, Inc on the other hand is a California-based company and has terms governed by the US State of Delaware.

Where English law does apply, the extent to which consumer law will protect the purchasers of cryptoassets such as social tokens is something of a grey area. The FCA's consumer research found that 89% of purchasers of cryptoassets were aware that they were not subject to regulatory protection[144]. At present then such purchasers do seem to be relatively sophisticated. The technical challenges for the newcomer in terms of setting up wallets, acquiring cryptocurrencies and acquiring tokens have also helped to ensure a degree of sophistication amongst purchasers. Those technical challenges are quickly being made easier however and that is likely to lead to increased access to the market for less experienced or less knowledgeable individuals. The application of consumer protections will probably therefore become a more prominent topic over time. This issue is of particular relevance in the field of social tokens which are used quite widely in the context of entertainment and celebrity culture.

Social tokens interaction with smart contracts

Social tokens are purchased and traded on platforms utilising smart contracts to govern the transaction. These contracts are generally quite simple, prescribing an agreed purchase price for the transfer of the token to a new owner, perhaps together with certain other limited information. Smart contracts that use the ERC-20 standard for example will also include information such as the total number of such tokens

144 HM_Treasury_Cryptoasset_and_Stablecoin_consultation.pdf (publishing.service.gov.uk)

in circulation and the current token balance of an account. It is rare to find highly complex smart contracts because, as well as complexity itself making problems with the contracts more likely, the cost in gas of processing them can be prohibitively high.

Most of the functionality of social tokens as perceived by the end user of the token, such as the bestowal of real world benefits, are handled off-chain rather than via smart contracts. By way of example, if an influencer or brand wants to produce a closed Instagram Live session for token holders exclusively, that right to that benefit does not sit on-chain or within the token or any smart contract. Instead it is simply a matter of a real world contract, or arrangement, between the influencer or brand and the token holder.

Regulatory challenges in the UK

As with many digital assets in the blockchain sector, social tokens do not fit neatly into the existing regulatory framework. The FCA has identified two types of regulated token in the UK:

— e-money tokens; and
— security tokens.

Social token issuers who wish to ensure that their tokens are not captured by FCA regulations will be keen for their tokens to avoid any of the attributes of an e-money or security token.

Within the category of unregulated token, the FCA has specifically identified the following two types of token:

— utility tokens; and
— exchange tokens

Many of the social tokens referenced in this article are likely to be considered “utility tokens” under the current guidance and, as such, would not be caught by the existing FCA regulations. Where tokens are used in the context of payment, they may be exchange tokens. While such tokens are themselves unregulated, certain payment activities in which they may be used could potentially be regulated under payment services regulation.

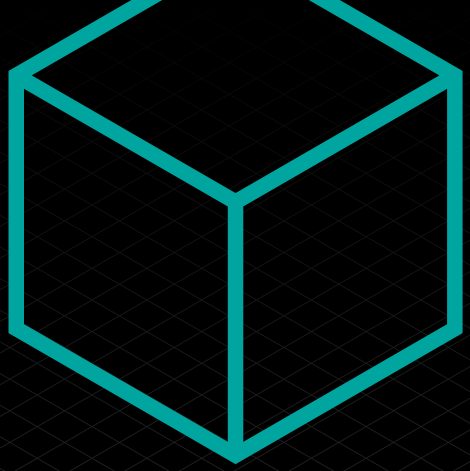
However, token issuers should be cautious when attaching rights to a token that could be construed as being similar to the characteristics of a share, a debt instrument or other type of financial instrument. Platforms and exchanges should also be cautious that their activities do not constitute “investment activity” on behalf of token holders, potentially opening up a classification of the platform or exchange operating a “collective investment scheme”. This is a particular risk where the token provides holders with a right to revenue from the ownership/management of assets/businesses.

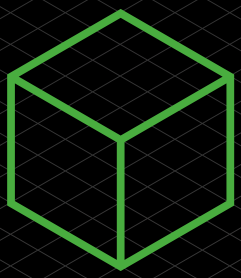
The FCA’s AML/CTF cryptoasset registration regime requires cryptoasset exchange providers and custodian wallet providers to register with the FCA and to meet various anti-money laundering and counter terrorist financing requirements. It is possible that a social token platform or exchange could be captured by these requirements.

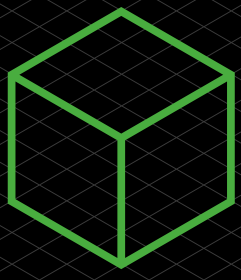
Any token issuer or platform/exchange which is considering launching in the UK should seek specialist legal advice in this area as soon as possible.

Part 2: Impacts on the Wider Landscape

Section 7 Smart Contracts and Data Governance






7

Section 7: Smart Contracts and Data Governance

Anne Rose (Mishcon de Reya LLP), Marc Piano (Harney Westwood & Riegels LLP (Cayman Islands)) and Akber Datoo (D2 Legal Technology (D2LT))

PART A: Smart Contracts

Anne Rose (Mishcon de Reya LLP) and Marc Piano (Harney Westwood & Riegels LLP (Cayman Islands))

This chapter is under review following the UK Law Commission's advice to the Government on smart contracts published on 25 November 2021.

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 guidance.

As at the date of this guidance, 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.

This section was written with a coding sub-group and with the help of expert evidence for which the Group is grateful. 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 guidance.

Objectives of the coding sub-group

The coding sub-group has four objectives:

— 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);

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

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

— 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)

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

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

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

Definitions
Drawing from definitions provided by Ciarán McGonagle:

— Smart Legal Contract (SLC): 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 SLCs
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 11.

— **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 guidance, 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 focused 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 and Libraries
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.

Subsequent to the D2LT evidence, D2LT have successfully completed similar work for two other capital markets trade associations, ISLA (The International Securities Lending Association) and ICMA (The International Capital Market Association) to create similar clause taxonomies and libraries for the GMSLA and GMRA documentation respectively. Furthermore, use cases have been identified across these trade associations to utilise these standards, such as in the automation of the close-out netting determination process[145], including the issuance of an NFT to represent legal opinions relied upon by the prudentially regulated trade association members for regulatory capital purposes.

"Digital Street" project

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 project 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.

145 Datoo A, and Clack CD (2021): Smart close-out netting <https://arxiv.org/abs/2011.07379>

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 guidance. 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 in Section 11.

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 guidance, 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 guidance, 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 11.

Regulatory considerations
As mentioned earlier, the 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" (VASPs) – see Part C Section 4 of this guidance for additional discussion.

Current FATF guidance[146] on a risk-based approach to virtual asset activities or operations and VASPs may apply to some stakeholders, parties or counterparties where smart 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 VASPs 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 guidance, but this issue is raised to ensure that parties and stakeholders consider any regulatory issues

146 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

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.

DAOs and the impact they may have on the legal profession
Marc Jones (Stewarts LLP)

What is a Decentralised Autonomous Organisation (DAO)?
In July 2021 the founder of Shapeshift, a crypto-exchange, announced that Shapeshift would over the following 12 months cease to be a company and become a DAO, with the open-source software which performs the "exchange" function passing to the holders of Shapeshift's digital token, FOX. The chief legal officer of Shapeshift explained: "Shapeshift is not an exchange, is not a financial intermediary and is not holding custody of any funds. It's simply an open-source interface for users to interact with their own digital assets."

On that view, a DAO is just software, not an entity. Unsurprisingly regulators are exercised at the prospect of, on the one hand, financial functions being carried out, but, on the other hand, there being no 'person' who is accountable for compliance with financial regulations (especially KYC and AML checks). A few weeks later the chair of the Securities and Exchange Commission expressed the view that DeFi platforms do have a degree of centralisation (including of governance mechanisms), saying "It's a misnomer to say they are just software put out in the web" – and that it would be possible for regulators to regulate them.

Ongoing at the same time is the EU's initiative to regulate digital assets with its draft Markets in Cryptoassets Regulation, a complex piece of legislation that amongst others things will potentially regulate tokens issued by DAO as securities and impose penalties on those engaged in establishing DAO if they do not comply with securities regulations. These examples, with a regulatory focus, highlight two opposing positions which meet head on with DAO:

— promoters of DeFi are not simply trying to disrupt traditional financial services/ markets but to escape altogether the regulations (and even the legal system) that apply to them; and

— the reality that all activity takes place within a legal system but these new technologies raise difficult questions about how they should be legally classified and treated.

The rest of this section will focus on those difficulties that arise at common law in determining what, if anything, is a DAO; and what or whom is responsible for a DAO.

Terminology
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 2019 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."*[147]

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

147 UKJT Legal Statement (n 4) paras 26 and 135

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. 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[148]) but legal personality is not one of them.

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

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. (It is also worth noting that the SEC determined in 2017 that The DAO's tokens were securities, which if the same view were taken now by the SEC and other regulators of other DAO tokens would have serious implications for those involved in establishing DAOs, but for present purposes does not really assist in the legal issue considered below of what, legally speaking, is a DOA).

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".[149] 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.

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

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.

PART B: Data governance requirements for 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".[150]

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[151], 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:[152]

"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".

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

151 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.

152 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

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).

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.

Three forms of smart contract

The UKJT Legal Statement[153] identified three different forms that smart contracts can take[154]:

1. A natural language contract in which some or all of the contractual obligations are performed automatically by the code of the computer program deployed on a distributed ledger. The code itself does not record any contractual obligations but is merely a tool employed by parties to perform those obligations.

2. A hybrid contract in which some contractual obligations are recorded in natural language and others are recorded in the code of a computer program deployed on a distributed ledger. At one end of the spectrum, the terms of a hybrid contract could primarily be written in code with natural language terms employed to add certain provisions (for example, governing law and jurisdiction clauses and dispute resolution mechanisms). At the other end of the spectrum, the terms of a hybrid contract could be primarily written in natural language and include, by reference, just one or two terms written in code.

3. A contract that is recorded solely in the code of a computer program deployed on a distributed ledger. No natural language version of the agreement exists: all the contractual obligations are recorded in, and performed by, the code.

All three forms of smart contract involve the use of computer code deployed on a DLT system either to perform contractual obligations or both to record and perform them. What distinguishes the three forms is the role played by the code. In the first form of smart contract, the code's role is confined to performing obligations which are recorded in a natural language contract. In contrast, in the second and third forms, the code is used to record contractual obligations as well as to perform them. Although smart contracts have today tended to start from natural language contracts forms, they are expected to evolve over time to those written directly in code (noting there are many forms of code from high-level programming languages through to assembly language). This will allow greater clarity of "digital thinking", the lens of automation in respect to the upstream and downstream systems smart contracts relate to (after all, it is rightly the "automaticity" characteristic that is the defining feature of smart contracts, as noted by the UKJT in its legal statement). Of course, systems communicate through the medium of not natural language and legalese – but data.

153See [142-148] of the UKJT Legal Statement
154Law Commission – Smart Contracts – Call for evidence, December 2020 (2.33-2.34)

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.[155] 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[156] (note that the variable limit 'limitArrivalTime' is defined as 2 hours elsewhere in the code).

155 Stephen J Choi and Mitu Gulati, 'Contract as Statute' (Michigan Law Review, 2006), Vol 104
156 Akber Datoo, 'Legal Data for Banking: Business Optimisation and Regulatory Compliance' (John Wiley, 2019)

```
138         // if the actual arrival time is over the limit the user wanted,
139         // we trigger the indemnity, which means status = 2
140         if (actualArrivalTime > insuranceList[flightId][i].limitArrivalTime) {
141           newStatus = 2;
142         }
```

Figure 12.2 The core logic code for the Fizzy smart contract application

The core logic code for the Fizzy smart contract application


```
138         // if the actual arrival time is over the limit the user wanted,
139         // we trigger the indemnity, which means status = 2
140         if (actualArrivalTime > insuranceList[flightId][i].limitArrivalTime) {
141           newStatus = 2;
142         }
```

Figure 12.2 The core logic code for the Fizzy smart contract application


```
117   /**
118    * @dev Update the status of a flight
119    * @param flightId <carrier_code><flight_number>.<timestamp_in_sec_of_departure_date>
120    * @param actualArrivalTime The actual arrival time of the flight (timestamp in sec)
121    */
122   function updateFlightStatus(
123     bytes32 flightId,
124     uint actualArrivalTime)
125   public
126   onlyIfCreator {
127
128     uint8 newStatus = 1;
129
130     // go through the list of all insurances related to the given flight
131     for (uint i = 0; i < insuranceList[flightId].length; i++) {
132
133       // we check this contract is still ongoing before updating it
134       if (insuranceList[flightId][i].status == 0) {
135
136         newStatus = 1;
137
138         // if the actual arrival time is over the limit the user wanted,
139         // we trigger the indemnity, which means status = 2
140         if (actualArrivalTime > insuranceList[flightId][i].limitArrivalTime) {
141           newStatus = 2;
142         }
143
144         // update the status of the insurance contract
145         insuranceList[flightId][i].status = newStatus;
146
147         // send an event about this update for each insurance
148         InsuranceUpdate(
149           insuranceList[flightId][i].productId,
150           flightId,
151           insuranceList[flightId][i].premium,
152           insuranceList[flightId][i].indemnity,
153           newStatus
154         );
155       }
156     }
157   }
```

Figure 12.3 An example of the Solidity smart contract coding language (taken from the Fizzy smart contract)

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 9 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.

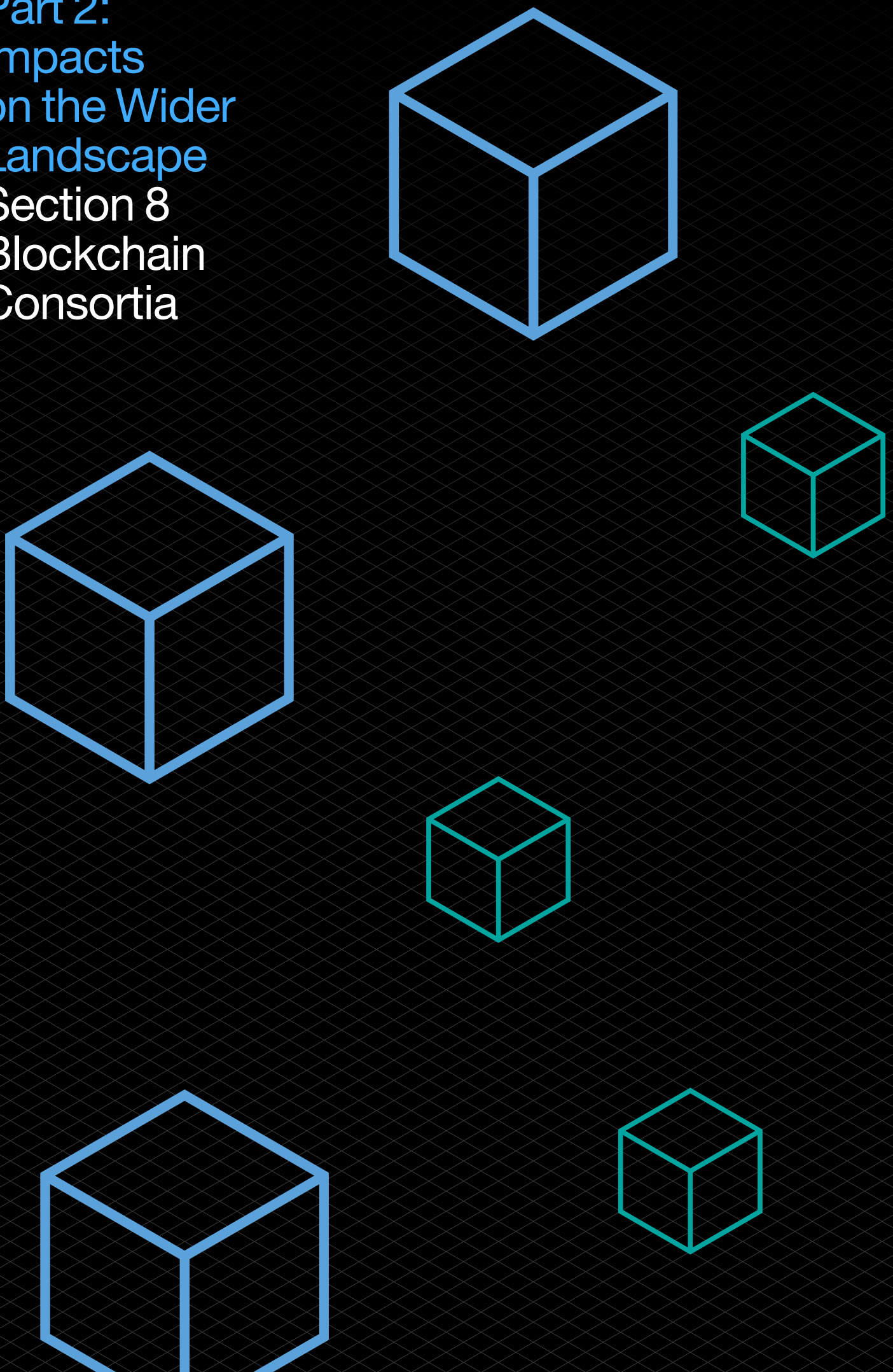
3. **Log Violation:** it may be necessary to accept certain data inputs, despite some concerns regarding data quality, whilst flagging it as being of low data quality for informational purposes.

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.

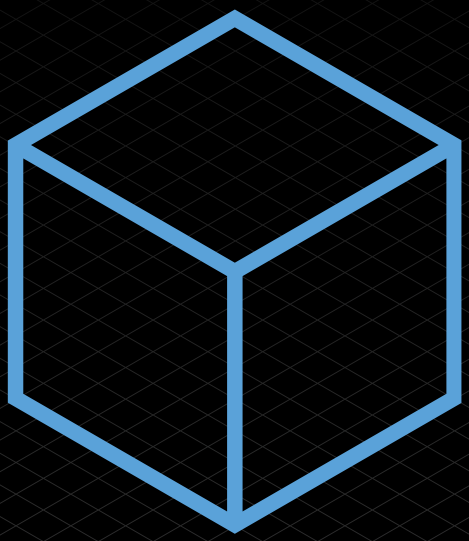
5. **Defer Decision:** a particular violation of a data quality threshold on an input might not be enough, in itself, to result in a definitive automated action, and the decision may simply be deferred.

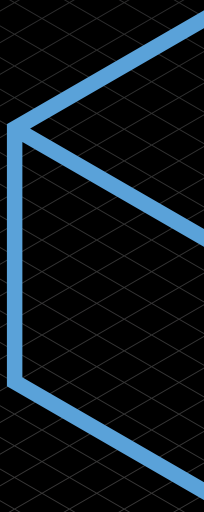
Part 2: Impacts on the Wider Landscape

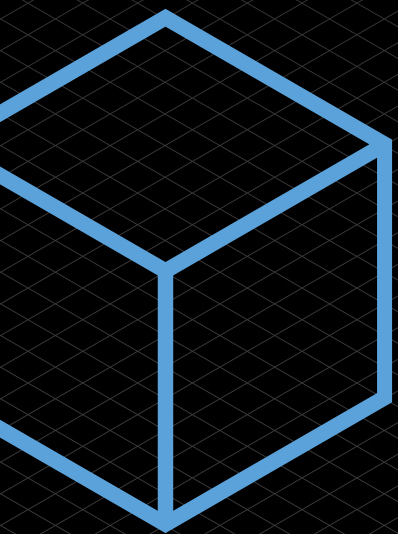
Section 8 Blockchain Consortia

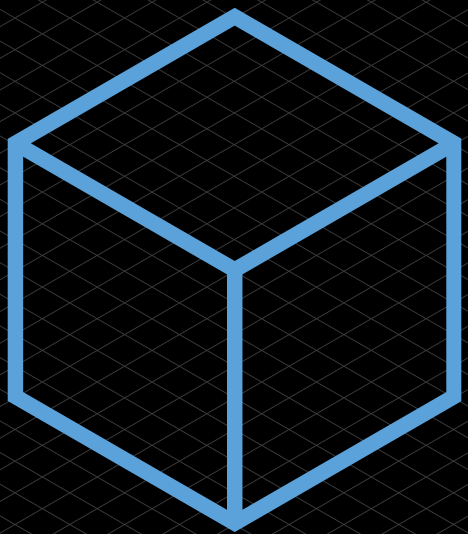


8









SECTION 8: 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 we.trade, which is a platform focused on trade finance;

— Aura, which aims to be a blockchain platform for the luxury goods sector to support the traceability, sustainability and authenticity of luxury goods; 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.[157]

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

— 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.

157 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

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, 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 in 2019, 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.

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.

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).
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

Governance continued

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. There fore, 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;
  — **Change management:** the consortium will need to create and document appropriate change management mechanisms and governance structures; and
  — **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).

Topic	Issues
Governance continued	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).

IPRs continued	— **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[158]). If the cryptoasset is regulated, then the members will need to identify all necessary compliance requirements (including with respect to AML/KYC).

158 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

Topic	Issues
Compliance continued	— 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 block-chain 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 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 9.

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 13.

Joining a consortium

Topic	Issues
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 it is 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 co-operation. If the consortium is not working well and members are unable to cooperate effectively, it is unlikely to achieve its commercial goals.

Due Diligence continued

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.

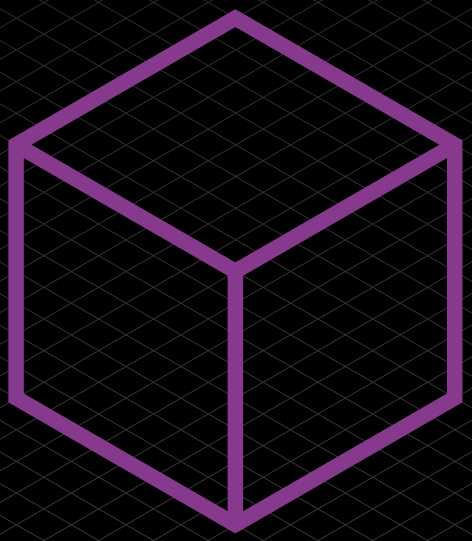
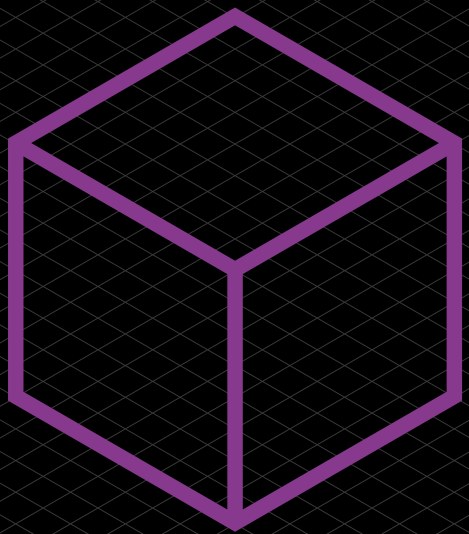
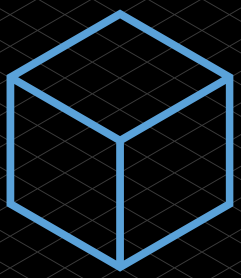
Conclusion

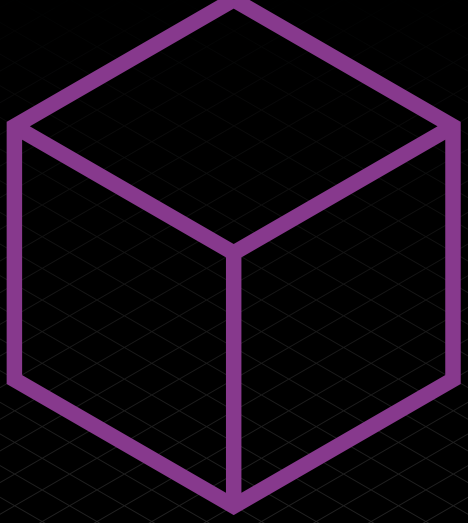
Blockchain consortia may be essential in order to develop and scale blockchain platforms which enable digital transformation across a sector or a group of industry stakeholders. However, there are a number of factors that businesses will need to take into account when forming or joining a consortium 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.

Part 2: Impacts on the Wider Landscape

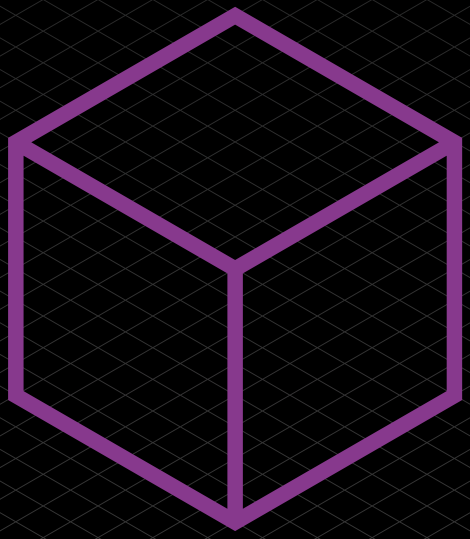
Section 9 Data Protection and Data Security

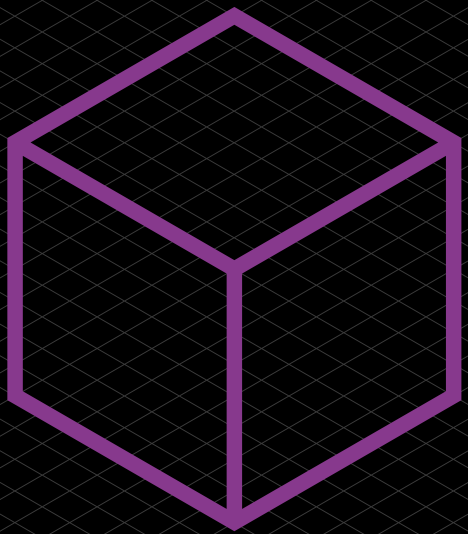




9





SECTION 9: DATA PROTECTION AND DATA SECURITY

Anne Rose (Mishcon de Reya LLP) and Adi Ben-Ari (Applied Blockchain)

PART A: Data Protection

Anne Rose (Mishcon de Reya LLP)

Introduction

The EU GDPR 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.[1] Since the 2020 guidance the UK has now left the EU and the UK GDPR applies in the UK, along with the Data Protection Act 2018 (DPA 2018).

UK GDPR contains similar obligations to EU GDPR, subject to some amendments made to UK GDPR to ensure the legislation works solely in the context of the UK, and save that the UK has the independence to keep UK GDPR under review. The DPA has also been amended to ensure that the Secretary of State has the power to make adequacy decisions in the UK, allowing the free flow of data between the UK and third countries deemed to have an adequate level of protection of personal data. In addition, on 28 June 2021, the UK was granted adequacy status by the European Commission, though this decision is due to be re-assessed in 2024.

At the time of writing this guidance, the UK has announced a new strategic approach to data protection, including potential future adequacy partnerships with countries such as the US, Australia, the Republic of Korea, Singapore, the Dubai International Finance Centre and Colombia, the aim being to aid the UK in exchanging data with the world's fastest-growing economies and aligning with its trade agenda post-Brexit. Maintaining equivalence with EU data protection laws may no longer be a priority for the UK, as it heads into a new pro-growth and innovative regime – we may start to see some divergence in the coming years, and it will be important to keep abreast of new developments.

Dual Regimes

In light of the amendments to data protection law since the 2020 guidance, if a controller/processor is carrying out processing activities or targeting/monitoring individuals in both the UK and the EU, there is now the added risk of dual enforcement by both the ICO and the EU Data Protection Authorities, as they will be subject to both UK and EU GDPR, since both have extra-territorial effect under Article 3 UK/EU GDPR. If activity is limited to the UK only, controllers/processors will now only be subject to UK GDPR.

For ease, this guidance refers to UK GDPR only and assumes that organisations are not subject to dual regimes. The 2020 guidance considered EU GDPR. For the avoidance of doubt, this guidance can also be applied to UK GDPR. 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 UK GDPR, hampers the allocation of responsibility and accountability. Moreover, UK 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.

1 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

For the 2020 guidance, the Group focused on the definition of "personal data" under EU GDPR and noted that depending on context, the same data point can be personal or non-personal and therefore subject to EU GDPR or not. In addition, the Group considered the impact of changes in technology that could increase the tension between blockchain and EU GDPR, as well as the possibility that blockchain could support EU GDPR. The Group did not go into detail on all the various issues, as these are discussed widely elsewhere.[2]

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

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 EU 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.[3] Dr Finck has written widely on the points of tension between blockchain and EU GDPR – including questions of when and under which circumstances on-chain data qualifies as personal data.[4]

Anne Rose, Solicitor at the law firm, Mishcon de Reya LLP, has also considered the tensions at play between blockchain and EU GDPR in an interactive entertainment context.[5]

What is Personal Data?
Article 4(1) UK 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 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) UK GDPR and Recital 26 UK GDPR:

2 For example, Michèle Finck, Blockchain Regulation and Governance in Europe (Cambridge University Press 2018)
3 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
4 See, for example, Michèle Finck, Blockchain Regulation and Governance in Europe (Cambridge University Press 2018)
5 Anne Rose, 'GDPR challenges for blockchain technology', (2019) 2 IELR 35

Article 4(5) UK 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, UK 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 UK 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".[6] 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".[7] 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.[8]

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."[9] 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 effort to boost the value of their profiles for advertising purposes".[10] In line with this reasoning, public keys or other sorts of identifiers used to identify a natural person constitute personal data.

---

6 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.

7 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

8 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

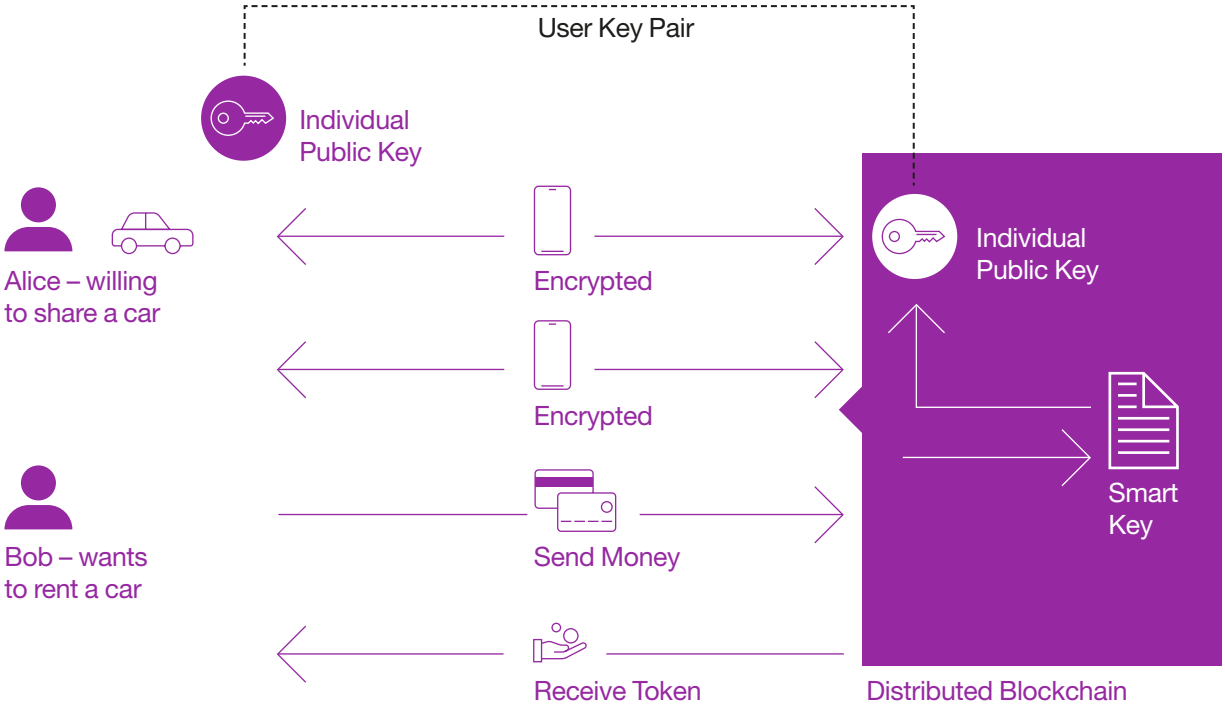
9 Article 29 Working Party, Opinion 04/2007 on the Concept of Personal Data (2007) WP 136 01248/07/EN, 16 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf> Accessed 13 April 2020

10 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

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 UK GDPR compliance will seek to avoid the processing of personal data to start with. However, as noted below, this is far from straightforward 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 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.[11]

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

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;[12]

— 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 Part B on data security measures. This would also help with compliance with data protection principles, such as the purpose limitation and data minimisation principles.[13]

While these steps all assist in preventing transactional data being classified as 'personal data' under the UK GDPR, there is at present no legal certainty for developers wishing to handle public keys in a UK 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 UK 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 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 UK GDPR) and the right to data portability (Article 20 UK 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.

12 In October 2019, the European Data Protection Supervisor (EDPS), in conjunction with the Spanish data protection authority, has also issued a joint paper on the hash function as personal data pseudonymisaton technique: <https://edps.europa.eu/sites/edp/files/publication/19-10-30_aepd-edps_paper_hash_final_en.pdf> (accessed 9 August 2021)
13 Under the UK 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 the UK GDPR, Article 5(1)(b) and (c)).

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 UK 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 UK GDPR?

— How should "erasure" be interpreted for the purposes of Article 17 UK GDPR in the context of blockchain technologies?

— How should Article 18 UK 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 UK 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 UK 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 UK 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?[14]

None of these questions has been formally addressed since the publication of the 2020 guidance.

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.

14 Michèle 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

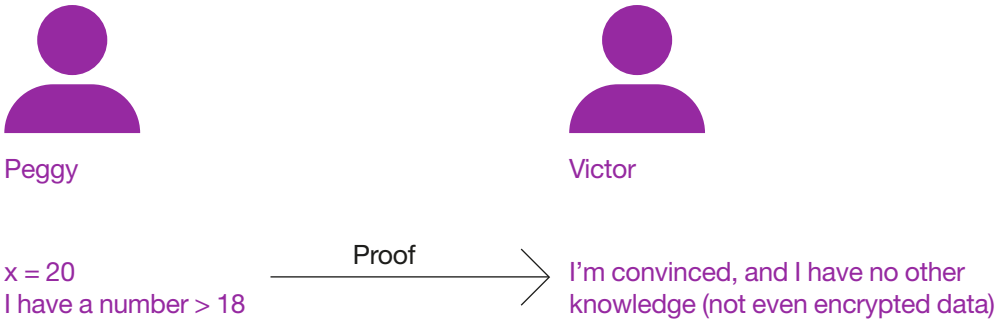
In order for a cryptographic scheme to be considered a ZKP, it must demonstrate the following properties:

— **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.



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 the UK 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 the UK 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 UK 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 a 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:

— **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.

— **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 is 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:

— Circuit production
— Proof generation
— 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:

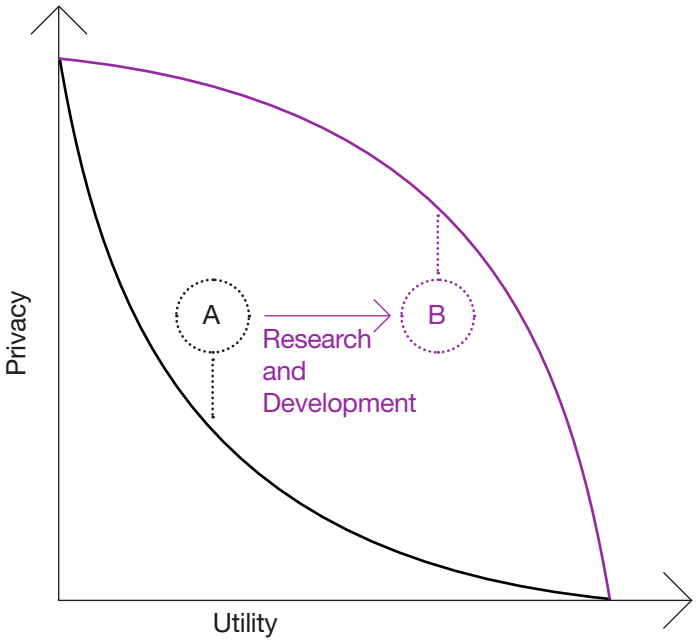
1. Rollups
2. Flat blockchains

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.

Hardware Secure Enclaves

An additional emerging technology for preserving data privacy is the hardware secure enclave (HSE). This is an area of a computer chip that is isolated by hardware and prevents other areas of the computer from having access to data inside. This means that even the system administrator of a device or someone with physical access to the machine would not have access to the data inside the HSE.

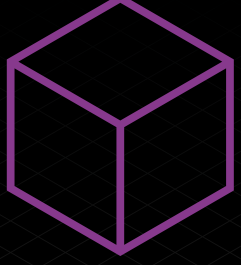
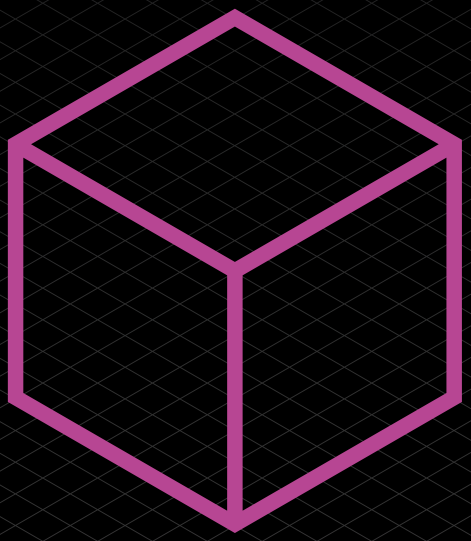
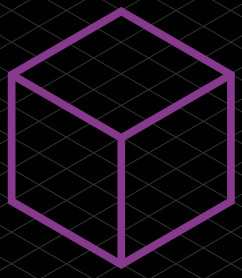
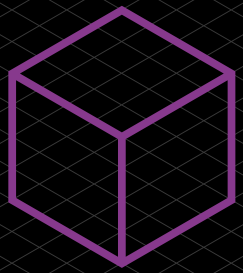
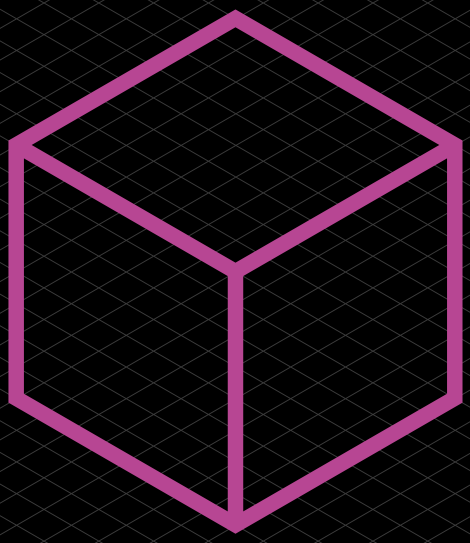
A common use of HSEs is to store private keys. A private key and public key pair is generated inside a hardware enclave. The public key is shared, but the private key never leaves the enclave. Data can be sent to the enclave for signing by the private key, but the key itself is never revealed. An example of hardware secure key storage is Apple Pay, where the private key to initiate payments is stored in an enclave on the phone, and the key itself cannot be shared with Apple or any apps. Instead, the key can sign transactions proving that they came from the device (in this case, use of the enclave is also tied to the biometrics tests conducted on the device).

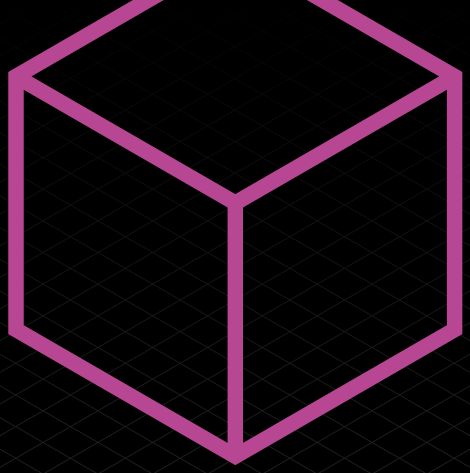
HSEs have many more uses beyond key storage. In fact, any data can be sent to an enclave, and any private processing can occur in the enclave. Unlike ZKPs and other software-based cryptography methods, hardware enclaves run at almost the same speed as regular tasks that run on the processor. This means that performance and scalability issues associated with software-based cryptography do not apply in a hardware secure enclave environment.

Intel's SGX (secure guard extensions) is an example of a relatively mature hardware secure environment that enables complex privacy-preserving applications.

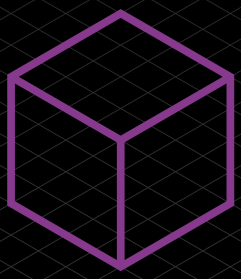
Part 2: Impacts on the Wider Landscape

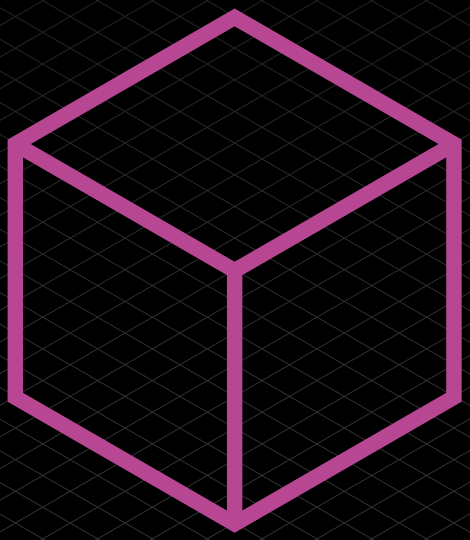
Section 10 Intellectual Property

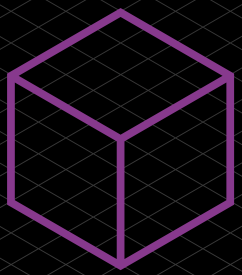






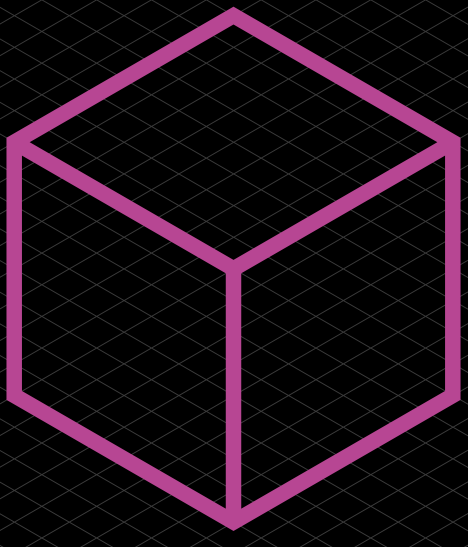


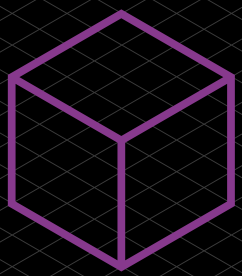
10











Section 10: Intellectual Property

Rosie Burbidge (Gunnercooke LLP), John Shaw (Foot Anstey LLP) and Charlie Lyons-Rothbart (Taylor Vinters 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.[15] 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.[16][17] 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.

15 Tresose, Goldenfein and Hunter, 'What Blockchain Can and Can't Do for Copyright' (2018) 28(4) AIPJ) 144
16 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)
17 Aurelio Lopez-Tarruella, 'The Regulatory Challenges of Blockchain Applications in the IP Ecosystem' (WIPO White Paper, 28 September 2021) <https://www.wipo.int/edocs/mdocs/cws/en/wipo_webinar_standards_2021_19/wipo_webinar_standards_2021_19_presentation5_lopez_tarruella.pdf> accessed 29 November 2021

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.[18] 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.[19] This has included making a hyperlink available, even if the user does not click on it.[20] 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.[21] 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.[22] 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.[23]

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 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

18 Copyright, Designs and Patents Act 1988, ch II
19 Paramount Home Entertainment International Ltd v British Sky Broadcasting Ltd [2013] EWHC 3479 (Ch) [12(7)] (Arnold J)
20 Warner Music UK Ltd and Sony Music Entertainment UK Ltd v Tunein Inc [2019] EWHC 2923 (Ch) [52]
21 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
22 Case C-610/15 Stichting Brein v Ziggo BV and XSALL Internet BV, Opinion of AG Szpunar, para 54
23 Case C-306/05 SGAE v Rafael Hoteles SA [2006] ECR I-11518, para 38

technically possible constitutes "communication".[24] [25] 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.[26] 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.[27] 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 decision in the joined cases of Youtube and Cyando provided good guidance on factors that should be considered by local courts when determining if a platform carries out an act of "communication to the public".[28]

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.[29] 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.[30] As a DLT application will still require the internet protocol network layer and will sit between the application and transport layers[31] 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

24 ibid paras 46-47
25 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
26 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
27 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
28 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]
29 Case C-607/11, ITV Broadcasting Ltd v TV Catchup Ltd [2013] EU:C:2013:147 paras 23 – 26
30 Warner Music UK Ltd, Sony Music Entertainment UK Ltd v Tunein Inc. [2019] EWHC 2923 (Ch) [54]
31 De Filippi & Wright, Blockchain and the Law: The Rule of Code, (Harvard University Press 2018) 48-49

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."[32] 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 protected 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.[33] 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.[34]

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.[35] 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 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".[36] This appears to be highly applicable to DLT. Further case law will shine a light on 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.

Recently, decisions have been made in relation to platform operators and the users of peer-to-peer networks. In the joined cases of YouTube and Cyando, the

32 Case C-610/15, Stichting Brein v Ziggo BV and XSALL Internet BV [2017] EU:C:2017:456 para 45
33 ibid para 46
34 Case C-160/15, GS Media BV v Sanoma Media Netherlands BV and Others [2016] EU:C:2016:644 para 51
35 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.
36 Ziggo (n 48) [48]

CJEU held that users of platforms carry out and "act of communication" within the meaning provided by case law, where they provide access to protected works to other internet users without the rightsholders' consent and that such a communication is a "communication to the public" when the content is made available to the public.[37]

The question of whether the platforms are also carrying out acts of communication to public was referred back to the local courts, but guidance was provided on the factors that should be considered when deciding. These include: if the operator knows or ought to know if users are making protected content available to the public illegally via its platform; if appropriate technological measures are in place to counter copyright infringements on that platform; if the platform operator participates in selecting content illegal communicated to the public; if tools are provided which are intended for illegal sharing of content, if the business model encourages users of its platform to illegally communicate to the public; and if the predominant use of the platform consists of making available content illegally.[38] Practitioners should be aware of these factors as they are likely to determine the question of infringement and mainly relate to the intentions behind the platform, systems in place and main use by users. DLT may not have the best reputation in this regard, but platforms linked to any blockchain will be able to provide evidence relating to use.

Perhaps even more relevant is the decision in Mircom International Content Management & Consulting (MICM) Limited v Telenet BVBA (Case C597/19) in which, consistent with the decision in YouTube and Cyando, the ECJ held that uploading pieces of a media file onto a peer-to-peer network constituted making available to the public within the meaning of the Copyright Directive.[39] The fact that the network in question in Mircom was used by a considerable number of people (evidenced by the high number of IP addresses registered by Mircom) meant that making available was aimed at an indeterminate number of potential recipients. As a result, it was considered that the works are made available to a new public when the works were published without the authorisation of the rightsholders.[40]

These decisions show that users of DLT and the operators of any platforms will be pursued in the event of copyright infringement. Practitioners should consider the factors set out by the courts when establishing platform liability and the high likelihood that uploading to a peer-to-peer network will amount to an infringement if the network is well populated.

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. Michèle Finck notes that governments could impose legal obligations on core developers[41] 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

37 YouTube C-682/18 and C-683/18, [75]
38 YouTube C-682/18 and C-683/18, [84 and 100]
39 Mircom International Content Management & Consulting (MICM) Limited v Telenet BVBA (Case C597/19) [49 and 50]
40 Mircom International Content Management & Consulting (MICM) Limited v Telenet BVBA (Case C597/19) [56]
41 Michele Finck, Blockchain Regulation and Governance in Europe (Cambridge University Press 2019), 52

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.[42] 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 the UK 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.[43]

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 Finck[44] and it seems that her notable conclusions on how blockchain and the UK 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 use.[45] 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

42 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
43 Ziggo, opinion of AG Szpunar (n 38) [51]
44 Finck, Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law? (n 37)
45 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

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.[46] 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.[47] 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.

Article 11 of the IP Enforcement Directive[48] 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.[49] 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.

46 L'Oreal SA v eBay International AG [2009] EWHC 1094 (Ch)
47 Case C-324/09 L'Oréal SA and Others v eBay International AG and Others [2001] I-06011
48 Council directive 2004/48/EC of 29 April 2004 on the enforcement of intellectual property rights (2004) OJ L195/16
49 Cartier International AG v British Sky Broadcasting Ltd [2016] EWCA Civ 658

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.[50] 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. Finck provides the useful summary that it is essentially a database that is replicated across a network of computers updated through a consensus algorithm.[51] The ledger aspect of DLT means that it is worth considering whether the two rights created by the Database Directive (96/9/EC)[52] (the Database Directive) which was implemented by the Databases Regulations 1997[53] (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".[54] 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".[55] 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.[56]

— *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".[57] 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.

50 Rosie Burbidge, 'The Blockchain is in Fashion' (2017) 107(6) TMR 1262 - 1297
51 Finck, Blockchain Regulation and Governance in Europe (n 53) 6
52 Council Directive 96/9/EC of 11 March 1996 on the legal protection of databases [1996] OJ L 77/20
53 The Copyright and Rights in Databases Regulations 1997, SI 1997/3032
54 Copyright, Designs and Patents Act 1988, s3A(2)
55 ibid s3A(1)
56 British Horseracing Board Limited v William Hill [2001] RPC 31 [30]
57 Satoshi Nakamoto. 'Bitcoin: A Peer-to-Peer Electronic Cash System', (October 2008) <https://bitcoin.org/bitcoin.pdf> Accessed 9 March 2020

— *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".[58] 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.[59] 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).

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".[60] 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.[61] 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".[62] 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.[63] 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.

58 Databases Regulations (n 65), Regulation 13(1)
59 British Horseracing Board Limited v William Hill (n 68)
60 Simon Stokes, Digital Copyright Law and Practice (5th Edition, Hart Publishing 2019) 87
61 Case C-203/02 British Horseracing Board Ltd v William Hill [2005] RPC. 13, para 1
62 British Horseracing Board Ltd v William Hill Organisation Ltd [2005] EWCA Civ 863
63 Stokes (n 72) 89

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.[64] Databases can therefore be protected by copyright as literary works in addition to tables or compilations (which are not themselves databases).[65] 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".[66]

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.[67] 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.[68] 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".[69] 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.

64 CDPA (n 66) s.3A
65 ibid s.3
66 ibid s.3A(2)
67 Stokes (n 72) 83
68 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
69 Forensic Telecommunications Services Ltd v West Yorkshire Police & Anor [2011] EWHC 2892 (Ch) [94]

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.[70] The three limbs are: (i) the information itself must have the necessary 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.[71] 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.[72]

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".[73] 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.[74] 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.[75]

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

70 Coco v AN Clark (Engineers) Ltd [1968] F.S.R. 415
71 Saltman Engineering Co v Campbell Engineering Co [1948] 65 R.P.C. 203
72 The Trade Secrets (Enforcement, etc.) Regulations 2018, SI 2018 No. 597 (implementing the European Trade Secrets Directive (2016/ 244/EU) [2016]), Regulation 2
73 Mars UK Ltd v Teknowledge Ltd [1999] 6 WLUK 149
74 Kerry Ingredients (UK) Ltd v Bakkavor Group Ltd [2016] EWHC 2448 (Ch)
75 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.

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 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.[76] A computer program that enabled a computer to run faster and more reliably has been held to be patentable.[77] 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 the time of writing.

Numerous patents have been applied for and registered, but there does not appear to be any patent litigation on the immediate horizon. Whether the patents that are on the register are able to sustain a validity attack remains to be seen. 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 focused 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.[78] 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.[79]

76 Stokes (n 72) 136
77 Symbian Ltd v Comptroller General of Patents, Designs and Trademarks [2008] EWCA Civ 1066
78 CDPA (n 66) ss 3(1)(b) and (c)
79 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

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".[80] This comment was affirmed in Nova in which Jacob 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."[81]

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.[82] 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.[83] 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,[84] but also on the decision in SAS Institute.[85] In SAS Institute, Arnold J referred to the "design" of a program as well as its code as potentially benefitting from protection.[86] 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 guidance. However, copyright can subsist within computer code and given that an electronic coin has been defined as "a chain of digital signatures",[87] 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.[88] 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. Twhe 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.[89]

80 Navitaire Inc v EasyJet Airline Co Ltd (No.3) [2004] EWHC 1725 (Ch)
81 Nova Productions Ltd v Mazooma Games Ltd [2007] EWCA Civ 219
82 Case C-406/10 SAS Institute Inc v World Programming Ltd [2012] EU:C:2012:259
83 SAS Institute Inc v World Programming Ltd [2013] EWHC 69 (Ch) [249]
84 Baigent v Random House Group Ltd [2006] FSR 44; [2008] EMLR 7
85 Stokes (n 72) 157
86 SAS Institute Inc v World Programming Ltd [2010] EWHC 1829 (Ch) [251]-[261]
87 Nakamoto (n 69)
88 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
89 UKJT Legal Statement (n 4) 44

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.

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 11 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.

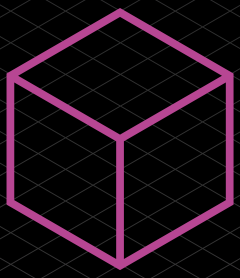
Conclusion

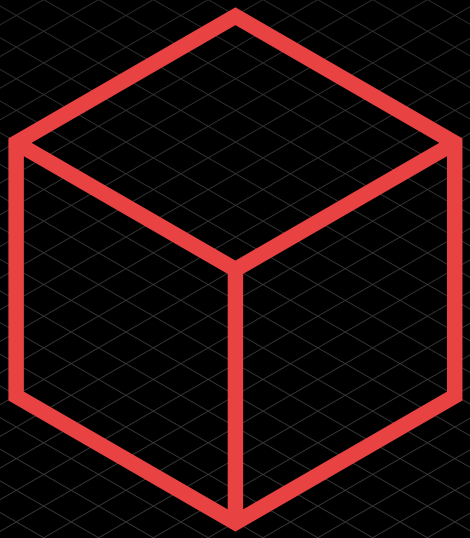
There are a number of interesting issues relating to intellectual property and DLT that would benefit from further guidance, decisions and commentary. In respect of copyright, it will be interesting to see how the court treats DLT and linked applications and whether existing case law relating to communicating 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.

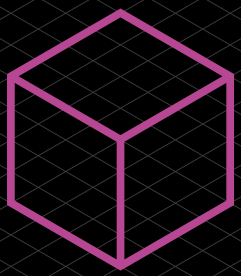
Whether DLT is treated as a novel technology or whether it will be treated in such a way so as to fit within the existing framework of intellectual property law (as has been found so far in respect of other legal issues) remains to be seen. So far, there have been very few calls for bespoke legislation 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.

Part 2: Impacts on the Wider Landscape

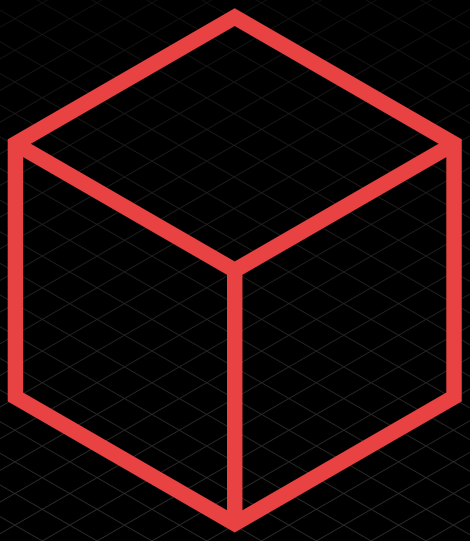
Section 11 Dispute Resolution

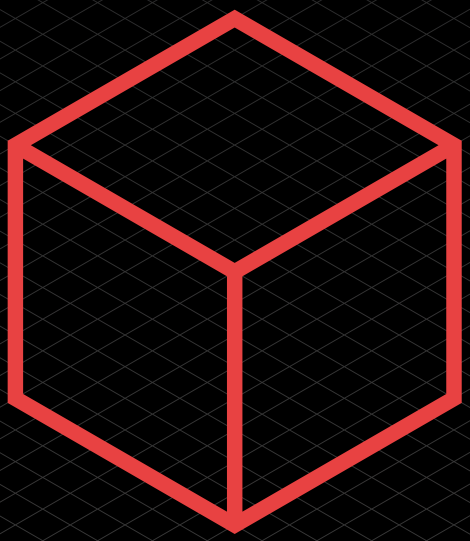


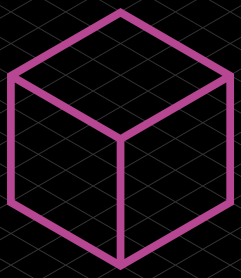


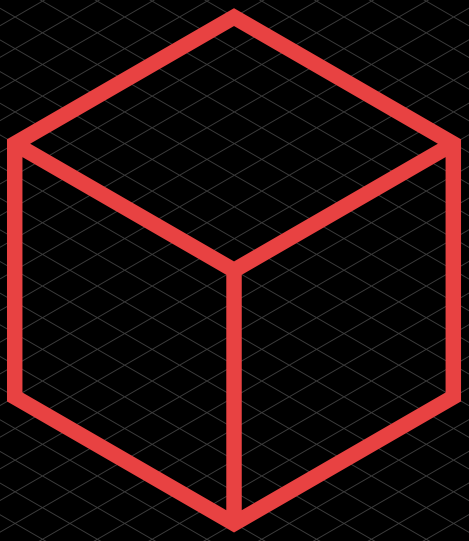


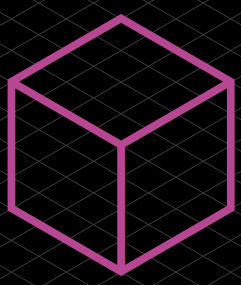
11











SECTION 11: DISPUTE RESOLUTION

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

PART A: DLT and Litigation

Will Foulkes (Stephenson Law LLP)

Introduction

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 sections, 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 7. 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 Delivery 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 Delivery 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 understand sufficiently 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 Delivery 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.[90] 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.

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 and smart 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.

Part B therefore begins 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

90 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

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 2);

— distinct consensus protocols, methods of exchanging and retaining data, anonymity features, use of public and private keys (see Section 9); and

— single or multi-channel architectures that do, or do not allow for compliance with regulatory requirements such as those under the UK GDPR (see Section 9)

In this context, there is 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.

Part B also 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 and reliability of current on-chain mechanisms to resolve full range of potential disputes

A review of numerous currently available on-chain dispute resolution mechanisms identifies the following concerns:

— 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,[91] 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 were 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[92] – The DAO hack in June 2016 demonstrated the potential for smart contracts not to function as envisaged[93] – 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.[94] 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.[95]

91 A term used to describe any network or application using distributed ledger technology, whether private / public or permissioned / permissionless.
92 For example, the hack of Coincheck in 2018 resulting in loss of cryptoassets with a reported value of more than $500 million.
93 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.
94 See e.g. the current consultation by the Law Commission of England and Wales (the Law Commission) on Digital assets <https://www.lawcom.gov.uk/project/digital-assets/> Accessed October 2021; and the 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
95 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.

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

1. Jurisdiction

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;

— 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.[96]

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.[97] They should be drafted so as to make clear that they create binding legal

96 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.
97 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.

relationships not only between each individual user (or node) on the system and the relevant administrator or operating authority (R(O)A),[98] 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 to have agreed to abide by and be legally bound by its terms".[99] A similar effect can be achieved by the use of master or framework agreements, as are typically used in DLT trading and settlement systems.[100]

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.[101] 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.[102] Specialist pools of arbitrators with relevant experience of DLT disputes are likely to develop over time.

98 A term adopted by the FMLC in its report (n 106) para 6.16
99 UKJT Legal statement (n 4) para 148
100 For example, the DLT derivative trading platforms considered in the ISDA / Clifford Chance paper (n 106)
101 The New York Convention has been adopted by 163 states, making it one of the foundational instruments of international arbitration.
102 Examples include the World Intellectual Property Organisation (WIPO) and the International Centre for Dispute Resolution (ICDR)

— **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.

— **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.[103] 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).[104] This can impede the tracing of misappropriated digital assets, especially given the speed with which such assets can be transferred.

103 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.

104 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.

— **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 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.[105] 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.

— T**ype 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).[106] 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.

105 UKJT Legal Statement (n 4) para 164

106 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[107] (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,[108] 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.[109] 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.

2. 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.

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.[110] However,

107 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.

108 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.

109 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); Litecoin Foundation Limited v Inshallah Limited [2021] EWHC 1998 (Ch); and Toma v Murray [202] EWHC 2295 (Ch).

110 Dicey, Morris & Collins, The Conflict of Laws, (15th edn, Sweet & Maxwell, 2018) 32-040 et seq

under Regulation 593/2008 on the law applicable to contractual obligations[111] (the Rome I Regulation),[112] 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.[113]

— 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 following UK 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".[114] 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.[115]

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"

111 Council regulation (EC) 593/2008 of 17 June 2008 on the law applicable to contractual obligations (Rome I) [2008] OJ L177/6
112 These rules continue to apply in the UK, as retained EU law, following Brexit: see The Law Applicable to Contractual Obligations and Non-Contractual Obligations (Amendment etc) (EU Exit) Regulations 2019.
113 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".
114 ibid, para 7.245
115 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.

legal principles.[116] 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".[117] 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.[118] 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.[119]

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.[120] 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".[121]

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. 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

116 UKJT Legal Statement (n 4) paras 136-148 Note also the desire expressed by the Law Commission in its current consultation on Digital assets (see footnote [155] above) to strengthen the certainty accorded by English law to the legal status of digital assets so as to "incentivise the use of the law and jurisdiction of England and Wales in transactions concerning those assets".
117 AA v Persons Unknown [2019] EWHC 3556 (Comm) [57] and [59] (Bryan J), followed and applied in Litecoin Foundation Limited v Inshallah Limited [2021] EWHC 1998 (Ch) and Toma v Murray [202] EWHC 2295 (Ch).
118 The rules of the Rome I and Rome II Regulations continue to apply in the UK, as retained EU law, following Brexit: see The Law Applicable to Contractual Obligations and Non-Contractual Obligations (Amendment etc) (EU Exit) Regulations 2019.
119 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
120 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]
121 UKJT Legal Statement (n 4) para 36

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.[122] 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.[123] 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.[124]

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.[125] 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".[126] 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".[127] 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.[128] 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 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).[129]

122 As explained by Dicey, Morris & Collins (n 122) para 22-025
123 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.
124 As in Art. 14(1) of the Rome I Regulation
125 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
126 UKJT Legal Statement (n 4) para 97
127 FMLC report (n 106) paras 6.5 and 7.1-7.4
128 ibid para 6.9
129 Dickinson in Fox and Green (n 130) para 5.110

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.[130]

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.[131] 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.

3. 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.[132] The scale of such criminal activity is difficult to quantify but it is clearly significant and could run into tens of billions of dollars.[133]

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)[134], 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'".[135] The problem is compounded by the increasing use of devices such as tumblers, mixers and private coins to enhance the anonymity of cryptoasset transactions.[136]

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 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.

130 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.

131 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

132 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. An October 2020 advisory issued by the US Treasury's Financial Crimes Enforcement Network (FinCEN) warned of the increasing severity and sophistication of ransomware attacks <FinCEN Advisory, FIN-2020-A006> Accessed October 2021.

133 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 2021 Crypto Crime Report by Chainalysis estimated the value of illicit cryptocurrency transactions during 2020 exceeded US$ 5 billion. Although this was less than the preceding year, the value of ransomware activity was estimated to have increased over 300%.

134 ibid

135 ibid, executive summary at p. 9; and para 4.1.1.

136 Tumblers and mixers combine unrelated transactions together, making it more difficult for a third party to trace particular cryptoassets. FinCEN's October 2020 Advisory (see footnote [193] above) drew attention to the increasing prevalence of ransomware attacks demanding payments in Anonymity-Enhanced Cryptocurrencies, such as Monero.

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."[137] 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.[138]

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".[139] 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".[140] The adoption by the FATF in June 2019 of Guidance which brings virtual assets and virtual asset service (VASPs) providers within the ambit of the FATF's Recommendations (with which FATF member countries are required to comply) is an encouraging step forward.[141] However, in its Second 12-Month Review of the Guidance, the FATF warned that there was not yet sufficient implementation of the Guidance to enable a global AML regime for virtual assets and VASPs; the lack of regulation or enforcement of regulation in some jurisdictions was "allowing for jurisdictional arbitrage and the raising of [money laundering / terrorist financing] risks".[142]

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:[143]

— 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.

137 EU Report (n 144) para 4.1.6
138 Dean Armstrong, Dan Hyde and Sam Thomas, Blockchain and Cryptocurrency: International Legal and Regulatory Challenges (Bloomsbury Professional, 2019) paras 3.20-3.22
139 EU Report (n 144) para 4.1.2
140 HM Treasury, Transposition of the Fifth Money Laundering Directive: response to the consultation (January 2020) para 2.23.
141 FATF Guidance (n 8)
142 FATF, Second 12-Month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers, July 2021 <12-Month-Review-Revised-FATF-Standards-Virtual-Assets-VASPS.pdf (fatf-gafi.org)> Accessed October 2021.
143 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.[144] 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.[145] 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 have registered (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.[146]

— 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.[147]

— 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.[148] 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 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.

144 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
145 Regulation 56 of the AML Regulations
146 Regulation 18 of the AML Regulations
147 Regulation 19 of the AML Regulations
148 Regulation 27 of the AML Regulations

— The Cryptoasset Service Provider must in certain circumstances undertake enhanced due diligence measures, including (i) when dealing with high-risk third countries;[149] (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.[150]

— 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.[151]

— 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.[152]

— 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).[153] 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;[154]

— 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.[155] The UK's approach achieves clarity and avoids the risk of tokens being created in such a way as to evade the regulations.

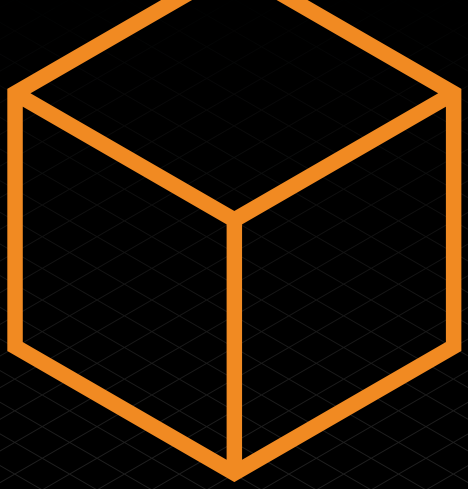
The main gap in the rules remains that identified above, namely whether it suffices only to regulate exchanges and custodian wallet providers. This omits, among other participants, miners and those using peer-to-peer exchanges. The EU Policy Department described both omissions as 'blind spots' in the fight against money laundering and terrorist financing.[156] 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.

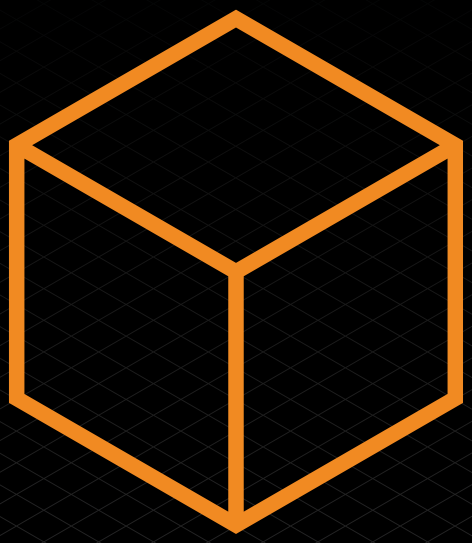
It is also important that whatever their scope, the rules are enforced. However, the pace of registration of Cryptoasset Service Providers by the FCA has been slow. As at 31 August 2021, only nine firms had been registered, with over 70 further firms awaiting registration. By then, an even larger number of firms had been identified by the FCA to be operating in the crypto space without the necessary registration or any pending application for registration, which clearly gives rise to real risks for those dealing with such firms.[157]

149 These include (among other countries) Iran, Libya, the Bahamas and the US Virgin Islands.
150 Regulations 33 and 35 of the AML Regulations
151 Regulation 40 of the AML Regulations
152 Regulation 31 of the AML Regulations
153 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)
154 EU Report (n 144) para 5.3.4
155 Fifth AML Directive (n 163) Art. 1(2)(d)
156 EU Report (n 144) paras 5.3.3 and 5.3.5
157 As the FCA has recognised: <FCA Warns 111 Crypto Firms Are Operating Illegally in UK — Says 'This Is a Very Real Risk' – Regulation Bitcoin News - CryptoMarketRecourse> Accessed October 2021

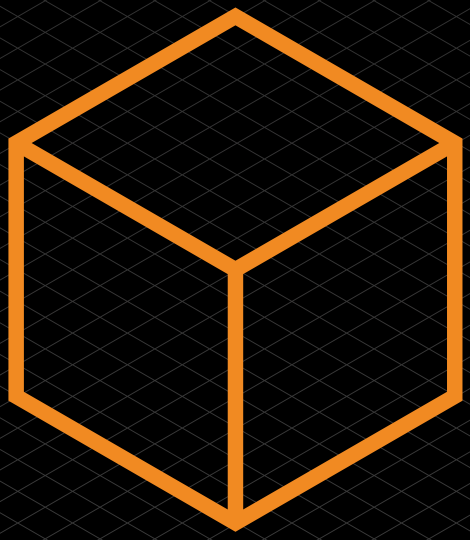
Part 2: Impacts on the Wider Landscape

Section 12 Competition





12



Section 12: Competition

Brendan McGurk, Will Perry and Antonia Fitzpatrick (Monckton Chambers)

Introduction

The principal purposes of competition law include enhancing consumer welfare (including through promoting innovation and price competition) and maximising productive and allocative efficiency by ensuring that competition takes place 'on the merits', requiring suppliers of goods and services to compete against each other on a level playing field and subject to rules and principles protecting the process of competition.[158]

Blockchain not only enables those seeking to transact business to do so without the traditional constraints of space (where one might need to transact in person) or time (where trading might be confined to office hours); it offers a way of transacting business digitally that is distinct from existing forms of online trading. The characteristics of a blockchain database offer many advantages over existing forms of digital trading: it provides a permanent, accurate record of transactions, that does not require the involvement of a 'middle-man' which, in the age of big tech often means two-sided platforms. Blockchain enables digital platforms to be run not centrally (as they are by the biggest tech companies like Amazon, Google and Facebook) but on a completely decentralised basis by all of those who participate in the particular chain. However, as discussed below, the technology is equally capable of facilitating concentrations of power and being used in a highly centralised fashion.

The potential competitive benefits that adoption of blockchain may bring are therefore apparent: if platforms can be operated by their participants on a decentralised basis, it is conceivable that users of those platforms may retain greater control of the content they produce on those platforms and thus the value of that content which might otherwise have been acquired by a powerful gatekeeper. One can see this, for example, in relation to blockchain's use for content distribution: the traditional model of content distribution tends to favour distributors over creators; blockchain technology may, by disrupting centralised platforms, eventually level the playing field.

As an example, YouTube provides a centralised platform enabling users to upload their content to the platform, albeit that YouTube will, as consideration for providing those hosting services, profit from that content. While many YouTubers make a healthy return, a very substantial proportion of revenues generated from their content ends up in YouTube's pockets. Blockchain offers an alternative to this model. For example, Flixxo, a decentralized content distribution platform, allows creators to offer their content to very specialized audiences, who pay cryptocurrency tokens to fund and enjoy their projects. To earn Flixxo tokens, participants in Flixxo simply make the videos on their computer available to the network on a peer-to-peer basis. Users in this decentralised model bear more of the running costs of the platform, but in turn retain more of the profits of the content they produce, not least since viewers will forego paying subscriptions to centralised platforms and can instead pay content providers directly.

Blockchain also gives online users more control over their data in relation to advertisers who would otherwise target them based on their knowledge of those users' browsing habits and preferences. Blockchain enables users to operate anonymously (or at least, pseudonymously), making it harder for those users to be identified and targeted by advertisers. New companies like Papyrus operate platforms that enable users to know exactly who is paying to advertise to them, and the source of the data about them on which those advertisers rely. Individuals can expressly identify their data-sharing preferences so that advertisers will know with certainty what type of adverts they wish to receive rather than seeking to profile

158 Of course some competition theorists, such as Robert Bork and the Chicago School, would contend that "antitrust laws, as they now stand, have only one legitimate goal, and that goal can be derived as rigorously as any theorem in economics … [- namely,] the maximisation of consumer welfare." The Antitrust Paradox (The Free Press, 1978 reprinted 1993), pp 50-51

individual users by parsing web-browsing and other online data which may be less accurate. These users can also decide not to share any of their browsing habits or other usage data, though in those circumstances, advertisers can offer to pay users directly for that data.

Blockchain is therefore capable of aggregating and distributing all of the online data that users create across the entire network, making it accessible to all potential advertisers on a level playing field for the acquisition of that data, thus enabling users to retain more of the value of the data trail they create, and promoting greater competition amongst those advertisers. This is in contrast to the situation were data acquired (through user agreement to company terms and conditions) is kept on secure company servers and put up for sale to bidders who wish to target those users, and where the revenues for that data is retained by selling companies, rather than users whose data is being sold. This promotes consumer welfare in giving users greater control over their data and privacy, ensuring that adverts are more accurately targeted and allowing users to monetise the value of that data, rather than advertisers paying Google or Facebook for the same. As Fred Ehrsam puts it:

> *"While some blockchain-based data will be encrypted and private, much of it will also be open out of necessity…this open data has the potential to commoditize the data silos most tech companies like Google, Facebook, Uber, LinkedIn and Amazon are built on and extract rent from. This is great for society: it incentivises the creation of a more open and connected world. And it creates an open data layer for AIs to train on."*[159]

Blockchain coupled with the use of smart contracts[160] will also promote competition in the context of property transactions, where blockchain platforms now allow real estate to be tokenized and traded like cryptocurrencies. Traditionally, properties for sale or lease have been listed through estate agents – again operating as a centralised platform on the supply side. As Deloitte have pointed out, new decentralised platforms may eventually assume the listing, payment and legal functions traditionally provided by intermediaries, thereby removing the middle-man, cutting transaction costs and increasing the speed at which such transactions might take place.[161] Tokenising assets like a house will facilitate joint ownership and will enable greater fluidity in buying and selling shares in individual properties. All of this will promote consumer welfare.

The distinction between permissioned and permissionless blockchains

Blockchains can be public/permissionless or private/permissioned. The distinction between these two general types has consequences for an analysis of how blockchains are capable of being instrumentalised to harm competition. Anybody can use public/permissionless blockchains, and users are anonymous. Private/permissioned blockchains, in contrast, are operated by a single entity or group of entities who control all aspects of the operation of the chain, and have developed protocols to govern their actions. Those features have the corollary that "[p]rivate blockchains have the potential to lead to entrenchment of power within a blockchain system, as a select group of people can effectively act as gatekeepers because of the restricted access to digital keys".[162] In this section, we therefore focus principally on uses of private/permissioned blockchains.[163]

159 Fred Ehrsam, Blockchains are a data buffet for Ais, Medium (6 March 2017)

160 A smart contract is a piece of computer code capable of verifying, executing and enforcing a set of instructions constituting an agreement between two parties. Smart contracts operate under a set of pre-conditions which, when satisfied, lead to the discharge of the obligations in the contract that were contingent on the satisfaction of those conditions. In the property context, a landlord might agree to give the tenant the door code to the rental property as soon as the tenant pays the security deposit. Both the tenant and the landlord would send their respective portions of the deal to the smart contract, which would hold onto and automatically exchange the door code for the security deposit on the date the lease begins.

161 https://www2.deloitte.com/us/en/pages/financial-services/articles/blockchain-in-commercial-real-estate.html

162 Alex Latham, 'Blockchain and Competition Law' (2020) 41 E.C.L.R, p 602, <https://www.bristows.com/app/uploads/2021/01/2020.12-ECLR-Blockchain-and-competition-law.pdf>

163 For a more complete taxonomy of blockchains see (which considers public/permissioned and private/permissionless types), see EY's "Discussion Paper on Blockchain Technology and Competition" of April 2021, p 11 < https://www.cci.gov.in/sites/default/files/whats_newdocument/Blockchain.pdf> For a discussion of the potential interaction between collusive agreements and public blockchains, see Thibault Schrepel, "Collusion by Blockchain and Smart Contracts", Harvard Journal of Law and Technology (2019), pp 128-133 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3315182>

Competition law concerns

All that follows should be read subject to the fact that there is nothing inherently anticompetitive about the uses of blockchain. However, for all the potential benefits to consumers, there are also a large number of competition law concerns. We have addressed those concerns as follows. First, we address potential harms to competition falling within the scope of Article 101 TFEU / the Chapter I Prohibition under the Competition Act 1998. Second, we consider potential harms falling under Article 102 TFEU / the Chapter II Prohibition under the Competition Act. Third and finally, we reflect on potential enforcement problems.

The three overarching conclusions that emerge from this analysis are:

— Competition concerns arising out of uses of blockchain can be effectively analysed under the existing analytical framework for competition harms. As is apparent below, possible anti-competitive conduct falls into existing categories of infringements. In this regard, we agree with Thibault Schrepel, the leading commentator on the competition law implications of blockchain, that the applicable theories of harm "are entirely standard concerns that competition agencies already investigate in all manner of different market settings involving other types of technology". [164]

— The types of competition law harms that will arise in this context are likely to depend on two main factors: (a) the extent of transparency / data sharing within the blockchain and (b) the extent to which power is concentrated in the hands of the blockchain owner(s). Although the underlying technology may be the same, there is no one-size-fits all approach to evaluating anticompetitive conduct involving blockchain.

— Perhaps the greatest challenge blockchains present for competition lawyers and regulators is enforcement. As with the likely competition law harms, enforcement challenges will depend on the blockchain's degree of transparency and concentration of power.

The domestic Courts have not yet had to grapple with the questions raised in this chapter and in particular whether the types of conduct considered constitute abuse of dominance. The analysis in this chapter is, for that reason, necessarily conceptual and, based on first principles. As cases start to be considered by the Courts and regulators, the issues raised in this chapter will, in due course, provide a basis on which to refine the analysis.

1. Potential competition harms within the scope of Article 101 TFEU / Chapter I Prohibition

Article 101 TFEU and the Chapter I Prohibition in UK competition law (s.2 of the Competition Act 1998) prohibit "agreements between undertakings, decisions by associations of undertakings or concerted practices" which "have as their object or effect the prevention, restriction or distortion of competition" within the internal market (Article 101) or which may affect trade within the United Kingdom (the Chapter I Prohibition).

Consortia and access

Permissioned blockchains are often consortium platforms. By way of indication as to the prevalence of blockchain consortia, in August 2017 more than 40 had been set up globally, including, for example, PTDL (Post-Trade Distributed Ledger Group), B3i (Blockchain Insurance Industry Initiative) and the R3 Consortium, which developed the Corda distributed ledger platform to facilitate synchronised peer-to-peer contract execution.[165]

164 https://www.oecd.org/daf/competition/antitrust-and-the-trust-machine-2020.pdf

165 For more detail see Renato Nazzini, "The Blockchain (R)evolution and the Role of Antitrust", King's College London Dickson Poon School of Law Legal Studies Research Paper Series (2019-2020), p 2-3, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3256728>

Access to private/permissioned blockchains or consortia depends on the authorisation granted by the owner or owners of the chain. Potential competition law infringements arising from refusal to grant access are also considered in our discussion of potential Article 102/Chapter II Prohibition infringements below. From the perspective of Article 101/the Chapter I Prohibition, if competitors within a market use a single blockchain, then there are inherent features of that chain that may cause concern. Those features are, in the broadest terms: (i) data transparency between competitors; (ii) co-operation between competitors; and (iii) the presence of mechanisms that can control transactions/competitor behaviour (in particular, smart contracts). Those three features and combinations thereof are discussed in the following paragraphs in the course of the discussion as to how blockchain has the potential to cause Article 101/Chapter I Prohibition harms.

Information exchange: horizontal and vertical

If competitors are able, through their membership of a consortium, to access information about the price at which they are entering into transactions and/or the level of rebates or discounts they are offering customers, that will reduce price competition and constitute a form of information sharing that violates competition law. If pricing of products begins to coalesce as a result of such information sharing, that would be clear evidence of coordination or collusion in breach of, in particular, the Chapter I prohibition. Similar risks arise if competitors each have access to each other's customer lists, costs, volumes of sales, etc, as this would also likely constitute unlawful information exchange. As ever, the exchange of information that relates to competitors planned future conduct on the market in question carries the greatest risk of violating competition law. Participants in a chain on which competitors operate will therefore have to consider the governance rules and software protocol, and the extent to which they permit rivals to obtain access to that very type of information. It may be sufficient, at least in some cases, to encrypt such information.

It is crucial also to consider that where vertically-related parties are members of the same blockchain, data transparency (and/or use of smart contracts) may facilitate anti-competitive regulation by upstream entities of their downstream buyers through, for example, resale price maintenance (i.e. preventing distributors from discounting their price, which eliminates intra-brand competition) and selective distribution agreements (i.e. which stipulate that sales may be made only through certain channels).

To date there have been only a few competition cases on internet selling, but when presented with the opportunity the CJEU and the UK Court of Appeal have not held back from analysing online sales and distribution agreements through the lens of Article 101 TFEU. In Ping Europe Ltd v CMA [2020] 4 CMLR 13, the Court of Appeal noted[166] that EU law considers website sales to be a form of "passive selling" (i.e. sales in response to unsolicited orders), and classifies agreed restrictions on such selling (e.g. through selective distribution) as "hardcore" restrictions on sales to end purchasers, which in turn are considered to be equivalently anti-competitive to "object" restrictions on competition under Article 101 TFEU/the Chapter I Prohibition. In Case C-230/16 Coty Germany GmbH v Parfümerie Akzente GmbH [2018] 4 CMLR 9, the CJEU held that there was no object restriction where a distribution agreement for luxury cosmetics confined online sales to websites which highlighted the luxury character of the brand, and prohibited sales via third-party sites, but only on the basis that this restriction of competition could be justified as proportionate to preserve the luxury image of the goods.[167]

As for the concern that arises from vertical information sharing on blockchains specifically, the solution may lie in the formal demarcation of sub-groups of users of the blockchain (e.g. as buyers and sellers) and separation of their activities, to restrict the sharing of sensitive activity information that could otherwise give rise to competition concerns.[168]

166 See: Ping Europe Ltd v CMA [2020] EWCA Civ 13; [2020] 4 CMLR 13, ¶¶26-29, 39.
167 See: Case C-230/16 Coty Germany GmbH v Parfümerie Akzente GmbH [2018] 4 CMLR 9, ¶36.
168 Alex Latham, 'Blockchain and Competition Law', p. 606.

Research and development, and standardisation agreements

Many if not most existing blockchain consortia exist to facilitate R&D agreements (to develop new technologies or improve existing ones) and/or standardisation agreements (agreements on common technical standards to ensure inter-operability).[169]

Many R&D agreements do not restrict competition at all. EU law recognises that such agreements can be problematic from a competition law perspective only if the combined market shares of the parties exceeds 25% on any relevant product and/or technology market (below that threshold, R&D agreements fall under the R&D Block Exemption Regulation, provided that other conditions for the application of that Regulation are fulfilled).[170] Where that threshold is exceeded, competition concerns can arise where the parties have market power on the relevant markets and/or where competition with respect to innovation is appreciably reduced.[171] If the parties to the agreement could independently have developed competing technologies that could be used for a particular purpose then the R&D agreement may restrict competition. When considering the competition implications of blockchain R&D, however, as Renato Nazzini has observed, there is a need to move beyond a classic structuralist assessment based on market share to consider competition between different blockchain applications and technologies, disruptive innovation, and the role of network effects in delivering efficiencies.[172]

Although the existence of common standards, facilitated by standardisation agreements, will generally be pro-competitive because they facilitate the compatibility of products and services, competition law recognises that Standardisation Agreements can restrict competition if: (i) standardisation between competitors has the corollary of eliminating price competition; (ii) the adoption of a single standard limits innovation and/or erects barriers to entry to the market for competitors; and/or (iii) the agreement prevents certain players from gaining access to the results of the standard-setting process. The respective solutions to those concerns in respect of blockchains are: (i) as indicated above in relation to horizontal information exchange more broadly, the adoption of strict protocols to ensure that no sensitive pricing information, or other sensitive commercial information relating to the intended use of the relevant application/technology; (ii) permitting parties to use alternative, competing technologies and/or ensuring interoperability; and (iii) providing access on FRAND (fair, reasonable and non-discriminatory) terms.[173]

Blockchain consortia are themselves a form of standardisation agreement (blockchains, as shared ledgers, could not operate without common technical standards and protocols as between their users)[174] and it will also be important to consider the basis on which participants are involved in setting or amending governance rules. If only some participants have access, some competing parties may have access while others do not, with the risk that governance standards are set in a way that favours those who benefit from such access over those who do not. The procedure for setting the consortium's governance rules and any applicable standards by which its blockchain operates will have to be transparent and based on FRAND terms.

Collusion through or by the blockchain, and the use of smart contracts

Since co-operation and transparency/data visibility are inherent characteristics of blockchains, there are multiple forms of anti-competitive co-ordination and collusion between competitors that may be made easier by blockchain technology, some of which have already been considered. Other obvious examples of collusion that may be facilitated by blockchains are: (i) the setting up of a cartel; (ii) the more effective monitoring of deviation from a cartel agreement (price fixing, customer or market

169 Renato Nazzini, "The Blockchain (R)evolution and the Role of Antitrust", p. 3.
170 Commission Regulation (EU) No 1217/2010 (14 December 2010), Article 4(2).
171 Guidelines on the applicability of Article 101 of the Treaty on the Functioning of the European Union to horizontal cooperation agreements (2011/C 11/10), para 133
172 Renato Nazzini, "The Blockchain (R)evolution and the Role of Antitrust", p 4
173 Renato Nazzini, "The Blockchain (R)evolution and the Role of Antitrust", p 5
174 Renato Nazzini, "The Blockchain (R)evolution and the Role of Antitrust", p 5

allocation, or bid rigging), due to the real-time recording of transactions; and (iii) collusion by the entity or consortium operating the blockchain in the division of markets or price fixing.

The use of new technology to automate the monitoring and enforcement of a cartel is far from unprecedented: in its decision in Online sales of posters and frames, the CMA found that Trod Limited and GB eye Limited, both online suppliers of posters, had agreed that they would not undercut one another's prices for posters and frames sold via Amazon's UK website. The cartel was implemented through price-monitoring software (algorithms), which the parties configured to give effect to it.[175]

Smart contracts are programmable codes which facilitate, verify, and self-enforce the performance of agreements, through an "if X then Y" logic. They can be used in a way that is analogous to the way in which the colluders in Online sales of posters and frames used algorithms.[176] Schrepel has analysed the ways in which smart contracts may be used to create and maintain discipline and stability within collusive agreements (which discipline and stability, by definition, cannot be provided by the law) under the headings of the "visibility effect" and the "opacity effect". The "visibility effect", which applies to colluders themselves, describes colluders' enhanced ability to monitor and/or police one another's behaviour that is provided by the chain/smart contract, by which governance of the agreement, and in particular the identification of deviant behaviour, is automated. The visibility effect strengthens the cohesion of the anti-competitive agreement. The "opacity effect", which applies to non-colluders, describes the enhanced secrecy that the chain provides with respect to the information on the chain from the perspective of outsiders, in particular relevant regulators and enforcement agencies, protecting colluders from detection.[177]

The first blockchain competition case

What is widely recognised as the first blockchain competition/antitrust case, United American Corporation v Bitmain Incorporated and others (Case No. 1.18-cv-25106), first came before the Court of the Southern District of Florida in December 2018. In March 2021, the Court granted the Defendants' motion to dismiss the Plaintiff's First Amended Complaint (with prejudice) under Federal Rule of Civil Procedure 12(b)(6), on the basis that the Plaintiff had failed to state a claim on which relief could be granted under §1 of the Sherman Act, which (comparably to Article 101 TFEU) provides that: "Every contract, combination in the form of trust or otherwise, or conspiracy, in restraint of trade or commerce among the several States, or with foreign nations, is declared to be illegal." With the claim having been dismissed at such an early stage, it is difficult to draw many general conclusions as regards how courts will deal will allegations of collusion in a blockchain context and/or undertake enforcement action against colluders in the future. However, the following brief comments can be made.

The facts and allegations in the Bitmain case centred upon a 'hard fork' in the Bitcoin Cash blockchain that took place in November 2018. Bitcoin Cash is a public/permissionless blockchain originally derived from Bitcoin Core, the first Bitcoin cryptocurrency. 'Forks' are periodic updates to blockchains. Whereas 'soft' forks enable users who elect not to go through the relevant update to continue to communicate on the same network (because the existing software is compatible with the updated version). In a hard fork, users must update in order to continue to participate: after a hard fork, the old rules will be incompatible with the new rules.[178] Different proposals for updates relating to the same chain may compete with one another, i.e. in a "hash war", where the mining servers[179] participating in a blockchain

175 CMA Decision in Case 50233, Online sales of posters and frames (12 August 2016), <https://assets.publishing.service.gov.uk/media/57ee7c2740f0b606dc000018/case-50223-final-non-confidential-infringement-decision.pdf>
176 See in particular: Thibault Schrepel, "Collusion by Blockchain and Smart Contracts", pp 117-166
177 Thibault Schrepel, "Collusion by Blockchain and Smart Contracts", pp. 143-151
178 United American Corporation v Bitmain (Case No. 1.18-cv-25106), §I.B.2. The judgment is available at <https://www.courtlistener.com/docket/8382061/united-american-corp-v-bitmain-inc/>
179 Mining" refers to the process by which "Consumers – that is, individuals or individuals that operate servers – compete to "mine" virtual currencies by using computer power that solves complex math puzzles. The computer servers that first solve the puzzles are rewarded with new cryptocurrency, and the solutions to those puzzles are used to encrypt and secure the currency" United American Corporation v Bitmain, §I.B.1

network "vote" on which set of rules or protocol they prefer, and "the rules set mined with the most computer hashing power would prevail and continue the … blockchain going forward.[180] The November 2018 update to the Bitcoin Cash chain concerned two competing proposals, the "Bitcoin ABC" protocol and the "Bitcoin SV" protocol.

The Plaintiffs, United American Corporation ("UAC"), backed Bitcoin SV in the hash war, and lost to the Defendants, who all backed Bitcoin ABC. UAC's complaint was not that the hard fork was per se anticompetitive. Rather, UAC alleged that all of the Defendants (whom the Honorable Kathleen M. Williams in her judgment grouped into the Mining Defendants, the Exchange Defendants and the Developer Defendants) colluded in a two-part scheme: (i) first, to determine that Bitcoin ABC was the winning protocol in the hash war by increasing their mining capacity in the short term as a way of influencing the "vote"; and (ii) second, to secure the benefits of their win by implementing a "checkpoint" on the resulting Bitcoin Cash ABC blockchain, which allowed anyone with 51% hashing power (based on mining power) to cement centralised control of the chain by ensuring that they would prevail in any future disputes regarding the consensus rules on the chain. UAC pleaded losses in the form of losses to the value of Bitcoin SV and a decrease in the value of both currencies created by the fork. Those allegations were pleaded under §1 of the Sherman Act as both a per se violation (analogous to an "object" infringement of Article 101 TFEU) and a "rule of reason" violation (analogous to an "effects" infringement of Article 101 TFEU).[181]

The Defendants succeeded on their motion to dismiss due to a "multitude of pleading deficiencies" on the Plaintiff's part, among which three stand out for comment.[182]

First, the judge found that UAC had failed to plead conspiracy, which is the first essential element in a §1 Sherman Act claim. In particular, the judge found no express allegation in UAC's pleading that all of the Defendants had entered into an agreement (whether horizontal, vertical, or "hub-and-spoke") to undertake the impugned conduct. As the judge observed, the allegation regarding the relocation of hashing power prior to the fork would in any event have related only to the Mining Defendants, and not to the Developer or Exchange Defendants. Even then the pleaded allegations were not strong enough to suggest an agreement as opposed to independent action. As regards the "checkpoint" implemented by the Developer Defendants, UAC did not allege that those Defendants implemented it by agreement with any of the other Defendants.[183] Moreover the judge was unconvinced that the "checkpoint" was, as UAC alleged, implementing with the purpose of centralising cementing control of the ledger for anyone with adequate hashing power: "It may be equally plausible that checkpoints serve another purpose, instead of centralising a cryptocurrency market, such as providing security for the blockchain or as an efficiency measure."[184]

Second, UAC failed adequately to plead that the "Bitcoin Cash market" was a distinct relevant product market for the purpose of a rule of reason analysis (the judge accepted that the relevant geographic market was global). At its highest, UAC's case was that Bitcoin Cash was "'unique' because of its utility for peer-to-peer daily transactions" and was "the most widely adopted form of cash-like cryptocurrency".[185] However the judge noted that that plea merely "leaves us hanging": she had been told nothing that would allow her to discern the extent to which consumers preferred Bitcoin over other cryptocurrencies, or why Bitcoin Cash would be a market of its own as opposed to being in the same market as similar cryptocurrencies primarily used for transactions. Further, UAC had made no factual assertions which were capable plausibly of demonstrating whether or not there

180 United American Corporation v Bitmain, §I.B.5. "Hashing power" refers to the computing power that is used to solve the relevant puzzles, see: United American Corporation v Bitmain, §I.B.1 and §I.B.5
181 The judgment is available here: https://www.courtlistener.com/docket/8382061/united-american-corp-v-bitmain-inc/
182 United American Corporation v Bitmain, §II.B.
183 United American Corporation v Bitmain, §II.B.2, and subsections.
184 United American Corporation v Bitmain, §II.B.2.d.(3)
185 United American Corporation v Bitmain, §II.B.3.a.(2).

was cross-elasticity of demand (i.e. a measure of demand-side substitutability that suggests that two products are part of the same market) between the market for Bitcoin Cash and the market for Bitcoin Core or other cryptocurrencies.[186]

Third, UAC was unable adequately to plead that there had been actual or potential harm to competition as a result of the alleged conduct. UAC alleged that the "quality" of the Bitcoin Cash market had been harmed by the introduction of the checkpoint (the core allegation was that for the blockchain to remain "secure and trusted" its processes needed to remain "distributed and decentralised"), but: (i) there was no allegation that any change in price, output, or any other particular change had harmed competition; (ii) no facts were pleaded to explain how and why competing developers would be unable to propose innovations to improve upon software protocols used to mine Bitcoin Cash; and (iii) in any event the allegation of harm to the "quality" of the market through the introduction of the "checkpoint" rested on the allegation of agreement between all of the Defendants (particularly the Miners and Developers) which could not be made out.[187]

Due to the foregoing and other fatal shortcomings in its pleading, UAC could not make out its case on a rule of reason violation. The judge found that UAC had also failed to plead a per se violation: the alleged conduct could not be categorised (as was pleaded) either as something "in the nature of bid rigging" (because not all of the Defendants were competitors and there was no agreement between competitors to co-ordinate bids/prices to a third party) or as a "group boycott" (again because not all of the Defendants were competitors, so there could be no agreement among competitors to withhold services from a third party).[188]

In all, what is immediately striking about the judgment in the Bitmain case is that there is nothing exceptional about the way in which the judge disposed of it. Simply, she considered pleaded facts in the light of an existing legal framework and found that those facts did not give rise to a cause of action. Furthermore, and crucially, UAC's claim was dismissed not because the existing legal framework was inadequate to test complex facts relating to competition on blockchain networks but because there was no properly pleaded case on the fundamentals of conspiracy/agreement, the relevant market, and harm to competition. Shortcomings of that kind can apply in any competition case involving allegations of covert unlawful agreements: in that regard, there is nothing special about blockchain.

The most significant feature of the Bitmain case might be that following the judge's request that the parties give her a "tutorial" on the core concepts at stake in the complaint, the lawyers on both sides "strived to make… a neutral presentation to the court".[189] It may be that UK courts can use the existing provisions of the CPR on concurrent expert evidence (PD35 paras 11.1-11.4) to similar effect in future competition/blockchain cases.

"Cartel management for groups that don't trust each other"?

In 2015, a Financial Times journalist observed with regard to blockchains that "what the technology really facilitates is cartel management for groups that don't trust each other".[190] Although blockchain technology may facilitate cartel management, and other anti-competitive harms falling within the scope of Article 101/the Chapter I Prohibition, that is not necessarily so. Renato Nazzini has underlined the point forcibly: "Blockchains… could be an electronic means of setting up a cartel. If this were the case, it would not be the blockchain itself or its operation or application [that was unlawful], but the use that the parties make of it to give effect to their unlawful agreement."[191] As regards uses of blockchains that do not amount to cartels or infringements of Article 101/the Chapter I Prohibition by object, Nazzini

186 United American Corporation v Bitmain, §II.B.3.a.(2).
187 United American Corporation v Bitmain, §II.B.3.b.
188 United American Corporation v Bitmain, §II.B.4.a-b.
189 Transcript of discussion <https://www.jonesday.com/en/insights/2021/06/jones-day-talks-takeaways-from-a-landmark-cryptocurrency-antitrust-case>
190 Izabella Kaminska, 'Exposing the "If we call it a blockchain perhaps it won't be deemed a cartel" tactic, Financial Times (11 May 2015), < https://www.ft.com/content/bb7f42ec-a049-3739-b74d-131e9357694c>
191 Renato Nazzini, "The Blockchain (R)evolution and the Role of Antitrust", p 8

has further advocated in favour of a robust effects analysis : “It will be essential to balance any potential anti-competitive effects against the benefits of the technology and the need that information is to [be] shared for such benefits to accrue. There can be no blockchain without a degree of transparency. The question is how much transparency is required for the blockchain application under review to work, and how much information can, instead, be securely blacked out. And all will be a matter of degree.”[192]

2. Potential harms within Article 102 / Chapter II

Article 102 TFEU and the Chapter I Prohibition in UK competition law (s.18 of the Competition Act 1998) prohibit abuse of a dominant position. The scope for abuse of dominance or collective dominance (i.e. by blockchain consortia)[193] in the blockchain context is at present limited. There are only two obviously dominant undertakings in this space: Bitcoin and Ethereum. Though, as these platforms rely on public/permissionless blockchains, the likelihood of unilateral abuse is insignificant for the reasons discussed above.

However, that is not to say that conduct in breach of Article 102 TFEU / Chapter II CA 1998 is unlikely to occur in future. In the same way that tech giants saw remarkable growth in their market power alongside the rise of the internet via “network effects”, the same may well be true for blockchain-based services. To this effect, the OECD has commented how “in cases where blockchain-based business models successfully disrupt non-blockchain models, the cross-platform network effects might be expected to give one blockchain a degree of market power”; and that “we might expect that there would be particularly strong network effects in the increasing number of ‘industry’ blockchains that are being formed by consortia of upstream and downstream firms that serve a certain market (see for instance those in shipping or diamonds) or that serve a broader set of markets (for example in the case of Libra)”.[194]

Another key concept here is that of “single source” information or data – i.e. that permissioned blockchain owners are likely over time to build up unique historic datasets on the chain which only they have access to – such as transaction data or medical records history. The richer the historic datasets, the harder it will be for newer rivals to compete. This dynamic increases the likelihood that blockchain-based markets become “winner takes all” markets.

Finally, it is important to note that undertakings may establish dominance in the blockchain space by lawfully or unlawfully leveraging dominance in other markets.[195] For example, in the context of payment activities, the French competition authority has commented that “data collected by Big Tech in the context of their core business activities could give them a significant advantage in the payments industry and, conversely, the data collected via the payment services they offer could allow them to make their respective platforms more attractive”.

Once undertakings begin to establish dominant positions, there is likely to be ample opportunity for permissioned blockchain owners to engage in uncompetitive conduct. As the founder of Etherum has considered: “The consortium or company running a private blockchain can easily, if desired, change the rules of a blockchain, revert transactions, modify balances, etc.”[196] Whilst it all possible manifestations of abuse of dominance in the blockchain context cannot be predicted, the most likely can be grouped as follows: i. abuse that is designed to increase market share of a dominant blockchain owner; ii. refusing or limiting access to a blockchain with the effect of market foreclosure; iii. predatory innovation; and (iv) exploitative abuse.

192 Renato Nazzini, “The Blockchain (R)evolution and the Role of Antitrust”, pp 8-9, insertion added
193 The Chapter II Prohibition and Article 102 both refer to abuse “by one or more undertakings”
194 Pike and Capobianco, ‘Antitrust and the trust machine’ (2000), p 8 <http://www.oecd.org/daf/competition/antitrust-and-the-trust-machine-2020.pdf>
195 See Opinion 21-A-05 of 29 April 2021 on the sector of new technologies applied to payment activities, p5 <https://www.autoritedelaconcurrence.fr/sites/default/files/attachments/2021-06/21-a-05_en.pdf>
196 Buterin, On Public and Private Blockchains, Ethereum Fondation Blog (2015); available at <https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains>

i. Abuse intended to increase market share

In 'winner takes all' markets, characterised by network effects and single source information, there may be significant commercial incentives to engage in abuse that directly increases customer numbers. There are two clear types of abuse that could be implemented with this in mind: abuses on the market on which the blockchain services are offered (so-called "own market abuses"), and abuses on related markets that entrench dominance in the blockchain market.

The classic example of an own-market abuse is predatory pricing. This is where an undertaking charges prices at levels that have no economic purpose other than to eliminate or weaken competition. In the blockchain context, the most obvious form of predatory pricing is where a blockchain owner reduces transaction fees to artificially low levels in order to foreclose the market. Whether or not prices are "predatory" is fact-specific. Though applying the predatory pricing doctrine in digital markets comes with various conceptual challenges.[197] For example, Lina Khan has argued that "[t]he fact that Amazon has been willing to forego profits for growth undercuts a central premise of contemporary predatory pricing doctrine, which assumes that predation is irrational precisely because firms prioritize profits over growth".[198] It may therefore be challenging to distinguish the dividing line between conduct which builds up a customer base (i.e. "loss leading") and conduct which eliminates rivals. That challenge is particularly pronounced where predation in one market can be cross subsidised by a firm's dominance in related markets.

Another type of own-market abuse is the imposition of exclusive purchasing agreements, where dominant blockchain owners provide services on condition that customers abandon any rival products it may be using.[199] Relatedly, the blockchain owner might also give loyalty rebates: for example, blockchain owners looking to foreclose a financial transactions market might grant significant rebates to important financial services customers. The incentive to ensure exclusivity may be particularly pronounced if the customer has an ability to "port" historic data stored on the blockchain to other chains. Both exclusivity purchasing agreements and loyalty rebates may be objectively justified. Though, as with the predatory abuses considered above, particular evaluative challenges are posed in digital markets.

The second type of abuse designed to attract customers is where a dominant undertaking leverages dominance in other, related markets to foreclose the market on which the blockchain operates. Although some of the abuses considered above may also apply, the most obvious "leveraging" abuses in the blockchain context are tying and bundling. This is where the dominant undertaking requires customers using a "tying product" in a different market to acquire a "tied product" (i.e. the blockchain-based product). For example, a dominant retail business might require companies it buys products from, or sells products on behalf of, to use its own blockchain-based platform for completing the transaction and tracking delivery. Whilst a dominant digital wallet application provider might ensure its application is only compatible with one type of blockchain-based payment option. Such practices may be capable of objective justification. Though, as above, it may be challenging to distinguish between conduct that seeks to eliminate competition and conduct that generates network effects that are beneficial for consumers.

ii. Refusing or limiting access

Once a blockchain owner becomes dominant in a given market, there is clear scope for abuse in either refusing to deal or providing access to the chain on unfair or discriminatory terms.[200]

197 See OECD, 'Abuse of dominance in digital markets' (2020), pp.31 et seq.; available at<https://www.oecd.org/daf/competition/abuse-of-dominance-in-digital-markets-2020.pdf. https://www.oecd.org/daf/competition/abuse-of-dominance-in-digital-markets-2020.pdf p 32

198 Khan, 'Amazon's Antitrust Paradox', Yale Law Journal, 126 (2017), p.44; available at <https://ssrn.com/abstract=2911742>

199 Note that Exclusivity may be contractual or de facto

200 On this issue, see Opinion 21-A-05, pp.120 et seq

Refusal to supply constitutes an abuse of dominance where, in essence, an undertaking refuses to supply (or supplies on unacceptable terms – i.e. constructive refusal to supply[201]) without objective justification, products or services which constitute an "essential facility" or "objectively necessary" input. This will be the case where the input cannot be duplicated or can only be duplicated with significant difficulty (i.e. it would not be economically viable) in the foreseeable future. Although this doctrine was initially developed in the context of access to physical infrastructure, it has since been applied to less tangible inputs, such as computerised airline reservations systems,[202] cross border payments systems,[203] and intellectual property rights.[204] The EU Commission's Article 102 Enforcement Priorities state that "an input is likely to be impossible to replicate … where there are strong network effects or when it concerns so-called 'single source' information".[205] As discussed, both factors are likely to arise in relation to blockchain. In this context, essential input arguments are likely to focus on the economic viability of setting up a rival blockchain and attracting a critical mass of customers. This will clearly vary from case to case. However, commentators have pointed out that "there are several features of blockchain that clearly distinguish it from other inputs and services to which the essential facilities doctrine has previously been applied – most notably the fact that the source code underpinning the design of a blockchain is largely publicly available and is readily accessible to competing developers".[206] Where a refusal to supply results in foreclosing of the market, a dominant undertaking may still be able to objectively justify that conduct in the blockchain context. For example, access may be refused to users with inadequate cybersecurity practices which pose a threat to the operation of the blockchain.

Due to the incentive to generate networks effects and single-source information, blockchain owners may generally wish to grant access where possible. Refusal to deal situations may be less common than situations where blockchain owners provide blockchain-based services on terms that are discriminatory or not objectively justified. Even if this falls short of a constructive refusal to supply, it may still fall foul of Article 102 / Chapter II. Both provisions specifically prohibit dominant undertakings from "applying dissimilar conditions to equivalent transactions with other trading parties, thereby placing them at a competitive disadvantage". Though it is important to note that differential conduct is not per se unlawful where it can be objectively justified. For example, when it comes to price discrimination, the courts have recognised that different prices can be applied to different categories of buyer; in particular that newer entrants to the market can be incentivised through lower prices.[207] Another example of differential conduct is the operation of "dual speed blockchains" (as already de facto exist with Bitcoin) – i.e. different transaction speeds depending on how much the user is willing to pay. As a general rule, the more the market share of the blockchain owner increases, the harder it will be to justify differential treatment.

To address access issues, regulators and courts may turn to existing competition law principles from the licensing of Standard Essential Patents (SEPs). Where intellectual property constitutes an essential input, dominant firms are required to license access on terms that are fair, reasonable, and non-discriminatory (FRAND). Those terms are standardised regardless of what a customer is willing to pay and are set with reference to the true value of the SEPs licensed.[208] Courts have been willing to set FRAND prices in appropriate cases.[209] There is no reason in principle

201 For an example of constructive refusal to supply, see Case T-486/11 Orange Polska v Commission
202 See London European-Sabena, OJ [1988] L 317/47
203 Commission Notice on the Application of the Competition Rules to Cross-border Credit Transfers, OJ [1995] C 251/3
204 Discussed below
205 Communication from the Commission, 'Guidance on the Commission's enforcement priorities in applying Article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings', fn.58; available at<https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52009XC0224%2801%29#ntc52-C_2009045EN.01000701-E0052.>
206 Leahy and Davis, 'Innovating for the greater good: how to design a competition law compliant blockchain' (2020); available at <https://technologyquotient.freshfields.com/post/102g0n8/innovating-for-the-greater-good-how-to-design-a-competition-law-compliant-blockc.>
207 See Attheraces v British Horseracing Board [2007] EWCA Civ 38.
208 See Unwired Planet International Ltd v Huawei Technologies Co. Ltd & Anor [2020] UKSC 37, para 114.
209 Most notably, in Unwired Planet v Huawei [2017] EWHC 711 (Pat), where Birss J said at para 169 that "courts all over the world have now set FRAND rates. I am sure the English court can do that as well." This judgment was later affirmed by the Court of Appeal and Supreme Court.

why this approach could not be applied in the blockchain context. Less clear is the extent to which these principles are capable of applying to the licensing of other proprietary information, especially large datasets stored on a blockchain; although there is a growing consensus that such datasets can constitute an essential input in digital markets and may be required to ensure interoperability and competitive tension.[210] To take a practical example, a joint Competition Commission of India and Ernst & Young paper on blockchain and competition considers a hypothetical blockchain application which records regular data from IoT devices installed in cars. The report considers how "[t]his data could be used by insurance providers to determine the car insurance premium based on the risk profiles developed from the historical data. If a new insurance company is denied access to this hypothetical blockchain application, it is possible that it may not be able to compete effectively in the market."[211]

iii. Leveraging dominance in the blockchain-based market

The third category of abuse is what has been described as "predatory innovation". This is an emerging theory of harm which has been primarily considered by Schrepel. He defines this harm as "the alteration of one or more technical elements of a product to limit or eliminate competition".[212] As Schrepel recognises, identifying predatory innovation may be difficult in practice. However, he has commented that "predatory innovation remains one of the most anticipated and dangerous anticompetitive strategies that can be implemented on private blockchain". The basis for Schrepel's conclusion is as follows.[213]

"First of all, predatory innovation on blockchain is cheap as it can be implemented at no cost. Its implementation can also be very fast, in fact, interactions/validations via blockchain only take a few seconds or minutes at most. Although transactions and modification are not invisible on public blockchain, they can be on private blockchains — the access to information and the history of the blockchain can be limited to some users. And predatory innovation on blockchain can have a radical effect: it will produce immediate effects by excluding a targeted user which also is a competitor. Lastly, predatory innovation practices can take different forms with multiple effects, beyond the mere exclusion from the blockchain. A company that owns a private blockchain can indeed modify its governance design so that a user's access is purely and simply denied, or, to a lesser extent, that the user can no longer read all the information on the blockchain, register transactions or take part in the block validation process."

iv. Exploitative conduct

The fourth and final category of harm is so-called "exploitative" abuse. This is where undertakings abuse dominant positions "to reap trading benefits which it would not have reaped if there had been normal and sufficiently effective competition".[214] Whilst this type of abuse has traditionally been directed towards the charging of excessive prices, there is an emerging theory of harm concerned with the exploitation of user data; something of particular relevance in the blockchain context given the likelihood of network effects and single-source data. For example, in 2019, the German competition authority decided that Facebook had abused a dominant position in the way it collected, merged and used user data because this exceeded what was necessary for Facebook to operate its platform and consumers had no

210 See, for example, the French and German competition authorities' joint report, 'Competition Law and Data' (2016), pp.17-18; available at <https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Berichte/Big%20Data%20Papier.pdf;jsessionid=821DE929A6BEF735EF2B0EE63D4A9B25.1_cid362?__blob=publicationFile&v=2.> See also Brinsmead, 'When does information become an essential facility?', fifteen eightyfour; available at<http://www.cambridgeblog.org/2021/05/when-does-information-become-an-essential-facility/.>

211 CCI and EY, 'Discussion paper on blockchain technology and competition', p.43; available at https://www.cci.gov.in/sites/default/files/whats_newdocument/Blockchain.pdf.

212 Schrepel, 'Predatory Innovation: The Definite Need for Legal Recognition', SMU SCI. & TECH. L. REV (2018); available at <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2997586.>

213 Schrepel, comments to the European Commission for its conference on competition policy in the era of digitization, in particular the panel entitled "Digital Platforms' Market Power" (2018), p.8; available at https://ec.europa.eu/competition/information/digitisation_2018/contributions/thibault_schrepel.pdf.

214 Case C-27/76, United Brands v Commission, para 249.

ability to opt-out of the processing activities.[215] Theories of harm of this kind are still being shaped in UK and European law, where it has belatedly been recognised that the use and abuse of data is not merely a matter for privacy law and data regulators, but is a concern for competition lawyers (in that privacy standards may impact on the quality of a service offering). However, similar reasoning may in future be applied to the exploitation by blockchain owners of transaction data and other user data. If this data is processed in a way that strikes an unreasonable balance between the blockchain owner's interests and that of the blockchain participants, this may be unlawful.

3. Potential enforcement problems for competition regulators

Issues with competition enforcement in a blockchain context appear to hinge on two factors: the degree of transparency on the blockchain and the concentration of power in the hands of the blockchain owner(s). With this in mind, we consider enforcement of two types of blockchains: "decentralised" blockchains (permissioned or permissionless blockchains, that are characterised by more transparency and less concentrations of power) and "centralised" blockchains (permissioned blockchains characterised by less transparency and greater concentrations of power). Though it should be flagged that these concepts are somewhat artificial and are not separated by any clear dividing line.

Regulating "decentralised" blockchains

The first problem regulators are faced with is the detection of anti-competitive practices that may be perpetrated through encrypted means within a particular blockchain network, and the identification of the perpetrators of those competitive harms. As has been noted: "The pseudonymity of transactions on the blockchain, combined with the anonymity of the nodes on the chain create obstacles in terms of enforcement. Thus the distributed network architecture of blockchain constitutes a real barrier to competition law enforcement."[216]

In addition, where blockchain is used as part of a decentralised network, there is no single target of blocking action – there being no single server to target – like there would be in relation to an identifiable company conducting anti-competitive practices through their own identifiable servers. For the same reason, there is no single, central person against whom a regulator might seek an injunction or to apply sanctions or in respect of whom remedial orders might be made (or at least certainly not on a public or permissionless blockchain). The notion of a dawn raid against a particular participant and the seizing of their computer will be entirely ineffective for the same reason that a hacker seeking to amend the chain by hacking a particular node and amending a single particular transaction will be revealed by the history of the transactions on the chain to be an incorrect outlier. The problems surrounding the taking of enforcement action multiply when many of the network's constituent users operate in other jurisdictions.

In competition law terms, who is the undertaking or undertakings that may be targeted with enforcement action? Is it each individual participant in the network, or only those constituting the majority that adopted the practice (or amending the governance rules – most obviously on a private, permissioned blockchain) giving rise to the anti-competitive harm or effect[217]? Each individual is engaged in economic activity on the chain, albeit that the adoption of governance rules by a certain sub-section of individuals may constitute an agreement between an association of undertakings. Similar considerations apply where the blockchain is dominant on a particular market: there, is the fact that all participants on the chain are beneficiaries of the block's monopoly, such as to render them collectively dominant? Or would dominance only reside in those sub-set of users whose amendment

215 See https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Meldungen%20News%20Karussell/2019/07_02_2019_Facebook.html. For the complex subsequent procedural history, see Heinz, 'Bundeskartellamt hits "don't like" button on Facebook', Kluwer Competition Law Blog (2019); available at http://competitionlawblog.kluwercompetitionlaw.com/2019/02/11/bundeskartellamt-hits-dont-like-button-on-facebook/.
216 Schrepel, comments to the European Commission, p 3.
217 At least on an open or public blockchain: private blockchains can modify their governance design anytime and do no need a majority to agree or acquiesce.

of the governance rules or software protocols had led to the chain's position of dominance? Or only those users on the chain whose market power in the relevant markets renders them dominant? Or indeed only those sub-set of users who have market power by reference to the chain's particular applications?[218]

In any event, the answer may be that in order to 'take down' the operation of a blockchain network that is found to be engaged in anti-competitive practices it will be necessary to encode disabling measures into the network's own internal system of governance. But if that encoding had not been undertaken from the outset, then again, one envisages that a competition regulator would need the power – as is being discussed in the context of the new Digital Markets Unit (DMU) – to undertake pro-competitive interventions by way of orders that would, in this case, lead to the re-coding of the blockchain itself. Again, that requires a regulator to know who to target in order to issue an enforceable order.

For open blockchains the governance rules are embedded in code. The protocol part of the software defines the consensus mechanism, being the mechanism by which governance rules might be altered. The software protocol also defines the consensus mechanism for private blockchains. However, as noted above, governance is always complemented by an ordinary agreement between participants through, in particular, cooperation agreements. The question will be whether that agreement constitutes an agreement between all participants for the purposes of the Chapter I prohibition. If that agreement is an agreement which, inter alia, provides for the pursuit of transactions on that blockchain by way of the governance rules and software protocols that may have an exclusionary effect, it is likely that all participants would be regarded as parties to an anti-competitive agreement. The CMA can use their powers to raise information requests to seek to ascertain the identity of participants, and recourse might even be had to Norwich Pharmacal Order, being a disclosure order available in England and Wales which allows information to be obtained from third parties who have become 'mixed up' in wrongdoing.

Moreover, if the blockchain is immutable, it just will be the case that visible transactions that constitute a competition law violation will remain on the permanent digital record, at least for all users of that chain to see. It may be a form of information sharing that cannot be deleted. The impact of the breach may dissipate as market conditions move on and insofar as that particular form of breach is addressed either through effective sanctions and/or remedial measures including recoding, the fact that the record of the previous competition law breach cannot be deleted or destroyed may therefore have no lasting impact.

Regulating "centralised" blockchains

As more economic activity is undertaken online, competition regulators have had to consider the extent to which the existing rulebook and enforcement toolkit continue to be sufficient to protect the process of competition, and thus the maximisation of efficiency and consumer welfare. That has led, in the United Kingdom, to the establishment of the DMU within the Competition and Markets Authority. The DMU – which currently operates on a non-statutory basis pending the anticipated passage of new legislation conferring on it new powers to promote competition on digital markets – will operate as a pro-competition regulator for digital markets and platforms, and in particular will "oversee a new regulatory regime for the most powerful digital firms, promoting greater competition and innovation in these markets and protecting consumers and businesses from unfair practices".[219] In that regard, the DMU will oversee and enforce the new pro-competition regime for digital firms with Strategic Market Status (SMS), meaning the activities of major tech companies where the risk of anti-competitive harm is greatest.

218 Shrepel, Is Blockchain the Death of Antitrust Law? p 304
219 https://www.gov.uk/government/collections/digital-markets-unit

In July 2021, the Government published a consultation on proposals for the new pro-competitive regime that will apply to digital markets.[220] including in relation to the criteria to be applied to designate those with SMS. What is envisaged is a new agile approach to regulating big tech firms, where an evidence-based assessment will be used to identify those firms with substantial and entrenched market power, in at least one digital activity, providing them with a strategic position.[221] This includes situations where the effects of the firm's market power are likely to be widespread or significant. These firms will be designated with Strategic Market Status and will be subject to (i) a new enforceable Code of Practice which will be designed to shape firms' behaviour to prevent anti-competitive outcomes before they occur; and (ii) a range of potentially pro-competitive interventions by the DMU.

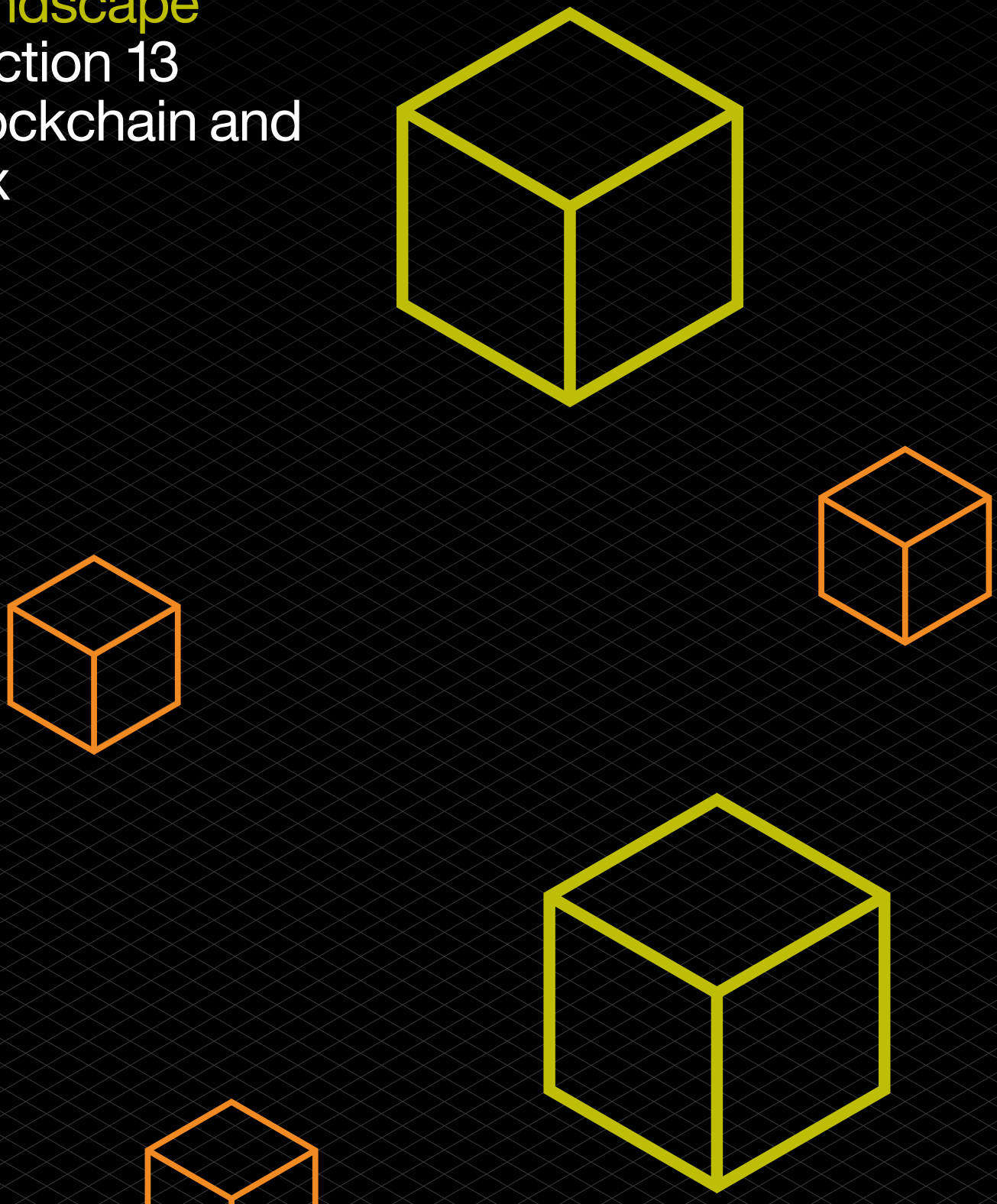
As matters stand, it seems likely that many online companies who adopt blockchain technology will not fall within scope of the new pro-competitive regime that will be enforced by the DMU, but will remain subject to existing competition law provisions. However, as discussed above, it seems likely that blockchain-based services will operate in markets characterised by network effects and single source information. Therefore, as these markets mature and dominant positions are established, companies may begin to fall within the DMU's remit.

Before that stage is reached, it seems likely that regulators will have to adapt in a piecemeal fashion. Whilst the existing analytical framework for evaluating competition harms seems more than adequate, the main concern is whether regulators will forever be playing 'catch-up'. In our view, getting ahead of the curve requires three main steps. First, regulators need to ensure they have the necessary technical expertise to understand exactly how relevant blockchain technologies operate. For example, in the same way 'algorithmic auditors' are starting to shed light on the implications of algorithmic coding, similar professionals will be needed in the blockchain arena. Second, regulators will need to ensure they oversee grey areas where traditionally siloed areas of law overlap. For example, when it comes to the interaction of competition and privacy / data protection law, the CMA's DaTa Unit and the Digital Regulation Cooperation Forum (which consists of the CMA, FCA and ICO) are both designed to address unique challenges posed by digital markets. Third, regulators should be willing to push the boundaries of competition law to ensure all forms of anticompetitive abuse are addressed. That may be easier said than done but is imperative to ensure blockchain technologies fulfil their promise of enhancing consumer welfare.

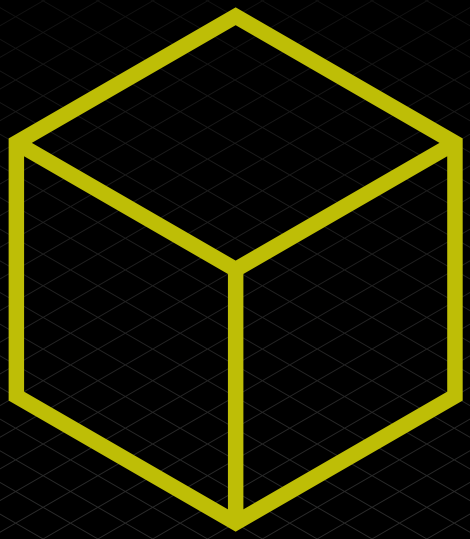
220 https://www.gov.uk/government/consultations/a-new-pro-competition-regime-for-digital-markets
221 This will not require the DMU to undertake formal market definitions to precisely define the parameters of the market in which the activities of the undertaking in question take place (see para 54 of the Consultation)

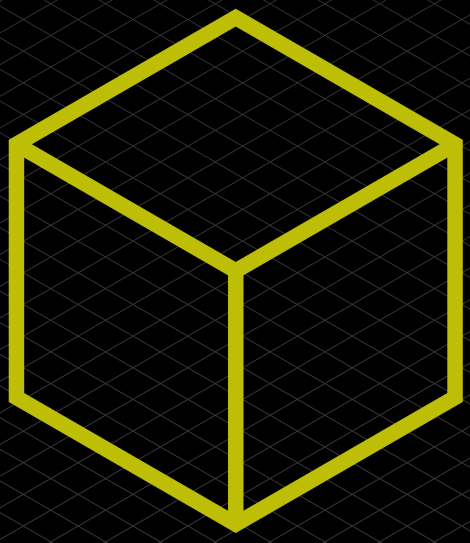
Part 2: Impacts on the Wider Landscape

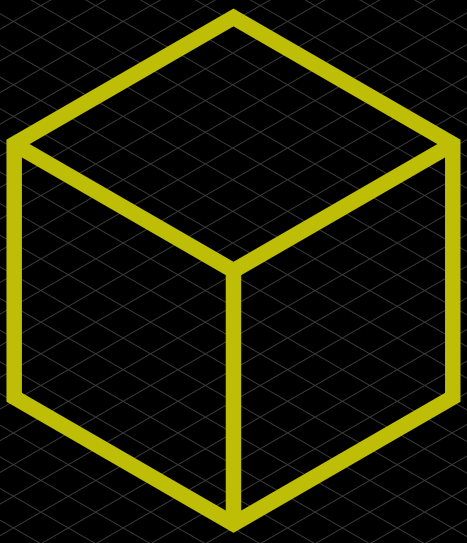
Section 13 Blockchain and Tax



13







Section 13: Blockchain and Tax

Ceri Stoner and Jennifer Anderson, Wiggin LLP

Introduction

Tax policy is critical to providing certainty and enhancing transparency in a virtual space. Investors, individuals and businesses all need clear and consistent tax rules that establish tax liabilities and treatments to improve certainty and minimise costs. From a tax authority perspective, an effective tax framework is equally important in order to enable compliance and reporting on transactions and minimise tax evasion. Furthermore, the ability, and perhaps the inevitability, of this transformative technology to revolutionise the tax system itself should not be overlooked.

As the UK's fintech revenue and investment increase[222], the UK government has repeatedly reiterated its claim to be a world leader in this sector. The actions it has taken to realise this aim include the launch of a new taskforce in 2021 to consider the possibility of a new 'Britcoin' in the form of a CBDC. It is essential that the UK's tax system keeps up with these real-world developments as best it can. It is therefore unsurprising that in the last year HMRC has sought to consolidate and improve its previously piecemeal efforts to regulate this area. HMRC's new, more comprehensive, Cryptoassets Manual was launched on 30th March 2021.

Blockchain technology and its impact on tax frameworks is, of course, a global issue. Consequently, the UK's approach should continue to be developed and informed by the international landscape and, in particular, the EU's DAC 8 and OECD's reports and proposals on the tax treatments and policy issues.

Blockchain technology is often looked at from a purely commercial perspective, as a transformative way of exchanging value. However, the digital exchange of value throws up three key tax issues for legal tax practitioners:

1. Taxation of cryptoassets and blockchain

2. Impact of blockchain on tax authorities

3. Impact of blockchain on the in-house tax function

It is crucial that these complex issues are addressed in order to establish a functional tax system which overlays the technology.

The scale of the challenge is significant. As previous sections have discussed, blockchain technology is being harnessed to provide a peer-to-peer network for conducting transactions without a third-party intermediary, utilising SLCs to embed business logic into a transaction through computer code which automates the logic, i.e. "if X, then Y". Blockchain also provides a neat data store for recording those transactions and a consensus mechanism for validating transactions and limiting fraudulent or false transactions.

As such, 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 secure, immutable and resilient against disruption. Fraud is less likely (albeit false information can still be entered) and easier to spot;

— **Transparency:** traceable, validated transactions; and

222 Kalifa Review of UK fintech, 26 February 2021

— Real Time Information: any participant can keep a copy of the ledger and are able to read and access data.

Taxation of cryptoassets and 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. The UK tax treatment of any transaction involving blockchain and cryptoassets is therefore dependent on general taxing principles, supplemented by the HMRC guidance available and some limited European case law (which is focused on VAT).

Cryptoassets are, of course, 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 and indeed other tax authorities. 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:

i. The legal nature of the cryptoassets created. The categorisation of the cryptoasset for tax purposes will dictate its tax treatment – for example, whether it is deemed to be a tangible or intangible, security or civil asset, will fundamentally alter how it will be taxed.

ii. 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, as discussed in Section 12, i.e. when a change to a protocol 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?

iii. 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 is 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 multifaceted and, as indicated above, in the first instance it pivots on the definition of a cryptoasset.

HMRC does not consider a cryptoasset to be a form of money or currency. From a tax perspective, the term cryptoassets is defined by HMRC[223] as "cryptographically secured digital representations of value or contractual rights that can be transferred, stored and traded electronically". This definition differs subtly but significantly

223 Cryptoassests: Tax for Individuals (first published 2018) <https://www.gov.uk/government/publications/tax-on-cryptoassets/cryptoassets-for-individuals and https://www.gov.uk/hmrc-internal-manuals/cryptoassets-manual/crypto10000 at CRPTO10100>

from the legal analysis of a cryptoasset endorsed by the UK Jurisdiction Taskforce (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[224] 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. The OECD is leading the charge on this. In October 2020, it published a G20/OECD approved report on 'Taxing Virtual Currencies: An Overview of Tax Treatments and Emerging Tax Policy Issues'. This provided a global overview of the tax treatments of virtual currencies in different jurisdictions homing in on the associated policy issues. A more detailed follow-up report is expected by the end of 2021.

As also explored in Section 3, the UK government's Cryptoasset Taskforce (comprising HM Treasury, FCA and Bank of England) has recognised three types of cryptoasset since October 2018[225]. In HMRC's March 2021 Cryptomanual[226], this has been increased to four:

— **Exchange Tokens:** Used as a method of payment and an increasingly popular form of investment (for example, Bitcoin). 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.

— **Utility Tokens:** Provide the holder with access to specific goods or services, typically on a blockchain platform. These may also be traded. 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'.

— **Security Tokens:** Provide the holder with specific rights or interests in a business, such as debt due by the business or a profit share in the business.

— **Stablecoin:** Tokens which are pegged to something that is considered to have a certain and stable value, such as a fiat currency or precious metal, in order to minimise volatility (for example, Tether).

It should be noted that not all tokens receive equal attention in the HMRC guidance. There is a continued focus on exchange tokens by HMRC which, whist understandable given that they have received most investment, will nonetheless inevitably cause issues for tax practitioners and HMRC compliance officers alike, when grappling with the taxation of other tokens. If a token is not an exchange token, there remain areas where HMRC remains silent.

In terms of validation of transactions, HMRC does now recognise proof of state networks, where the ability to create a new entry is determined by a user's wealth in the cryptoasset (or 'stake') rather than solely proof of work networks which rely on having the computer power to solve a puzzle before anyone else does.[227] This

224 UKJT Legal Statement on cryptoassets and smart contracts, published November 2019 <https://35z8e83m1ih83drye280o9d1-wpengine.netdna-ssl.com/wp-content/uploads/2019/11/6.6056_JO_Cryptocurrencies_Statement_FINAL_WEB_111119-1.pdf >
225 Cryptoassets Taskforce: Final Report <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752070/cryptoassets_taskforce_final_report_final_web.pdf>
226 HMRC's Crytoassets Manual, launched on 30 March 2021 at CRYPTO10100 <https://www.gov.uk/hmrc-internal-manuals/cryptoassets-manual>
227 https://www.gov.uk/hmrc-internal-manuals/cryptoassets-manual/crypto10300

reflects the shift from energy intensive activities (for example Bitcoin mining) to networks perceived to be more environmentally friendly.

One helpful clarification from HMRC is what is not now considered a cryptoasset, i.e. crypto-derivatives[228]. These will instead typically be considered to constitute derivative contracts and will therefore be taxed under the UK's existing rules (namely Part 7, Corporation Tax Act 2009) when entered into by a company.

Substance of transaction

The tax treatment of all types of token is dependent on the nature and use of the token not the definition of the token. HMRC therefore does not consider cryptoassets to be currency or money per se[229]. HMRC recognises a number of roles for cryptoassets:

— 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. In HMRC's view,[230] a transaction where a cryptoasset is given or received by way of consideration is a transaction effected for non-monetary consideration (in most cases), i.e. a barter transaction.

— 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.

— Supporting capital raising and/or the creation of decentralised networks through Initial Coin Offerings (ICOs).

Tax System

Application of 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.

HMRC guidance to date has focused on the UK tax treatment of cryptoassets and transactions in or involving cryptoassets (focusing so far 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 they ultimately dispose of their cryptoassets.

Income tax and national insurance contributions (NICs) on cryptoassets will arise in certain circumstances where they receive the cryptoassets from:

— their employer as a form of non-cash payment

— mining, transaction confirmation or airdrops[231]

228 HMRC Crptoassets Manual at CRYTO10150 (https://www.gov.uk/hmrc-internal-manuals/cryptoassets-manual)
229 HMRC Crptoassets Manual at CRYTO10100 (https://www.gov.uk/hmrc-internal-manuals/cryptoassets-manual)
230 Cryptoassets Taskforce: Final Report <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752070/cryptoassets_taskforce_final_report_final_web.pdf< and at <https://www.gov.uk/hmrc-internal-manuals/cryptoassets-manual/crypto10250>
231 https://www.gov.uk/government/publications/tax-on-cryptoassets/cryptoassets-for-individuals#which-taxes- and https://www.gov.uk/hmrc-internal-manuals/cryptoassets-manual/crypto20050

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, provides the cornerstone for 'best practice'.

Income Tax and Withholding Taxes

i. Employment taxes
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. [232]

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".

ii. Airdrops
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.

iii. Trading
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.[233] 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.[234]

Capital Gains Tax[235]

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, 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;

232 https://www.gov.uk/hmrc-internal-manuals/cryptoassets-manual/crypto21100
233 https://www.gov.uk/government/publications/tax-on-cryptoassets/cryptoassets-for-individuals#income-tax and https://www.gov.uk/hmrc-internal-manuals/cryptoassets-manual/crypto10000
234 https://www.gov.uk/hmrc-internal-manuals/cryptoassets-manual/crypto20250
235 https://www.gov.uk/hmrc-internal-manuals/cryptoassets-manual/crypto22100

— using cryptoassets to pay for goods or services; and giving away cryptoassets to another person.[236]

It should, however, be noted that HMRC states that 'disposal' is a broad concept and therefore 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) plus any allowable expenses, including certain exchange fees.

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[237]

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.[238] This means that any corporation tax legislation which relates solely to money (for example, the foreign currency rules in Corporation Tax 2009) does not apply to exchange tokens or other types of cryptoasset.

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".[239]

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[240] have priority over the chargeable gains rules"[241]. 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).

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[242]. Also, in the same way as

236 https://www.gov.uk/government/publications/tax-on-cryptoassets/cryptoassets-for-individuals#capital-gains-tax and https://www.gov.uk/hmrc-internal-manuals/cryptoassets-manual/crypto22100
237 https://www.gov.uk/hmrc-internal-manuals/cryptoassets-manual/crypto41000
238 https://www.gov.uk/government/publications/tax-on-cryptoassets/cryptoassets-tax-for-businesses#corporation-tax and https://www.gov.uk/hmrc-internal-manuals/cryptoassets-manual/crypto10000
239 ibid
240 Corporation Tax Act 2009 Part 8
241 https://www.gov.uk/government/publications/tax-on-cryptoassets/cryptoassets-tax-for-businesses and https://www.gov.uk/hmrc-internal-manuals/cryptoassets-manual/crypto41150
242 https://www.gov.uk/government/publications/tax-on-cryptoassets/cryptoassets-tax-for-businesses#corporation-tax and https://www.gov.uk/hmrc-internal-manuals/cryptoassets-manual/crypto41300

for other assets, businesses can also crystallise losses for exchange tokens (and potentially other forms of cryptoasset) 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.[243]

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."[244] 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[245]

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."[246]

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[247], has been incorporated into HMRC guidance as follows:

1. "Exchange tokens received by miners for their exchange token mining activities will generally be outside the scope of VAT on the basis that:
   i) the activity does not constitute an economic activity for VAT purposes because

243 https://www.gov.uk/hmrc-internal-manuals/cryptoassets-manual/crypto41450
244 https://www.gov.uk/government/publications/tax-on-cryptoassets/cryptoassets-tax-for-businesses#stamp-duty-and-stamp-duty-reserve-tax and https://www.gov.uk/hmrc-internal-manuals/cryptoassets-manual/crypto10000
245 https://www.gov.uk/hmrc-internal-manuals/cryptoassets-manual/crypto45000
246 https://www.gov.uk/government/publications/tax-on-cryptoassets/cryptoassets-tax-for-businesses#vat and https://www.gov.uk/hmrc-internal-manuals/cryptoassets-manual/crypto45000
247 For example, CJEU case, Skatteverket v David Hedqvist C-264/14 (22 October 2015) and First National Bank of Chicago (C-172/96)

there is an insufficient link between any services provided and any consideration; and
ii) there is no customer for the mining service.

2. When exchange tokens are exchanged for goods and services, no VAT will be due on the supply of the token itself.

3. 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"[248]

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.

Bitcoin Exchanges

In 2014, HMRC decided that under Item 1, Group 5, Schedule 9 of the Value Added Tax Act 1994, the financial services supplied by Bitcoin Exchanges – exchanging bitcoin for legal tender and vice versa – are exempt from VAT.

This was confirmed in the Court of Justice of the EU (CJEU) in the Swedish case, David Hedqvist (C-264/14).

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 tax authorities

The impact of blockchain on tax policy and tax evasion have been largely unexplored to date. Investments and transactions in blockchain generate value and represent a potentially important tax base that needs to be defined and recognised by countries, who will then need to decide the extent to which they will tax this base. The tax evasion implications of blockchain also form an important part of the overall regulatory framework.

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. However, there is also the risk that new alternative payment methods actually threaten tax transparency and pose a substantial risk of tax evasion.

For tax reporting and collection to work well for individuals and businesses, there should be a greater degree of uniformity internationally. The OECD is developing a standardised tax reporting and exchange framework, commonly referred to as the 'crypto-CRS' standard, following a public consultation on the topic in 2021. Progress is slow however and publication of the new standard is not expected until the first half of 2022.

As a result of this work, the European Union is also looking to publish the 8th version of the Directive on Administrative Cooperation (DAC 8) which will expand the rule for administrative cooperation and exchange of information into the areas

248 https://www.gov.uk/government/publications/tax-on-cryptoassets/cryptoassets-tax-for-businesses#vat and https://www.gov.uk/hmrc-internal-manuals/cryptoassets-manual/crypto45000

of cryptoassets and virtual currencies.[249] The focus is on increased tax transparency and addressing tax evasion in respect of the new alternative means of payment and investment. The new rules will be enforced by virtue of significant new penalties. Observers expect DAC 8 to be implemented in the next 12 to 18 months.

Blockchain technology certainly 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 digitalised 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.

Blockchain technology could also 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.

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 endeavour to get this balance right or they risk lowering medium- or long-term tax revenues.

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 practical as well as policy 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:

— **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:** older 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

249 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12632-Tax-fraud-&-evasion-strengthening-rules-on-administrative-cooperation-and-expanding-the-exchange-of-information_en

— **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
— **Legislative basis:** it will be vital to establish a proper legal basis for the collection of data and use of data

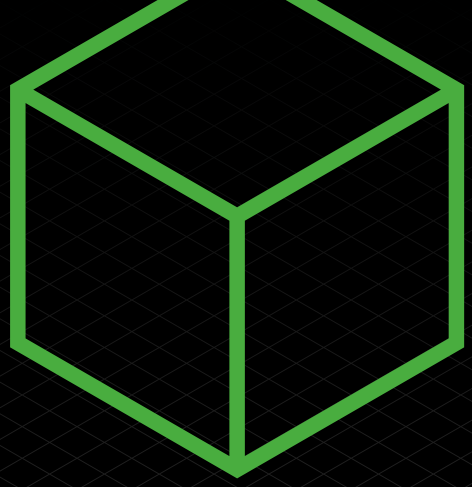
Impact of Blockchain on in-house tax function
This section would not be complete without briefly touching upon the potential impact of blockchain on in-house tax functions.

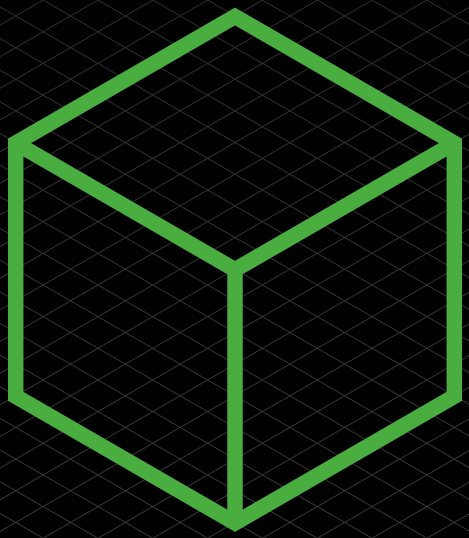
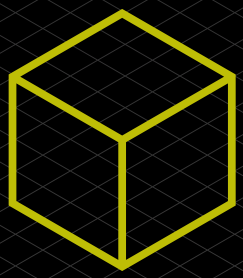
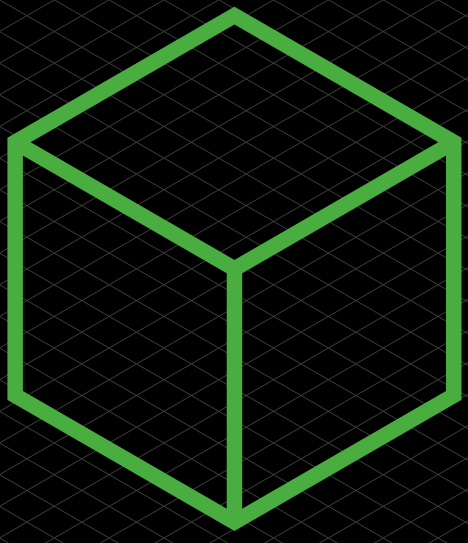
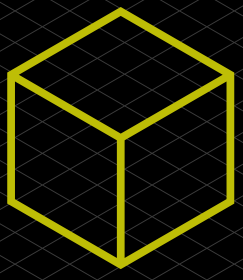
Compliance, in terms of reporting and disclosure, is generally one of the primary purposes of the in-house tax function. One of the greatest challenges for the modern tax function is the increasing demand for data from tax authorities across the globe, to be delivered at an ever-increasing speed. Blockchain 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 to 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.

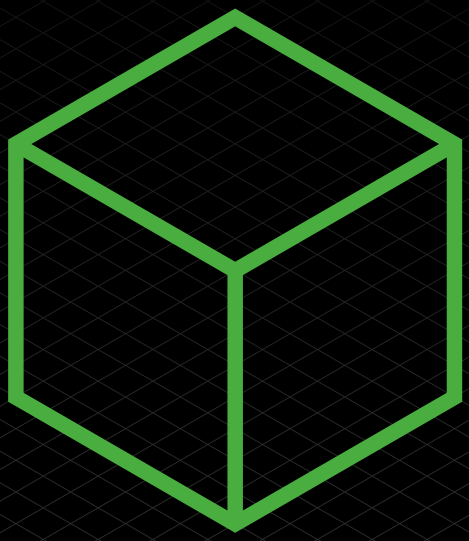
Part 2: Impacts on the Wider Landscape

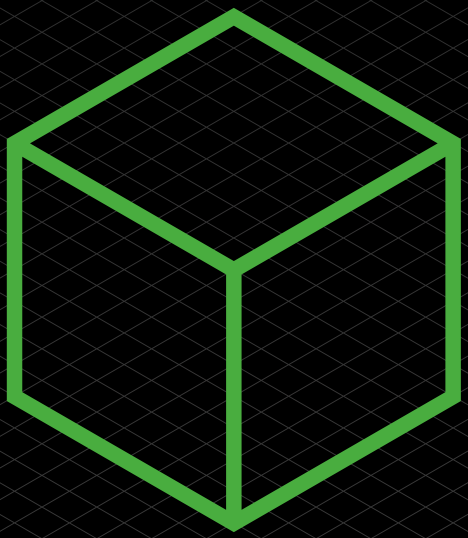
Section 14 Blockchain and ESG

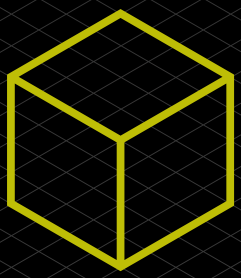


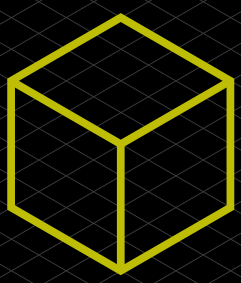





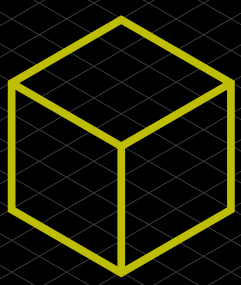
14











Section 14: Blockchain and ESG

Nicola Higgs, Stuart Davis, Paul Davies and Charlotte Collins
(Latham & Watkins LLP)

Introduction

As the popularity of cryptoassets has grown and mainstream financial institutions have begun to show an interest in them as an investable and tradable asset class, attention has started to focus on the cryptocurrency industry's environmental, social, and governance (ESG) performance.

Voluntary and mandatory ESG-related reporting requirements have emerged in recent years, as keen investor interest in ESG matters has grown. Consequently, financial institutions and other corporates find themselves under unprecedented scrutiny in terms of their ESG credentials. Therefore, they are under increasing pressure to ensure that their business, clients, associations, and investments do not have a negative impact from an ESG perspective.

The vast majority of the world's financial institutions manage climate risk and other ESG risks in their own portfolios. As a result, many financial institutions perform related diligence on corporates they look to service, whether by traditional lending, capital markets underwriting, or direct investment. Equally, listed companies are some of the first to face formal ESG disclosure regimes and so are mindful of their various ESG "exposures", while asset managers are also facing greater pressure to ensure that investments align with investor demands and expectations. Though the focus has been primarily on the ESG performance of cryptocurrency miners (given their role in the creation of cryptocurrencies and the energy requirements associated with that process), the ESG performance of the broader cryptocurrency industry increasingly needs to be considered, particularly as institutional investment in cryptoassets is accelerating. Accordingly, investors in cryptocurrency miners, in cryptoasset service providers, and even in companies that put cryptoassets on their balance sheets must now weigh the potential for increased returns against the possible negative impact on their ESG credentials.

For example, most listed corporates now have an ESG policy in place and, at one level or another, are looking to finance themselves by relying on ESG-linked products (sustainability-linked bonds or loans, ESG swaps, etc). Concurrently, many corporate treasuries (especially in the US, but also in Europe) are looking to invest a portion of their balance sheet assets in digital assets (Bitcoin in particular). For public companies looking to issue ESG products and also allocate a portion of their balance sheet to digital assets, the challenges in reconciling ESG-related promises to investors with the company's underlying ESG profile are acute.

It is necessary to distinguish cryptocurrencies as an asset class from the distributed ledger technology (DLT) they rely on. DLT is a set of technological solutions that enables a single, sequenced, standardised, and cryptographically-secured record of activity to be safely distributed to, and acted upon by, a network of participants. DLT has a wide number of potential use cases in financial services and many of those applications will be designed in a way that does not rely on the complex consensus models utilised by some cryptocurrencies and does not, therefore, necessarily present material ESG concerns. However, given the significant attention cryptocurrencies are receiving with respect to environmental considerations, this section focuses on the ESG considerations relating to cryptocurrencies rather than exploring the broader potential for DLT use cases in financial services, which would require a case-by-case assessment in relation to ESG issues.

Environmental considerations

Environmental concerns have circulated in popular media relating to the amount of energy expended in mining cryptocurrencies and the consequent emissions, particularly those that rely on a proof of work consensus model (such as Bitcoin and Ether) rather than proof of stake, or proof of authority, consensus models. Such emissions, it has been argued, have the potential to significantly contribute to the acceleration of global warming.

According to research by the University of Cambridge, the majority of Bitcoin miners have been based in China250, a country heavily reliant on coal for energy. However, recent policy decisions and initiatives to shift from fossil fuels to clean energy sources have started to reduce the cryptocurrency mining carbon footprint. Further, in September 2021, the Chinese government introduced a blanket prohibition on the trading and mining of cryptocurrencies, and it is yet to be seen what impact this will have on the carbon footprint of cryptocurrency mining in the longer term.

Nevertheless, a growing range of blockchain protocols supporting the issuance of cryptoassets that do not rely on energy-intensive consensus models are coming to the market, including permissioned networks, which the financial industry is increasingly adopting. Even so, the popularity of Bitcoin and other well-known cryptocurrencies as an asset, and their broader importance to the cryptocurrency market, means that environmental questions continue to be highly relevant in this sector.

Where and how cryptocurrency is mined is a growing area of focus for investors who do not want to buy cryptocurrency that is created in a way that causes excessive energy waste or environmental damage. Today nearly 40% of cryptocurrency mining relies on renewable energy sources, as an increasing number of miners aim to reduce carbon emissions and meet investors' demands. Anecdotes have circulated about investors seeking sustainably mined 'virgin' bitcoins at a premium, as these bitcoins are less likely to be associated with problematic activities, and therefore less likely to raise ESG or reputational risks. Some institutions even want to mine their own supply to be able to prove their coins' provenance to clients.

Climate focus: the impact of the Paris Agreement

The Paris Agreement is a legally binding international treaty on climate change, adopted by 196 countries at the United Nations Climate Change Conference in Paris on 12 December 2015. Its goal is to limit global warming to below 2°C, compared to pre-industrial levels. Those 196 countries are now looking to build their own legislative frameworks to ensure that they can achieve the carbon reduction goals set out in the Paris Agreement. They aim to achieve these goals by imposing carbon reduction requirements on companies operating in their jurisdictions. In practice, for the vast majority of companies, this requirement will likely involve aligning with the Task Force on Climate-related Financial Disclosures (TCFD), a private sector task force whose recommendations are widely recognised as authoritative guidance on the reporting of financially material, climate-related information.

The TCFD recommendations and supporting disclosures include the following:

— Governance: disclose the organisation's governance around climate-related risks and opportunities

— Strategy: disclose the actual and potential impacts of climate-related risks and opportunities on the organisation's businesses, strategy, and financial planning where such information is material

— Risk management: disclose how the organisation identifies, assesses, and manages climate-related risks

— Metrics and targets: disclose the metrics and targets used to assess and manage relevant climate-related risks and opportunities where such information is material

A number of governments and financial regulators around the world have expressed support for the TCFD recommendations and are integrating them into their guidance and policy frameworks, including the UK, Australia, New Zealand, Canada, Hong Kong, Japan, Singapore, and South Africa, as well as some EU Member

250 https://cbeci.org/mining_map

States. In the UK, for example, the FCA has introduced climate-related disclosure requirements for listed companies. These require companies to disclose, on a "comply or explain" basis, whether they have made disclosures consistent with the TCFD recommendations. Further, a TCFD-aligned international reporting standard is currently under development, which could pave the way for mandatory TCFD compliance.

For the reasons highlighted above, many cryptocurrency miners and firms may find having to disclose their greenhouse gas emissions publicly as a highly sensitive exercise. They may also find it challenging to ensure the accuracy of those disclosures.

However, some cryptocurrency firms are starting to explore carbon offset and energy efficiency/sustainability programmes. For example, the Energy Web Chain is an Ethereum-like base layer network protocol for the purpose of building renewable energy applications on the blockchain. Unlike the Ethereum or Bitcoin protocols, Energy Web Chain uses a proof of authority consensus model, which, Energy Web Chain argues, is more energy efficient due to its permissioned, proof of authority consensus. These types of blockchain consensus models have been gaining prominence as a result of energy efficiency concerns and may become an increasingly important factor in the success of these platforms. Energy Web has also recently partnered in the launch of the Crypto Climate Accord (CCA), a private sector-led initiative inspired by the Paris Agreement. The CCA focuses its efforts on decarbonising the cryptocurrency industry, aiming for all blockchains to be powered by 100% renewable energy sources by 2025, as well as net-zero emissions for the entire crypto industry by 2040.[251]

Social considerations

Social impacts have moved to the forefront during the COVID-19 pandemic. Bitcoin and other cryptocurrencies have notable arguments concerning their own social benefits. Cryptocurrencies aim to allow users to seamlessly transfer value in all parts of the world via a monetary network that is robust, free of censorship, and resistant to intervention by state actors and geopolitical conflicts. The only barrier to entry for aspiring market participants is an internet connection.

As mentioned previously, many cryptoasset service providers (CSPs) have taken significant steps to implement compliance safeguards such as anti-money laundering (AML) and countering terrorist financing (CTF) frameworks even in advance of formal regulatory requirements being imposed on them, though this is not universally the case. For example, the increasing use of decentralised finance (DeFi) platforms in order to trade cryptoassets or provide/take liquidity through lending or market-making platforms raises concerns as to whether these unregulated platforms may be used to sidestep the compliance safeguards of regulated platforms. DeFi platforms do not tend to impose AML "know your customer" (KYC) standards on their users, and governments and regulators have raised concerns as to whether the anonymity associated with these platforms could lead to undetected market manipulation or financial crime. However, a range of AML/KYC solutions tailored to the DeFi space are emerging even in this traditionally unregulated area.

On the other hand, cryptocurrency activity is not inherently opaque, and a benefit of cryptocurrency transactions is that they are largely transparent and traceable (with the exception of privacy coins[252]). Blockchain analysis has been recognised as an important tool for cryptoasset service providers to consider when dealing with assets that have originated from anonymous or private sources.[253] Still, important questions remain as to how AML/KYC requirements should be adjusted to take into

251 https://cryptoclimate.org/

252 Privacy coins are coins that provides the user community with a higher level of anonymity than is typical for cryptocurrency. Privacy-related features may include encryption, the bundling of transactions (so that individual users cannot be linked to individual transactions), and stealth addresses.

253 See the Joint Money Laundering Steering Group's Sectoral Guidance on Cryptoasset Exchange Providers and custodian wallet providers.

account the traceable nature of the blockchain (e.g. how many 'hops' a cryptoasset service provider should analyse to be comfortable with the source of the asset). However, as the industry matures, and as regulators and international bodies such as the FATF continue to work with the sector, market standards in this area should continue to emerge.

While market participants in the cryptocurrency industry may be able to use their social impacts as a method of competitive advantage, particularly by contrasting their activities with any perception that cryptocurrency is an avoidance mechanism for taxation and other regulatory regimes, or a driver for criminal activity, they must be able to demonstrate meaningful social contribution by understanding the metrics customarily used to measure social impacts.

Governance considerations
Governance, and in particular the transparency of a cryptocurrency market participant's governance framework, forms a key driver of opportunity or exposure. Considerations include:

— Does the management body take into account sustainability issues in the course of business?

— Is the operation structured to align with the long-term ideal of being sustainable by maintaining a diverse management team?

— Does the firm operate with tax transparency?

— Is financial crime, bribery, and corruption risk adequately managed?

— Does the operation have systems in place to protect against cyberattacks that could result in losses for investors and breaches of privacy?

— Is executive pay linked to sustainability targets?

— How does the firm address diversity and inclusion within the organisation?

Some of these questions may challenge high-growth companies that often operate under regimes that have not adapted to their business model, particularly in the case of financial crime legislation. Over time, governance will organically improve as digital asset businesses become more mainstream and list on public exchanges (whether through IPOs, direct listings, SPACs, or otherwise), as they will be forced to adhere to formalised governance and disclosure models as would any other publicly-traded company. In line with the current focus on ESG matters, governance-related disclosures are also expanding for listed companies, with various jurisdictions beginning to introduce additional governance-related disclosure standards regarding diversity and inclusion. For example, in the UK the FCA is introducing new requirements for listed companies to disclose in their annual financial report whether they meet specific board diversity targets on a "comply or explain" basis.

Conclusion
With ESG reaching increased prominence, businesses cannot escape its impact. Whether caught directly because they fall within the formal disclosure regimes, or indirectly because the corporates and financial institutions they deal with fall within those regimes and/or must justify their ESG credentials to investors and other interested parties, ESG is a key consideration across all markets and sectors. Therefore, ESG considerations cannot be ignored by digital asset businesses, particularly given the environmental concerns that have been highlighted in the press.

For these reasons, it is advisable for any cryptocurrency firm looking to access finance from financial institutions to holistically review its ESG credentials and narrative and consider how it would like to publicly present its performance against traditional ESG metrics. For ESG-conscious financial institutions looking to trade,

invest, or custody digital assets, it will be critical to review the cryptocurrency firm's ESG credentials and narratives to ensure that they are in line with their own ESG objectives, as well as client expectations. And for corporate treasuries exploring the possibility of adding cryptocurrency hedges to their balance sheet, a well-devised strategy and execution is imperative to ensure consistency with internal ESG policies.

Cryptocurrency firms must also bear in mind the strong regulatory framework that continues to build around ESG, and the level of scrutiny in this area. Any ESG-related claims must be fully substantiated and the data upon which they are based must be accurate and reliable.

Annexes

Annex 1:
Members of TLA Blockchain Legal & Regulatory Group

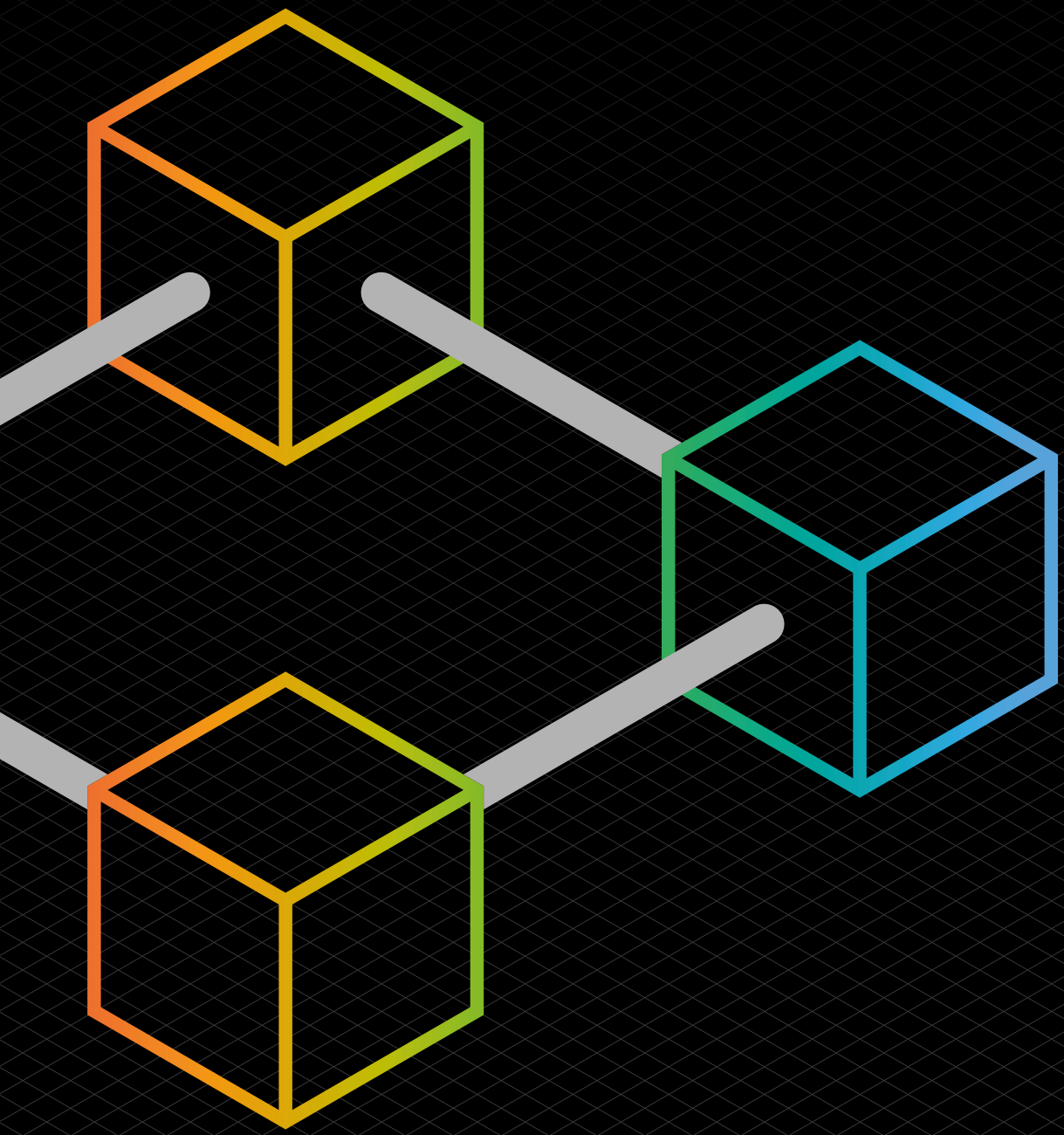
—

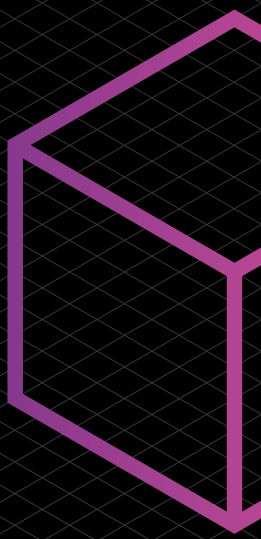
Members
Adi Ben-Ari, Applied Blockchain
Adam Rose, Mishcon de Reya LLP
Adrian Brown, Harney Westwood & Riegels LLP (Cayman Islands)
Akber Datoo, D2 Legal Technology
Albert Weatherill, Norton Rose Fulbright LLP
Alex Cravero, Herbert Smith Freehills LLP
Alex Thornton de Mauroy, Stephenson Harwood LLP
Alexander Murawa, Reed Smith LLP
Alexander Zelinsky, Velvet
Alexandra Clark, New Media Law
Alison Mynott, Dentons & Co
Anna Donovan (Dr.), UCL
Anne Rose, Mishcon de Reya LLP
Antonia Fitzpatrick, Monckton Chambers
Ben Sigler, Stephenson Harwood LLP
Birgit Clark, Baker McKenzie LLP
Brendan McGurk, Monckton Chambers
Brett Hillis, Reed Smith LLP
Brian Gray, Brian Gray London
Byron O'Connor, Infinity Works
Callum Sommerton, Mishcon de Reya LLP
Cassius Kiani, Atlas Neue
Catherine Goodman, Paul Hastings
Catherine Hammon, Osborne Clarke LLP
Ceri Stoner, Wiggin LLP
Chantelle Gough, Hill Dickinson LLP
Charlie Morgan, Herbert Smith Freehills LLP
Charlotte Collins, Latham & Watkins LLP
Charlotte Lyons-Rothbart, Taylor Vinters LLP
Charlotte Wilson, Mishcon de Reya LLP
Ciáran McGonagle, ISDA
Claire Harrop, Freshfields Bruckhaus Deringer LLP
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
Dorothy Livingston, Herbert Smith Freehills LLP
Eitan Jankelewitz, Sheridans
Elena Georgiou, Mishcon de Reya LLP
Estelle Tran, Barclays
Fleur Kitchingman, Herbert Smith Freehills LLP
Francesca Bennetts, Allen & Overy LLP
Gabrielle Tanner, Wiggin LLP
Gary Maw, Irwin Mitchell LLP
Gareth Malna, Stephenson Law LLP
Guy Stevenson, Baker McKenzie LLP
Heenal Vasu, Allen & Overy LLP
Howard Womersley Smith, Reed Smith LLP
Jacob Reilly, Dentons & Co
James Klein, Shoosmiths LLP
Janet Morrison, Diageo
Jason Pugh, D2LegalTech
Jason Rozovsky, R3
Jennifer Anderson, Wiggin LLP

Joey Garcia, Isolas LLP (Gibraltar)
John Shaw, Foot Anstey LLP
Jon Baines, Mishcon de Reya LLP
Jonathan Emmanuel, Bird & Bird LLP
Josie Payne, Wiggin LLP
Julie Farley, Herbert Smith Freehills LLP
Kate Parker, 5 Paper Buildings Chambers
Katie Nagy de Nagybczon, CMS Cameron McKenna Navarro Olswang LLP
Kyle Phillips, Fieldfisher LLP
Laura Douglas, Clifford Chance LLP
Laura Price, Mishcon de Reya LLP
Lawrence Akka, Twenty Essex
Mahmood Lone, Allen & Overy LLP
Marc Jones, Stewarts LLP
Marc Piano, Harney Westwood & Riegels LLP (Cayman Islands)
Marco Dalla Vedova, Dalla Vedova Studio Legale
Martin Dowdall, Allen & Overy LLP
Martin Fanning, Dentons & Co
Martin Hevey, Herbert Smith Freehills LLP
Mary Kyle, City of London Corporation
Matthew Blakebrough, Charles Russell Speechlys LLP
Matthew Farrar, UK Tote Group
Matthew Gregory, Norton Rose Fulbright LLP
Max Nicolaides, Mishcon de Reya LLP
Michelle Howell, Macfarlanes LLP
Nagia Paraschou, Wiggin LLP
Natasha Blycha, Herbert Smith Freehills LLP
Nathalie Hoon, Mode
Niall Roche, Mishcon de Reya LLP
Niara Lee, Mishcon de Reya LLP
Nick West, Mishcon de Reya LLP
Nick White, Charles Russell Speechlys LLP
Nicola Higgs, Latham & Watkins LLP
Niki Stephens, Mishcon de Reya LLP
Nina O'Sullivan, Mishcon de Reya LLP
Oliver Millichap, Mishcon de Reya LLP
Omri Bouton, Sheridans
Patrick O'Connell, Linklaters LLP
Patrick Rennie, Wiggin LLP
Paul Davies, Latham & Watkins LLP
Paul Glass, Taylor Wessing LLP
Peter Dalton, Herbert Smith Freehills 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 Austin, Bird & Bird LLP
Sam Quicke, Linklaters LLP
Sarah Lima, Dentons & Co
Sian Harding, Mishcon de Reya LLP
Stephen Carter, K2 IP
Steven Newbery, 36 Commercial
Stuart Davis, Latham & Watkins LLP
Stuart Whittle, Weightmans LLP

Sue McLean, Baker McKenzie LLP
Sufi Rahimi, Dentons & Co
Thomas Hulme, Brecher LLP
Tom Bleasley, Radcliffe Chambers
Tom Grogan, MDRxTECH
Tom Rhodes, Freshfields Bruckhaus Deringer LLP
Will Foulkes, Stephenson Law LLP
William McSweeney, The Law Society
Will Perry, Monckton Chambers

ANNEX 2:
Specialist Consultees
—
Aaron Wright, Professor, Cardozo School of Law and Co-Founder, OpenLaw
Adi Ben-Ari, CEO, Applied Blockchain
Akber Datoo, CEO, D2 Legal Technology
Alessandro Palombo, CEO, Jur
Cassius Kiani, Chief Product Officer, Atlas Neue
Ciarán 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
Sarah Green, Law Commissioner for commercial and common law, Law Commission





The Law Society

TECH LONDON ADVOCATES

BLOCKCHAIN LEGAL AND REGULATORY