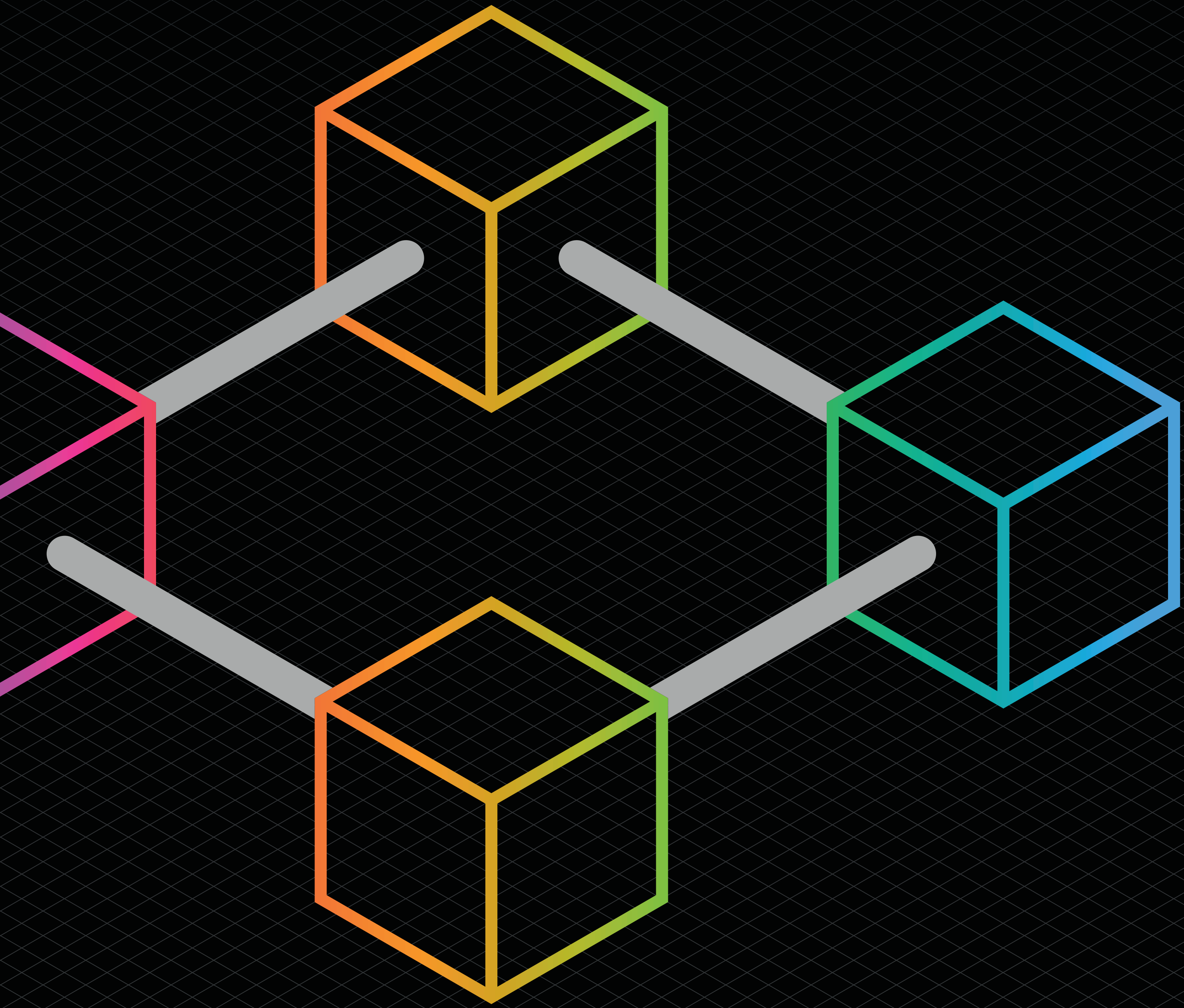
The Law Society

TECH LONDON ADVOCATES
BLOCKCHAIN LEGAL AND REGULATORY

Blockchain: Legal & Regulatory Guidance

Third Edition



Society for Computers & Law
The leading educational charity
for the tech law community
www.scl.org

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 1:
DEVELOPING TECHNOLOGIES

PART 2:
IMPACTS ON THE WIDER LANDSCAPE

1.

Foreword

The third edition of this valuable guidance recognises the transformational changes that have occurred in the digital environment in the three short years since the first edition was published in mid-2020.

The legal community is much in need of the education upon which TLA's Blockchain Legal and Regulatory Guidance focuses.

In my Foreword to the second edition, I suggested that three major developments were imminent. They were (i) the launch of central bank digital currencies, (ii) the widespread adoption of digital transferable documentation, and (iii) the transition from analogue programmes to smart machine-readable documents. In addition to these challenges, lawyers now need to learn quickly to deal with the consequences of the ubiquitous availability of ChatGPT and generative artificial intelligence more generally.

Both the Law Commission and the UK Jurisdiction Taskforce continue to consider and suggest solutions for the legal impediments to the adoption of digital technologies. The TLA's Guidance is now comprehensive and wide-ranging. It will provide the necessary blockchain education for lawyers practising in every field from crime and family to competition and commercial.

I wholeheartedly congratulate the contributors and welcome the third edition of TLA's Blockchain Legal and Regulatory Guidance.

The Rt Hon Sir Geoffrey Vos, Master of the Rolls

Presidential Foreword

Distributed Ledger Technologies (DLTs) are a rapidly evolving set of technologies that have the potential to transform the way we live, work, and do business. The potential applications of DLTs are vast, including finance, supply chain management, and healthcare.

In the legal sector, DLTs can potentially revolutionise how we deliver legal services. For example, DLTs can create secure and tamper-proof records of contracts, wills, and other legal documents. They can also be used to automate the execution of contracts and to provide real-time dispute resolution.

The Law Society is committed to helping our members understand and embrace the potential of DLTs. The third edition of the Blockchain Legal and Regulatory Group provides an up-to-date framework and much-needed guidance on using blockchain in legal services.

Solicitors are critical in assuring new technologies have been designed, developed, deployed and used responsibly and ethically. We have a duty to our clients, the public, and the profession to ensure that new technologies are used in a way that upholds the rule of law and protects the interests of our clients.

As new technologies evolve, solicitors must stay up to date with the latest developments and understand the potential risks and benefits of these technologies. We must also prepare to adapt our practices to accommodate new technologies and ensure that we provide our clients with the best possible advice and representation. This publication will be a valuable resource for our members as they work to understand and apply these ground-breaking technologies.

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 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.[1]

I want to thank the Tech Law Advocates and the Society for Computers and Law for their work producing this publication and the many experts who contributed.

The legal profession is well-placed to play a leading role in developing and using new technologies. We have a long history of upholding the rule of law and protecting the interests of our clients, and we are committed to using new technologies in a way that benefits society.

Lubna Shuja, President of The Law Society

[1] 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>

Introduction

The Guidance

Welcome to this revised and expanded third edition, which updates the 2022 guidance.

In the last edition, I referred to DLT increasingly offering opportunities to build new platforms, products and protocols, from non-fungible tokens (NFTs) and stablecoins to CBDCs and a growth in DeFi. In the past year, we've seen how DLT can be used alongside cloud computing, AI, AR, VR and IoT to build virtual reality spaces in a metaverse to enable users to engage in lifelike interactions with other users in a computer-generated environment. We've also witnessed an increasing interest in DAOs, digital securities and digital assets.

Lawyers continue to assume 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. Lawyers also need to understand that the metaverse is code: ones and zeros, overlaid with vast amounts of data; a manufactured environment, in which all assets are synthetic, created and experienced from within.

For this reason, the focus of this edition is on education. To this end, I am delighted to report that we have collaborated with the Society for Computers and Law (SCL) for this edition and all future editions. SCL is a registered educational charity which promotes the use and understanding of information technology in the context of the law and is celebrating its 50th anniversary this year.

To enhance your learning and content retention, several chapters have an accompanying video which are deliberately designed to enhance your knowledge, understanding and memory of the content covered within each chapter. SCL has created an instructional video which explains how to use the training platform and get your NFT.

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.

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 the 2022 guidance, we heard from experts including the Law Commissioner for Commercial and Common law Professor Sarah Green, and Alessandro Palombo, CEO of Jur. This year, due to a number of train strikes and our desire to do everything in person, we have not heard from any speakers. A full list of experts who have addressed and fed into the Group's work is set out at Annex 1.

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) are practised and implications for areas of litigation: smart contracts, data and governance, blockchain consortia, data protection, intellectual property rights, dispute resolution, competition, tax, ESG and family law. We have also included a new chapter on the emergence and development of so-called decentralised autonomous organisations (DAOs). A high-level overview of DAOs is now included under this Part. We anticipate this overview will be significantly revised in the next edition follow rapid and material developments since publication. 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[2]. 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).*”[3]

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?

At the time of writing, sadly, ChatGPT was not able to predict future trends in the DLT landscape for 2023 (despite numerous attempts at typing in varying commands). As many readers will be aware, the information is based on a training process that finished, ChatGPT tells us, in 2021 so it can’t give you its views on future trends and recent changes in law, guidance or cases will have passed it by.

[2] 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

[3] 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

However, if you ask it to tell you a story about the use of blockchain in 2023 it focuses on DAOs and concludes that "Overall, the future of blockchain in 2023 was bright and full of possibility". The future of blockchain is bright and experts in this space are needed to ensure this technology flourishes and functions effectively.
Throughout 2023 we expect to see a greater focus in six areas in particular.

First, DAOs will continue to gain significant traction for ownership and governance of associated DLT projects and activities, as well as communities with a shared interest to organise and operate absent connection with a technical project. We expect the structuring, governance and associated activities of DAOs to become increasingly complex, particularly as the value of their assets and associated project transaction volumes increase and they and their projects interact more frequently with mainstream financial services. DAOs (or subDAOs) may require regulatory registration or licensing for certain of their activities, permissioning and/or transfer-restricted governance tokens may become more popular and some DAOs must be capable of meeting existing sophistication or wealth requirements to carry out their core functions. Growing public awareness, general market events and incidents affecting (or explicitly not affecting) DAOs during 2022 together with heightened legal, regulatory and judicial considerations will lend to their increasing acceptance. Decentralisation will become critical for the success of DAOs and aspects of the sector more generally, requiring a demonstrable and practical roadmap, careful navigation of multi-jurisdictional legal and regulatory matrices, and carefully considered governance arrangements (including an increasing use of subDAOs). Market sophistication and awareness of the options, advantages and disadvantages of use of corporate vehicles as part of a DAOs structure and operations will increase. In turn, the potential legal, regulatory and tax risks and exposure of governance tokenholders may be amplified and require specialist advice and planning.

Second, the growth in AI and DLT integration. This integration will demonstrate a level of advancement in blockchain technology with a sufficient number of applications.

Third, we expect to see continued growth in digital assets (particularly those which exploit the incredible utility of blockchain technology). This growth will only continue as regulators and policy makers issue further guidance to ensure consumers are adequately protected.

Fourth, we expect to see more transparency and greater corporate governance as DLT becomes a core focus of all businesses. This will involve more thorough, independent, technical due diligence and functional analysis of smart contract code, historical data, and projected performance.

Fifth, the technologies powering the metaverse will get better and faster; and hardware will get smaller and cheaper. These changes will allow brands to access a wider audience as the space becomes more accessible.

Finally, there is an increasing trend where many people feel as though their digital identities are the most authentic version of themselves, and these people spend time and money accordingly. Businesses will increasingly need to consider how they can create value for this new type of customer. We expect that users will gravitate to exchanges that are either regulated or self-custodial (or both) and that consumers will migrate to hardware-secured wallets.

Recent and forthcoming changes to guidance

The UK has taken several steps to embrace DLT and other novel digital technologies.

At the time of writing, since we published the second edition, there have been a number of developments: the Law Commission of England and Wales has published (i) its consultation paper on digital assets (with final recommendations due to be published in 2023); ii) advice to the government on smart contracts; and its law reform recommendations to allow for the legal recognition of electronic versions of trade documents. In addition, the Law Commission has launched a public call for evidence for information about how DAOs can (and should be characterised), and how the law of England and Wales might accommodate them now and in the future; and a review as to which country's laws would apply to a dispute involving digital subject matter, and which courts would have the power to hear the dispute. This review will ensure that English law remains a chosen law and the jurisdiction of choice for commercial parties.

In addition, the UKJT has now turned its attention to the way in which English law can support the issue and transfer of equity or debt securities on blockchain and DLT systems. A legal statement was published early this year following the public consultation event in late 2022. In the UK, we have also seen a flurry of inquiries and calls for evidence from the UK Digital, Culture, Media and Sport (DCMS) Committee and the HM Treasury's consultations on a new regulatory regime for cryptoassets.

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. We can expect accelerated recognition and regulation of this sector during 2023 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.

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. The importance of education in this space cannot be overstated and I am thrilled that SCL are now involved in helping to produce this guidance.

Special thanks goes out to Caroline Gould (CEO, SCL) and Simon Forrester, (Video Producer, SCL) without which this guidance wouldn't be possible.

Special thanks also to all those who have written submissions to this guidance and Sarah Jarvis (Placeworks) for her eagle eye, time and expertise in reviewing and editing this new guidance.

About SCL

Who We Are

SCL is a registered educational charity and the leading UK organisation for those advising and practising within the tech law sector. Our mission is to inform and educate legal professionals and the wider audience on the impact of IT on law and legal practice through the promotion of best practice, thought leadership, and the fostering of a global tech law community.

SCL has an international membership made up of private practice and in-house IT lawyers, consultants, legal technologists, barristers, students, academics, and other tech law professionals.

Our tagline is 'tech law for everyone' and our core values are Education, Collaboration and Community.

What We Do

Events and Training

We provide unrivalled essential training on key tech law topics devised and delivered by experts in the field. From annual updates on Data Protection and IT Contracts, expert half-day masterclasses and conferences dedicated to AI and the Tech of Tech Law, through to networking events for trainees and students and our online informal conversation series, Tea & Tech – there really is something for everyone at every stage of their tech law career.

In addition to our yearly calendar of events, the SCL Tech Law Essentials is a rolling programme of seminars and content in key areas of practice that is consistently updated to ensure that new law and new problems are addressed, whilst ensuring that the enduring essential knowledge and skills tech lawyers need to gather and maintain throughout their careers are covered.

And, finally, there is our flagship Annual Conference which will be a very special event this year as we celebrate our 50th Anniversary. It is a must-attend event for all those interested in law and technology looking to be part of the ever-expanding opportunity that a career in law and technology represents.

News and Editorial

Tech law is a fast-moving sector and it's important to stay up to date, so we present articles, news, blogs and insights from thought-leaders across the sector on our website, e-newsletters and our social media platforms. We also produce a bi-monthly C&L digital magazine and a monthly News Review packed with incisive and relevant content.

Our Community
SCL is proud to foster a thriving and supportive community of legal professionals who come together to share experience, ideas, and expertise. The Society is shaped by its members and the wider community and works hard to offer meaningful support at every career stage, from students to senior partners. Our special interest Groups ensure that relevant topics and important issues are represented and explored and are a fantastic way of getting more involved in the Society and supporting our work.

Our Initiatives
Over the years we have launched many exciting projects and taken part in many valuable collaborations with other organisations.

Our key current initiatives include:
The SCL Adjudication Scheme Adjudication Scheme – a three-month procedure for "technology" disputes.

SCL AI for Schools - an SCL outreach initiative aimed at helping underprivileged 6th form students consider a career in the tech law sector.

The SCL AI Contractual Clauses Project – a project led by the SCL AI Group to draft contractual clauses for AI contracts (with accompanying drafting notes). Currently out for consultation with the SCL membership and launching very soon.

Blockchain Legal & Regulatory Group Report 2023 - SCL has been delighted to be involved in the production of the 3rd edition of the Blockchain Guidance which for the first time includes training videos as well as written guidance.

To find out more about this amazing community please visit scl.org.

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	The European Union's General Data Protection Regulation (EU) 2016/679
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	The UK's retained version of the EU GDPR
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 regulatory treatment of cryptoassets in the UK, 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.

It provides an overview of the current UK regulatory landscape, including identification of gaps and issues within the existing framework, regulatory intervention and enforcement to date and the broader legal context for treatment of cryptoassets in the UK. It also sets out an overview of proposed future UK regulation and a brief outline of the wider international regulatory context.

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 UK regulatory approach to cryptoassets and how this fits into a global context.

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 and On Chain Compliance

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.

As an update to last year's chapter, this section covers a conceptual change of focus away from 'intermediaries' to the underlying technology to deal with this principal compliance risk. 'Embedded supervision' is a term used by many, but this is a natural first step to embedded compliance as a concept.

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 or within the United Kingdom Gambling Act 2005.

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. Key takeaways are the harsh terms and conditions to expect as a participant on a social token platform and the regulatory issues to watch out for when engaging with social tokens.

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.

DAOs

This high-level overview introduces the concept of a DAO, key features, the importance and practicability of the concept of decentralisation, operational elements, use cases, legal, regulatory and tax considerations and current trends. DAOs are rapidly evolving and maturing and the subject of fast-moving legal, regulatory and judicial treatment. This chapter will be significantly revised in the next edition.

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.

Blockchain and Family Law

This chapter considers the issues arising within the voluntary settlement process, things for new couples to be aware of, and what should be considered when attempting to reach an agreement or inviting a Court to become involved.

The Legal and Regulatory Impacts of Non-Centralisation

This chapter focuses on how non-centralised networks can disrupt P2P platforms by helping to solve their unique challenges, and the potential legal and regulatory hurdles arising from this disruption.

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. Clarity as to the territorial scope of these regimes would be particularly welcome. In particular, it is not clear whether the territorial scope in relation to activities relating to fiat-linked stablecoins will differ form that for activities in relation to other cryptoassets.

- 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 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, whilst supporting innovation.

- To aid certainty, legislation and/or regulatory guidance should also be provided clarifying which regulatory requirements apply to different types of cryptoassets, to avoid unhelpful overlap between different regulatory regimes intended to regulate different types of cryptoassets (e.g. security tokens, digital settlement assets and other qualifying cryptoassets, respectively).

- 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”, as well as new cryptoasset activities that are proposed to be captured within the expanded regulatory perimeter.

- 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, the FMI sandbox should be used to assess how the UK legislative and regulatory framework for post-trade infrastructure needs to be adapted to facilitate market adoption of DLT technology and adapt relevant laws and regulations accordingly. 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.

Law Society & TLA Activities:

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

Types of cryptoassets, NFTs and Social Tokens

- The key recommendations of a few types of cryptoassets have significant crossover with other section of the guidance. We recommend that an analysis shouldbe done at the outset of any project to consider a number of legal, technical andcommercial 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[4].

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?

[4] Smart contracts | Law Commission. Accessed 02.11.21.

- 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.

Blockchain and Family Law

Errors can be avoided through educating legal practitioners and judges about cryptoassets and how they interact with technology and the financial world. Terminology such as wallets, public/private keys, trading accounts, can help understand what we are advising on day to day.

There should be a standard glossary of terms provided to help with order templates. This could be incorporated into the Master Orders that we have for financial proceedings and Children Act proceedings. These definitions can be prepared by those within family law who are experienced in cryptoassets, of which there are more now than there were five years ago.

Caution should be placed on those who have entered this community within the last 24 months claiming to be experts. There are many who consider cryptoassets as a quick way to enter into the High Net Worth community, particularly when there were significant spikes in the value of these assets both in 2017 and 2020. As has already been illustrated, those values can drop just as quickly. This tends to result in interest diminishing and those with less experience disappearing to another popular topic. There needs to be consistency with engagement in cryptoassets, whether they are going through a spike or a drop in value, as their volatility means the value will swing back and forth over many years.

1

Part 1: Developing Technologies

Section 1

An Overview of DLT

Section 1: An Overview Of DLT

Tom Grogan, MDRxTech LLP; Water Hernandez-Cruz, Mishcon de Reya LLP

For readers less familiar with the concepts explored in this guidance, this section gives an overview of distributed leger technology (DLT). It shows how the use of ledgers has evolved, 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.

The evolution of ledgers

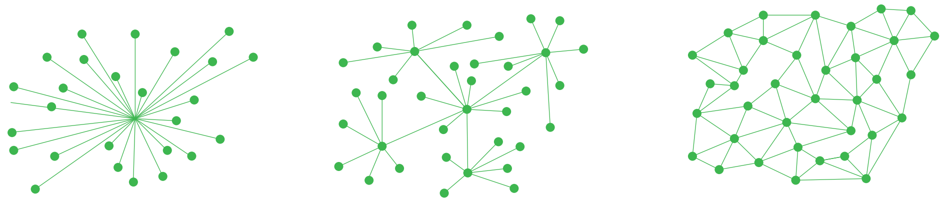
DLT refers to a group of technologies that use different techniques and structures to store, synchronise and maintain a shared ledger of digital records across a network of computing centres.

The idea of maintaining a ledger is not a new one. The earliest ledgers date back to c.4,000BC in Mesopotamia. These ledgers were kept on clay scripts or carved into stone, and were used to record and demonstrate definitive ownership, and the transfer of ownership, of crops in storage. Recording the ownership and movement of value has been a central tenet of human civilisation ever since. The form and structure of these ledgers however has evolved (and continues to evolve) with time.

The Mesopotamian example describes what we now call a centralised ledger (see Fig 1 below), in which a single definitive ledger exists within an ecosystem. In many circumstances, such centralised ledgers are effective, and many 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 becomes 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 ledgers. These intermediaries may for example be financial institutions, which keep and maintain ledgers relating to our finances. Decentralised ledgers, just like their centralised cousins, are widely used today but also have their own drawbacks. They too have points of failure which can have widespread impact on 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 this intermediary causes loss to its stakeholders through negligence or fraud, those stakeholders often 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.



Centralised

Decentralised

Distributed

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.

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 Task Force (FATF), **cryptoassets** are in this guidance 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 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.

i. Exclusivity
To enable network participants to exclusively control 'their' records or cryptoassets, 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.

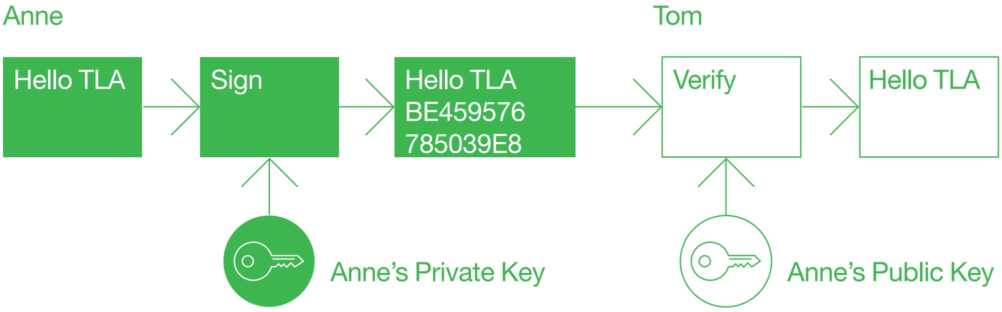


Fig 2 – Public key or asymmetrical cryptography-enabled messaging

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 Coin (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 (3) 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 below for some high-level examples of consensus protocols.

2. Consensus protocols

A range of different consensus protocols might be adopted by DLTs. The following is a 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. In 2022 we saw the Ethereum Foundation complete The Merge, leading to the adoption of proof of stake by the Ethereum blockchain network. Other well-known implementations of proof of stake include Stellar, DASH and NEO.

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 a majority of validators reject a proposing validator's ledger entry, the proposing validator loses its lock-up.

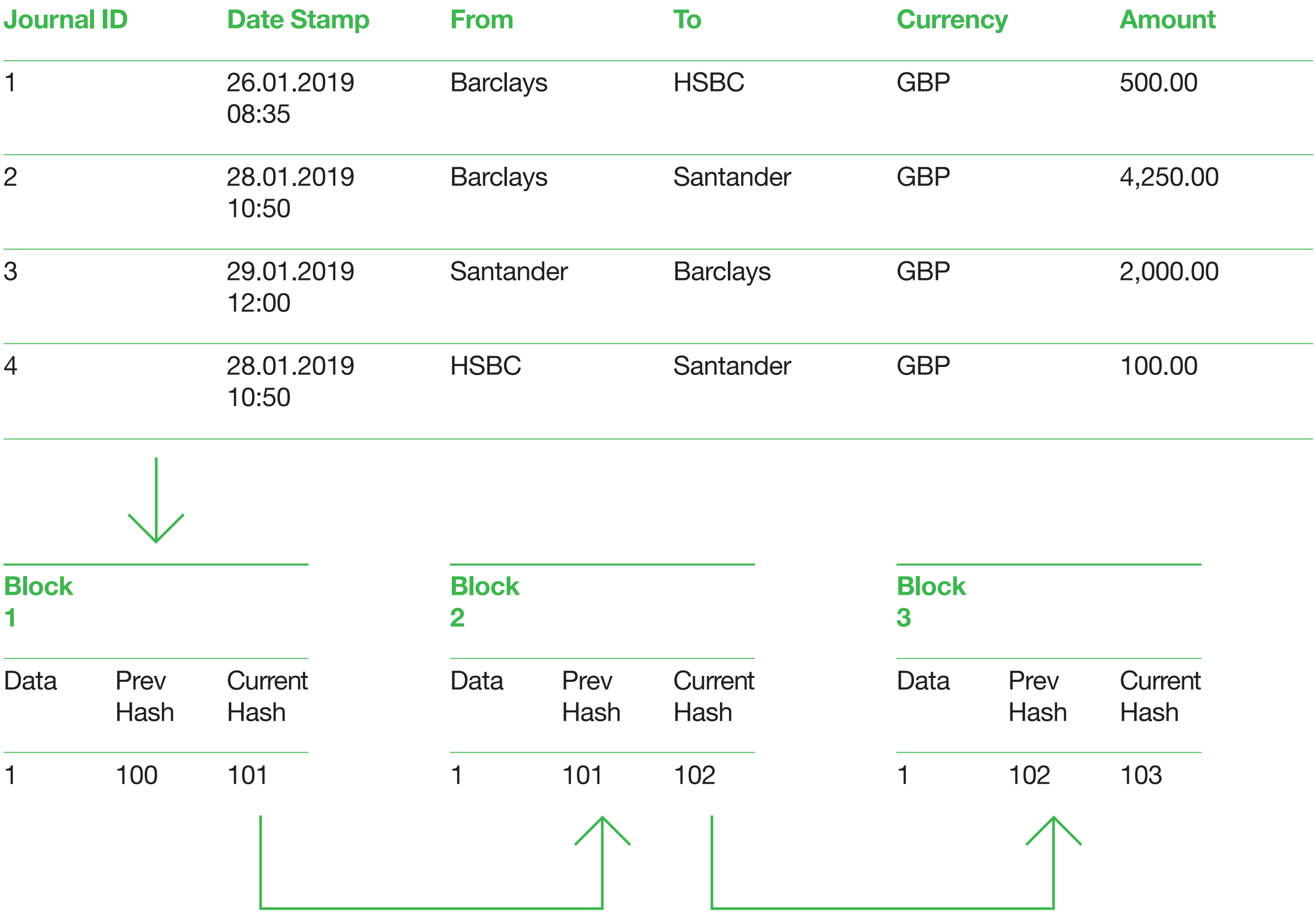
In addition to deterring validators from proposing fraudulent new entries (for fear of losing their lock-up), proof of stake DLTs also ensure that the state of their ledger is dictated by those invested in them – those investors will wish to ensure the integrity of the ledger as, if doubt is cast upon 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 is blockchain, which 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.



Journal ID	Date Stamp	From	To	Currency	Amount
1	26.01.2019 08:35	Barclays	HSBC	GBP	500.00
2	28.01.2019 10:50	Barclays	Santander	GBP	4,250.00
3	29.01.2019 12:00	Santander	Barclays	GBP	2,000.00
4	28.01.2019 10:50	HSBC	Santander	GBP	100.00

Block 1

Data	Prev Hash	Current Hash
1	100	101

Block 2

Data	Prev Hash	Current Hash
1	101	102

Block 3

Data	Prev Hash	Current Hash
1	102	103

Fig 3 – Blockchain structure

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:

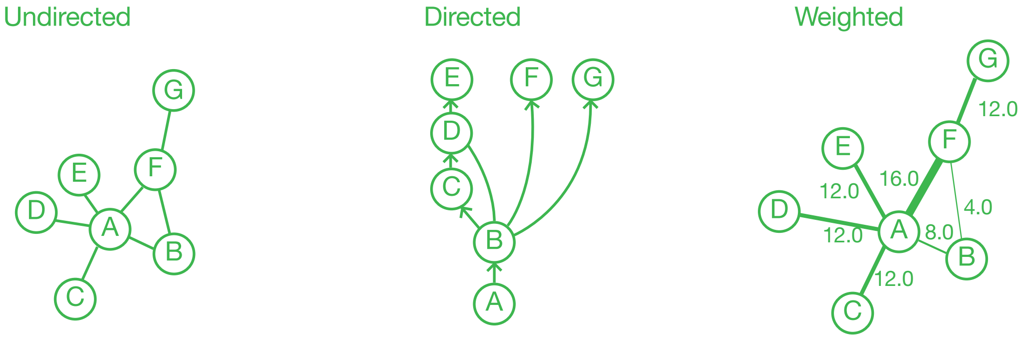


Fig 4 – Forms of acyclic graphs

- **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. The application of DAGs 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 is an alternative DLT and close cousin of the directed acyclic graph, developed by Leemon Baird in 2016.

Hashgraph is perhaps best known for its so-called ‘gossip protocol’, whereby every node spreads ‘gossip’ regarding its information (i.e. records or transactions, known in Hashgraph as ‘events’) and events it has heard (via the gossip protocol) from others, to two randomly chosen neighbourswhich 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. A potential disadvantage is Hashgraph’s inherent assumption that fewer than a third of nodes are bad actors (i.e. those who forge, delay, replay and drop incoming and/or outgoing events): if this is not (or cannot be reliably be proved to be) the case, security concerns may arise.

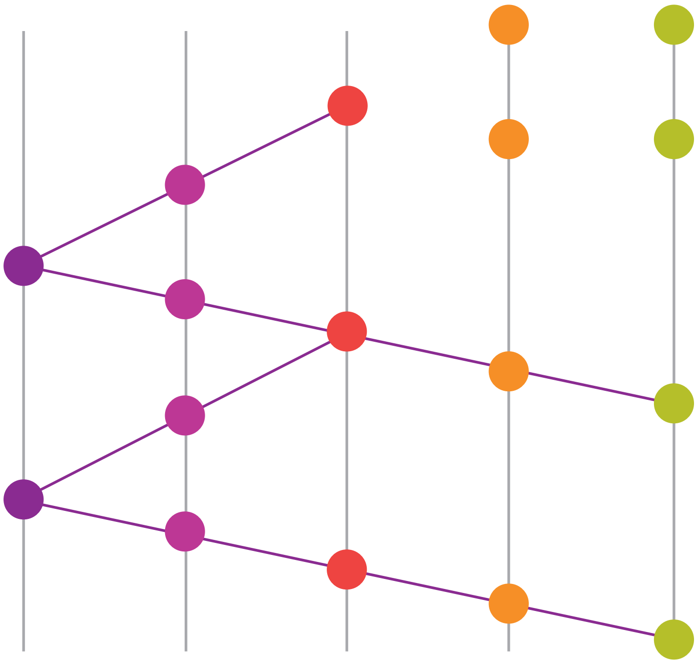


Fig 5 Hedera Hashgraph structure

4. Layer 2 protocols and beyond

In recent years so-called layer 2 protocols have emerged as a key feature of the DLT ecosystem. Layer 2 protocols are separate protocols which may or may not themselves be DLTs, which operate on top of underlying DLTs. Polygon is perhaps the most well known layer 2 protocol, which operates on top of the Ethereum blockchain.

Typically, a layer 2 protocol receives and processes user transactions, and periodically writes aggregated updates to the underlying DLT. In this way, layer 2 protocols are often seen as a scaling solution to DLT, enabling faster settlement times and lower transaction fees. They are not without their drawbacks, and thoughtful implementations should consider how best to obtain the security benefits associated with DLT while also availing themselves of the scalability afforded by layer 2 protocols.

In more recent times we are beginning to see the emergence of so-called layer 3 solutions. In these implementations we must trade-off between additional complexity and benefits.

To be clear, layer 2 or layer 3 procotols need not be themselves distributed ledgers, and careful thought should be given as to the most appropriate structure for a given implementations.

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" for the Bitcoin public blockchain) is time-consuming and costly to run.

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

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

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

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

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:

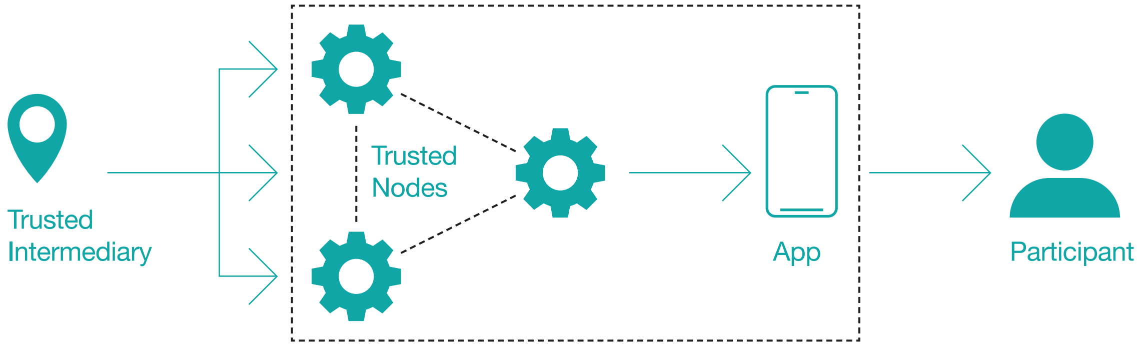
- **Trusted intermediary:** the trusted intermediary downloads the blockchain software and sets up the nodes that comprise the network. It is not necessary to have only one trusted intermediary, although this is common; the process may in fact involve multiple trusted intermediaries with authority over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

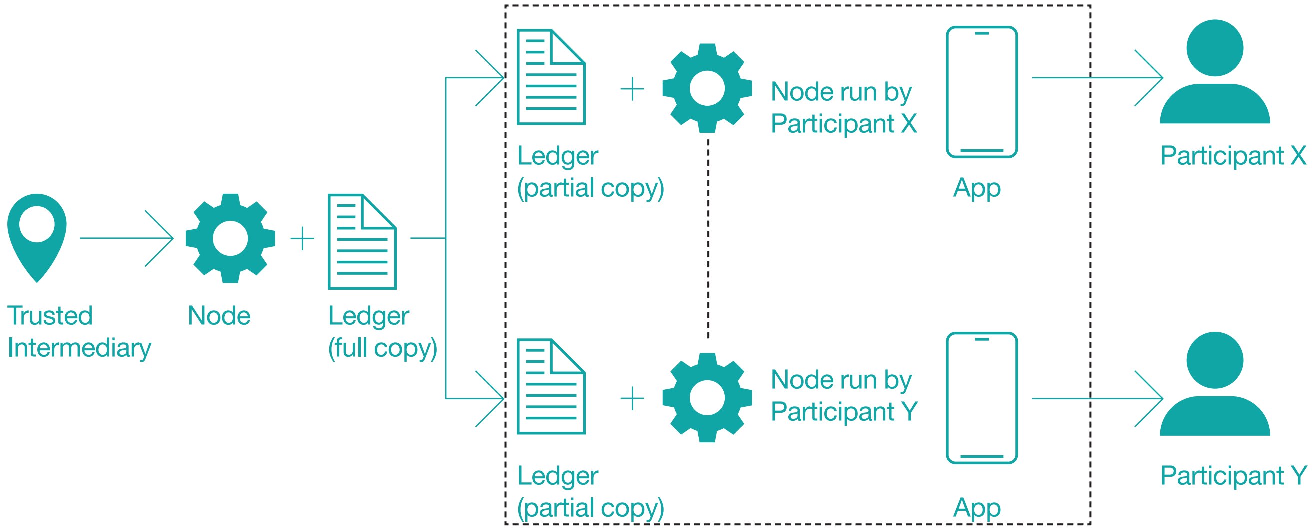
- **Participants:** the participants access the trusted intermediary's nodes via the app. Using the app, participants can send data to be recorded on the private blockchain and view the data recorded on the private blockchain.

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 10). 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

Chloe Kearns, Morrison Foerster; Laura Douglas, Clifford Chance LLP; Martin Dowdall, Sidley Austin LLP

Introduction

At present, there is no specific UK regulatory regime for cryptoassets, other than in relation to anti-money laundering **(AML)** and counter-terrorist financing requirements for cryptoasset exchange providers and custodian wallet providers. Currently, the UK's approach to the 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 transferable securities, a deposit, electronic money (**e-money**) or another type of regulated financial instrument.

However, the scope of the UK's regulatory regime for cryptoassets will soon expand significantly. In particular, forthcoming legislation will extend the application of existing payment services and e-money regulation to fiat-referenced stablecoins and bring most cryptoassets within the existing financial promotions regime. The UK government is also consulting on a broader regime for the regulation of cryptoassets.

This chapter sets out:

— an overview of the current UK regulatory landscape, including:
- gaps and issues within the existing framework;
- regulatory intervention and enforcement to date; and
- the broader legal context in the UK;

— an overview of proposed future UK regulation;

— a brief outline of the wider international regulatory context; and

— certain recommendations for UK regulators when designing the regulatory framework.

Current UK regulation

Categorisation of cryptoassets

The UK's current approach to regulating cryptoassets is articulated in the Final Guidance on Cryptoassets[5] **(the Final Guidance)**, published by the Financial Conduct Authority **(FCA)** in July 2019. The Final Guidance identifies the following categories of cryptoassets, which may be 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)**[6], such as shares, debentures or units in a collective investment scheme. Whether a cryptoasset constitutes a security token, i.e., a specified investment, will generally need to be assessed on a case-by-case basis.[7]

[5] FCA, Guidance on Cryptoassets Feedback and Final Guidance to CP19/3 (Policy Statement, PS19/22) <https://www.fca.org.uk/publication/policy/ps19-22.pdf> Accessed December 2022.

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

[7] The Final Guidance sets out 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 will often require the exercise of judgement when determining the extent to which a cryptoasset's substantive characteristics are similar to a particular type of specified investment.

B. E-money tokens

E-money tokens are cryptoassets that meet the definition of e-money under the Electronic Money Regulations 2011 **(EMRs)**.[8] For this purpose, e-money is defined as:

i. electronically (including magnetically) stored monetary value as represented by a claim on the issuer;
ii. which is issued on receipt of funds for the purpose of making payment transactions; and
iii. 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 the definition of e-money give rise to uncertainties, such as when a cryptoasset is considered "accepted as a means of payment" by a party. Additional ambiguities arise from the fact that the term "monetary value" is not defined, although this term is commonly understood to mean fiat currency. This particular characteristic may change during the life of a cryptoasset, meaning that a cryptoasset may become, or cease to qualify as, e-money at some point after its issuance.

The Final Guidance indicates that cryptoassets may move between categories throughout their lifetime.[9] This creates particular uncertainties, as an e-money issuer generally requires authorisation 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 the relevant regulatory permissions. As such, different ongoing conduct of business rules will apply depending on the type of cryptoasset.

Similar uncertainties arise in the case of 'hybrid' tokens which exhibit characteristics of more than one category of cryptoasset (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. In practice, many 'cryptocurrencies' marketed to consumers currently fall within the category of unregulated tokens. There are, however, some exceptions to this, such as cryptocurrency derivatives.

Overview of current UK regulation

As noted above, cryptoassets that constitute e-money tokens will be subject to the EMRs. Below, we have set out a high-level overview of existing regulatory rules which apply to security tokens and other cryptoassets that fall within the regulatory perimeter, and to firms dealing with cryptoassets.

A. Rules applying to security tokens

Different types of security tokens are subject to different regulatory rules. For example:

i. security tokens meeting the definition of "transferable securities" under the UK version of the Markets in Financial Instruments Regulation **(MiFIR)**[10] are within the scope of prospectus rules and requirements;

[8] The Electronic Money Regulations 2011, SI 2011/99.
[9] The Final Guidance, paragraph 22.
[10] Regulation (EU) No 600/2014 of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Regulation (EU) No 648/2012 (Retained EU Legislation).

ii. security tokens that do not meet the MiFIR definition of transferable securities (for example because there are contractual restrictions on transfer) may nevertheless fall within the UK crowdfunding regime;[11]
iii. 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.[12]

Determining the applicable regulatory rules for a given type of security token will be a question of fact requiring careful case-by-case analysis. The position is complicated by the lack of clarity over the meaning of some key terms in the relevant legislation.[13] A general clarification as to the meaning of "instruments of payment", as used in the definition of "transferable securities", would provide greater certainty to market participants.

B. Cryptocurrency derivatives

In April 2018, the FCA published a statement indicating that cryptocurrency derivatives may be financial instruments for the purpose of the EU Markets in Financial Instruments Directive **(MiFID2)**[14] (but that it did 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 be under Section C of Annex I MiFID2. The FCA should consider providing clarity on its position with respect to the classification of cryptocurrency derivatives; this point would have significant ramifications for firms that deal in cryptocurrency derivatives, as different rules apply to different classes of derivatives under MiFID2.

In the absence of additional guidance from the FCA, it seems likely that cryptocurrency derivatives will 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 in question meets the conditions. For example, cryptoassets representing "rights to receive services" may not count as relevant underlyings for the purposes of Section C(10); similarly, not all physically-settled derivatives will fall within Section C(10). Alternatively, cash-settled contracts for differences (CFDs) 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 MiFID2 financial instruments, consideration would also need to be given as to whether such cryptoasset derivatives are nevertheless specified investments falling within one of the broader categories of futures, options and CFDs under the RAO.

The FCA has provided some guidance that would be relevant where a cryptoasset derivative falls within a broader category of specified investments. Recently, the FCA introduced new conduct of business rules restricting how firms can sell, market or distribute CFDs and similar products (including those that reference cryptocurrencies) to retail consumers.[15] On 6 January 2021, it also introduced a ban on the sale, marketing or distribution of derivatives and exchange of traded notes referencing cryptoassets to retail clients.[16]

[11] Related financial promotion rules for non-readily realisable securities may also apply to other specified investments.

[12] The Alternative Investment Fund Managers Regulations 2013, SI 2013/1773. A security token of this kind 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.

[13] For example, the term "instruments of payment" as used in the definition of "transferable securities" is not clearly defined. The test for determining whether a particular cryptoasset structure qualifies as an AIF is also complex, despite the existence of relevant case law and FCA guidance.

[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. Post-Brexit, MiFID2 has been on-shored via statutory instruments and amendments to the FCA Handbook and the Prudential Regulation Authority Rulebook.

[15] 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 December 2022.

[16] FCA, Prohibiting the sale to retail clients of investment products that reference cryptoassets (Policy Statement PS20/10, October 2020) <https://www.fca.org.uk/publication/policy/ps20-10.pdf> Accessed December 2022; see also COBS 22.6.

C. Money Laundering Regulations

Regulators, including the FCA, have highlighted the risk of cryptoassets being used for financial crime.[17] Since January 2020, "cryptoasset exchange providers" and "custodian wallet providers" carrying on business in the UK have needed to be registered with the FCA and to comply with AML-related requirements set out under the UK's Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 **(MLRs)**.[18] Registration involves a detailed application process and the majority of applicant firms to date have withdrawn their application or been refused registration by the FCA. The FCA recently provided feedback to assist applicants in distinguishing between good- and poor-quality registration applications.[19]

In August and September 2022, the MLRs were amended to bring in additional requirements for registered cryptoasset businesses (i.e., cryptoasset exchange providers and custodian wallet providers that are registered with the FCA). Among other things, the amendments have:

i. introduced a change of control regime for the acquisition of registered cryptoasset businesses, which requires persons who wish to acquire or increase their existing control over such businesses to seek prior approval from the FCA before an acquisition can take place; and[20]
ii. extended the Financial Action Task Force's Recommendation 16 (known as the "Travel Rule") to cryptoassets. From 1 September 2023, registered cryptoasset businesses will be required to send and record information (including names and account numbers) relating to the originator and beneficiary of relevant cryptoasset transfers.[21]

Who falls within scope of the MLRs?

The definition of "cryptoasset" introduced under the MLRs is broad, encompassing both regulated and unregulated types of cryptoassets.[22] There are, however, some uncertainties as to what businesses and activities are captured by the definitions of "cryptoasset exchange provider" and "custodian wallet provider".[23] In particular:

i. The definition of "cryptoasset exchange provider" includes firms "exchanging, or arranging or making arrangements with a view to the exchange of" (i) cryptoassets for money, (ii) money for cryptoassets or (iii) one cryptoasset for another. HM Treasury's **(HMT)** response to its consultation on the relevant rules suggests that this language is intended to capture firms facilitating peer-to-peer exchange services or completing, matching, or authorising a transaction between two people. However, the words "arranging" or "making arrangements with a view" are also used in Article 25 RAO, where they carry a different meaning. In the context of Article 25 RAO, 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. Guidance published by the Joint Money Laundering Steering Group **(JMLSG)**[24] aims to provide practical advice on this point but cautions that various types of activities may require case-by-case analysis.

[17] See, for example, the FCA's Dear CEO Letter dated 11 June 2018 ("Cryptoassets and financial crime") <Dear CEO letter: Cryptoassets and financial crime (fca.org.uk)> Accessed December 2022.
[18] Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, SI 2017/692. Cryptoasset exchange providers and custodian wallet providers also fall within the regulated sector for the purposes of the Proceeds of Crime Act 2002 and the Terrorism Act 2000. As a result, they are required, in practice, to report knowledge or suspicions of money laundering and/or terrorist financing to the National Crime Agency via Suspicious Activity Reports. Separately, from 30 March 2022, registered cryptoasset businesses have been required to submit an Annual Financial Crime Report (the "REP-CRIM return") to the FCA.
[19] FCA, Cryptoasset AML/CTF regime: feedback on good and poor quality applications (25 January 2023) <https://www.fca.org.uk/cryptoassets-aml-ctf-regime/feedback-good-poor-quality-applications> Accessed March 2023.
[20] Regulation 60B and Schedule B MLRs.
[21] See Part 7A MLRs.
[22] "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."
[23] Regulation 14A MLRs.
[24] 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 2022. Practitioners may also wish to refer to guidance published by the Financial Action Task Force (October 2021) <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets-2021.html> Accessed December 2022.

ii. 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.

As regards the territorial scope of the MLRs, the FCA had stated that:

> *"just because a firm interacts with UK customers, does not mean it needs to be registered with us and adhere to the MLRs under the regime. The current regulatory scope for cryptoasset activities, which is set out in legislation, means overseas firms can relatively easily undertake cryptoasset activity in the UK but remain outside of the FCA's remit – which has created risks of regulatory arbitrage and a confusing position for consumers and firms."*[25]

On that basis, it seems the current focus of the FCA under the MLRs regime is on firms that provide cryptoasset exchange and custodian wallet services from the UK. However, the forthcoming extension of the UK regulatory financial promotions regime and licensing framework to capture cryptoassets more broadly will also impact non-UK firms seeking to promote or provide cryptoasset services on a cross-border basis into the UK (as discussed further below).

D. Licensing and conduct of business requirements

The licensing and conduct of business requirements that apply to firms dealing with cryptoassets differ depending 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 activity that the firm is carrying on in relation to the cryptoasset. A brief overview of the position is set out below.

i. Licensing and registration

Firms carrying out regulated activities in the UK with respect to security tokens or regulated cryptocurrency derivatives will need to be authorised under FSMA with the relevant regulatory permissions, just as they would when carrying out activities with respect to traditional types of securities. Issuers of e-money tokens will need to be authorised or registered as such under the EMRs (unless authorised as a credit institution) and firms dealing with e-money tokens may be carrying out regulated payment services requiring authorisation or registration under the Payment Services Regulations 2017 **(PSRs)**.[26] To carry out 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 still required to register with the FCA under the MLRs (see above). Whilst not a formal licensing regime, FCA registration does involve the submission of detailed information about the firm and the FCA will only register a firm if it is satisfied the firm, its beneficial owners, officers, and managers are "fit and proper".

[25] FCA written evidence to the Treasury Committee's inquiry into the cryptoasset industry (September 2022) <https://committees.parliament.uk/work/6843/the-cryptoasset-industry/publications/written-evidence/?SearchTerm=financial+conduct+authority&DateFrom=&DateTo=&SessionId=> Accessed December 2022.

[26] Payment Services Regulations 2017, SI 2017/752.

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[27] 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.

ii. 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. However, they do embed certain assumptions about how financial markets operate that do not necessarily hold true of cryptoassets. This creates 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.

Issues and gaps under existing UK regulation

A lack of clarity under existing regulation gives rise to some uncertainty as to the scope and application of those rules. Two specific examples are set out below. More generally, as can be seen from the overview set out above, the scope of existing regulation is very limited. In general, many ‘cryptocurrencies’ constitute unregulated tokens and are not currently subject to existing regulation (beyond the MLRs regime described above, if applicable). There are a number of key areas in which there is currently no regulation. At present, for example, UK financial services regulators do not have conduct, prudential or consumer protection powers over the cryptoasset market. The FCA has warned that the lack of regulation gives rise to potential harm to consumers and market integrity.[28] Further, the Bank of England **(“BoE”)** has highlighted the need for enhanced regulatory frameworks to manage the systemic risks that will emerge should cryptoasset activity and its interconnectedness with the wider financial system continue to develop.

A. Custody of cryptoassets
As previously noted in this section, there remains uncertainty as to which services and activities, other than holding private keys for clients, may qualify as custody or safekeeping and administration of cryptoassets. At present, custody of cryptoassets is a regulated activity in the UK only in respect of cryptoassets that are regulated financial instruments. However, for these types of regulated cryptoassets, further questions arise about how FCA client asset rules under CASS[29] might apply. This is particularly the case, for example, where a regulated custodian safeguards a private key but cannot be said to safeguard the

[27] 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 2022.
[28] Aside from the harms caused by the promotion of cryptoassets to consumers, the FCA has recently warned, among other things, that the lack of safeguarding requirements for cryptoassets may allow firms to lend consumer assets to third parties to generate revenue, potentially putting those assets at risk; and that the absence of regulation relating to the trading of cryptoassets means that the cryptoasset market may be more vulnerable to traditional forms of market manipulation. See the written evidence submitted to the Treasury Committee by the FCA in September 2022.
[29] The Client Assets sourcebook, the FCA Handbook.

cryptoasset itself, or where the cryptoasset may not be considered property (or an "asset" of the client) from a legal perspective.

B. Settlement of transactions in cryptoassets and implications of CSDR book-entry form requirements
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.

There are practical challenges in applying certain existing regulatory requirements governing post-trade market infrastructure to cryptoassets, including the Central Securities Depositories Regulation **(CSDR**). In particular, cryptoassets that are transferable securities and are traded or admitted to trading on a MiFID trading venue are subject to requirements under CSDR for the securities to be recorded in book-entry form in a central securities depository (**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, subject to certain reporting requirements. However, this may not always be a viable practical solution. The new UK FMI sandbox (as discussed below) is expected to allow for possible solutions to these types of practical issues to be explored in a controlled environment.

The broader legal context in the UK

It is important for market participants to understand how cryptoassets are treated from a broader legal perspective, in addition to understanding the regulatory characterisation and treatment of cryptoassets. Key issues include whether English law recognises cryptoassets as property and, if so, how they can be transferred, how security can be taken over them and how ownership rights can be enforced.

A. The treatment of cryptoassets as property
In November 2019, the UK Jurisdiction Taskforce issued a statement (the **"Legal Statement"**), which confirmed that cryptoassets are capable of being owned and transferred as property under English law and that smart contracts are capable of constituting binding legal contracts. Whilst the Legal Statement itself is not binding, these questions have also been considered by the English courts, notably in the case of AA v Persons Unknown,[30] 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. Subsequent decisions have likewise recognised that cryptoassets are capable of being treated as property.

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

Not every use of DLT will result in creation of a cryptoasset that qualifies as property under English law. A clear example is where DLT is used for record keeping purposes only, for example, if DLT is used in the book-building phase of a digital securities issuance. In other cases, a cryptoasset (or crypto-token) may be a digital record of ownership 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.[31] 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 the FCA's client asset rules.

In July 2022, the Law Commission of England and Wales published a Consultation Paper setting out its recommendations for law reform in respect of certain digital assets as objects of property rights, inviting feedback by 25 November 2022.[32] The Consultation proposed introducing a third category of personal property called "data objects", intended to deal specifically with digital assets, which do not seem to fit neatly into either of the two existing categories of property under English law, namely things in possession and things in action. Whilst to date, English case law has been flexible enough to recognise that digital assets including Bitcoin and non-fungible tokens **(NFTs)** can attract property rights, the sub-classification as a particular type of property will impact questions such as how to establish ownership of the asset, how it is transferred, whether the asset can be held on trust and how security can be granted over it, how it is treated in insolvency and what remedies may be available in a claim involving cryptoassets.

B. Issues relating to conflicts of laws
There are often difficult questions about which law will apply to proprietary aspects of dealings in cryptoassets – namely, 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.

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 sufficient.

Regulatory intervention and enforcement

Given the narrow scope of the UK cryptoasset regulatory regime, the FCA currently has limited powers to intervene or take enforcement action against cryptoasset businesses.

To date, as might therefore be expected, there has been limited public intervention or enforcement action of this kind. In June 2021, the FCA publicly imposed requirements on one FCA-authorised firm operating in the cryptoasset industry, stipulating that the firm was not permitted to undertake any regulated activity in the UK without the FCA's prior consent. It also warned that another leading cryptoasset business may have been providing financial services or products in the UK without the required authorisation. Further, in March 2022, the FCA issued a warning to operators of crypto ATMs in the UK (none of whom have been registered with the

[31] The Law Commission Consultation Paper mentioned below proposes imbuing such crypto-tokens with "property" status in their own right (in a similar way to the fact that a piece of paper is property in its own right, regardless of what is written on it).
[32] Law Commission, Digital Assets: Consultation paper (Consultation paper 256, July 2022) <Digital assets | Law Commission> Accessed December 2022.

FCA under the MLRs to date) to shut down their machines or face enforcement action. It has since announced that it is working with law enforcement partners, including local police forces, to “disrupt and disable illegal Crypto ATMs” and that it has exercised its powers to enter and inspect the premises of certain suspected illegal operations.[33]

Beyond the limited intervention set out above, the FCA’s actions have largely focused on raising consumer awareness of the risks associated with investing in cryptoassets,[34] as well as reminding authorised firms with exposure to cryptoassets of the need to, among other things,[35] manage financial crime risks, and managing the regulatory ‘gateway’ by refusing numerous applications for registration under the MLRs where firms were found not to have met the required standards (and, in some cases, working with firms to improve their systems and controls).

Looking ahead, we expect to see an uptick in intervention and enforcement action when the future UK regulatory changes outlined below are implemented and, in particular, once the financial promotions regime has been extended to unregulated cryptoassets. Consistent with this, the FCA warned in a statement published in February 2023 that it will take “robust action” against firms breaching the financial promotions requirements for cryptoassets once they come into force.[36]

Future regulation in the UK

Addressing key gaps in existing regulation has been a priority for HMT, the FCA and the BoE, and the UK is due to implement significant changes to the existing regulatory regime. An overview of the expected changes is set out below. Further, as explained below, the UK is consulting on the shape of a wider UK regulatory framework for cryptoassets.

<u>Stablecoins and central bank digital currencies (CBDCs)</u>

A. Regulation of fiat-linked stablecoins

    In April 2022, HMT published its response to its consultation on the UK regulatory approach to cryptoassets, stablecoins, and the use of distributed ledger technology in financial markets (the **Stablecoin Consultation Response**).[37]

    The Stablecoin Consultation Response confirmed that HMT plans to extend regulatory authorisation, governance, conduct of business, and reporting requirements under existing payment services and e-money regulations to include certain activities relating to fiat-linked stablecoins. HMT has identified the regulation of stablecoins as a priority given the potential for stablecoins to become a widespread means of payment.

    The Stablecoin Consultation Response’s proposals are limited to stablecoins that reference a single fiat currency or a basket of fiat currencies. However, these proposals will apply to firms engaged in “activities that issue or facilitate the use of stablecoins used as a means of payment” as well as firms that provide or arrange custody of stablecoins.

    Additionally, the definition of “electronic money” under the EMRs will be extended to include fiat-linked stablecoins. As a consequence, holders of such

[33] FCA press release (February 2023) “FCA takes action against unregistered crypto ATM operators in Leeds” Accessed February 2023.

[34] See, for example, the consumer warnings issued by the FCA on 11 January 2021 and 11 May 2022, alongside comments in various FCA speeches.

[35] See the notice issued by the FCA on 24 March 2022 to all authorised firms with exposure to cryptoassets; the joint statement on sanctions and the cryptoasset sector issued on 11 March 2022; and the Dear CEO Letter titled “Cryptoassets and financial crime” issued on 11 June 2018.

[36] FCA, “Cryptoasset firms marketing to UK consumers must get ready for financial promotions regime” (February 2023) <Cryptoasset firms marketing to UK consumers must get ready for financial promotions regime> Accessed February 2023.

[37] HMT, “UK regulatory approach to cryptoassets, stablecoins, and distributed ledger technology in financial markets: Response to the consultation and call for evidence” (April 2022) <O-S_Stablecoins_consultation_response.pdf (publishing.service.gov.uk)> Accessed December 2022.

stablecoins will have a statutory right to redeem their coins on demand and at par value. In recognition of the fact that the holder of a stablecoin may not always have a relationship with the issuer, the proposals provide that holders should generally be able to make a claim against either the issuer of the stablecoin or the customer-facing entity as appropriate. Issuers of fiat-linked stablecoins will also need to safeguard funds received in exchange for stablecoins on a one-to-one basis.

References to custodial services are intended to capture wallet providers as well as exchanges offering similar services. Such firms will be subject, among other vthings, to:

- prudential and organisational requirements;
- reporting requirements;
- conduct of business requirements;
- operational resilience requirements;
- custody/safeguarding requirements; and
- consumer protections.

B. Provision for stablecoin regulation and proposed digital settlement assets regime under the FSMB

Following the publication of the Stablecoin Consultation Response, a draft of The Financial Services and Markets Bill 2022 **(FSMB)** was published. That draft is currently making its way through Parliament. The FSMB will pave the way for the regulation of fiat-linked stablecoins, and possibly the regulation of other cryptoassets (in relation to which, please see further below).

Specifically, the FSMB introduces powers for HMT to bring stablecoins used as means of payment and similar "digital settlement assets" **(DSAs)** within the scope of regulation. DSAs are defined as a digital representation of value or rights, whether or not cryptographically secured, that:

i. can be used for the settlement of payment obligations;
ii. can be transferred, stored or traded electronically; and
iii. uses technology supporting the recording or storage of data (which may include DLT).

The definition of DSAs is potentially very wide and one which, as explained below, can be expanded by HMT in future. Under the FSMB, as currently drafted, HMT is to be granted a range of powers to regulate services and activities relating to DSAs. In particular, HMT will:

- be empowered to establish an FCA authorisation and supervision regime for issuers of DSAs and payment service providers using DSAs, drawing broadly on existing e-money and payments regulation to mitigate conduct, prudential and market integrity risks;
- have powers to recognise operators of systemic payment systems using DSAs and service providers to those payment systems, bringing them within scope of BoE supervision, via amendments to its existing powers to recognise systemic payment systems under the Banking Act 2009. Similarly, the Payment Systems Regulator (**PSR**) will have powers to regulate payment systems using DSAs, including powers to give directions relating to direct and indirect access to such systems; and
- be empowered to extend the FMI special administration regime **(SAR)** to systemic DSA firms, with appropriate modifications. The FMI SAR is a bespoke administration regime for recognised payment and settlement systems and service providers to mitigate the risks to financial stability associated with their failure. In May 2022, HMT consulted on how it intends to extend the FMI SAR to systemic DSA firms, including how the FMI SAR would take precedence over the payment and e-money special administration regime **(PESAR)** in cases of overlap.[38]

[38] HMT, "Managing the failure of systemic digital settlement asset (including stablecoin) firms: Consultation" (May 2022) <https://www.gov.uk/government/consultations/managing-the-failure-of-systemic-digital-settlement-asset-including-stablecoin-firms> Accessed December 2022.

An important distinction between the two special administration regimes is that the FMI SAR would impose an objective on administrators to pursue the continuity of a failed payment system's services ahead of the interests of its creditors, whereas the focus of the PESAR is on the prompt return of customer funds. As both objectives may be important in the case of a failed systemic DSA firm, HMT's consultation proposed that the FMI SAR for systemic DSA firms impose an additional objective on administrators, covering the return or transfer of funds and custody assets. The BoE would also be required to consult with the FCA before exercising its powers under the FMI SAR with respect to a systemic DSA firm.

C. BoE work on a proposed UK CBDC
For a number of years, the UK has been considering whether to introduce a retail CBDC that would complement existing forms of central bank (and commercial bank) money. A retail CBDC would be a new form of digital money, denominated in Sterling and issued by the BoE, that could be held and used by retail end users, i.e. consumers.

In March 2020, the BoE published an initial discussion paper on CBDC, which outlined a possible approach to the design of a UK CBDC.[39] Responses were published in July 2021[40]. In April 2021, the Bank and HMT set up a joint CBDC Taskforce to coordinate the exploration of a potential UK CBDC. Alongside this, the BoE published a discussion paper on new forms of digital money (including both systemic stablecoins and a UK CBDC) in June 2021,[41] which assessed and sought feedback on the possible opportunities and risks that a UK retail CBDC could bring.

Following the initial work of the CBDC Taskforce during 2021 and 2022, in February 2023, HMT and the Bank of England published a consultation[42] on the design of a potential UK retail CBDC. This consultation paper sets out analysis conducted by HMT and the Bank of England to date on the potential case for a UK retail CBDC and seeks feedback on the key features of a potential retail CBDC model. If the UK does decide to proceed with a retail CBDC, this will be a major infrastructure project spanning several years. Therefore, it is expected that the earliest 'go-live' date for a UK CBDC would be towards the end of this decade.

HMT consultation on future financial services regulatory regime for cryptoassets

In February 2023, HMT published a consultation and call for evidence on the future financial services regulatory regime for cryptoassets **(the Cryptoasset Consultation)**.[43] The Cryptoasset Consultation sets out the UK government's proposal to regulate cryptoassets other than fiat-referenced stablecoins.[44]

The Cryptoasset Consultation closes on 30 April 2023. The UK government has not yet confirmed when it plans to implement the new regulatory proposals, but final rules could be made during 2024-2025 and possibly even earlier.

[39] BoE, "Central Bank Digital Currency: opportunities, challenges and design" Discussion Paper (March 2020) <https://www.bankofengland.co.uk/paper/2020/central-bank-digital-currency-opportunities-challenges-and-design-discussion-paper> Accessed December 2022.

[40] BoE, "Responses to the Bank of England's March 2020 Discussion Paper on CBDC" (June 2021) <https://www.bankofengland.co.uk/paper/2021/responses-to-the-bank-of-englands-march-2020-discussion-paper-on-cbdc> Accessed December 2022.

[41] BoE, "New forms of digital money" Discussion Paper (June 2021) <https://www.bankofengland.co.uk/paper/2021/new-forms-of-digital-money> Accessed December 2022.

[42] HMT, "The digital pound: A new form of money for households and businesses?" (February 2023) < https://www.gov.uk/government/consultations/the-digital-pound-a-new-form-of-money-for-households-and-businesses> (accessed February 2023).

[43] HMT, "Future financial services regulatory regime for cryptoassets Consultation and call for evidence" (February 2023) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1133404/TR_Privacy_edits_Future_financial_services_regulatory_regime_for_cryptoassets_vP.pdf> (accessed February 2023).

[44] The UK government's approach to the regulation of fiat-referenced stablecoins is set out in the Stablecoin Consultation Response. See above for a description of these proposals.

In the Cryptoasset Consultation, HMT rules out creating a bespoke regulatory regime for cryptoassets. Instead the Cryptoasset Consultation proposes:

- extending the scope of FSMA to cover a wide range of cryptoasset services thereby requiring firms providing these services to be authorised under FSMA;
- utilising the Designated Activities Regime **(DAR)** (a proposed regulatory framework to be created by the FSMB) to impose requirements on certain cryptoasset activities even when such activities are not subject to an authorisation requirement under FSMA or otherwise;
- imposing disclosure and transparency obligations on issuers of cryptoassets and the operators of trading venues where cryptoassets are traded; and
- introducing a market abuse regime for cryptoassets.

A. Extension of FSMA to cryptoasset services

In-scope cryptoassets

The Cryptoasset Consultation proposes introducing the FSMB definition of "cryptoasset" into FSMA. The FSMB defines cryptoassets as:

"any cryptographically secured digital representation of value or contractual rights that—

(a) can be transferred, stored or traded electronically, and

(b) that uses technology supporting the recording or storage of data (which may include distributed ledger technology)."

This is a broad definition and the Cryptoasset Consultation sets out the following indicative, non-exhaustive list of the types of cryptoassets that could be subject to regulation under these proposals.

- exchange tokens;
- utility tokens;
- NFTs;
- asset-referenced tokens;
- commodity-linked tokens;
- crypto-backed tokens;
- algorithmic tokens;
- governance tokens; and
- fan tokens.

The UK government's intention is to include cryptoassets in the list of "specified investments" in Part III of the RAO. This clarifies that persons (natural or legal) who are carrying out certain activities involving cryptoassets "by way of business" would be performing regulated activities and therefore require authorisation under Part 4A of FSMA. The effect of this is that the FCA will be able to exercise its general rule-making powers in relation to cryptoasset activities. This will allow the FCA to write tailored rules for cryptoassets as opposed to simply applying existing rules for traditional financial instruments.

In-scope activities

The Cryptoasset Consultation sets out a list of illustrative cryptoasset activities that HMT proposes to bring within the regulatory perimeter.[45] These activities are:

[45] This Cryptoasset Consultation also lists the activities that are within the scope of the Stablecoin Consultation Response. In this section we focus only on those activities that are not covered by this earlier consultation. The Cryptoasset Consultation notes also that additional activities such as mining or validating transactions or operating a node on a blockchain may be addressed in future regulation.

i. issuance activities:

a. admitting a cryptoasset to a cryptoasset trading venue; and
b. making a public offer of a cryptoasset (including as part of an ICO);

ii. exchange activities: operating a cryptoasset trading venue (the exchange of cryptoassets for other cryptoassets, the exchange of cryptoassets for fiat currency and the exchange of cryptoassets for other assets (e.g. commodities)) [46];

iii. investment and risk management activities:[47]
a. dealing in cryptoassets as principal or agent;
b. arranging (bringing about) deals in cryptoassets; and
c. making arrangements with a view to transactions in cryptoassets;

iv. lending, borrowing and leverage activities:
a. operating a cryptoasset lending platform; and

v. safeguarding and/or administration (custody) activities:
a. safeguarding or safeguarding and administering (or arranging the same) a cryptoasset other than a fiat-backed stablecoin and/or means of access to the cryptoasset.

HMT states that its intention is to incorporate the full scope of activities that currently require registration under the MLRs into the regulatory perimeter of FSMA. This reduces the scope for potential confusion as to which regime applies but does mean that cryptoasset firms currently registered under the MLRs will need to seek authorisation going forwards and be subject to additional regulatory obligations. The Cryptoasset Consultation states that the FCA will adopt a timely and proportionate authorisation process for complete and accurate applications and will endeavour to avoid duplicative information requests of businesses, taking into account the supervisory history of businesses during the authorisation process.

The Cryptoasset Consultation notes also that additional activities such as mining or validating transactions or operating a node on a blockchain may be addressed in future regulation.

Proposed territorial scope

The UK government proposes to regulate cryptoasset activities that are provided from the United Kingdom or to customers in the United Kingdom (regardless of where the service provider is located).

HMT states in the Cryptoasset Consultation that this approach is in line with other areas of the UK's regulatory perimeter. However, some key features of existing regulatory regimes are not mentioned in the Cryptoasset Consultation. In particular, the "overseas person" exclusion in the RAO, and the general "characteristic performance" test, are not mentioned. It is also not entirely clear whether the territorial scope of the activities identified in the Stablecoin Consultation Response will be the same as for the activities addressed in the Cryptoasset Consultation given the former is based on the existing payment services regime and the latter on FSMA. Regarding the former, the FCA has stated that it: "would not generally expect a payment services provider incorporated and located outside the UK to be within the scope of the regulations, if all it does is to provide internet-based and other services to UK customers from that location."[48]

[46] The Cryptoasset Consultation states that post-trade activities may be covered in a future phase of regulation.
[47] The Cryptoasset Consultation states that providing investment advice and managing portfolios of cryptoassets may be covered in a future phase of regulation.

[48] Section 15.6 of Chapter 15 of the FCA's Perimeter Guidance Manual (PERG).

Exemptions and equivalence

The Cryptoasset Consultation proposes an exemption from authorisation for non-UK firms providing services to UK customers from outside the UK on the basis of "reverse solicitation" (i.e. where services are provided by non-UK firms entirely at the initiative of the UK customer). HMT notes in the Cryptoasset Consultation that any such exemption would be defined so as to prevent misuse and regulatory arbitrage. On this basis, we might expect this exemption to be defined narrowly. HMT will also pursue equivalence arrangements that would allow firms authorised in other jurisdictions to conduct cryptoasset activities in the UK if they are subject to equivalent standards in their home jurisdiction and suitable cooperation mechanisms exist between the relevant UK and overseas regulators.

B. Designated Activities Regime (DAR)
HMT is also proposing to regulate other cryptoasset activities under the DAR. This would allow regulators to impose direct requirements on firms carrying on such activities, even where they fall outside of the authorisation regime under FSMA or otherwise. The DAR could even be used to ban certain activities. One example given in the Cryptoasset Consultation (which the UK government is considering) is a requirement for certain public offers of cryptoassets to be conducted via a regulated platform.

C. Disclosure and transparency obligations
The Cryptoasset Consultation proposes an issuance and disclosures regime for cryptoassets. This will be based on the approach taken in the forthcoming Public Offer and Admissions to Trading Regime with suitable tailoring to the unique features of cryptoassets.[49]

Disclosure requirements will apply to firms when (i) admitting a cryptoasset to a trading venue and/or (ii) making a public offer of cryptoassets (including ICOs).

The Cryptoasset Consultation proposes:
i. imposing a minimum standard of information that must be disclosed to investors which will be based on a "necessary information" test;
ii. putting in place arrangements to ensure liability and compensation for untrue or misleading statements included in disclosure documents;
iii. a requirement for an appropriate level of due diligence of the contents of disclosure and admission documents;
iv. an appropriate level of protection for investors in relation to marketing materials. Trading venues will need to impose rules governing marketing materials and product appropriateness; and
v. controls and procedures to prevent harmful offers (e.g. measures to detect fraud). Trading venues will be required to reject the admission of cryptoassets to trading where they consider that they may result in investor detriment.

D. Market abuse regime for cryptoassets
The Cryptoasset Consultation proposed a market abuse regime for cryptoassets. This will be a dedicated regime based on, but separate from, the UK Market Abuse Regulation **(MAR)**.[50]

The regime will apply only to cryptoassets that are traded on UK trading venues making it narrower in scope than MAR which applies to financial instruments traded on EU as well as UK trading venues.

The proposed market abuse regime would impose obligations on in-scope trading venues, and offences would apply regardless of where the person is based or where the trading takes place.

[49] See Financial Services and Markets Act 2000 (Public Offers and Admissions to Trading) Regulations 2023 < https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1122741/Draft_SI_Admissions_to_Trading_and_Public_Offer_Regime.pdf> (accessed February 2023).
[50] UK MAR is based on the EU Market Abuse Regulation (596/2014) brought into UK law through the European Union (Withdrawal) Act 2018 (EUWA).

Market participants will be required to establish systems and controls to prevent and detect market abuse. All regulated firms conducting cryptoasset activities will be required to disclose inside information and maintain a list of persons with access to such information.

Call for evidence on other areas

In the Cryptoasset Consultation, HMT requests additional evidence on the following areas that could potentially be regulated in the future:

i. Decentralised finance;
ii. Other cryptoasset activities including post-trade activities (e.g. clearing and settlement in relation to cryptoasset transactions), cryptoasset investment advice, cryptoasset portfolio management, crypto mining and validation; and
iii. Sustainability of cryptoasset activities.

Promotion of cryptoassets to UK consumers to be regulated

At present, the marketing of unregulated cryptoassets to UK consumers is not subject to FCA regulation and is overseen only by the Advertising Standards Authority.[51] Although the Advertising Standards Authority has issued numerous rulings to cryptoasset firms in relation to misleading advertising, it has very limited powers in comparison with the FCA and cannot, for example, impose fines on firms that are in breach of its rules.

In January 2022, HMT published its response to its consultation on bringing certain cryptoassets into scope of the FCA's existing financial promotions regime (the **Financial Promotions Consultation Response**). The Financial Promotions Consultation Response confirmed that HMT intends to bring the marketing of "qualifying cryptoassets" to UK consumers within scope of that regime.[52] The definition of "qualifying cryptoassets"[53] is expected to capture a wide range of unregulated cryptoassets, subject to some exclusions, such as NFTs. The regime will apply even where the person communicating the promotion is based overseas[54], and regardless of how the promotion is communicated (for example, whether the relevant adverts are placed through traditional print or on social media).

A related consultation on the draft FCA rules for the promotion of cryptoassets and other high-risk investments closed in March 2022.[55] The final rules for cryptoassets have not yet been published. However, the FCA has indicated that those rules will closely follow the final rules for high-risk investments, which were published in August 2022 and came into force on 1 February 2023.[56]

The FCA consultation indicates that firms looking to market relevant cryptoassets to UK consumers will need to satisfy numerous requirements when designing and communicating adverts. Among other things, it is likely that firms will be required to ensure that relevant adverts:

— are fair, clear, and not misleading;

— include a prescribed risk warning in a prominent place;

— do not include any form of incentive to invest;

[51] The relevant rules are set out in the Advertising Code (The UK Code of Non-broadcast Advertising and Direct & Promotional Marketing, also referred to as the "CAP Code") and specific guidance was issued in relation to cryptoasset adverts in March 2022 (see the Enforcement Notice titled "Advertising of Cryptoassets: Cryptocurrencies", issued by the Committee of Advertising Practice on 22 March 2022). Among other things, firms must make clear that cryptoassets are not regulated by the FCA and are not protected by the UK's financial services compensation schemes.
[52] HMT, "Cryptoasset promotions: Consultation response" (January 2022) <Cryptoasset_Financial_Promotions_Response.pdf (publishing.service.gov.uk)> Accessed December 2022.
[53] HMT has indicated that it will adopt the following definition: "any cryptographically secured digital representation of value or contractual rights which is fungible and transferable".
[54] Firms that intend to obtain a licence or an anti-money laundering registration with an overseas regulatory authority, instead of the FCA, should be aware that they will still need to comply with these rules, to the extent that they promote relevant cryptoassets to UK consumers.
[55] FCA, "Strengthening our financial promotion rules for high risk investments, including cryptoassets" (Consultation Paper CP22/2, January 2022), <CP22/2: Strengthening our financial promotion rules for high risk investments, including cryptoassets (fca.org.uk)> Accessed December 2022.
[56] FCA, "Strengthening our financial promotion rules for high-risk investments and firms approving financial promotions" (Policy Statement PS22/10, August 2022) <PS22/10: Strengthening our financial promotion rules for highrisk investments and firms approving financial promotions (fca.org.uk)> Accessed December 2022.

— are reviewed and approved by an FCA-authorised firm with competence and expertise in the cryptoasset market and the required permissions to approve such promotions.[57]

Further, firms will need to ensure that “direct offer financial promotions” (i.e., promotions that contain an offer or invitation to enter into an agreement and a mechanism by which customers can respond in order to invest their money) are communicated only to customers that the firm has categorised as more sophisticated, and that first time investors are given a 24-hour cooling off period.[58]

It is unclear precisely when the new rules will be implemented, although we expect this to happen during 2023.[59] In a statement published in February 2023, the FCA warned firms to start preparing now for the new regime.[60]

Other relevant changes

Other proposed changes to UK regulation include those set out below.

A. UK FMI sandbox
The UK Financial Services Bill 2022 is expected to make relevant legislative amendments empowering HMT, the FCA and the BoE to create statutory rules for the development of so-called ‘FMI sandboxes’. Unlike the existing regulatory sandbox that is operated by the FCA, these new FMI sandboxes will enable HMT to disapply certain legislative (statutory) provisions that would otherwise apply to financial market infrastructure, in order to generate a test environment. The powers are wide enough to enable the creation of settlement mechanisms for payments and financial instruments using DLT and related technology, including digital assets and stablecoins. As part of the UK government’s package of financial services reforms announced in December 2022 (referred to as the ‘Edinburgh Reforms’) the Chancellor confirmed plans to launch the FMI sandbox in 2023.[61]

B. Decentralised structures and DAOs
In general, current legal and regulatory frameworks are not particularly well-adapted to truly decentralised structures. In fact, there are greater challenges in applying concepts of ‘same risk, same regulation’ to decentralised structures where regulatory supervision and accountability mechanisms may need to be designed differently from those applied to existing regulated firms.

In November 2022, the Law Commission of England and Wales launched a call for evidence on how decentralised autonomous organisations **(DAOs)** can be characterised and how they might be accommodated under English law.[62] This will be an important piece of the jigsaw in designing a future regulatory framework that could accommodate regulation and supervision of DAOs.

[57] Pursuant to a planned exemption announced by HMT in February 2023 (see HMT “Government approach to cryptoasset financial promotions regulation policy statement”) firms that are registered with the FCA under the MLRs will be able to issue their own cryptoasset financial promotions and will not need to obtain approval from an FCA-authorised firm. HMT, “Government approach to cryptoasset financial promotions regulation policy statement” (February 2023) <Government approach to cryptoasset financial promotions regulation policy statement - GOV.UK (www.gov.uk)> (accessed February 2023).

[58] Specifically, investors who are categorised as “restricted”, “high net worth”, or “certified sophisticated”.

[59] For completeness, before the financial promotions regime can apply to cryptoassets, FSMA and the Financial Services and Markets Act (Financial Promotion) Order 2005 will need to be amended, and the FCA will need to publish its final rules. HMT has not yet brought forward the relevant draft legislation. The FCA has indicated that it will publish its final rules when such legislation has been made. For completeness, firms are due to be given a four-month transitional period (reduced from six months, pursuant to an announcement by HMT made in February 2023 – see HMT “Government approach to cryptoasset financial promotions regulation policy statement”).

[60] FCA, “Cryptoasset firms marketing to UK consumers must get ready for financial promotions regime” (February 2023) <Cryptoasset firms marketing to UK consumers must get ready for financial promotions regime> Accessed February 2023.

[61] UK Government, “Financial Services: The Edinburgh Reforms” (December 2022) <https://www.gov.uk/government/collections/financial-services-the-edinburgh-reforms> Accessed December 2022.

[62] Law Commission, “Decentralised autonomous
organisations (DAOs)” Call for evidence (November 2022) <https://www.lawcom.gov.uk/project/decentralised-autonomous-organisations-daos/#:~:text=We%20launched%20a%20public%20call,now%20and%20in%20the%20future> Accessed December 2022.

HMT's Cryptoasset Consultation includes a call for evidence on how the UK should approach regulation of decentralised finance (DeFi). HMT indicates it intends to take a proportionate, innovation-friendly approach, but also sets out its intention that DeFi should be regulated in such a way as to ensure the same regulatory outcomes are achieved as for other cryptoasset activities. HMT notes this may take longer to achieve due to the rapidly evolving nature of the sector and globalised and borderless nature of DAOs and other DeFi structures. The call for evidence identifies one possible way of regulating DeFi activities as creating a new regulated or designated activity of "establishing or operating a protocol" but asks for broad feedback on how DeFi could and should be regulated in the UK.

C. Changes to criminal legislation
Separately, and whilst this chapter is not intended to address the implications of existing criminal legislation in the UK for cryptoassets, we note that there have also been proposed changes to such legislation. For example, the Economic Crime & Corporate Transparency Bill, which was presented to Parliament on 22 September 2022, makes certain amendments to the Proceeds of Crime Act 2002 that are intended to help law enforcement agencies, such as the National Crime Agency, to seize, freeze and recover cryptoassets used by criminals to launder the proceeds of crime.

What else might we expect?

HMT has confirmed its intention to expand the regulatory perimeter in order to capture a wider range of cryptoassets, including those used for investment purposes. Once the FSMB gains Royal Assent (expected in Q2 2023) HMT will be able to lay secondary legislation setting out the detail of the extended regulatory perimeter covering DSAs and other cryptoasset activities. The FCA will then need to consult on relevant rules to bring the regulatory regime into operation. These are expected to include minimum capital, liquidity and other prudential requirements for firms requiring authorisation under the new regime, as well as ongoing conduct of business rules for authorised firms and rules on admission and disclosure requirements where cryptoassets are traded in the UK. Firms that are already authorised under FSMA would also need to apply for a variation of their permissions to include newly regulated cryptoasset activities.

HMT indicates in its February 2023 consultation that once phases 1 and 2 of the new UK cryptoasset regulatory framework are in place, it may consult further on regulating additional cryptoasset-related activities to the extent they are not already covered – such as safeguarding and administration services for stablecoins, other post-trade activities, aspects of advising and managing and validation and governance of protocols.

More generally, we expect the regulation of cryptoassets to remain subject to scrutiny and discussion by regulators and the UK Government going forward. Other developments which practitioners and market participants may wish to monitor include the Treasury Committee's ongoing inquiry into the cryptoasset industry. The inquiry, which was launched in July 2022, has a wide scope and is considering, among other things, the UK's regulatory response to cryptoassets to date, including how regulation can strike a balance between protecting consumers and encouraging innovation.[63] To date, the Committee has received evidence from market participants, consumer interest groups and the FCA, among others. We expect that the Committee will report on its findings and issue a series of recommendations once the inquiry concludes, possibly sometime in 2023.

[63] The scope of the inquiry is wide-ranging and is intended to consider the role of cryptoassets in the UK, including the opportunities and risks posed to consumers, businesses, and the Government; the opportunities and risks that the introduction of a BoE CBDC might bring; and the potential impact of DLT on financial institutions and financial infrastructure, among other things.

The international context

The European Union

The EU's proposed Markets in Crypto-Assets Regulation **(MiCA)** will, assuming that it is approved by the European Parliament, establish a regulatory framework for cryptoasset services across the EU. MiCA applies to the issuance, offering to the public, and admission to trading of cryptoassets as well as the provision of certain cryptoasset services in the EU.

MiCA defines a "crypto-asset" as a "digital representation of a value or a right which may be transferred and stored electronically, using distributed ledger technology or similar technology". This is a broad definition and would likely capture coins such as Bitcoin and Ethereum. MiCA further defines three subcategories:

A. "Asset-referenced token", defined as "a type of crypto-asset that is not an electronic money token and that purports to maintain a stable value by referencing to any other value or right or a combination thereof, including one or more official currencies". This includes stablecoins linked to multiple fiat currencies and/or other assets or indices;

B. "Electronic money token" or "e-money token", defined as "a type of crypto-asset that purports to maintain a stable value by referencing to the value of one official currency". This includes stablecoins linked to a single fiat currency; and

C. "Utility token", defined as "a type of crypto-asset which is only intended to provide access to a good or a service supplied by the issuer of that token".

MiCA does not apply to cryptoassets that are "unique and not fungible with other crypto-assets" meaning many NFTs will fall outside MiCA. However, NFTs that are not truly unique and fractional interests in NFTs may fall within the scope of MiCA.

The new regulation is not expected to take effect until 2024. Specifically, certain provisions in MiCA relating to issuers of asset-referenced tokens and e-money tokens will apply from 12 months after the date MiCA enters into force. All other provisions will apply from 18 months after the date MiCA enters into force. MiCA also includes limited transitional measures for certain cryptoasset service providers.

Separately to MiCA, Regulation (EU) 2022/858 sets out a pilot regime for market infrastructures based on DLT **(the DLT Pilot Regime)**. The DLT Pilot Regime lifts certain requirements of the existing regulatory framework on a temporary basis, in order to allow financial market infrastructure operators and new entrants to use blockchain technology to operate a multilateral trading facility and/or a securities settlement system for tokenised financial instruments (or "security tokens"). The DLT Pilot Regime will allow companies to test their DLT and assess how it operates, or should operate or adapt, in a regulatory environment to meet the relevant requirements. It is intended to offer a safe environment to operate a DLT market infrastructure for up to six years, subject to periodic reviews by supervisors.

The United States

Since cryptoassets have numerous potential applications, various US government authorities at both the state and federal level are helping to shape the regulatory landscape that surrounds them. In the capital markets context, both the Securities and Exchange Commission (**SEC**) and the Commodity Futures Trading Commission (**CFTC**) exercise regulatory authority over cryptoassets that is not clearly defined. Historically, the SEC has regulated "securities", while the CFTC has regulated commodities and derivatives; however, the universe of cryptoassets does not squarely fit into any of these categories. Banking regulators have provided some guidance to financial institutions on their ability to engage in cryptoasset activities. In particular, the Office of the Comptroller of the Currency (OCC) has published several Interpretive Letters clarifying that banks are allowed to engage in certain activities involving cryptoassets, provided they do so in a safe and sound manner and after notifying their primary federal regulator.

In March 2022, President Joe Biden issued an executive order, which called for an interagency process to examine the risks and benefits of digital assets. Further, numerous federal regulators and members of the United States Congress have expressed a desire to regulate cryptoassets more closely. In the absence of Congressional action, federal law enforcement authorities have taken action against entities involved in cryptoasset activities. For example, in February 2022, the SEC brought an enforcement action against a crypto lending company for offering unregistered securities that were in the form of digital assets.[64] State enforcement authorities have also taken an active role in cryptocurrency regulation and enforcement. For example, the Texas State Securities Board has, to date, entered into more than 50 administrative orders involving individuals and cryptocurrency entities.[65] Numerous states also introduced legislation regarding cryptocurrency and other cryptoassets during their last legislative sessions. These developments, along with recent high-profile cryptocurrency and cryptocurrency exchange failures, could lead to greater oversight of cryptoassets in the near future.

Other international developments

A. BCBS consultations on the prudential treatment of cryptoassets
In December 2022, the Basel Committee on Banking Supervision **(BCBS)** published its framework setting out international standards for the prudential treatment of cryptoassets, for implementation by 1 January 2025.[66] Once implemented by BCBS member jurisdictions, this framework will apply to banks' exposures to cryptoassets (and may also be applied to other financial institutions subject to regulatory capital requirements based on BCBS standards).

The final BCBS prudential standard on banks' cryptoasset exposures divides cryptoassets into two broad groups:

i. Group 1: cryptoassets including tokenised traditional assets (Group 1a) and cryptoassets with effective stabilisation mechanisms (Group 1b). Cryptoassets need to meet strict classification conditions to fall into Group 1. Group 1b stablecoins must be issued by supervised and regulated entities and have robust redemption rights and governance. Algorithmic stablecoins are not eligible to fall within Group 1b. Group 1 cryptoassets are generally subject to capital requirements based on the risk weights of underlying exposures as set out in the existing Basel Framework.

ii. Group 2: other cryptoassets (such as Bitcoin) which do not meet classification conditions and which are considered to pose additional and higher risks. These cryptoassets would be subject to a new, conservative prudential treatment, including a 1250% risk weighting and an aggregate exposure limit. Under the proposed framework, it is not generally possible to use Group 2 cryptoassets for hedging purposes, except to a limited degree where Group 2 cryptoassets meet certain "hedging recognition criteria". These are referred to as Group 2a cryptoassets, with Group 2 cryptoassets where hedging is not recognised falling within Group 2b.

BCBS's consultation on the prudential framework published in summer 2022[67] had proposed a mandatory 2.5% "infrastructure risk add on" to address unforeseen risks associated with DLT. However, in response to issues raised in industry responses to the BCBS consultation, the final BCBS standards no longer require the infrastructure risk add-on to be applied automatically. Instead,

[64] SEC, "BlockFi Agrees to Pay $100 Million in Penalties and Pursue Registration of its Crypto Lending Product" (Press Release, February 2022) <https://www.sec.gov/news/press-release/2022-26> Accessed December 2022.
[65] See Texas State Securities Board, "Cryptocurrency Enforcement" <https://www.ssb.texas.gov/cryptocurrency-enforcement> Accessed December 2022. See also Texas State Securities Board, "Texas State Securities Board Joins with Other State Regulators to Settle with Digital Asset Lending Platform BlockFi for $50 Million for Sales of Unregistered Securities" (Press Release, February 2022) <https://www.ssb.texas.gov/news-publications/texas-state-securities-board-joins-other-state-regulators-settle-digital-asset> Accessed December 2022.
[66] BCBS, "Prudential treatment of cryptoasset exposures" (December 2022) <https://www.bis.org/bcbs/publ/d545.htm> Accessed December 2022.
[67] BCBS, "Prudential treatment of cryptoasset exposures - second consultation" (June 2022) < Prudential treatment of cryptoasset exposures - second consultation (bis.org)> Accessed December 2022.

authorities will be empowered to activate such an add-on based on any observed weaknesses in the infrastructure on which particular cryptoassets are based. This is an important change, as there had been concerns in the industry that an automatic infrastructure add-on would make it economically unviable for banks (or other firms subject to Basel standards) to hold and trade even in Group 1 cryptoassets, such as tokenised securities and fiat-backed stablecoins.

The consultation response also clarifies that it does not intend for custodians to apply credit, market, and liquidity risk requirements of the framework to customer assets (again, a potential concern that had been raised in consultation responses). Nevertheless, UK national policy makers will need to give these issues careful consideration in the development of prudential rules relating to cryptoasset exposures, with international implementation of the Basel Framework expected by 1 July 2025.

B. International standards for globally systemic stablecoins
In October 2020, the Financial Stability Board **(FSB)** published a set of 10 high-level recommendations for the regulation, supervision and oversight of global stablecoin (GSC) arrangements.[68] Those high-level recommendations called for the regulation, supervision and oversight of GSCs in a proportionate manner, in order to address associated financial stability risks posed by GSCs, under the principle of 'same activity, same risk, same regulation'.

In October 2022, the FSB published a review of those high-level recommendations for GSCs,[69] in which it proposed certain updates in order to address recent market developments (including the Terra-Luna collapse in May 2022). Among other things, the FSB's review noted that most existing stablecoin arrangements do not meet the FSB's existing high-level recommendations to be GSCs and proposed extending the scope of the recommendations to stablecoins with potential to become GSCs. Comments were due by 15 December 2022 and the FSB aims to finalise its updated high-level recommendations for GSCs by July 2023.

In July 2022, the Bank for International Settlements' Committee on Payments and Market Infrastructures **(CPMI)** and the International Organization of Securities Commissions **(IOSCO)** also published final guidance on stablecoin arrangements.[70] That guidance confirmed that the Principles for Financial Market Infrastructures (PFMI) should apply to systemically important stablecoin arrangements for the transfer of stablecoins, thus extending existing international standards for payment, clearing and settlement systems to cover systemically important stablecoin arrangements. The CPMI and IOSCO indicated they will continue to examine regulatory, supervisory and oversight issues associated with stablecoin arrangements and coordinate with other standard-setting bodies.

C. FSB consultation on regulation of cryptoasset activities
In October 2022, the FSB also published a consultation on a proposed framework for the international regulation of cryptoasset activities, based on the principle of "same activity, same risk, same regulation".[71] The proposed framework includes nine recommendations on regulatory, supervisory and oversight approaches to cryptoasset activities and markets, which aim to address associated financial stability risks and promote a consistent regulatory framework, and to strengthen international cooperation, coordination and information sharing globally. Comments were due by 15 December 2022.

[68] FSB, "Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements" (October 2020) <https://www.fsb.org/2020/10/regulation-supervision-and-oversight-of-global-stablecoin-arrangements/> Accessed December 2022.

[69] FSB, "Review of the FSB High-level Recommendations of the Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements: Consultative report" (October 2022) <https://www.fsb.org/2022/10/review-of-the-fsb-high-level-recommendations-of-the-regulation-supervision-and-oversight-of-global-stablecoin-arrangements-consultative-report/> Accessed December 2022.

[70] CPMI and IOSCO, "Application of the Principles for Financial Market Infrastructures to stablecoin arrangements" (July 2022) <https://www.bis.org/press/p220713.htm> Accessed December 2022.

[71] FSB, "International Regulation of Crypto-asset Activities: A proposed framework – questions for consultation" (October 2022) <International Regulation of Crypto-asset Activities: A proposed framework – questions for consultation - Financial Stability Board (fsb.org)> Accessed December 2022.

High-level considerations for the UK regulator when designing the framework

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 new rules may interact with the existing regulatory frameworks (such as e-money regulation) and any overlaps should be addressed. It is also important to ensure that definitions and taxonomies are carefully calibrated based on the substantive characteristics of the relevant cryptoassets to (i) avoid unhelpful overlaps between regimes and (ii) 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 likely too broad for use in any potential new licensing regime. As such, we would welcome the introduction of a narrower definition.

It is also necessary to carefully consider the territorial scope of any new licensing regime for firms (i) dealing in or (ii) providing services relating to, relevant types of cryptoassets, particularly in light of the cross-border nature of many cryptoasset structures. We would welcome clear rules or guidance on when activities will be considered to have been carried on in the UK, in order to provide greater certainty to market participants. We also advocate for the introduction of 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. Such carve-outs are necessary for the avoidance of duplication and overlaps with other jurisdictions' rules; as such, the introduction of such carve-outs would be in line with the UK's broader policy and approach with respect to the territorial scope of financial services regulatory regimes.

4

Part 1: Developing Technologies

Section 4
Types of Cryptoassets

Section 4: Types of Cryptoassets, Defi and On-Chain Compliance

Marc Piano, Harney Westwood & Riegels LLP (Cayman Islands).

Introduction

This section looks at different types of cryptoassets: in Part A: Central Bank Digital Currencies **(CBDCs)**, Part B: stablecoins and Part C: 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)** and on chain compliance.

Part A: Central Bank Digital Currencies

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."[72]

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"[73].

As set out in the BIS 2020 Report[74], CBDCs may be wholesale-only or general purpose.

[72] BOE June 2021 Discussion Paper, section 1.1

[73] Bank of International Settlements, March 2018, p 1 <https://www.bis.org/cpmi/publ/d174.pdf>

[74] "Bank of International Settlements, 2020 <https://www.bis.org/publ/othp33.pdf>

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[75]:

> *"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[76].

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."* [77]

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 involving CBDCs, with 40% already testing proof-of-concept programmes[78].

The Eastern Caribbean Central Bank (the monetary authority for Anguilla, Antigua and Barbuda, Commonwealth of Dominica, Grenada, Montserrat, St Kitts and Nevis,

[75] "Central Banks and the Future of Digital Money", Consensys AG, January 2020, pp 17-18
[76] BIS 2020 Report, page 4
[77] "Central Bank Digital Currency: opportunities, challenges and design", Bank of England, 12 March 2020, Chapter 5.2
[78] "About 80% of Central Banks Are Exploring CBDC Use Cases, Bison Trails Report Says", Coinbase, 19 May 2021

Saint Lucia, and St Vincent and the Grenadines) introduced its CBDC, DCash, on 31 March 2021 for public use[79].

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[80]. The PBOC intends to conduct a large-scale trial at the Winter Olympics in Beijing in February 2022[81].

The United Kingdom published terms of reference[82] 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[83]. 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."*[84]

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[85].

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.

[79] "DCash – an ECCB initiative – About the Project", Eastern Caribbean Central Bank
[80] "Background and Implications of China's Central Bank Digital Currency: E-CNY", Jiaying Jiang Karman Lucero, Stanford Law School, 6 April 2021
[81] "China Ramps Up CBDC Pilot Plans Ahead of 2022 Winter Olympics", CBDC Insider, 6 August 2021
[82] "Terms of Reference (ToR), April 2021 - Central Bank Digital Currency (CBDC) Taskforce", HM Treasury, April 2021
[83] "Membership of CBDC Engagement and Technology Forums", Bank of England, 29 September 2021
[84] BoE June 2021 Discussion Paper, section 1.1
[85] BIS 2020 Report, page 4

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[86] 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[87]. 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*".[88] 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.[89] 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.

The BIS published a dedicated paper on this topic in March 2021 **(the BIS mCBDC Paper)**, introducing the concept of "multi-CBDC arrangements" **(mCBDC)**[90]. 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:

[86] BoE March 2020 Discussion Paper, Chapter 6

[87] "Progress of Research & Development of E-CNY in China", Working Group on E-CNY Research and Development of the People's Bank of China, July 2021, Section 3.2.7

[88] "China and the dawn of digital currency", Geoff Yu (BNY Mellon), Aerial View, November 2020

[89] "China's Digital Currency Is About To Disrupt Money", Enrique Dans, Forbes, 7 April 2021

[90] "Multi-CBDC arrangements and the future of crossborder payments", BIS Papers No 115, Bank of International Settlements, March 2021

— 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."*[91]

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[92] and Principle 10 on financial inclusion[93] 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[94], 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."*[95] 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 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

[91] BIS 2020 Report, section 3.1
[92] "Public Policy Principles for Retail Central Bank Digital Currencies (CBDCs)", G7, October 2021, page 12
[93] G7 PPP, page 13
[94] "Cashing In: Cashing In: How to Make Negative Interest Rates Work", Ruchir Agarwal and Signe Krogstrup, IMFBlog, 5 February 2019
[95] BoE June 2021 Discussion Paper, section 4.5

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 firms 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 Updated FATF Guidance)[96], as does the Financial Stability Board (FSB) in its final report and high-level recommendations on "Global Stablecoin Arrangements" (the FSB Stablecoins Report)[97], 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. A sufficient number of central banks are investigating or developing CBDCs to warrant close scrutiny of developments in this area, given the potential impacts of CDBCs across multiple spheres of consideration beyond the scope of this guidance. 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.

[96] "Updated guidance on a risk-based approach to virtual assets and virtual asset service providers", Financial Action Task Force, October 2021, paragraph 17

[97] "Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements - Final Report and High-Level Recommendations", Financial Stability Board, October 2020, Glossary definition of "digital asset", page 5

Part B: Stablecoins

This section provides a high-level overview of so-called stablecoins (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"*.[98]

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).

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.

[98] "Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements - Final Report and High-Level Recommendations", Financial Stability Board, October 2020, Glossary definition of "stablecoin", page 5

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[99] (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[100] 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[101] (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 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

[99] "Global Stablecoin initiatives – Public Report" The Board of the IOSCO, March 2020, page 5
[100] "What Is Money?", International Monetary Fund, Finance & Development, September 2012
[101] "New forms of digital money – discussion paper", Bank of England, 7 June 2021, section 5

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

The collapse of TerraUSD in May 2022 attracted significant attention and regulatory scrutiny around stablecoins and their role.

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, including awareness of emerging local and international legal and regulatory developments.

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[102]. 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)**[103]. 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"*.[104]

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."*[105]

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"*.[106]

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**)[107]. 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"*[108] 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"[109].

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 regulation, with a focus on stablecoins (the **HMT Consultation**)[110]. This is a comprehensive consultation

[102] "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
[103] "Principles for financial market infrastructures", Technical Committee of IOSCO, Committee on Payment and Settlement Systems, Bank of International Settlements, April 2012
[104] FSB Stablecoin Report, page 2
[105] FSB Stablecoin Report, page 2
[106] FSB Stablecoin Report, page 7
[107] "Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements - Progress Report on the implementation of the FSB High-Level Recommendations", Financial Stability Board, 7 October 2021
[108] FSB Update Report, Executive Summary (page 1)
[109] FSB Update Report, section 2 (Progress in implementation at jurisdictional level), page 12
[110] "UK regulatory approach to cryptoassets and stablecoins: consultations and a call for evidence", HMT, 7 January 2021

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 published its response to the consultation in April 2022[111].

The UK government intends to apply the principle of "same risk, same regulatory outcome" in developing regulations governing stablecoins[112] 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[113]. 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[114].

In line with this approach, the Financial Services and Markets Bill **(FSMB)** was introduced to the UK Parliament on 20 July 2022. The FSMB introduces the concept of "digital settlement assets" **(DSAs)**, defined as:

> *"a digital representation of value or rights, whether or not cryptographically secured, that—*
>
> *(a) can be used for the settlement of payment obligations,*
>
> *(b) can be transferred, stored or traded electronically, and*
>
> *(c) uses technology supporting the recording or storage of data (which may include distributed ledger technology)"*[115].

DSAs clearly include the concept of stablecoins.

The FSMB extends the Bank of England's oversight of payment systems under the Banking Act 2009 to both payment systems using DSAs and DSA service providers, and payment systems regulations under the Financial Services (Banking Reform) Act 2013 to payment systems using DSAs[116]. The FSMB also empowers the Treasury, in consultation with the Financial Conduct Authority, the Bank of England and, where relevant, the Prudential Regulatory Authority and the Payment Systems Regulator,[117] to make regulations in connection with: payments that include DSAs, payment systems that include arrangements using DSAs, recognised DSA service providers, and service providers connected with or in relation to such systems and services, including in the event of their insolvency[118]. As at the date of this publication, such regulations are not yet available.

In the absence of the regulations, the HMT Consultation includes some high-level requirements which may form part of any authorisation regime and are set out in section 3.23. These 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"[119], extending this criteria to stablecoins performing a retail or wholesale payment system function[120]. A stablecoin arrangement with "significant potential" to be systemic at launch would need to be captured from launch by such regulation[121], echoing the FSB Report.

[111] "UK regulatory approach to cryptoassets, stablecoins, and distributed ledger technology in financial markets: Response to the consultation and call for evidence",
[112] HMT Consultation, section 2.1
[113] HMT Consultation, section 2.3
[114] HMT Consultation, section 2.5
[115] FSMB, Part 1, Chapter 2, section 22(2)
[116] FSMB, Part 1, Chapter 2, section 21
[117] FSMB, Part 1, Chapter 2, section 22(8)
[118] FSMB, Part 1, Chapter 2, section 22(1)
[119] HMT Consultation, section 3.31
[120] HMT Consultation, section 3.32
[121] HMT Consultation, section 3.32

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[122].

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[123]. This may also extend to location requirements for systemic stablecoin arrangements[124]. As at the date of this report, there are no further details available in the FSMB or the government’s response to the HMT Consultation feedback. 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 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.”*[125]

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[126].

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.”*[127]

This BoE June 2021 Discussion Paper considers different regulatory models for meeting the Financial Policy Committee expectations[128], noting that some stablecoin issuers already operate under electronic money regulations (which may need enhancements)[129].

[122] HMT Consultation, section 3.36
[123] HMT Consultation, section 3.38
[124] HMT Consultation, section 3.39
[125] BoE June 2021 Discussion Paper, section 5.1
[126] BoE June 2021 Discussion Paper, section 5.3.5
[127] BoE June 2021 Discussion Paper, section 5.2
[128] “Financial Stability Report, Financial Policy Committee Record and stress testing results – December 2019”, Bank of England, 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.”
[129] BOE June 2021 Discussion paper, sections 5.3.1 and 5.3.5

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[130.]

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**)[131]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 which "have a stabilisation mechanism that is effective at all times"[132], based on a "redemption risk test" and a "basis risk test" set out in SCO60.12 to SCO60.1, be eligible for inclusion in 'Group 1b' cryptoassets. By contrast, all other stablecoins will fall into 'Group 2a' cryptoassets (that fail to meet the classification conditions but pass the Group 2a hedging recognition criteria) or 'Group 2b' (that fail to meet the classification conditions and fail the Group 2a hedging recognition criteria). Algorithm-based stablecoins or those stablecoins that use protocols to maintain their value are not eligible for Group 1[133].

The Basel Consultation Document's treatment of stablecoins relates to stablecoin holdings, rather than stablecoins issued by the relevant financial institution. It proposes that 'Group 1' cryptoassets be eligible for capital treatment generally based on the existing Basel III framework exposure to 'Group 2' cryptoassets (i.e. those not falling to be classified under Group 1a (tokenised traditional assets) or Group 1b (stablecoins) 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"[134]. 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.

No stablecoin in any group will be an eligible form of collateral in itself 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"[135].

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,

[130] BOE June 2021 Discussion Paper, section 5.3.5

[131] "Consultative Document – Prudential treatment of crypto asset exposures", Basel Committee on Banking Supervision, Bank of International Settlements, June 2021

[132] Basel Consultation Document, "Refinement of the classification conditions", page 3

[133] Basel Consultation Document, "Introduction", page 1

[134] Basel Consultation Document, section 3, page 18

[135] Basel Consultation Document, section 2.1, page 13

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[136]). 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?

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[137]), 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[138]: *"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[139] 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 [140]

[136] "Biden Administration Seeks to Regulate Stablecoin Issuers as Banks", Wall Street Journal, 1 October 2021
[137] IOSCO Stablecoins Report, pp 7-8
[138] BoE June 2021 Discussion Paper, section 5
[139] "FATF Report to the G20 Finance Ministers and Central Bank Governors on So-called Stablecoins", FATF, June 2020
[140] Draft Updated FATF Guidance, Box 1

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.

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 and The Case for On-Chain Crypto Compliance, through the use of Blockchain Technology

Joey Garcia, Isolas LLP (Gibraltar)

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)** along with on chain compliance.

1. 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[141], 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.

[141] https://undocs.org/en/S/RES/2462(2019)

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[142] 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[143] 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 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[144]. 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.

[142] https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf

[143] Section 131 to 140 https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets-2021.html

[144] 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.

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 Interpretations 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;*
- *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[145], there is as yet

[145] https://blog.chainalysis.com/reports/2021-global-crypto-adoption-index

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[146].

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[147] 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[148].

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[149]. 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[150]. 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.

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

[146] https://www.vietnam-briefing.com/news/vietnam-establishes-research-group-study-regulations-cryptocurrencies-
[147] https://www.bsp.gov.ph/Regulations/Issuances/2021/1108.pdf
[148] https://www.bsp.gov.ph/Media_and_Research/Primers%20Faqs/FAQs_VASP.pdf
[149] https://www.sec.or.th/EN/Pages/Shortcut/DigitalAsset.aspx#AUDIT
[150] https://www.sec.or.th/EN/Pages/News_Detail.aspx?SECID=8994

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[151] 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[152] 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[153] 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.

The Regulated VASP and the evolution of Decentralised Finance (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.

[151] 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
[152] https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf
[153] https://www.fca.org.uk/publication/policy/ps19-22.pdf

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.[154] 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.

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[155] 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

[154] https://blog.chainalysis.com/reports/2021-global-defi-adoption-index
[155] https://www.sec.gov/litigation/admin/2018/34-84553.pdf

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[156] 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 (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

[156] 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

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[157] 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[158] 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[159] 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.

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.

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

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[160]. However, whether a non-custodied wallet, relating to a DeFi platform constitutes a cryptoasset firm is potentially not yet completely clear.

2. On Chain Compliance

Joey Garcia, Isolas LLP (Gibraltar), Dr Shlomit Azgad-Tromer Co-founder, CEO and Chief Legal Officer of Sealance Corp

Introduction

The development of regulatory standards and compliance frameworks for an emerging and developing market is a critical factor, particularly when the technology being used and implemented is also developing.

A recent US example – a bankruptcy filing by Celsius, a digital asset lending platform – revealed the names and transaction history of nearly half a million depositors. The

[160] 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

Celsius case also illustrates a risk that arises from the transparency and traceability of the blockchain. The privacy standard in most public blockchains is based on pseudonymity, which can be easily pierced to track user activity and balance. As a result, data leaks of names and wallet addresses can cause privacy harms to blockchain users, since anybody with an internet connection can easily match the on-chain activity and wallet addresses of named Celsius users disclosed in the filing with the dates and amounts of every transaction on their wallet, exposing wallet owners to the risk of theft or extortion.

To mitigate this risk, digital asset holders employ additional privacy enhancing technologies to protect confidentiality of their financial information. The problem is that current techniques to manage illicit finance risk on blockchains rely on transparency and traceability in order to assess user identity. As a result, the same tools used to protect legitimate privacy interests on public blockchains can also frustrate government investigations into malicious activity.

One widely used privacy protocol was Tornado Cash, which was sanctioned in summer 2022 by the US Treasury Department's Office of Foreign Assets Control (OFAC) on the grounds that it had been used in connection with more than $7 billion in illicit financial activity. This puts innocent blockchain users in a bind: rely on privacy through pseudonymity – which can be compromised – or have their funds associated with criminal activity, increasing the risk that they could face penalties, funds could be blocked, or their risk profile increased, potentially limiting their freedom to transact.

Arguably, this potential clash between privacy and compliance is an outcome that can be avoided using technological advances that can harness the power of the blockchain to enforce compliance in a privacy preserving manner, such that it sustains financial confidentiality and privacy for consumers and users, while providing law enforcement and regulators the tools required to enforce compliance, view suspicious information and prevent illicit activity with selective disclosure designated to specific authorised agents. These emerging technologies could serve to strike a better balance between national security, crime prevention and the fight against illicit finance, on the one hand, and the right to privacy, on the other, while harnessing blockchain technology. for its own native compliance.

This section identifies two fundamental premises of financial regulators in designing regulation for crypto markets and argues that — although useful — they face limitations as crypto markets, and the associated decentralised network services ('Web3'), mature. First, financial regulators assume compliance in crypto could lean on the role of financial intermediaries, and that these intermediaries indeed exist in the decentralised financial system, and moreover, are able and fit to carry regulatory responsibilities and, accordingly, liability. Second, financial regulators lean on the transparency of transactions on the blockchain, facilitated by the pseudo-anonymous nature of the users' wallet addresses, as an essential feature of crypto compliance, assuming that the traceability of transactions and addresses is an exclusive means to identify users, through heuristics, given the prominence of blockchain analytics as a methodology designed to enforce compliance-based surveillance and big data techniques. This second assumption about traceability as an exclusive tool renders anonymous and privacy preserving technologies as means to facilitate money laundering. Recent examples of these trends include the actions against Tornado Cash, but also the Virtual Asset Guidance published in October 2021 by the Financial Action Task Force, several stablecoin and digital asset bills being considered by the US Congress and the Markets in Crypto-Assets regulations (MiCA). These and many other jurisdictions are currently considering how to bring digital assets into the regulatory perimeter that applies to financial services, often leaning on the two assumptions that the methodology for compliance and enforcement in crypto can be manifested by expanding the search for financial intermediaries and by enforcing blockchain transparency and traceability.

We would posit that both these assumptions are not adequate for the permissionless and decentralised ecosystem of crypto. Anonymity and privacy are considered means of illicit finance despite representing fundamental values, simply because current compliance methodologies lean on transparency and heuristic based surveillance. Likewise, the search for financial intermediaries as agents of legal enforcement in a decentralised financial system of peer to peer transactions lacking intermediaries, is arguably designed to fail. Digital assets in Web3 often lack an institutional issuer since they are created by individual users interacting with a protocol, and often users trade among themselves and with protocols using an unhosted wallet without financial intermediaries. Because of these incorrect assumptions, our view is that current regulatory frameworks lack the ability to address permissionless financial environments that characterise the emergence of Web3, and as a result could lead to regulatory gaps as these environments evolve. However, the ability of emerging technology to address the risks correctly identified by relevant authorities and policy makers, through the adoption of the technology to embed on-chain compliance by adopting the same consensus principles that underlie blockchain technology to programmatically enforce compliance obligations. It is therefore on that basis worth exploring the merits of such programmable on-chain compliance as a rule-based, blockchain native approach to crypto compliance.

How Crypto Compliance Works Today

Crypto compliance today is largely a replica of anti-money laundering regulation in traditional finance, in that these requirements assume the existence of an intermediary gatekeeper standing at the entrance to the financial system and confirming and validating the identity of participants[161].

In the following, we identify two flawed premises underlying current approaches to regulating Web3: the search for intermediaries in a decentralised environment, and the assumption that traceability and transparency are exclusive means to regulate this space.

The Search for Intermediaries

Current financial regulations target financial intermediaries responsible for performing critical aggregation and settlement functions on behalf of customers. Since these financial intermediaries maintain their transaction records on private, internal ledgers, modern financial regulations have placed financial obligations on them to ensure that they act in the interests of their customers, and otherwise mitigate information and economic asymmetries. To comply with these regulatory obligations, financial institutions implement regulatory requirements through policies, internal compliance controls and monitoring processes. Recognising that Web3 disintermediates the provision of financial services, current regulatory approaches search for alternative individuals or entities upon which to impose these regulatory obligations. However, such approaches do not generally taken into account a clear understanding of the underlying technology and are likely to fail since the alternative intermediaries identified typically do not possess the information to comply with relevant obligations or are ill-suited to regulatory compliance because they are functionally very different from traditional financial intermediaries.

Blockchain Analytics

Because most of the blockchain ledgers today are pseudonymous, law enforcement currently leverages blockchain analytic services that use heuristic, best-effort matching of public transaction information with private information. These heuristic techniques critically rely on the transparency of the blockchain and use big-data

[161] From a US perspective the first anti-money laundering regime to arise was the so-called Bank Secretary Act ("BSA"), a series of U.S. statutes and regulations that emerged in the 1970s, have evolved over the intervening years, and were most recently revised through the U.S. PATRIOT ACT. Legislated for a financial system managed by intermediaries, the BSA's initial purpose was to ensure that banks would collect information about their customers (and their customers' counterparties and transactions) that would provide law enforcement with information designed to provide intelligence for prevention of crime. The BSA establishes reporting and recordkeeping requirements for regulated banks and Money Service Businesses (MSBs), including the filing of suspicious activity reports ("SARs") with FinCen in Treasury. A second tenet of anti money laundering is the requirement to Know Your Customer ('KYC") that is sometimes referred to as Customer Due Diligence (CDD) and is rooted in the Patriot Act and its amendments to the BSA.

techniques to identify and inspect it into data that can fuel compliance and risk management.

The Case for On-Chain Compliance

We believe that current approaches to crypto compliance are inefficient and unsustainable. As argued in the following section, imposing intermediary requirements from ad hoc decentralised players creates grave cybersecurity and espionage risks, undermines consumer protection, and threatens national security as blockchain technology gains broader adoption. Furthermore, it conflicts with the rights to financial confidentiality and to privacy, and jeopardises the innovation of decentralised finance with its promise. On-Chain compliance would address these concerns and provide a better, privacy preserving and blockchain native approach to regulating crypto ecosystems.

Consumer Protection and Information Security Risks

Forcing an intermediary-based approach on the decentralised crypto ecosystem presumes the existence of reliable entities that can collect the information, report it to law enforcement and keep it safe from cyber attacks. However, this is a problematic presumption, since in the decentralised settings many of the intermediaries (especially as captured by the aforementioned expansive definitions) are themselves ad hoc players who may be nefarious, and even if well-meaning, are incapable of protecting sensitive personal and commercial information. In particular, the collection and retention of personal information (e.g. names and physical address) of members of the public should not be carried by entities that are not well equipped to protect it, and lack the training, the resources and the culture of compliance to do so in a safe way. Imposing an intermediary status on such entities substantially increases the risk of data theft and concomitant harm to law-abiding citizens.

When blockchain-based assets are used for payments, as the vision of stablecoins entails, current crypto regulation would arguably not be suitable, appropriate or be able to deal with the inherent risks in the appropriate way. The intermediary-based approach may impose AML obligations on merchants who would be required to collect the personal information of all customers who make payments using an unhosted wallet, in order to relay this information to the money service businesses (MSBs) and banks that serve these merchants. Blockchain-based asset holders would thus be effectively required to disclose their home address to merchants they transact with. This is not merely impractical, but also arguably dangerous as an invitation to extortion or home invasion, if the merchant is rogue or had its systems compromised by a cyber attack. This risk is aggravated by criminals' ability to observe wallets' balances on public blockchains, to identify 'juicy' targets. (Recall that blockchain analytics and its transparency-based heuristics rely on such information being broadcast on public and immutable blockchains.) In a world where cryptocurrencies are a major payment currency, as the future of stablecoins and CBDC entails, transparency of every transaction is not merely an individual risk for a data breach, it is a potential espionage risk in exposing national financial data to prying eyes. Indeed, the prudent regulatory path would be to require stablecoins and CBDC to keep financial confidentiality as traditional banks do, but to allow them on-chain compliance mechanisms, compatible with their nature as a smart contract in a Web3 environment.

Crucially, on-chain compliance would be enforced without compromising the financial privacy and security of cryptocurrency users. While identity information may be recorded on the blockchain ledger, it could be cryptographically protected and not publicly visible. Instead, sensitive personal information (direct or derived) would be visible only to authorised parties, subject to the predetermined policy.

Blockchain-Native Approach: Regulating DeFi

Instead of enforcing principles of traditional financial regulation on a decentralised financial system, on-chain compliance allows regulators to harness the power of the blockchain to enable stronger blockchain based enforcement that is compatible with Web3 infrastructure. One prominent example of the need for an on-chain, blockchain-native approach to compliance is DeFi. DeFi protocols can be distinguished from traditional market infrastructures in several ways. First, typically assets in DeFi are held directly by users in 'unhosted' wallets or through smart contract-based escrow rather than by a centralised service provider or custodian in an account on the asset owners' behalf. Second, settlement and execution are conducted by software (smart contracts) rather than financial intermediaries. Rather than relying on a centralised service provider, operator, or organisation that ultimately exercises discretion, DeFi protocols are governed by open-source code. DeFi is a decentralised financial arena, with no intermediaries. Users may create intermediary or proxy contracts that redirect calls and transactions to a modified contract as a way of updating an earlier contract but they are always self sovereign and hold their assets directly without a custodian.

In the absence of an entity that can serve as an intermediary, on-chain compliance could regulate and enforce compliance in DeFi as a natural, programmable upgrade to the smart contract. For example, on-chain compliance can be compatible with unhosted (self-custodied) wallets without entrusting any third party with control or custody of the funds. Once unhosted users are identified and verified by a legitimate now your customer (KYC) provider, programmable on-chain compliance can monitor the trade and automatically issue reports off the blockchain, without any intermediary intervening in the process. Even for the most sophisticated compliance reports such as SARs, red flag tests can be coded into an on-chain policy and provide jurisdictional compliance.

This would arguably align the concept of DeFi regulation with the compliance focused regulatory standards set out under the FATF Recommendations which continue to be transposed in national law and regulation around the world. It would also allow for the development and use of the technology to address the relevant risks which are prevalent in the DeFi ecosystem, without the approach of defining every decentralised network, protocol or service as a Virtual Asset Service Provider and bringing the activity within the scope of legacy frameworks and standards.

Modernising AML Rules

On-chain compliance is an opportunity to modernise AML rules utilising consensus rules running on a blockchain. Instead of struggling to harmonise KYC practices, or exposing the financial system to a central panopticon with the implications on cyber security compromised, on-chain crypto compliance provides an opportunity for financial institutions to rely on other institutions' attestations and use them for risk management without moving information or exposing it to the user. Sanctions can be enforced on-chain and updated in real time, to prevent any transaction from going through absent compliance. And reports can be administered automatically off chain, saving important time and providing law enforcement with better chances to prevent crime from happening. Saving the redundancy of duplicate KYC checks in every entry would reduce the compliance burden from the financial industry, improve customer and user experience, and allow compatibility of the AML infrastructure with the future of stablecoin and CBDC payments, with robust enforcement that does not rely on intermediaries.

Conclusion

The current tension between privacy and compliance represents an uneasy compromise in traditional financial services that will be tested as crypto markets evolve and achieve broader mainstream adoption. In this evolving ecosystem, it is clear that the current regulatory solutions, which rely upon financial intermediation and blockchain analytics premised on the immutable and transparent nature of the blockchain, will confront limitations; and that attempts to force the regulatory model on decentralised and peer-to-peer transactions will broadly sweep in innocent conduct and hamper innovation in this space. This paper has suggested an alternative solution that can harness the power of modern cryptography and blockchain programmability to overcome the seemingly binary choice between compliance and privacy. Regulators and law makers assessing approaches to govern this evolving space of financial activity should assess the possibilities of adopting these novel tools, to achieve higher efficiency for compliance on the one hand, and privacy and information security on the other.

5

Part 1: Developing Technologies

Section 5

Non-fungible tokens

Section 5: Non-fungible tokens

Anne Rose (Mishcon de Reya LLP), Will Foulkes and Gareth Malna (Gunner Cooke), and Omri Bouton (Sheridans)

Introduction

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. Thereby, NFTs address one of the challenges posed by digital assets: replicability.

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 or within the United Kingdom Gambling Act 2005.

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:
Legal and regulatory areas of focus for NFTs 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 to the left 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 a claim to is the NFT itself: the token. (For more on IPR see Section 11.)

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.

Interaction of NFTs with the financial services regulatory landscape in the UK

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'[162] 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 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 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 regulatory regime

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

under the Financial Services and Markets Act 2000 (Regulated Activities) Order 2001 **(RAO)** if tokens amount to "specified investments";

under the Markets in Financial Instruments Directive **(MiFID)** if the tokens amount to 'financial instruments';

under the Electronic Money Regulations 2011 **(EMRs)** if the tokens amount to e-money; and

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

Activities carried out by persons involved in cryptoasset activity, including where such activities involve NFTs, are also captured by the UK's money laundering regime, regulated by the FCA. We consider that regime in more detail below.

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

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 key exercise, therefore, 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 activities involving 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, units in a collective investment scheme, 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 under 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
   ii. 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).

The FCA has also been keen in recent times to apply a rigorous analysis as to whether a cryptoasset,(including NFTs) might amount to a unit in a collective investment scheme rendering the issuer of that token a firm that would be managing a collective investment scheme, which is an activity that would also require FCA authorisation under Part 4A Financial Services and Markets Act 2000 ("FSMA").

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, nnex 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 NF

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
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;

iii. 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:

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

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

b. 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;

c. 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;

d. issuing payment instruments or acquiring payment transactions;

e. money remittance;

f. payment initiation services;

g. 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.

Future Developments
At the time of writing, HM Treasury is consulting on a "Future financial services regulatory regime for cryptoassets". Under the new regime, financial services activities will be regulated, not the assets themselves and so any activity involving NFTs that would otherwise amount to one of the types of activity brought under the regime will be regulated in the same way. It is anticipated that this new regime will be effected through amendments to FSMA.

The FCA and HM Treasury are also working on putting before Parliament secondary legislation relating to the promotion of cryptoassets in the UK. Under the proposed regime, only authorised persons or those registered with the FCA under the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 will be permitted to issue promotions for cryptoassets in the UK. Importantly, however, NFTs will be excluded from the definition of cryptoassets for these purposes.

Part B:
NFTs and the regulation of gambling in Great Britain

Niki Stephens and Sian Harding (Mishcon de Reya LLP)

Introduction

The definition of "gambling" in the Gambling Act 2005[163] (the primary piece of legislation governing gambling in Great Britain[164]) **(the Act)** 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, awarded 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 therefore 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 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 by persons in Great Britain.

[163] As amended by the Gambling (Licensing and Advertising) Act 2014.
[164] For the purposes of this section, Great Britain means England, Scotland and Wales and excludes Northern Ireland.

"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"—*
   a. *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*
   b. *does not include a sport.*

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[165] 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

[165] 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).

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[166] 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[167] 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[168] 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.

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.

[166] 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).

[167] 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.

[168] In its 'Virtual currencies, esports and social casino gaming - position paper', published in March 2017, available at <https://assets.ctfassets.net/j16ev64qyf6l/4A644HIpG1g2ymq11HdPOT/ca6272c45f1b2874d09eabe39515a527/Virtual-currencies-eSports-and-social-casino-gaming.pdf>

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).

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[169].

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 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).

"Blurred lines" and financial products

Following a call for evidence and public consultation, on 27 April 2023 the Department for Digital, Culture, Media and Sport (the **DCMS**) (the Government department with responsibility for regulation of gambling) published a long-awaited white paper setting out the government's policy proposals for changes to gambling regulation in Great Britain (the **White Paper**)[170]. The White Paper repeats concerns previously raised by the Commission that there has been an increase in novel products that are *"blurring the lines between gambling and other markets such as financial investments and video games", including those that "use emerging technologies, such as non-fungible tokens"*.

The Commission's view is that products that push the boundaries with financial products pose a risk to consumers. Following the collapse of Football Index in 2021[171] (and the subsequent independent inquiry by the government), the

[169] Section 14(5) of the Act.
[170] High stakes: gambling reform for the digital age - UK Government
[171] 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.

Commission is particularly sensitive to product 'novelty' in this regard (as well as generally with respect to products that involve the use of new technology, such as NFTs). In June 2022, the Commission changed its licensing policy to make explicit that it will not generally grant a licence to products whose name, branding, marketing or game rules contain language associated with financial products (such as 'stock'), or which may give the impression that they are an investment or financial product rather than a gambling product.

Therefore, in addition to considering whether a product might fall into the remit of gambling regulation, it is also important to be mindful of the Commission's sensitivity to 'novel' products generally, and in particular where a product might resemble a financial product or have elements of 'investment' in its design.

DCMS Committee Inquiry
Gambling regulation in the UK is currently the subject of a great deal of scrutiny and potential change. Separately to the publication of the White Paper by the DCMS, the DCMS Select Committee, a cross-party committee responsible for scrutinising the work of the DCMS, is conducting its own examination of the government's approach to the regulation of gambling.

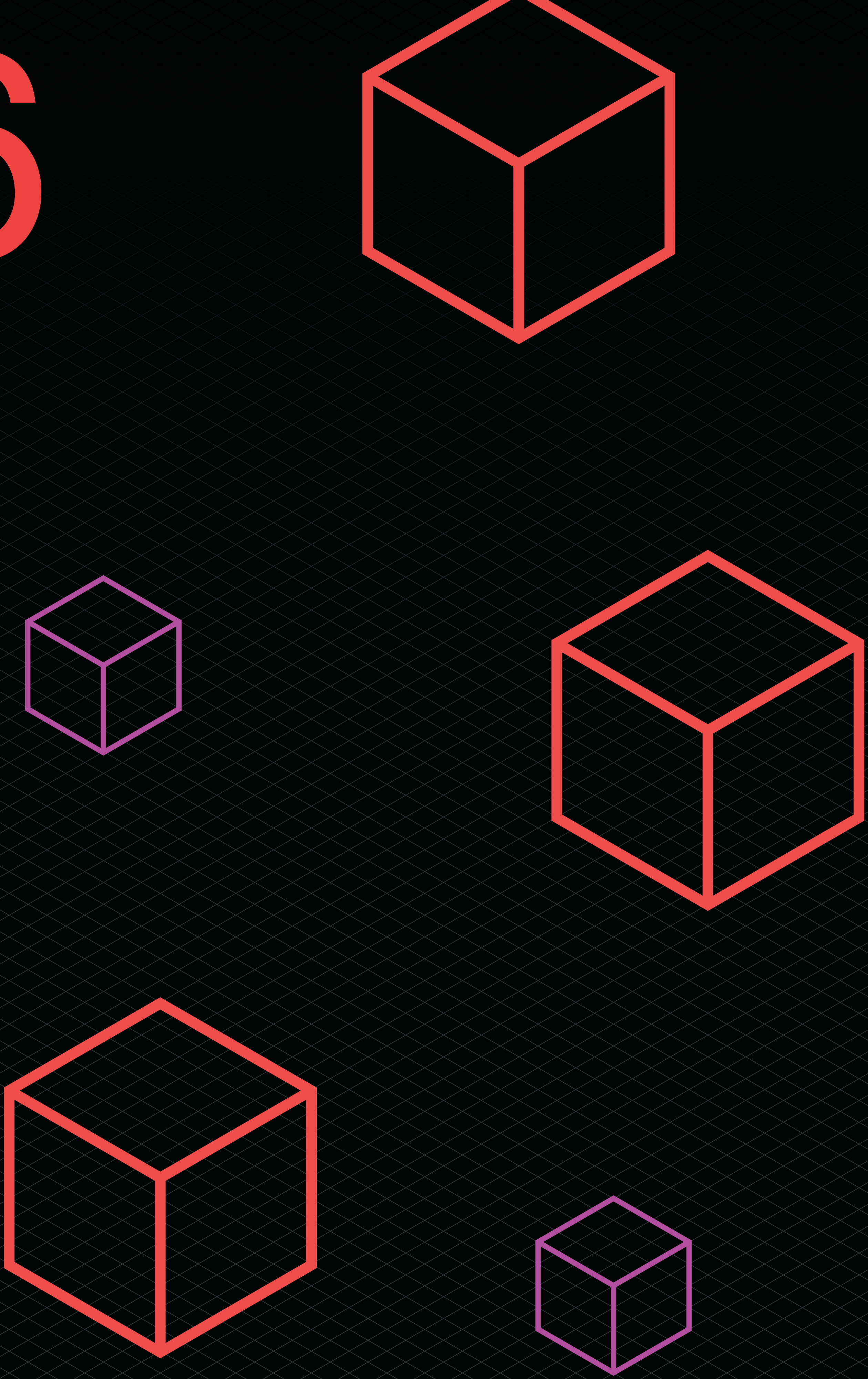
The inquiry invited written evidence on: the scale of gambling-related harm in the UK; what the key priorities should be in the government's review of the Gambling Act (which, as above, has since been published); how broadly the term 'gambling' should be drawn; the possibility of a regulator staying abreast of innovation in the online sphere; and what additional problems arise when online gambling companies are based outside the UK jurisdiction. The DCMS Select Committee will receive written and oral evidence on these topics.

Although the findings of the DCMS Select Committee's inquiry are unlikely to result in any immediate changes to the Act, they may well influence the government and Commission's approach to gambling regulation, including as the policies set out in the White Paper are developed and implemented. It is therefore noteworthy that the terms of reference of the inquiry include an examination of the definition of 'gambling', and into the ways the Commission regulates innovative products.

Conclusion
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. As described above, regulators, including the Commission, are increasingly sensitive to novel business models and products, especially where those involve digital assets. Gambling regulation is also the subject of heightened political interest in the UK, and significant changes are likely to now be made following the publication of the White Paper, although the extent to which the Commission's approach to NFTs and other 'Web3' products may change in the future remains to be seen.

It is therefore critical that any business that issues NFTs and/or that proposes to encourage consumer engagement by 'gamifying' the use of NFTs should seek specialist advice in order to understand the potential impact of gambling regulation. Seeking specialist advice at an early stage can help in identifying potentially problematic elements and provide an opportunity for adjustments to be made, particularly if the intention is for the business to remain outside the scope of the Act. It also has the benefit of readying the business for any potential interest and enquiries by the Commission.

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 8.) 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[172]. 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.

[172] HM_Treasury_Cryptoasset_and_Stablecoin_consultation.pdf (publishing.service.gov.uk)

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 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) and Marc Piano (Harneys (Cayman Islands))

PART A: Smart Contracts

Introduction

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

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

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

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

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

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

Experts and evidence

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

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

- **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.

1. 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 12.

— **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.

<u>ISDA</u>

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[173], including the issuance of an NFT to represent legal opinions relied upon by the prudentially regulated trade association members for regulatory capital purposes.

3. "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.

4. 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

[173] https://arxiv.org/abs/2011.07379 - Datoo A, and Clack CD (2021): Smart close-out netting

parameters for any particular transaction. However, we observe that this requires such parties and their legal counsel to have undertaken diligent digitisation scoping on a contract and transaction basis to ensure that digitised contracts and transactions are legally enforceable and commercially viable.

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

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

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

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

Additional comments

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

- already occur at scale, using standard-form documents and standardised transaction flow;

- operate within a range of known or knowable variables and events, each of which can be accommodated during the digitisation and automated transaction process;

- can access external third-party data (through sources known as "oracles") available in a standard and processable form from trusted sources, where required; and

- produce deliverables or outputs in forms that can be accommodated as part of the digitisation process.

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

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

Inadequate digitisation scoping may risk breach of contract or frustration due to unanticipated issues arising from automatic execution. This may heighten transaction risk for the parties and unnecessarily strain commercial relationships.
Legal counsel may be exposed to liability when facilitating a digitised contract or transaction where full consideration has not been given to the digitisation and transaction flow process, and unintended consequences arise. We note that there is no judicial determination on these specific points as at the date of this 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 12.

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 12.

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".[174]

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[175], 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:[176]

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

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

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.

It should be noted that where smart contracts are implemented on a DLT such as a blockchain, they natively already provide for a degree of data quality assurance with respect to the data they store. For example, on a blockchain, hashes are used to link the blocks on the blockchain preventing tampering of the data, and cryptographic signatures are used to provide for provenance and non-repudiation. Smart contracts cannot directly

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

[175] 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.

[176] 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

query the distributed ledger to retrieve data – they only have access to the payload of those transactions explicitly directed to them as addressees, to data stored in their own, local variables, or to data held by other smart contracts and made available through suitable functions. Also, smart contracts cannot access data (for example, through an API or querying an external database) outside the blockchain, since otherwise different results might be obtained with the passage of time – therefore causing issues in respect of repeatability. Therefore, data required for the operation of a smart contract is obtained through the use of an oracle smart contract (an "oracle"), which, using standard transactions that are recorded on the distributed ledger, allow external data sources to push data in (either for example, upon explicit solicitation or periodically)[177].

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.[178] 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.

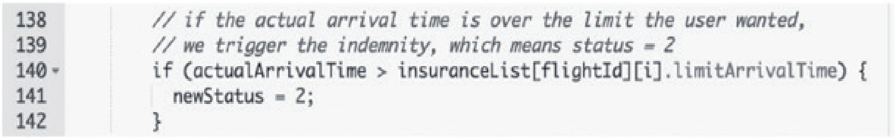
It is the fact that smart contracts seek to automate performance, and therefore need to automate the process of applying fact to a contract at hand, that elevates the importance of data governance from the traditional legal agreement context. A smart contract operates through Boolean logic – a form of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

[177] "Data quality control in blockchain applications", Cinzia Cappiello, Marco Comuzzi, Florian Daniel and Giovanni Meroni – available at: https://www.researchgate.net/publication/335399935_Data_Quality_Control_in_Blockchain_Applications

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

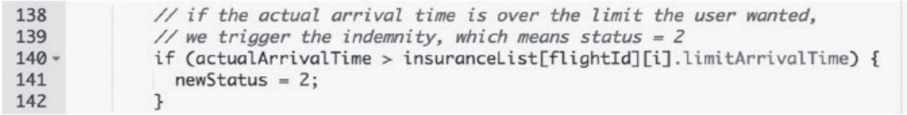
hours, the compensation terms are automatically triggered and given effect. Putting this into colloquial Boolean algebra, "if the plane is late by more than 2 hours, then compensation must be paid out". The key code representing this logic is shown below[179] (note that the variable limit 'limitArrivalTime' is defined as 2 hours elsewhere in the code).



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

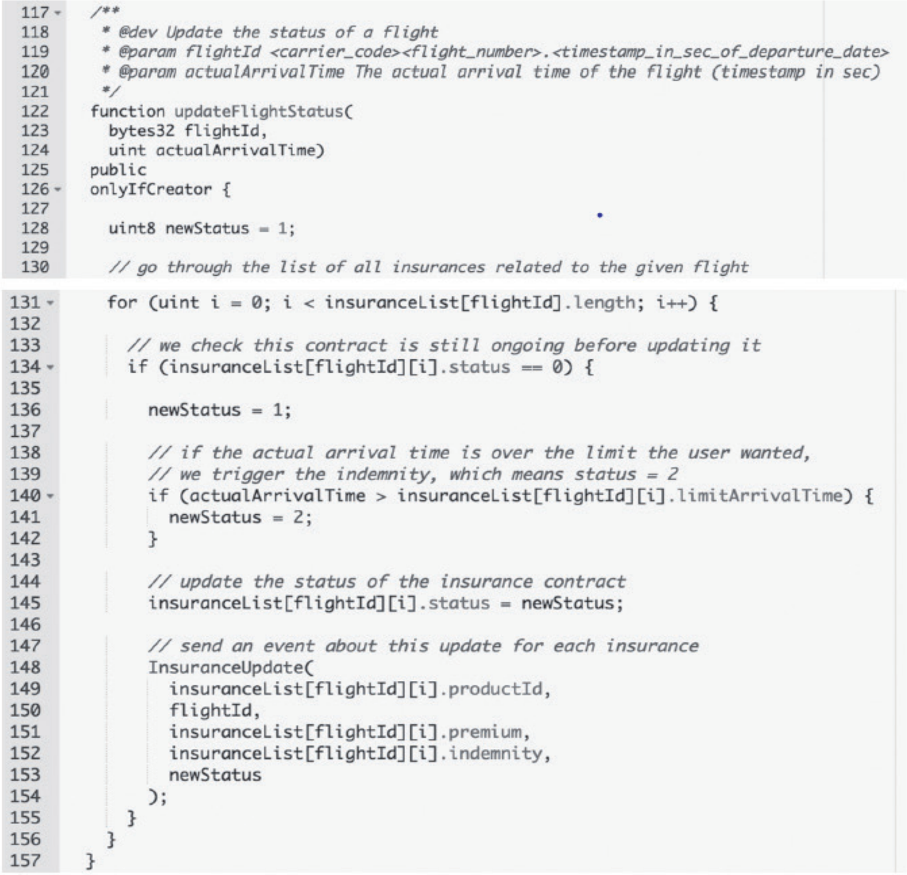
Figure 12.2 The core logic code for the Fizzy smart contract application

The core logic code for the Fizzy smart contract application



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

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



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

  uint8 newStatus = 1;

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

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

      newStatus = 1;

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

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

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

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

[179] Akber Datoo, 'Legal Data for Banking: Business Optimisation and Regulatory Compliance' (John Wiley, 2019)

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 10 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.

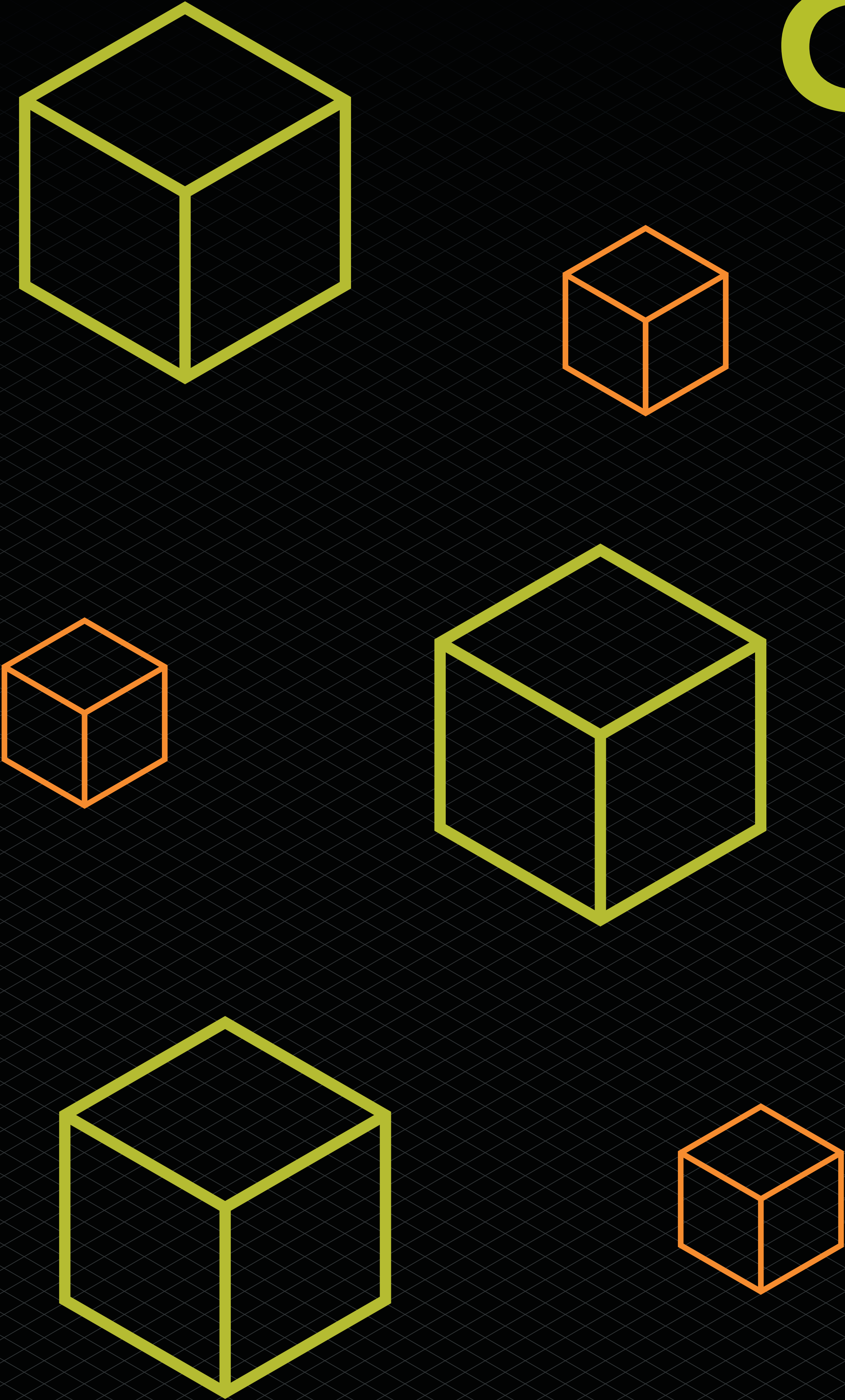
5. **Defer Decision:** a particular violation of a data quality threshold on an input might not be enough, in itself, to result in a definitive automated action, and the decision may simply be deferred.

Part 2: Impacts on the Wider Landscape

Section 8

Daos – Decentralised Autonomous Organisations

8



Section 8: Daos – Decentralised Autonomous Organisations

Luis Powery and Marc Piano, Harney Westwood & Riegels LLP (Cayman Islands); Arthur Horsfall, Guy Wilkes and Grace Houghton, Mishcon de Reya LLP (London); Petri Basson and Karel Olivier, Hash Directorships (Cayman Islands); Marc Jones, Stewarts Law LLP (London)

Part A – What is a DAO?

1. Introduction, definition and summary of key features

The idea of a decentralised autonomous organisation **(DAO**) was first articulated by Vitalik Buterin in 2014 as “an entity that lives on the internet and exists autonomously, but also heavily relies on hiring individuals to perform certain tasks that the automaton itself cannot do” [181]. This is distinguished from a decentralised organisation **(DO)**, defined in the article as “a set of humans interacting with each other according to a protocol specified in code, and enforced on the blockchain”, because “in a DO the humans are the ones making the decisions, and a DAO is something that, in some fashion, makes decisions for itself” [182].

In practice, most so-called DAOs are in fact DOs, because although both have internal capital (i.e. a treasury, however structured), few so-called DAOs are capable of making autonomous decisions and instead rely on human interaction and decision-making, with some degree of automation and blockchain technology involved in the governance process and implementing the outcome of decisions. This is somewhat confusing. Nonetheless the concept of humans using the blockchain to organise, interact and make decisions in pursuit of a common purpose, has become colloquially known as a DAO.

With this in mind, from this point forward this section refers to a “DAO”, even though such references are to associations of humans with the features of a DO; however inaccurate, that is now common parlance. We are not yet aware, at the date of this publication, of any “true DAOs”, only DOs with varying degrees of success in their current challenge of decentralisation. Given the anticipated legal and regulatory landscape around DAOs, this challenge is particularly critical for the future viability of these associations.

DAOs, then, such as they are, are an association of often anonymous or pseudonymous members with internal capital. The DAO uses technology to communicate and exchange ideas in pursuit of a common purpose, as well as blockchain technology to vote on, and in some cases, implement agreed governance proposals.

Voting on a governance proposal is typically conducted through the use of a “governance token”. These are fungible or non-fungible digital asset tokens recognised by the DAO, and associated support websites (such as Snapshot), as having voting rights in the DAO and which may also serve as a “badge” of DAO membership. Voting is typically conducted through the DAOs own front-end website, or a third-party support site, allowing the wallet holding the tokens to be recorded as voting for or against a proposal.

Proposals that pass represent “the will of the DAO” and constitute a mandate for implementation or enforcement by the DAO as a whole. Implementation may be through the blockchain (where such changes are capable of implementation through smart contracts, particularly where a DAO governs a blockchain protocol, or the direction of treasury assets), or the instruction of third parties to perform functions in pursuit of implementation of the mandate, and adherence may be by behaviour or governance process changes.

[181] “DAOs, DACs, DAs and More: An Incomplete Terminology Guide”, Decentralized Autonomous Organizations, Vitalik Buterin, 6 May 2014

[182] “DAOs, DACs, DAs and More: An Incomplete Terminology Guide”. Decentralized Autonomous Organizations, Vitalik Buterin, 6 May 2014

The purpose of a DAO is generally unrestricted, ranging from control over blockchain protocols, to decentralising access to space. As of early December 2022, around 10,000 to 11,000 DAOs are recorded[183].

2. Decentralisation

The first effort to recognise the ideal of a DAO was "The DAO" project developed and launched by slock.it during 2016. Slock.it's presentation of the history of the DAO and the lessons learned, succinctly sets out the rationale for a DAO and the philosophy behind decentralisation as a concept:

> *"When you need funds to grow your company in the cryptospace, doing a token sale is a promising option and in this case would have helped guarantee an initial, decentralized user base for the Ethereum Computer and the Universal Sharing Network.*
>
> *"But after coding up a simple crowdfunding contract, we could not stop ourselves from giving the token holders more power. And with this, the story of the DAO started.*
>
> *"In the beginning, we created a slock.it specific smart contract and gave token holders voting power about what we — slock.it — should do with the funds received.*
>
> *After further consideration, we gave token holders even more power, by giving them full control over the funds, which would be released only after a successful vote on detailed proposals backed by smart contracts. This was already a few steps beyond the Kickstarter model, but we would have been the only recipient of funds in this narrow slock.it-specific DAO.*
>
> *We wanted to go even further and create a 'true' DAO one that would be the only and direct recipient of the funds, and would represent the creation of an organization similar to a company, with potentially thousands of Founders.*
>
> *"In this truly decentralized and autonomous model which we detailed in a whitepaper, people would create an organization together, and we as slock. it would be just one of the many companies that would offer products and services to it. Offers would take the form of Proposals detailed in smart contracts and giving the project even more flexibility.*
>
> *"After getting as much legal advice as we could, we came to the conclusion this model was also superior to token crowdsales in general. Nothing like this had ever happened before though, and therefore all legal advice was just that, advice. But we already believed in the dream of Decentralized Autonomous Organisations and were excited to be part of this revolution.*
>
> *"We made all the code open source so anyone could start one of these DAOs, audit their code and make improvements to their feature set."*[184]

Although it is a philosophical ideal and the purported core feature of DAOs, decentralisation as a concept is, and is likely to remain, difficult to define or quantify to any degree of confidence. This difficulty creates uncertainty and an inconsistency of approach for DAOs, their participants, legal advisers, other service providers, lawmakers and regulators.

Vitalik Buterin's original article examined the rationale of decentralising human organisation:

[183] https://deepdao.io/organizations and https://snapshot.org/#/ accessed on 27 November 2022.
[184] "The History of the DAO and Lessons Learned", The Quest For Autonomy, Christopher Jentzsch, slock.It, 24 August 2016

> *"The idea of a decentralized organization takes the same concept of an organization, and decentralizes it. Instead of a hierarchical structure managed by a set of humans interacting in person and controlling property via the legal system, a decentralized organization involves a set of humans interacting with each other according to a protocol specified in code, and enforced on the blockchain. A DO may or may not make use of the legal system for some protection of its physical property, but even there such usage is secondary."* [185]

Since this description was published in 2014, the constituent elements of a DAO (which, as noted above, is currently in practice a DO) generally extend far beyond mere code, although the code/blockchain aspect itself remains a key element of its identification – separate to other forms of human organisation – and operation.

Typically, a DAO constitutes:

- a front-end website which may or may not facilitate interaction with governance processes;

- a suite of off-chain documentation explaining its purpose, operation and initial governance processes;

- community participation through online for a Discord or other social media channels;

- one or more smart contracts (including multisignature, or multisig, wallets) for issuing governance tokens, executing some operational elements, and holding internal capital such as a treasury;

- and, in many cases, use of third-party websites to facilitate the governance process such as presenting and voting on governance proposals.

The obvious point here is that a DAO does not spontaneously come into existence. The above components evidence a concerted effort by a group of people acting together to create the infrastructure through which a DAO can be created and operated. The number of participants in that group, and their geographic spread may vary, but they are very clearly not decentralised, by necessity. This same group of DAO founders will typically oversee the inception and initial development of a DAO and seek to steward it towards increased membership and participation, with a view to eventually fully vesting management and control into the community of token holders. In this way, many DAOs start of largely centralised but may aspire to significantly more decentralisation than when they began life.

Additionally, many DAO founders – or eventually, the community – elect or appoint individuals to positions of supervision or management over some or all of the operations and/or governance processes of a DAO as a form of control layer. For example, The DAO had "curators" and other DAOs may convene a governing council or a functional equivalent. This approach may make day-to-day DAO operations more efficient, but it also risks being construed by regulators and lawmakers as evidencing control over the DAO by a small group of identifiable individuals, with concomitant regulatory consequences.

In the case of The DAO, the US Securities and Exchange Commission determined that such curators exercised significant control over the operations of the DAO, which had implications for US securities law purposes[186]. The Financial Action Task Force, in its guidance to Recommendation 15 relating to anti-money laundering obligations for "virtual asset service providers" **(VASPs)**, similarly notes:

[185] "DAOs, DACs, DAs and More: An Incomplete Terminology Guide", Decentralized Organizations, Vitalik Buterin, 6 May 2014

[186] "Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO", Section III(B)(4)(a), Securities and Exchange Commission, Release No. 81207 / July 25, 2017

> *"In cases where a person can purchase governance tokens of a VASP, the VASP should retain the responsibility for satisfying AML/CFT obligations. An individual token holder in such a scenario does not have such responsibility if the holder does not exercise control or sufficient influence over the VASP activities undertaken as a business on behalf of others"* [187],

further noting that:

> *"Where it has not been possible to identify a legal or natural person with control or sufficient influence over a DeFi arrangement, there may not be a central owner/operator that meets the definition of a VASP"* [188].

DAOs and their legal advisors should therefore carefully consider the level of control exercised over a DAO by founders, both initially and on an ongoing basis, and any subsequent layers of management or control in the future.

DAO "decentralisation" may be further challenged by reference to its initial service provider setup. For example, slock.it in the same blog post above note that:

> *"For the DAO to be truly independent of slock.it, the default service provider to the DAO would have to be replaced by a set of independent curators. A lot of well-known experts from the Ethereum community volunteered to do this job, which gave the project additional traction. Slock.it saw its main responsibility as continuing to help with the development of the DAO framework, alongside many volunteers on github"* [189].

Although the curators and their roles were intended to move The DAO towards independence, their role was influenced by the SEC's analysis of The DAO's activities. The SvEC also determined that the continuing role of slock.it in overseeing The DAO constituted "significant managerial efforts"[190]. Nonetheless, slock.it recognised that it could not continue to be the default service provider to The DAO if it was truly to be independent and believed the appointment of curators could help move the needle towards independence.

In practice, many DAOs continue to retain some sort of relationship with its founders, at least initially, through significant token allocations or engaging a company owned by the founders as a service provider, such as a "Labs" entity, which provides research and development services to the DAO or the relevant protocol it governs. This again may lend to challenge by regulators who may construe the relationship between a Labs or other default service provider entity and a DAO as one of control. As a rule of thumb, if a party can intervene in the operations of a DAO or its protocol in the case of an emergency, that party may be construed as having a control relationship. DAOs and their legal advisors should carefully consider such arrangements, their purpose and intended duration. Eventually, that link may need to be severed to defend against a control challenge with legal and regulatory obligations potentially also arising if such a determination is upheld.

3. How does a DAO operate?

The rules of the DAO are initially established by a core team of community members through the use of smart contracts. These smart contracts lay out the foundational framework by which the DAO is to operate. They are publicly accessible and auditable, often accompanied by extensive technical documentation, so that any potential member can fully understand how the protocol will function at every step.

[187] "Updated Guidance for a Risk-based Approach – Virtual Assets and Virtual Asset Service Providers", paragraph 68, Financial Action Task Force, October 2021

[188] "Updated Guidance for a Risk-based Approach – Virtual Assets and Virtual Asset Service Providers", paragraph 69, Financial Action Task Force, October 2021

[189] "The History of the DAO and Lessons Learned", The Birth of "The DAO", Christopher Jentzsch, slock.It, 24 August 2016

[190] Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934:
The DAO", Section III(B)(4)(a), Securities and Exchange Commission, Release No. 81207 / July 25, 2017

After these rules have been fully recorded on the relevant blockchain, the next step for the DAO is to source funding: the DAO needs to determine the best fund-raising strategy, and which governance mechanisms will work best for its purposes.

DAOs typically bestow governance and raise capital through token issuances whereby the DAO sells its governance token to raise funds that will be held in treasury, controlled by and for the benefit of the DAO. In return for payment of fiat or other digital assets, token holders are given certain voting rights, usually proportionate to their holdings. Voting power is often distributed across users based on the number of tokens they hold. For example, one user that owns 100 tokens of the DAO will have double the amount of voting power than a user that owns 50 tokens – although this can vary.

Generally, at this point, once the code is deployed it cannot be altered by any means other than by reaching a consensus amongst voting token holders, pursuant to the DAO's governance protocol. That is, no special authority can modify the rules of the DAO; it is entirely up to the community of token holders to decide.

Types of DAO and their uses

Protocol DAOs
This type of DAO is one of the most common. As the name indicates, these DAOs focus on supporting the governance of decentralised protocols. When tokens are used as the voting metric for introducing and approving any changes in the protocol, such governance structures represent protocol DAOs. A notable example of a protocol DAO would be MakerDAO – one of the original DAOs. MakerDAO utilizes smart contracts to help users borrow and lend cryptocurrencies at customized lending rates and estimates of repayable amounts. The platform utilizes the Maker protocol's governance token MKR for holders to use when voting on different proposals in the Maker protocol.

Collector DAOs
This type of DAO is a relatively new one. This type of DAO primarily focuses on pooling or collecting funds so that the community behind it can have collective ownership of blue-chip NFTs like the Bored Ape Yacht Club and other digital collectibles.

Service DAOs
This type of DAO is another relatively new one. Service DAOs create decentralized working groups for people to work. This can be to individuals, businesses or even other DAOs. This type of DAO arose from people trying to provide services to DAOs in areas where they were deficient – talent acquisition, talent management, legal uncertainties etc.

Investment DAOs
This type of DAO (also known as a Venture DAO) generally pools funds for investments in early-stage web3 startups, protocols and even off-chain investments. One of the more popular investment DAOs would be Krause House – a venture DAO trying to buy a professional NBA team.

Social DAOs
This type of DAOs are collaborative platforms for social networking in the cryptocurrency space. Social DAOs are focused on the self-organizing community aspect of DAOs by bringing together like-minded individuals such as builders, artists, and creatives. While Social DAOs are community focused, typically there is a barrier to entry such as owning a specific number of tokens, owning an NFT, or being personally invited. An example of a social DAO would be LexDAO – a decentralized legal guild focusing on the various aspects of 'crypto law'.

PART B – Pros and cons of a DAO

Pros	Cons
Decentralised – cannot be controlled/shutdown	Hacks (vulnerability of code, especially if open source; "flash loan" attacks in which money borrowed from a decentralised finance pool is used to arbitrage on a DeFi protocol, then the capital is returned to the pool quickly after making a profit from the arbitrage, and such profit remains after the borrowed capital is repaid) and exploits which, although not a "hack", exploit opportunities in protocols or systems to the advantage of the exploiter
Trustless/Autonomous	Legal uncertainty (regulatory implications/sanctions)
Enables global cooperation (especially for people in restrictive countries)	Lack of speed for decision making (potentially adds time for transactions)
Open source	Concentration of voting power

Pros

1. Decentralised

As noted above, whilst the decentralised nature of a DAO can sometimes be questionable, in principle the DAO will have no central body responsible for its governance. Unlike classic limited liability companies, which typically have a board of directors, whose role it is to put in place the decisions of those eligible to vote, a DAO's code is automatically updated when a decision is made. Decisions therefore do not require reliance on certain individuals to be run but instead rely on the code.

2. Autonomous

As described above there is continued discussion as to whether a DAO must be fully autonomous and automated to be considered a DAO (rather than a DO) or whether the concept of autonomy can be more broadly interpreted. Whilst we are unaware of any "True DAOs" in most cases the need for human oversight will be reduced from traditional off-chain organisations. Even where smart contracts require a human trigger to execute, they then do not require external human management to run them.

3. Global cooperation

The voting tokens in a DAO are not fixed to certain jurisdiction or require to be allotted under national regulations. This makes for a low barrier to access and allows anyone anywhere in the world to purchase tokens and be able to vote on the decisions of the organisation.

4. Open Source

The code which sets out the rules on which the DAO operates is available for everyone to see. This therefore provides clarity for all token holders as to how they can contribute to the running of the DAO but also allow other programmers to update and improve the programming for future DAOs.

Cons

1. Hacks

Whilst open source code can be a positive aspect to a DAO (in that it allows anyone to view and develop the programming on which the DAO is based), there are also drawbacks. If the coding includes imperfections and loopholes (which any would-be hacker can see) the DAO is susceptible to attack. Whilst there have been historical incidences of large losses as a result of flaws in a DAO's code, early errors have driven the improvement of the programming, and the tokens on which it is based on, to generally advance the security of DAOs.

2. Legal uncertainty

As highlighted in Part C, as DAOs continue to evolve and become more common place, their legal status and the regulations relating to DAOs will need to catch up. Whilst there is uncertainty, it is clear that the UK by way of the Law Commission's recent call for evidence wishes to understand what currently prohibits DAOs from choosing UK legal structures and how this can be addressed in the future[191].

3. Lack of speed for decision making

As all holders of governance tokens have the ability to vote on all the decisions of the DAO, this can slow down the time for transactions. Unlike with a UK company where day-to-day decisions are delegated to the directors, all decisions are put to the holders of the tokens. This can cause significant delays even if a voting mechanism does not require everyone to vote to make a decision.

4. Concentration of voting power

Whilst DAOs are predominantly intended to facilitate a more democratised organisational structure, allowing all members to vote on its decisions, a recent report [192] found that this is negatively impacted by the distribution of voting power.

The report reviewed the distribution of governance tokens of 10 major DAOs and found that fewer than 1% of the governance token holders held more than 90% of the voting power. As well as the voting distribution the report considered how many holders in the reviewed DAOs could create a proposal and how many could actually pass it.

Governance will vary from DAO to DAO, but the report considered DAOs with the following criteria: (i) that to create a proposal would require a holder to have between 0.1-1% of the governance tokens and (ii) would require 1-4% to be able to single handedly pass a proposal. This would mean that only 1 in 1,000 to 1 in 10,000 users in the 10 DAOs could make a proposal and between 1 in 10,000 to 1 in 100,000 users could pass a proposal single-handedly.

There is however a balancing act. If the threshold is too low, then the DAO would likely not function effectively due to the sheer volume of proposals. Whereas if the concentration of voting power is too high then this questions whether, in fact, the DAO can be considered decentralised due to power to making decisions on sitting with so few.

[191] Law Commission – Decentralised autonomous organisations (DAOs) Call for evidence, November 2022

[192] https://blog.chainalysis.com/reports/web3-daos-2022/

PART C –
Legal Implications to Consider when Setting up a DAO

1. Regulatory considerations

Legal implication to consider when setting up a DAO
Those considering setting up a DAO need to consider whether the DAO's activities or participants fall within the perimeter of UK financial services regulation.

For the most part, financial services regulation is technology-neutral. As such, when considering whether a DAO, or any part of it, is subject to regulation, it is necessary to look behind the structure and consider whether any part falls within the scope of the UK Financial Services and Markets Act 2000 (FSMA).

Pursuant to s.19 of FSMA, a person is prohibited from carrying on regulated activities by way of business in the UK unless it is authorised to do so by the Financial Conduct Authority (FCA), it is an exempt person or an exemption applies. This is known as the "General Prohibition".

A business will be carrying on regulated activities if it is:

— carrying on activities of a 'specified kind';

— in relation to investments of a 'specified kind'; and

— is doing so by way of business in the UK.

For a DAO, the analysis is not straightforward and is subject to legal uncertainty. The FCA has provided limited guidance on its treatment of cryptoassets generally in its publication Guidance on Cryptoassets Feedback and Final Guidance - PS19/22 (Policy Statement), but there is little guidance specifically on DAOs.

Territoriality

A DAO is only subject to UK regulation if any legal or natural person is undertaking regulated activities in the UK. However, the whole point of a DAO is that it is decentralised – operating cross border. Accordingly, it can be difficult to determine where the activity is carried on.

The FCA has provided limited guidance in its Policy Statement by reference to its more general Handbook Perimeter Guidance.

PERG 2.4 provides details around the link between regulated activities and the United Kingdom. It sets out that even where part of the activity is outside the UK, a person may still be carrying on a regulated activity in the UK. For example, a firm that is situated in the UK and is safeguarding and administering security tokens that are securities or contractually based investments for clients overseas will be carrying on activities in the UK even though the client may be situated outside the UK.

By Way of Business

Activity is only regulated if it is undertaken by way of business. A DAO which is controlled by a multitude of private individuals, who are not operating a trade and where participation is not for commercial purposes, may not be operating by way of business regardless of the underlying activity.

Specified Investments

A DAO is conventionally controlled by token holders. As a starting point, it is generally necessary to consider whether the tokens are specified investments under FSMA and potentially subject to regulation. Tokens which have characteristics which mean they are the same as or akin to traditional regulated instruments like shares, debentures or units in a collective investment scheme are within the regulatory perimeter and are known as "security tokens". Firms carrying on specified activities involving security tokens need to ensure that they have the correct permissions and are following the relevant rules and requirements.

This is important, not only for the DAO itself but also crypto exchanges which list the tokens. Exchanges cannot generally list security tokens unless they themselves are licensed by the local regulator to provide financial services.

Who is regulated?

Both legal and natural persons carrying out regulated activities require authorisation. In the case of DAOs, it is not straightforward which legal entity requires authorisation and is subject to regulation. Depending upon on the structure of the DAO any of the following could require authorisation:

a. A promoter of the DAO
b. A miner/minter of DAO tokens
c. An incorporated company or other legal entity used by the DAO to effect "real world" transactions
d. The DAO as a partnership of its token holders
e. The DAO as an unincorporated association of its token holders
f. An individual token holder
g. A token holder with special rights
h. A committee of token holders
i. An exchange dealing in DAO tokens

The implications of regulation

In order to advise on the implications of regulation, it is necessary to consider the rights and obligations which attach to a particular security token. Security tokens which have rights akin to debt securities will be regulated in a similar manner to conventional debt securities. Tokens which are units in a collective investment scheme will be regulated like other collective investment schemes.

However, with all security tokens it is necessary to consider how tokens are initially offered. If a token is a transferable security and the tokens will either be offered to the public in the UK or admitted trading on a regulated market, an issuer will need to publish a prospectus unless an exemption applies. If a prospectus is required, the specific disclosure requirements will depend on the type of security.

The regulatory treatment of a token may change over the token's lifecycle. For example, initially, a token may be regarded as regulated security token, but over time change to an exchange token.

Money Laundering Regulations

The UK's anti-money laundering regulations are set out in the Money Laundering, Terrorist Financing & Transfer of Funds (Information on the Payer) Regulations 2017 (MLRs).

Since 2019 cryptoasset exchange providers and custodian wallet providers acting in the course of a business carried on by them in the UK are subject to the MLRs and must be registered with the FCA.

Cryptoassets are widely defined as 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" and will almost certainly encompass DAO tokens.

The definition of cryptoassets exchange providers is similarly wide and includes the following (undertaken by way of business):

a. exchanging, arranging or making arrangements with a view to the exchange of, cryptoassets for money or money for cryptoassets,

b. exchanging, arranging or making arrangements with a view to the exchange of, one cryptoasset for another, or

c. operating a machine which utilises automated processes to exchange cryptoassets for money or money for cryptoassets.

As such it is not simply those businesses that sell or buy cryptoassets that are caught, merely facilitating the exchange of cryptoassets by another person may be caught.

2. Tax Considerations

Is a DAO a taxable entity?
It was thought to be a misconception that a DAO possesses separate legal personality with the ability to act independently of their promoters or owners. Under the law as it stands, they could be expressly incorporated as a separate legal person (as a company or partnership with its token holders being classed as separate legal entities such as trusts, individuals or companies. Failing this, the DAO is most likely to be classified as a general partnership.

DAOs are not currently recognised as legal entities in their own right. Potentially, in the abstract, they could be seen as a general partnership or a joint venture agreement between participants.

a. Some DAOs are linked to a legal entity such as a limited liability company. Such DAOs would have official legal status.

b. If they were to be classified as general partnerships, then they would be tax transparent (whereby we would look through the corporate structure to the true owners).
They are not considered to be separate legal entities, and the partners are thus jointly and severally liable.

DAOs that are not linked to legal entities might struggle to comply with laws as the decentralised nature makes it difficult to determine who is liable to file the tax returns. It is unclear whether they would be taxed as foreign companies if their members are resident abroad.

DAOs can still be an ‘entity’ for tax purposes. In the US regulations provide that a joint venture or other contractual arrangement may create a separate entity if the participants carry on a trade, business, financial operation or venture and divide the profits therefrom[193]. The key is that the DAO generates profits and divides them between their members.

Thus, to the extent that a DAO is created by investors who intend to vote and opt for investment proposals, contribute funds for investment, and share the profits, the DAO may be a separate tax entity. Some DAOs formed for purposes other than carrying on a trade or business and making profit, such as a DAO created for raising funds to purchase a copy of the US Constitution, are likely not considered tax entities.

Limited Liability Company

In the United States, both Wyoming and Vermont have recently passed legislation that allows DAOs to register as limited liability companies, under their own name, and with their own legal personality.

A **Wyoming LLC** is governed by “articles of organization”, operating agreements,

[193] Decentralised organisations: Tax considerations | Business Blockchain HQ

and smart contracts. All of these items can detail the rights and duties of the DAO's members. Under the terms of the legislation, a DAO is "a limited liability company whose articles of organization contain a statement that the company is a DAO."

Standard corporations are usually burdened with double taxation on income (business profits are taxed and then shareholders pay tax on dividends). LLCs receive pass-through treatment – allowing allocated profits to be taxed on each member's tax return. For example, DAO LLCs registered in Wyoming are usually regarded as pass-through entities meaning that their members are responsible for paying income taxes. Foreign members of DAO LLCs registered in Wyoming may be subject to the standard 30% withholding tax on their US source income. Since Wyoming is one of the few US states without state taxes on personal and corporate income, the DAO LLC registered there is subject only to an annual state tax of USD 60 or 0,0002% of all assets located and employed in Wyoming (whichever is greater)[194].

Aside from tax, investors have had growing concerns about the legal liability resulting from their investments in DAOs (i.e. their personal assets could be put at risk for any lawsuits or debts of the DAO). As a result, two states, Vermont and Wyoming, have allowed DAOs to register in their states as DAO LLCs which, like regular LLCs, provide the benefit of limited liability for the DAO members. This is also important for tax purposes as the members will not be personally liable for any tax liabilities of the DAO.

From a tax perspective, a DAO LLC, because it is registered under state law, may be treated as a domestic partnership for tax purposes. Although this is better for legal reasons, this may be detrimental for the US partners, who must report their share of the DAO's income and losses — regardless of whether the DAO makes a distribution. However, it may be possible for a DAO LLC to elect to be treated as a domestic corporation for tax purposes, which, on the one hand, would prevent passthrough taxation, but on the other hand would subject the DAO's income to US corporate tax.

Persons who own tokens issued by DAOs may also be subject to capital gains tax on the capital gains generated from the sale of their tokens. When a token is exchanged for another token, this will be a taxable event.

Foundation Company

Several jurisdictions including Switzerland, Singapore and the Cayman Islands offer memberless corporate vehicles such as foundation companies.

The Cayman Islands adopted the Foundation Companies Act, 2017. This introduced a new type of legal entity called a foundation company. This can function like a regular civil law foundation or a common law trust, but it is a body corporate, with limited liability, separate legal personality from its members and directors and other officers. It can sue and be sued and hold property in its own name and exist to further non-charitable purposes. Key features of foundation companies that distinguish them from other types of corporate vehicle available in the Cayman Islands include that the company does not have to have members following incorporation, amendments to its memorandum and articles of association can only be made if expressly stated and it is not allowed to pay dividends to its members.

Instead of members, the foundation company can have 'supervisors' who are not owners of the foundation. Their function is merely to ensure that the directors of the foundation company comply with their obligations, and act in accordance with the governing documents of the foundation company. The supervisors are supposed to act in the interests of the foundation company and not in their own interest, as they do not have any equity interest in the foundation company.

[194] https://www.withersworldwide.com/en-gb/insight/on-the-rise-distributed-autonomous-organizations-daos

Members of DAOs sometimes do not want to link legal entities to DAOs because they are concerned that this might lead to taxation of the DAOs. This is not an issue in the Cayman Islands as it does not impose any direct taxes. This leaves open the question of whether the foundation company can be set up in a tax haven to obtain similar benefits. However, this would likely result in reactive tax measures by governments and legislatures around the world. (See the option of a structural mix below.)

A structural mix

A structural mix involves different entities performing different and separate functions in support of a DAO. For example, a Cayman Islands foundation company can exist to support and act on the instructions of the members of a DAO. In turn, the foundation company contracts with a Bulgarian company that provides services to the DAO, under which the foundation company pays the Bulgarian company using DAO treasury funds (which may or may not be assets of the foundation company, or may be under the direction of the foundation company) in exchange for the Bulgarian company providing technical and organisational support to the foundation company for the benefit of the DAO. The Bulgarian company will pay tax on the income generated from providing services to the Cayman Islands company.

Malta has also begun to develop a new DAO-based corporate scheme. The Maltese scheme allows for the registration of 'Innovative Technology Agreements', for distributed ledger technologies. Whilst this does not grant DAOs legal personality, it does attempt to provide DAOs with some assurances, particularly in the context of local approval and recognition. The advantage of this approach is that it offers a high level of flexibility to DAOs, providing them with the ability to operate internationally, whilst establishing a foundation to comply with Maltese tax laws.

A Cayman Islands foundation company, Wyoming DAO LLC or a similar legal entity is strongly recommended. Such an entity will have mainly a protective function. Any services supporting the operation of the DAO may be provided by a second entity registered in a jurisdiction having low taxes and an affordable IT workforce. The risk here is the potential reactive tax rules when governments examine the approach, together with any potential regulatory implications on the arrangements or activities of or between the entities.

Where a DAO is located

Where a DAO is "located" depends on what question is being asked and by which court. A DAO may be treated as being present in one or many jurisdictions.
The issue is that they are ultimately transnational in that they may have a global presence, no principal HQ and do not submit to any specific jurisdiction — that is the very nature of a DAO. Because DAOs typically exist solely on the blockchain and do not register with any government authority as such, DAOs could potentially be classified as a foreign partnership for tax purposes — even in situations where all DAO owners are US tax residents.

However, with no physical place of business, an all-digital treasury, and members dispersed across multiple countries, counterparties generally want to contract with an entity that in some way represents, acts on behalf of, or "is" (depending on perspective) the DAO. That entity has to exist in some form somewhere, although depending on the purpose and activities of that entity, it may not be the corporate embodiment of a DAO in and of itself.

Under this approach, DAOs would be able to pick and choose the jurisdiction in which they find most favourable to establish one or more corporate vehicles to contract with the world. Competition amongst jurisdictions would increase in the hope of tapping into a new world of economic activity, as too would innovation amongst DAOs in the hope of making use of a regulatory regime that would best recognise their status.

DAOs may eventually also have opportunities to register in places with the most favourable tax rules. The diverted profits tax might come into play here - this is aimed at arrangements where sales are made to customers in the UK by a foreign company that has no permanent establishment in the UK (and thus is not usually liable to tax). For this to bite, it must be reasonable to assume that any activity is designed to ensure the non-UK company does not carry on its trade for UK corporation tax purposes.

That said, even if a DAO has a body corporate in a jurisdiction, the agreements that entity concludes may not be governed by the laws or subject to the courts of that jurisdiction. The risk then remains that identifiable DAO members may remain personally exposed. In some instances, it may be entirely irrelevant where the DAO is "located", e.g. damages sustained within England and Wales. In others, e.g. insolvency and tax, locus and situs of assets and activities may be critical.

A wider point is that, if a DAO incorporates an entity in a jurisdiction and the DAO is inextricably linked to that structure, does that effectively dissolve a "DAO", instead leaving a group of token holders whose liability may derive from their relationship with the corporate entity, rather being part of a DAO as an unincorporated association which can instruct the corporate vehicle? Can this be mitigated by ensuring corporate entities serve, rather than be, a DAO? Analysing anything to do with a DAO an English court will not attach any legal relevance to or recognise a DAO as a "creature of law". It will just analyse it in terms of legal individuals and entities involved in the specific enterprise. Depending on the court, question and context, it is unlikely that any satisfactory and broad answers will emerge anytime soon.

Tax[195]

In many cases, identifying that a transaction has occurred will be straightforward. The online purchase in the metaverse of real-world goods or services will likely follow established rules that apply to online transactions. However, where the transaction is the exchange of one virtual asset for another, such as an NFT acquired with cryptocurrency, it may be less obvious how the rules apply.

The UK's position on the direct tax treatment is relatively clear. Applying these principles to a hypothetical transaction where a UK consumer uses cryptocurrency to acquire a limited edition NFT accessory from the metaverse store of a UK company, the following tax liabilities could arise:

a. Capital gains tax (CGT) for the individual on the disposal of their cryptocurrency when buying the NFT, assuming that the value of the cryptocurrency has increased.

b. Corporation tax for the UK corporate on the profit generated from the sale of the NFT.

c. CGT for the individual on any future sale of the NFT, again assuming that its value has increased.

The indirect tax treatment, that is, the VAT position, is less clear. Spain is the only European jurisdiction at the moment with a clear tax ruling specifying that NFTs attract VAT. The question of which tax authority has jurisdiction can also be unclear. Current tax rules require the tax residency of the real-world parties to the transaction to be determined, but questions arise as to how these rules apply to a metaverse sale by a decentralised, member-owned and controlled organisation governed by blockchain-powered smart contracts. Perhaps this could be something that is dealt with by double-taxation treaties.

Collection and reporting: the Organisation for Economic Co-operation and Development consulted on a framework for the automatic exchange of information on cryptoassets.

[195] The metaverse: far from the wild west, by Dr Mark Watts, Bristows LLP

These proposals require a cryptoasset service provider to provide identifying information on its users and a list of cryptoasset transactions. This framework may need to be extended to capture metaverse platform hosts. In much the same way that online sales platforms have been forced to act as VAT collectors in respect of transactions facilitated by their platforms, metaverse providers may need to accept a degree of responsibility for policing tax in the worlds that they have created.

3. Liability of members of a DAO

Part D will consider in further depth the types of legal structure which may be implemented for a DAO but (as was the starting point of the Law Commission's recent call for evidence) for the purpose of this section we will consider a DAO in its pure form as an unincorporated arrangement or association of its participants.

This structure, under English law, can be considered in the following ways[196]:

a. Unincorporated associations
b. General partnerships
c. Form of trust arrangement
d. Arrangement of joint ownership of assets

The main distinction under the laws of England and Wales is that these structures do not in themselves have a separate legal identity.

Trust arrangements and arrangements of joint ownership of assets will depend how specific assets are held by the DAO. Whilst they acknowledge that a DAO may use a trust as constituent part of their overall organisational structuring, in most cases a trust will not arise. This section will therefore focus on unincorporated associations and general partnerships.

Unincorporated associations

There is no statutory definition of an "unincorporated association", however, it has been described in case law as:[197] "Two or more persons bound together for one or more common purposes, not being business purposes, by mutual undertakings each having mutual duties and obligations, in an organisation which has rules which identify in whom control of it and its funds rests and on what terms and which can be joined or left at will."

The key criteria for an unincorporated association are that it should:

i. Consist of two or more persons with a common purpose other than making a profit

Unlike general partnerships unincorporated associations are prevented from undertaking business for profit.

Although not established for a business purpose or for profit, an association will nevertheless usually have funds of some kind. Income from member subscriptions can be pooled in pursuit of the association's purpose **other than business for profit**.

Income may be used to cover the running costs of the association, but any incidental profits which are made (for example from investments) must be applied to the objects of the association rather than be shared by its members.

ii. Have contractual relations between those persons

There are no registration requirements to form an unincorporated association. It will come into existence as soon as a group of people agree to co-operate for a mutual purpose other than business.

[196] Law Commission - Decentralised autonomous organisations (DAOs) Call for evidence, November 2022
[197] Conservative and Unionist Central Office v Burrell [1982] 1 WLR 522, 525 by Lawton LJ.

If they then adopt specific rules or sufficiently clear but implied understanding is reached between them, then the contract forms the unincorporated association.

iii. Be governed by rules

As noted at point 2 the rules of the association will set out the rights and obligations of the members to manage and run the association. It is advised for the members to adopt written rules which can address multiple topics including:

a. Member subscriptions;
b. Voting rights of the members;
c. Positions in the association including any right of indemnity of those officials; and
d. Distribution of the association's assets on its dissolution.

iv. Be non-temporary

An unincorporated association can accommodate a changing membership as members join or leave simply by applying the rules of contract. If another person wishes to join the association, they must contract with each other member to be bound by the rules of the association.

If a member wishes to resign, they must follow the method prescribed by the rules. If the rules are silent on this matter then members are deemed to resign if they sufficiently show their intention to leave.

v. Not have distinct legal personality

Unless its members chose to incorporate a limited liability legal structure (as considered at Part D below) an unincorporated association will not have a separate legal identity separate from its members. This therefore poses an issue for the structuring of a DAO as the association itself cannot own property or enter into contracts with third parties.

Consequences of characterisation as an unincorporated association

As the unincorporated association does not have a separate legal identity, it will usually enter into a contract by an individual member or one or more of the executive committee members on behalf of the unincorporated association. The normal rules of agency will apply so if an agent makes it clear that they are contracting on behalf of an unincorporated association, the contract will be made only with the persons who are the agent's principal. There are two main classes of person who are likely to be held liable as principals under such a contract:

a. the entire membership of the unincorporated association; and

b. some or all of the members of the executive committee, as at the date of the contract which is being entered into.

An unincorporated association shall continue in existence with a changing membership until it is dissolved.

As noted below, the members may choose to take the additional step of incorporating their organisation, for example, by registering as a limited company.

If they do not incorporate a limited liability structure then the liability attaches to the persons who were members at the time ay contract was entered into and who authorised the contract. Members who are liable under a contract are jointly and severally liable for the full amount due unless liability is expressly limited under the contract to the amount of the association's funds. So a creditor could pursue just one member.

The rules of the association may also set out any right of indemnity of officials and trustees against the assets of the association in respect of liabilities incurred from activities undertaken on behalf of the association.

General partnerships

General partnerships are governed by the Partnership Act 1890 and are defined as the "relation which subsists between persons carrying on a business in common with a view of profit".

There must be a "business"

The definition of "Business" under s.45 of the 1890 Act is broad to include "every trade, occupation, or profession".

ii. The business must be carried on by persons acting in common

In other words, the persons must be carrying on a single business together for their common benefit, accepting some level of mutual rights and obligations as between themselves. It is not sufficient where only one of the persons is seeking only to improve their own, individual profitability.
The term "persons" includes bodies corporate, meaning an individual, a body corporate or a group of bodies corporate may form a partnership.

iii. The persons must have a view of profit

Unlike with an unincorporated association, this means that the partners must have the intention to make a profit, even if a profit is not actually realised. "Profit" means the net amount remaining after paying out of the receipts of a business all the expenses incurred in obtaining those receipts. This is in contrast with "gross returns", for example, the royalties received by an author.

A partner relationship arises from contract but like with an unincorporated association there are no formalities to satisfy. The partnership agreement may be express or else be inferred from the parties' conduct.

As noted above, the general partnership does not have legal personality separate from the partners who constitute it. Therefore, if a partner leaves the partnership or a new person joins, technically the old firm is dissolved and replaced by a new firm of partners who take on the assets and liabilities of the old firm and continue its business. It is possible, although currently unusual, for a partnership agreement to give a partner the right to transfer their share to a third party and make the third party a partner in their place. Again, this would result in the old firm being dissolved and a new firm created. In the past, partnerships with a large number of partners and freely transferable shares were more common than they are today.

Whether a partnership has formed is a question of fact and law, it is not for the parties to decide this for themselves.

In evaluating if a partnership has formed, a court will consider the following:

a. any agreement between the parties which reflects their true intentions

b. any common features of partnership are present

c. any other relevant evidence

Importantly, a court will look to the substance of the parties' relationship rather than any label that the parties choose to use. Simply saying that a relationship is a "partnership" is not itself conclusive as to whether a partnership actually exists, although it may be relevant. Equally, an express declaration by parties that their interaction does not constitute a partnership will not decide the matter.

Consequences of being considered a partnership
Like unincorporated associations, general partnerships in England and Wales do not have legal personality separate from the partners who constitute them, again meaning that they cannot enter contracts, own, or grant security over, assets. Any

property is normally held in the names of individual partners as trustees for the partnership. No debt can exist between any member of the partnership and the partnership itself and the partnership cannot technically be a creditor or debtor of its members. Partners do not have any rights or liabilities against the partnership itself because it has no separate legal identity. Rights and liabilities of the partnership are actually rights and liabilities of the partners either against third parties or each other. However, actions can be brought by or against partners in the name of the partnership.

A partner is both a principal and an agent of their co-partners. As principal, a partner is personally liable to meet the debts or liabilities of the partnership, whether or not they could be met out of the partnership assets.

A DAO could be classified as a general partnership if there is an express or inferred agreement between persons to carry on a business in common with a view to profit. Whether that is the case will depend on the specific DAO in question, and its nature, objects, and operations. We anticipate that for some DAOs, particularly where participants do not have a profit motive or if a profit motive is subsidiary to some other purpose for participating in the DAO, the possibility of inferring a partnership agreement will be small, but they might instead be an unincorporated association. For other, explicitly commercial DAOs, a categorisation as a partnership might be more likely, though it would still require showing that (some or all of) the DAO's participants were acting "in common".

The Law Commission therefore considers that where a DAO has not taken any steps to put in place a limited liability structure it will likely be characterised as an unincorporated association or a general partnership under the law of England and Wales.

The Law Commission notes however that considering DAOs as either unincorporated associations or general partnerships is only the starting point of analysis. Stopping analysis at this point would fail to consider in detail the different crypto-token ecosystem functions performed by participants within those ecosystems and fail accurately to reflect the realities of how DAOs are structured and operate in the market today.

Part D – Legal Entity Structures

1. How could a DAO benefit from a legal structure?

As noted by Vitalik Buterin in his genesis article: "A DAO may or may not make use of the legal system for some protection of its physical property, but even there such usage is secondary" [198].

Due to the 'decentralised' nature of DAOs and their constituent parts, DAOs are not generally recognised as legal entities in their own right and are therefore not capable of entering into legal agreements with third parties. This can result in practical difficulties in contracting with third parties to provide services to the DAO or to further its purpose.

Increasingly, corporate legal structures are established by a DAO's funders to enhance the capacity of a DAO to contract with the world. The activities of these companies are as varied as the potential purposes of a DAO. Each corporate structure may vary by level of control by the DAO over the structure, director and officer appointments and holding of internal capital by one or more corporate entities and appearing on their balance sheets. Typically, however, DAOs tend towards jurisdictions offering memberless corporate vehicles such as foundation companies

[198] "DAOs, DACs, DAs and More: An Incomplete Terminology Guide", Decentralized Organizations, Vitalik Buterin, 6 May 2014

(particularly in Switzerland, Singapore and the Cayman Islands), with flexible and often highly bespoke constitutional documents, primarily on the basis that no one or more individuals "owns" and can therefore control that vehicle or its assets contrary to DAO mandates.

Occasionally legal advisers may be asked to structure a "legal wrapper" for, or "incorporate", a DAO. What this means is not yet settled and may reflect an expression of intent rather than actionable structuring. The intent may range from establishing a corporate vehicle through which a DAO can contract with the world, acting on instructions from but otherwise independent of the DAO, to establishing a corporate vehicle which holds the DAO's assets and disposes of them in accordance with DAO proposals. Either way, a DAO is not a recognised legal concept in most jurisdictions so by definition cannot be incorporated.

a. UK legal structures

   The UK has multiple limited liability structures which could potentially be utilised by DAOs, including:

   i. private companies limited by shares;
   ii. private companies limited by guarantee;
   iii. public companies limited by shares;
   iv. unlimited companies;
   v. community interest companies;
   vi. limited partnerships;
   vii. private fund limited partnerships;
   viii. limited liability partnerships;
   ix. charitable incorporated organisations; and
   x. registered societies (co-operative societies and community benefit societies).

   The Law Commission in their call for evidence paper[199] have however highlighted that current trends in DAOs tend not to use UK legal structures but instead predominantly choose to establish themselves in other jurisdictions. We will therefore focus on these entities in further detail in the rest of this section but the Law Commission has sought further information as to why this is the case and by doing so aim to consider if the laws of England and Wales in any way inhibit. Therefore following this consultation we may start to see DAOs begin to consider the types of structures set out above.

b. Key issues with a DAO seeking to establish a legal entity with nexus to, or embodying, the DAO

While a handful of USA jurisdictions, such as Wyoming and Vermont, and non-USA jurisdictions like the Marshall Islands, have attempted to provide for DAOs to be incorporated into recognised legal structures, in practice the end result is often a company with some degree of automation of some record-keeping and management and governance functions, or some external control of the same. Ultimately, however, liability for the activities of that entity will remain with its appointed directors, officers and equity interest holders (if any). As noted above, the question is whether a DAO can really be "incorporated" or "wrapped" and the consequences for members of a DAO of any attempt to do so. In and of themselves, DAOs are not currently recognised as legal entities in most jurisdictions. Due to this, the structuring and regulatory advice that law firms provide can be vastly different depending on the project or aim of the DAO, the purpose of a corporate structure and its constituent entities, the jurisdiction founders or key members of a DAO are based in and which activities it intends to carry out. Corporate structures may provide some liability protections, but a DAO's founders, representatives or key members should seek expert legal advice and analysis on what these will be as against the desired protections sought.

The activities of corporate vehicles may require them to be regulated under local laws and regulations. Particular care should be taken if a corporate vehicle is established to issue governance tokens to DAO members or will receive existing governance

[199] Law Commission - Decentralised autonomous organisations (DAOs) Call for evidence, November 2022

tokens from the DAO for onward transmission to third party purchasers (sometimes known as a “treasury diversification”), as the laws and regulations local to potential purchasers must also be considered, particularly in the US.

Absent laws, regulations or regulatory guidance to the contrary, there is an argument that a corporate structure deploying a decentralised protocol or application and making changes to the code on instructions from the DAO is not “running” or benefiting from the protocol, as it typically does not receive revenue or fees for its services or from the protocol or applications operating. Instead, value accrues in and through the protocol itself and the potential increase in the market value of the associated digital assets, including the DAO governance tokens. There is a risk that this position may change in future, and DAOs and their legal advisors should monitor both global and local regulatory consultations and possible changes to laws carefully for any developments to the contrary.

Practically, many DAO members communicate and operate pseudonymously and some may be reluctant to disclose their personal details, known as “doxing”. Professional directors are sometimes engaged to be appointed to director roles on corporate structures, but changes to beneficial ownership regulations in several jurisdictions popular for corporate DAO structuring may require a revised analysis of this approach once those laws are settled and prior to their implementation, particularly where the end result is or will be a publicly searchable register of beneficial owners of a corporate entity.

Pseudonymity will also be impractical where engaging professional service providers to incorporate and maintain a corporate entity or provide services to it. Such service providers generally must identify a natural person as their client or, if the client is an entity, the ultimate beneficial owners, as part of their know-your-customer obligations. (Some jurisdictions allow for a solution that partially compromises between the legal requirements of client due diligence and the philosophical ideal of decentralisation.)

Whether incorporated or not, DAOs must still consider and comply with relevant sanctions regimes and applicable anti-money laundering laws and regulations, particularly when receiving or disbursing assets. Subject to the circumstances and nature of the relevant transaction, due diligence information may be required on third party recipients. DAOs should seek legal advice on when and how this may apply.

Part E –
Current DAO Trends

While the concept of a DAO can be very new and foreign, there is a definite trend towards maturity in this industry. It is not just a random group of individuals on the internet arguing about what to do next, as some may paint DAOs.

In many instances DAOs are very well-organized groups with well-defined reporting structures and governance mechanisms in place to guide and organize the DAO members. Many individuals are now taking on full time positions with the DAO; where there is a wide range of opportunities to work on, from purely technical development to community managers, marketing, accounting, and many more. The following are some of the current trends in the DAO ecosystem:

1. Community guidelines and By-Laws

As with any group of people working together – community guidelines are a critical component. They are an essential part as they guide the community and govern how actions are taken. For those who are used to a more traditional corporate structure, you can think of these guidelines as the by-laws. The guidelines define how the DAO will function, how proposals are created, how voting will take place, and many more. They should also include guidance on processes to follow in worst case scenarios – such as conflict resolution or split votes. Additionally, the guidelines may define specific requirements for significant actions such as winding down the existence of the DAO or fundamentally changing the operations. In these instances, the community guidelines will define specific requirements that should be met, like the quorum and percentage of 'yes' votes required for a vote to pass. For significant matters, a higher quorum and percentage may be required. This is to ensure that not only the community agrees, but also ensure that large token holders cannot force the DAO into a specific direction.

DAO guidelines will also define practical considerations such as appointment/removal of directors, a company secretary or any other official positions required where the DAO is linked to a legal entity. Additionally, the guidelines should ensure no votes or actions are taken that are against the law in a specific jurisdiction and checks and balances are in place to avoid votes being passed for actions that are potentially harmful to the DAO. This can be achieved through either the proposal process, voting or the appointment of a Council/DAO manager.

2. Councils

A general trend for DAOs is the implementation of councils to guide and manage the DAO and ensure it stays on track. The council not only fulfills these functions, but also takes care of the many administrative tasks. The council can take responsibility for certain operational tasks and will have the freedom to decide as defined in the community guidelines.

Council members are appointed via a vote and can normally nominate themselves or be nominated by a DAO member. Most DAOs have defined terms and mechanisms to remove council members in their community guidelines and the council is responsible for ensuring DAO votes are enacted and the DAO is managed effectively.

In many instances council members will formally engage with the DAO where it has a legal structure. This is to ensure that there are legally binding terms that define the relationship between the DAO and council members. Council members would also receive some remuneration for fulfilling their role. Remuneration is very important as this incentivises council members to be active participants and ensure the DAO moves forward. There have been a number of instances where council members are not remunerated, become inactive and the DAO stagnates. As the industry matures, some DAOs will also require council members to undergo AML procedures given the pseudo-anonymous nature of the industry.

One good example of why background checks are important is the Wonderland DAO. It was identified by a community member that one of the individuals managing the treasury known as ”0xSifu” was actually QuadrigaCX co-founder Michael Patryn – who had a history of being involved in illegal activities. After the removal of Patryn as the treasury manager, the founders decided to hand over the treasury to the community and wind down the project due to the loss of trust in the project. In the end, the fate of the project was decided in a community vote which is discussed further below.

Well-defined community guidelines and council transparency is extremely important. The Graph is an example of a DAO where the council is very transparent with all the members being publicly known with public voting by the council on their actions. The Graph also has a very well-defined proposal and voting process with a Graph Advocates Sub-DAO which is responsible for specific actions.

3. Proposals

It is essential for a DAO to have a defined structure around proposals that are put forward for a vote. In instances where no structure is defined, you will often see proposals that are not developed thoroughly, resulting in community questions and votes that stagnate.

The structure for proposals is normally defined in the community guidelines and will include where proposals are posted, how long they are up for comments, any “temperature check” steps to see whether the community feels that the proposal should go up for voting and the final requirements for a proposal to become a vote.

Each DAO has different requirements for proposals, but a proposal would usually include the following:

- Summary of actions/proposal
- Benefit for the DAO
- Costs
- Implementation requirements

It is important to have a filtering mechanism in place before proposals are put up for vote by the community. In a DAO where each proposal is a vote, you will get community apathy and low voting participation rates. You may also get harmful or illegal proposals which are easily passed due to the lack of review.

4. Voting

Voting is likely to be the most important part in any DAO and should be very well defined and managed. Every action of the DAO does not have to be a vote, however any significant action should have sufficient community support, well-defined quorums and voting percentages.

To achieve this, it is recommended that different classes of votes are defined. Low impact votes that will not have any significant impact on the operations of the DOA of the community can have low quorums and simple majority votes. You may see 1% of active tokens as a quorum and 51% majority votes here.

For more significant votes such as fundamental changes to the nature of the DAO or actions that involve large amounts of the DAO treasure, higher thresholds may be put in place. As an example, you may see 10% of active tokens as a quorum and a 65% majority required here.

Each DAO can define the classes of votes and participation required based on its community and how the operations will be run. Voting mechanisms may also evolve over time based on operations as well as where tasks are identified that may be delegated to the council or sub-DAOs/committees.

With the above in mind, the DAO also has several voting mechanisms that can be used. The following are just a few of the current voting mechanisms being used:

Token-based quorum voting

Token-based quorum voting is one of the most common voting mechanisms. For a proposal to pass, the quorum is required to be met and if so, the decision with the most votes pass. If the quorum is not met, then no further action is required as no decision has been made. This voting mechanism is the easiest to implement and is commonly used by a variety of projects.

This model is reliant on members of the DAO being actively involved. Without active community involvement, the quorum will have to be set at an extremely low level that there is almost no quorum required.

A current trend is that the quorum is set based on the nature of the vote. This allows minor changes or votes to require a low quorum (for example changing the token name from John Doe to Jane Doe). In contrast, if there is a proposal requiring expenses to be paid from the treasury, it will require a higher quorum to pass.

Curve and Compound are the most well-known DAOs using token-based quorum voting.

Quadratic Voting

Quadratic voting uses a mechanism that decreases the power of large token holders and increases the power of minor token holders. This decreases the chance of whales (large holders) swaying votes in their favour at the cost of minority holders. The voting mechanism works by increasing the cost of each additional vote that is cast by the power of two. For example:

Vote	Number of tokens required
1	1
2	4 +1 = 5
3	9 + 4 + 1 = 14
4	16 + 9 + 4 + 1 = 31

The major risk is where DAO members create multiple fake identities in order to vote for a specific proposal. A proposed solution for this can be that the DAO requires a proof of identity before members can vote.

Gitcoin is currently the most well-known project using quadratic voting.

Permission Relative Majority

This is a fork from token-based quorum voting as it eliminates the quorum requirement completely. The only factor that matters is how many votes were cast for or against the proposal. The side with the most votes wins. This is the easiest method of voting for a DAO with the lowest amount of effort required. The drawback is that a proposal can be created and if only a single person has voted at the end of the proposal, that vote stands. The risk here, for example, is that a DAO member creates a malicious proposal where the entire treasury is sold to a single wallet address.

Moloch DAO uses a slightly divergent method from this method. All proposals are required to be sponsored by a member of the DAO before it can proceed to voting.

Rage Quitting

A rage-quit vote is the process where a member of a DAO exits part or all of their stake, leaves with a proportional share of the assets in the DAO's treasury and quits their participation.

The Wonderland DAO employed this method after a successful vote was casted to remove the treasury management team. This resulted in a sharp decrease in the value of Wonderland tokens (wMEMO) below the value of the treasury of the DAO. Wonderland created a rage-quit proposal where members of the DAO who wanted to exit the DAO were able to receive the proportionate value of their token holdings paid out to them from the treasury. This was done to create a pathway for members of the DAO who wanted to exit but did not want to exit at a loss, which would have incentivized them to create proposals for short term gain and not the long-term health of the DAO itself.

Conviction-based voting

This method is based on the community's aggregated preference and uses time as a utility. Multiple proposals can be voted on by DAO members using their tokens, with members allocating more or fewer tokens to those votes they favour more. The longer DAO members stake their tokens to a specific vote, the more conviction it shows in the proposal. The increase of DAO member conviction slows over time. The decrease of the conviction rate is measured through the half-life decay curve.

The effect of this is that for whales the opportunity cost increases the longer they commit to the vote as their return decreases. This allows smaller holders to hold greater power overall. This method is new, with one of the drawbacks that it is a lengthy voting process.

Holographic Consensus

This mechanism is designed to screen proposals and separate the proposals that will likely fail from those that are likely to succeed. This is done by the community betting on proposals. If the proposal succeeds, then you receive your initial bet plus a reward. If the proposal fails, then you lose your bet. This method of voting is likely to be used in conjunction with another voting method as this is used primarily for screening proposals and incentivises community participation in the review of proposals.

Liquid Democracy

This functions very much like the well-known representative democratic systems employed by the US and other nations. Votes are delegated to an individual and they are empowered to make decisions on your behalf. This reduces the time commitment for members as only representatives are required to vote on proposals. The difference between this system and the standard model is that you can revoke your tokens from your selected representative and allocate them to another person at any point in time, hence the term liquid democracy.

Voting conclusion

Voting in a DAO can take various forms. It is important to balance the mechanism employed with the purpose of the DAO. A DAO that is created to invest in rare art for example, can use conviction voting as its primary mechanism to determine community interest in a piece.

Investment DAOs would probably prefer liquid democracy as they would need to make investment decisions based on identified market opportunities. In this manner liquid democracy would be the ideal vehicle as it would enable swift decision-making abilities.

Finally, consideration should be given for circumstances where almost any voting mechanism would result in an unjustifiable delay between the emergence of an event and the execution of the event. In the case of a hack of a wallet in the DAO, the decision to pause all operations of the DAO must be an option, even though DAO members were not consulted. They can be (and should) be consulted afterwards.

5. Sub-DAOs/Committees

Everything in a DAO does not necessitate a vote. For example, a grant provided to an organisation that will be paid if certain milestones are met, is not required to be voted on when each milestone is deemed to be completed. It is possible to have sub-committees in the DAO that operate within certain parameters.

For example, a DAO can have a public vote on the marketing budget for the current year of $500,000. If passed, then the marketing committee has discretion on how and where those funds are spent. Limitations can be placed on the committee such as:

- No single marketing event can exceed $100,000
- The budget can only be used for conferences
- All marketing expenses incurred should be publicly published

If the committee believes that there is an opportunity that exceeds the limitations, then they can create a proposal on which the community can vote to approve it.

6. Grants

Grants are an important function in any DAO as they incentivize community members to make proposals and contribute to improving the DAO. There should, however, be a well-defined process around the grants. Considerations can be :

- Vetting of proposals and the team/individual behind a proposal
- Well defined milestones that have to be achieved for grant payments to be released
- Performance reviews of grants to ensure the receiver of the grant has delivered
- Formal agreements between the DAO and the grant recipient
- KYC/AML checks on grant recipients

7. Operations

As DAOs further mature, more attention is being paid to the traditional day-to-day operations. The following areas are currently garnering increased attention:

Multisignature wallets/bank accounts

Not all service providers will accept tokens or stablecoins as their form of payment (though more and more are moving to do so). For certain expenses a bank account is required. The bank account is normally opened in the foundation companies name as the legal structure thereof allows the foundation to enter into binding agreements. A complexity with the opening of bank accounts is whether the bank is willing to work with cryptoassets and this should be confirmed before any further steps are taken.

For the DAO wallets itself, a multisig wallet is often used and advised. This allows for segregation of approvals which protects the assets in the wallet from theft by a single user. Individuals added to the multisig should be trustworthy and vetted. Any actions taken on the wallet should be managed by approved guidance or a DAO vote passing.

Financial statements/budgeting

Token holders **have** a right to know the balance of the treasury as well as the corresponding expenses and revenues being incurred. Though it is expected that a majority of this information is on-chain, there are certain expenses and perhaps revenues that could occur off-chain. In addition, it is overconfident to assume that all members of the DAO will have the knowledge, expertise and time to go through the blockchain to obtain financial standing of the DAO. In this sense, traditional financial statements are being created by more and more DAOs and published on their website.

It is increasingly common for DAOs to publish a budget projecting their finances for the coming year for commentary by DAO members. This includes salary expenses, marketing costs, regulatory and legal costs, and projected revenue (if part of the DAO). The format of the budgets can vary widely and each DAO can determine what should and should not be included.

8. Community members

DAOs are a collective group of members sharing a vision. You have your ‘never say die’, your ‘casual hangers-on’, your ‘only here for a while’ and everyone in between. But just as with any platform, there are opportunities for bullying, scamming and hurtful behavior. DAOs have started to publish “Rules” for interacting with the DAO and other members. These generally follow a similar approach:

- No racist, sexist or misogynist language
- No spamming
- No lewd, excessive cursing or expletive laden statements
- No threats of violence

These can be overarching rules with warning systems in place or outright bans from the Discord server and other platforms. This is an area that is garnering more and more attention to facilitate a healthy and supportive environment for members.

Part 2: Impacts on the Wider Landscape

Section 9 Blockchain Consortia

9

Section 9: 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 that can be formed, 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.

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 creation of blockchain consortia

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.

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.

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.

1. Creating a consortium

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

not carefully designed, it could fail to provide the right support to ensure that the members meet their objectives to work together cooperatively to achieve their common goal. 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).

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 blockchain platforms may include ensuring appropriate compliance due diligence from a financial crime perspective in situations where details of underlying transactions are not fully visible (both in terms of the users and the types of transactions that take place). There is an increased focus from compliance regulators around the need for appropriate third-party KYC/KYS due diligence (e.g. of app developers and users etc.). The risk that the platform could be used to facilitate illicit transactions (e.g. trade with sanctioned countries or involving restricted sectors or products) will also need to be considered. As such, the consortium will need to implement appropriate compliance policies, procedures and controls in the design of the platform, including making clear the rules and responsibility of members when admitting new participants. — Further, given that blockchain is a new technology and the law is playing catch-up, consortium members will need to consider how to approach, and 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.

- **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.

2. 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 10

Data Protection

10

Section 10: Data Protection

PART A: Data Protection

Anne Rose and Jon Baines (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.[200] 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)**.

As a result of the UK's exit from the European Union, GDPR no longer directly applies. However, it was in large part retained, in slightly amended form, and became the "UK GDPR". It is to be noted, however, that since Brexit, UK governments have indicated a willingness more fully to reform the domestic data protection laws, and it will be important to monitor developments in this respect, not least because there have been suggestions that the definition of personal data itself might be altered, and this could have significant implications for the legal and regulatory aspects of blockchain.

UK GDPR's objective is essentially two-fold. On the one hand, it establishes a framework of fundamental rights in respect of the handling of personal data, with various measures based on the right to privacy (Article 8 of the Charter of Fundamental Rights), and on the other hand, it seeks to facilitate the free movement of personal data (see Article 1, UK GDPR).

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.

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.[201]

[200] 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

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

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.[202] 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.[203]

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.[204]

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:

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).*

[202] 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

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

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

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".[205] 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".[206] 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.[207]

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."[208] 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".[209] In line with this reasoning, public keys or other sorts of identifiers used to identify a natural person constitute personal data.

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

Technical measures for re-identification – pseudonymous or anonymous?

Actors interested in using DLT and worried about 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.

[205] 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.

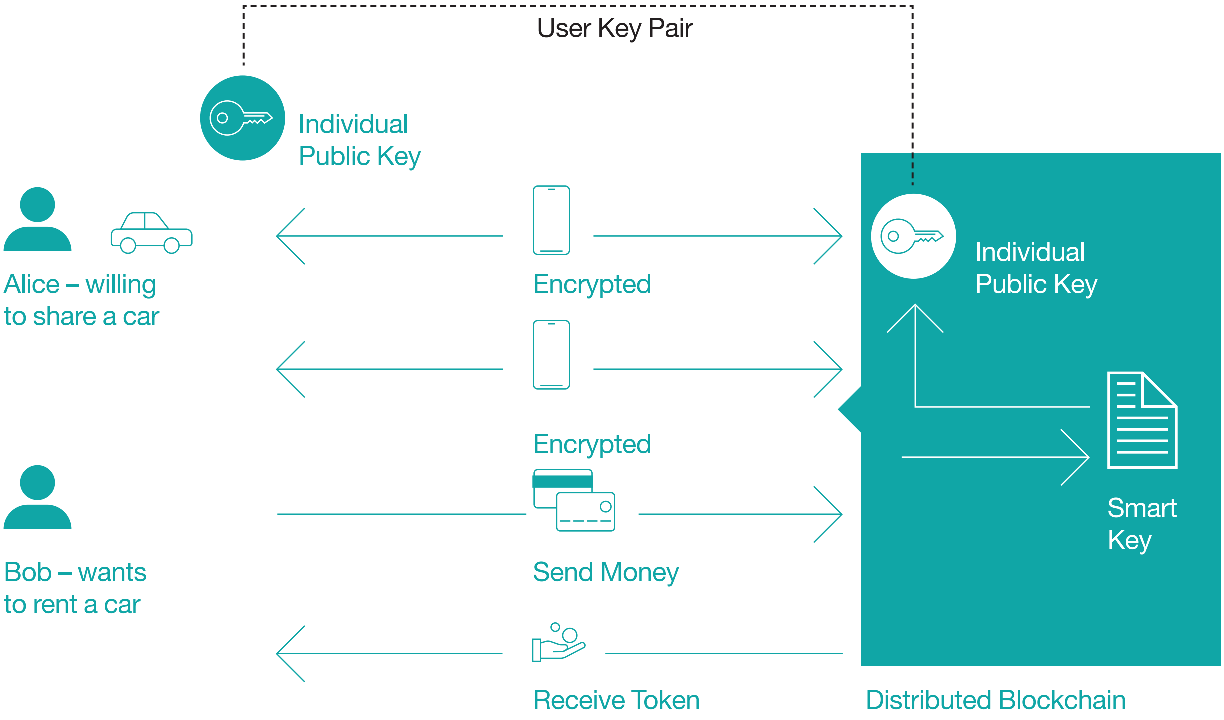
[206] Article 29 Working Party, Opinion 05/2014 on Anonymisation Techniques (2014) WP 216 0829/14/EN, 3 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf> Accessed 13 April 2020

[207] 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

[208] 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

[209] 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=CNILTEX-T000028450267&fastReqId=1727095961&fastPos=1ff> Accessed 13 April 2020

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.[210]
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;[211]

[210] Article 29 Working Party, Opinion 05/2014 (n 25) 14
[211] 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).

- 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.[212]

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.

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?

[212] 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)).

- 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?* [213]

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.

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

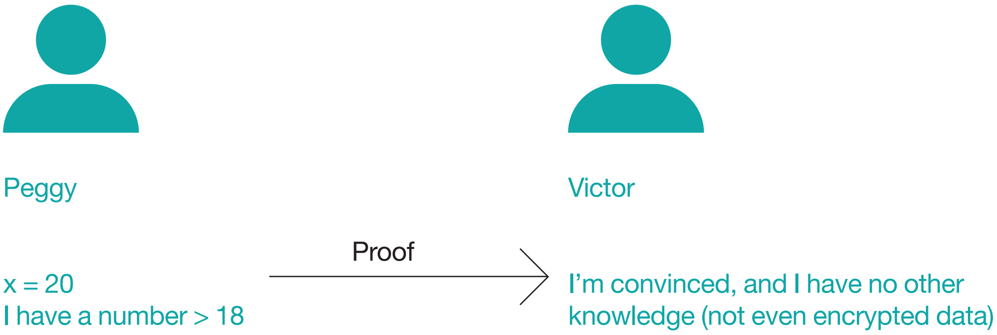
- **Completeness:** If the statement is true, an honest verifier will be convinced of this fact by the honest prover. That is, the algorithm must work in the sense that the party verifying the proof is satisfied that the proving party is in possession of the underlying data.

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

- **Soundness:** If the statement is false, no cheating prover can convince the honest verifier that it is true, except with some small probability.
- **Zero knowledge:** If the prover's statement is true, no verifier learns anything that was intended by the prover to be protected, other than the fact that the prover's statement is true.

Proof of age example

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


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

However, a person's age can constitute personal data for the purposes of data protection law, and many individuals would prefer not to share such information with a third party unless it is absolutely required. In fact, an important principle of 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:

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

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

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

ZKP and blockchain

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

1. Circuit production

2. Proof generation

3. Proof verification

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

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

ZKP and blockchain scalability

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

1. Rollups

2. Flat blockchains

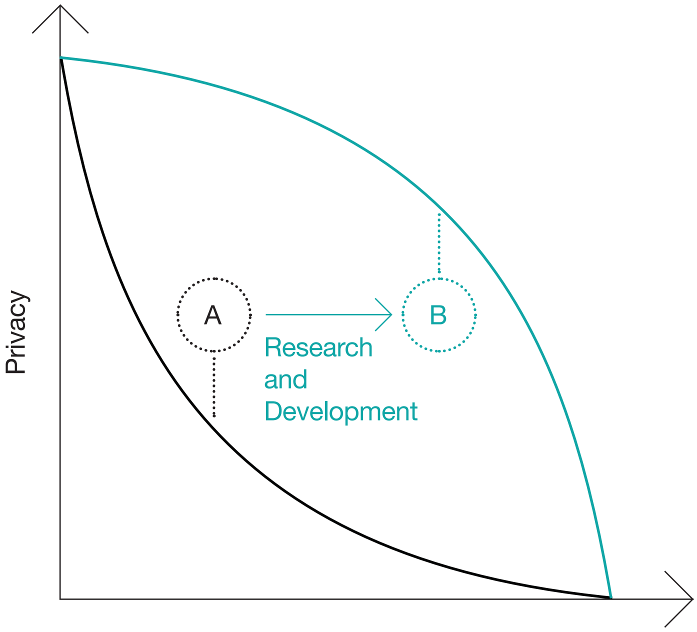
Rollups are designed to reduce the number of transactions on a blockchain by executing batches of transactions off-chain, rolling these up into a proof of the outcome of the transactions, and then posting only the proof to the blockchain. This greatly reduces the load on a blockchain, as it is no longer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

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

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

Other Privacy Enhancing Technologies (PETs)

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



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

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 11
Intellectual Property

11

Section 11: Intellectual Property

Hayleigh Bosher, Brunel University London; John Shaw, Brandsmiths; Kaetlin Gale, Foot Anstey LLP; Sophie Parkinson, Jani Ihalainen, Noonie Holmes, Rory Graham, Jack McAlone and Sophia Gofas, RPC; Terence Broderick, Arthur Roberts and Karen Fraser, Murgitroyd

Introduction

Many of the positive functionalities presented by Distributed Ledger Technology (DLT) have implications relating to Intellectual Property Rights (IPR). Intellectual Property Offices around the world are setting out guidance on how to address the goods and service for trade marks registered in this space. Whilst DLT's immutability provides an incorruptible record of transactions, this raises issues for any notice and takedown regime seeking to address copyright infringement. Patentability of DLT will require an analysis of any software purporting to have a technical effect. Supply chains will take advantage of DLT, but there remains the question of whether or not information stored on DLT remains confidential. Non-Fungible Tokens (NFTs) provide a cryptographically unique asset, but IPR is likely to subsist in any linked media which requires some form of transfer to any new owner.

Whilst the issues raised by DLT in respect of IPR should not be downplayed, they do not appear to be insurmountable for practitioners given the various existing IPR regimes. This third edition of the guidance echoes previous editions in its view that most tensions between the technology and IPR regimes can be addressed by practitioners while the remaining uncertainty would benefit from legislative or judicial clarification.

Trade Marks

The growth in the value of blockchain-backed assets in digital environments has raised questions of how trade marks should be registered where they relate to goods backed by blockchain.

Many influential brands have filed applications to register their trade marks for use in relation to blockchain backed assets and as NFTs, which has caused Intellectual Property Offices, such as the European Union Intellectual Property Office (EUIPO) and the United States Patent and Trademark Office (USPTO), to give consideration to the classification of virtual goods and services.

<u>European Approach to trade marks in virtual goods and services</u>

In summer 2022, the EUIPO published initial guidance[214] on the approach it intends to take for the classification of virtual and blockchain-backed goods for trade mark filings to reduce the number being rejected for lack of clarity.

For the first time, the draft EUIPO Guidelines for 2023[215] (2023 Guidelines) will include a description of 'virtual' goods as "non-physical items that are purchased and used in online communities or online games". Anyone wanting to register a trade mark for a downloadable virtual good should do so using Nice Classification Class 9, as they are considered digital content or images. Importantly, the term 'virtual goods' will not alone be sufficient for registration of a trade mark, as the EUIPO considers that the term "lacks clarity" and must be supplemented by a statement that sets out the content to which the blockchain-backed goods relate. An example might be: "downloadable virtual clothing, namely shoes".

The new 12th Edition of the Nice Classification also includes the term *"downloadable digital files authenticated by non-fungible tokens". This would appear to be the term*

[214] https://euipo.europa.eu/ohimportal/en/web/guest/news-newsflash/-/asset_publisher/JLOyNNwVxGDF/ https://euipo.europa.eu/ohimportal/nl/draft-guidelines-2023
[215] https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/contentPdfs/trade_marks/draft-guidelines-wp-2023/Trade_mark_Guidelines_2023_consultation_en.pdf

used by the EUIPO for any blockchain-backed digital good or NFTs, and highlights that the blockchain registration or NFT certifying ownership is to be treated as distinct from the digital 'item' itself (a theme which is revisited later in this section). It seems that the NFT alone cannot be accepted for classification purposes, and instead the downloadable digital good and blockchain-certification together would be acceptable, again in Class 9, for example as "downloadable digital clothing, authenticated using blockchain".

The new 2023 Guidelines also highlight that that there can be no one-size-fits-all approach when it comes to blockchain-backed digital assets. In particular, the above classification applies to downloadable digital goods only. Any non-downloadable blockchain-backed goods (e.g. a browser-only digital good or artwork) cannot fall within Class 9 and must be classified and therefore registered separately. The EUIPO considers that non-downloadable blockchain-backed items are distinct and should be classified in Class 42, i.e. as services. This means applications to register trade marks for virtual goods that can be used in-browser only or downloaded should seek registration in both classes.

The 2023 Guidelines are currently in draft form and will be reviewed by stakeholders before they are finalised. The approach suggests an awareness from the EUIPO of the requirement for certainty from brands who want to ensure that their trade marks are protected even when applied to blockchain-backed digital assets.

US Approach to trade marks in virtual goods and services

The USPTO has been less direct in providing guidance on how trade marks for metaverse and blockchain-backed virtual goods are to be registered. Instead, we can look to recent trade mark infringement case updates from the US courts to understand the approach that is likely to be taken.

In *Hermes v Rothschild*[216], the international brand and owner of the relevant IP rights in the infamous 'Birkin' bag, Hermes, have sued a Mr Rothschild for trade mark infringement and cybersquatting in relation to NFTs that were created using images of Birkin bags, so-called 'MetaBirkins'. The progression of this case in the US courts suggests that authorisation will be required for the commercial use of a trade mark when that mark is being used to create a separate digital asset. This is a position reflected in *Nike v StockX*[217], a similar US case in which the exchange StockX was sued by Nike over its use of the brand's logo in NFTs. These cases are ongoing in the US and demonstrate the risks of using trade marks registered for use in other classes in NFTs without proper authorisation from brand owners. The position taken by the US courts, while not final, appears to reflect the position taken in the UK and EU, where brand owners appear to be able to pursue unauthorised use of trade marks in relation to digital assets.

The UK Perspective to trade marks in virtual goods and services

The UK IPO has not yet published its proposed practice for the registration of trade marks for blockchain-backed goods, however it is possible that they will adopt the same approach as the EUIPO.

The most prominent case related to NFTs to date in the UK has been Osbourne v Persons Unknown[218]. While the case did not involve any alleged intellectual property infringement, it is worth mentioning here for the guidance it might provide on the attitude that UK authorities will take in relation to the registration of such assets, since the High Court decided that an NFT could be "property" for the purposes of an injunction. This is a pivotal decision that is likely to have a far-reaching impact on the way that NFTs are treated in the court system in England and Wales.

Practitioners are advised to review any trade mark portfolios and keep up with the emerging guidance from the Intellectual Property Offices as recent case law suggests

[216] Hermes v Rothschild USDC SDNY 22-CV-384
[217] Nike v StockX USDC SDNY 22-CV-983
[218] Osbourne v Persons Unknown [2022] EWHC 1021

that unauthorised use of trade marks will continue to be a battleground in the DLT space.

Copyright

There are two areas where copyright infringement may arise – in NFTs and items placed on the blockchain, and in the copy and use of the underlying code itself. For comments relating to copyright infringement and NFTs please see Section 5 This section focuses on copyright, and its infringement in the context of blockchain code. To do so, this section will explore (i) copyright protection in software generally; and (ii) the difference between software generally and blockchain software. This section will also address some issues that should not be ignored by the blockchain community, including copyright infringement in a blockchain ecosystem (including whether the immutability of blockchain is incompatible with the notice and takedown regime), copyright vulnerabilities in NFTs and a reminder to consider commercial relationships when advising on copyright infringement in an NFT context.

Copyright protection in software (generally)

Protectable copyright works include computer programs[219]. Whilst 'computer program' is undefined, it likely encompasses "programs in any form, including those which are incorporated into hardware"[220], including both source code and object code (that which is machine readable). Graphical user interfaces and the function of a computer program cannot be protected, as code, written in a different format, could produce the same function[221]. An IPO-commissioned report opined that whilst copyright protection will not extend to the functionality of software, it will cover the expression of computer code[222].

Software that underpins blockchain is open source

Practitioners should be wary of advising on copyright protection in a blockchain context. Where software, such a blockchain, is initially created/programmed by a human, and is then followed and built-on by a computer using automatic/embedded rules (creating further code), the usual rules of copyright are unlikely to apply.

Superficially, the copyright of the original code of a specific blockchain program will be attributed to the code-writer (subject to any employment provisions to the contrary) under standard copyright law. However, due to the decentralised nature of blockchain technology (and the licences that are wedded to the underlying software) it is likely that blockchain programs will not be copyright protectable.

The underlying works behind the theory of blockchain (e.g. the Satoshi Nakamoto white paper[223] that established the model for blockchain and the underlying C code behind Bitcoin[224] which was the first form of blockchain technology in action) would ordinarily be afforded copyright protection. However, the decision in Wright v BTC Core[225] highlights the complexity in this area, with the court finding that although copyright may subsist in a work such as the white paper, copyright does not subsist in the Bitcoin file format. This is because of a lack of fixation of the file format structure in any of the Bitcoin blocks. There is also the issue of copyright in the code itself.A short review of the Bitcoin website and associated licence(s) confirms that the MIT licence applies:

[219] as literary works under the s.1(1) Copyright, Designs and Patents Act 1988

[220] Section 1(2) of the Software Directive, which was implemented in the UK by the Copyright (Computer Programs) Regulations 1992 (SI 1992/3233) (Computer Program Regulations)

[221] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/549045/Study-I.pdf; SAS Institute Inc., v. World Programming Ltd., (C-406/10) [2012] 3 CMLR 4. See also Guarda P., Looking for a Feasible Form of Software Protection: Copyright or Patent, Is that the Question? [2013] 35(8) European Intellectual Property Review pp.445 – 454 at p.447

[222] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/549045/Study-I.pdf;

[223] https://www.ussc.gov/sites/default/files/pdf/training/annual-national-training-seminar/2018/Emerging_Tech_Bitcoin_Crypto.pdf

[224] https://bitcoin.org/en/

[225] [2023] EWHC 222 (Ch)

> "Copyright […]
>
> *"Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions: The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software."*

Copyright protection of the blockchain software appears to have been waived, and anyone seeking to implement blockchain technology (which was separated from Bitcoin in 2014) and rely on the software must also agree to waiving copyright protection to uphold the values and objectives of the open-source initiative. Although copyright protection is possibly afforded to the white paper (as an academic work), www.bitcoin.org is listed under the paper's heading and the MIT licence grants "permission… to any person obtaining a copy of… associated documentation files", which may be interpreted as applying to the white paper.

Any rights to software and computer code in Ethereum are similarly waived as they are licenced under the above MIT licence[226]. On initial consideration it appears that Ethereum maintains its rights to the website itself and all information, text, audio files, photos and imagery on the website. These rights are afforded to the Ethereum Foundation (a non-profit organisation dedicated to supporting Ethereum and related technologies[227]). However, on deeper analysis it is evident that unless otherwise marked, the website and all material (text, audio files, photos etc.) is licenced under the Creative Commons Attribution 4.0 International Licence (CCA4.0IL), which confirms that individuals are free to share, copy, redistribute and adapt material (even for commercial gain) so long as appropriate credit, evidence of any adaptions and a link to this licence is provided. Therefore, anyone that uses Ethereum software or information must rely on the MIT provisions and the CCA4.0IL provisions accordingly.

Some blockchains are decentralised systems, and the creators have sought to protect this by an apparent waiver of copyright protection, which is married to the underlying software, and must be passed down to any progeny. Practitioners should keep one eye on the open licences when advising on the protection of the creation of apps and websites that do not specifically rely on the blockchain software, should any of the software subsequently be used as this may impact IPR ownership

Copyright infringement in a blockchain ecosystem

The immutability of the blockchain makes it a particularly challenging environment in which to protect IP rights. If someone mints an image that has been taken or created by a third party (and therefore does not own the relevant copyright) what recourse is available to the copyright owner?

If an infringing NFT is put on sale in an NFT marketplace, it is possible to send a takedown notice to that marketplace to remove the infringing image from their platform, if it has not been minted. However, if the NFT has been minted and/or is associated with a cryptowallet, the platform will not be able to necessarily 'burn' (i.e. delete) or recover the asset from any purchaser.

Similarly, many blockchain operators will be unable to take any action in the event of an infringing work being uploaded on to the blockchain. While the decision in Osbourne v Persons Unknown[228] does show a willingness from the courts to apply the rules to fit a newer paradigm, it is unlikely that platforms will be under any degree of obligation in terms of NFTs listed for sale on their services. The owner or purchaser of the NFT could

[226] https://ethereum.org/en/terms-of-use/

[227] https://ethereum.org/en/foundation/

[228] Osbourne *v Persons Unknown* [2022] EWHC 1021

similarly be uncontactable or untraceable, as was the case in Osbourne v Persons unknown[229].

Copyright Vulnerabilities in NFTs: ownership and infringement

Clearly, NFTs do present new challenges to the legal framework. The form of ownership, sometimes straddling between the world of physical and digital ownership, also presents vulnerabilities that NFT owners and sellers should be mindful of.

The distinction between 'off chain' and 'on chain' ownership separates the ownership of the potential physical form of a work (like a physical piece of art minted as a digital NFT), and the associated rights between the two will differ. The purchaser may be transferred the copyrights in a work under a licence, or might get nothing at all, with the original artist retaining their rights through the original, physical, work. Likewise, rights may be retained by the platform (NFT licences are discussed in more detail below). For example, the terms and conditions of the Serenade platform state:

> *"The Artist hereby acknowledges, understands, and agrees that launching a Serenade Product on Serenade constitutes an express and affirmative grant to Serenade, its affiliates and successors a non-exclusive, world-wide, assignable, sublicensable, perpetual, and royalty-free license to make copies of, display, perform, reproduce, and distribute the Serenade Products on any media whether now known or later discovered for the broad purpose of operating, promoting, sharing, developing, marketing, and advertising the Platform, or any other purpose related to Serenade, including without limitation, the express right to: (i) display or perform the Serenade Products on the Platform, a third party platform, social media posts, blogs, editorials, advertising, market reports, virtual galleries, museums, virtual environments, editorials, or to the public; (ii) create and distribute digital or physical derivative Serenade Products based on the Serenade Products..."* [230]

Therefore, should someone utilise or disseminate their NFT it is possible that they are infringing on someone else's copyright. This will depend on the terms of the smart contract and the specific terms of a given NFT, as different rights (or none) may be given or retained in different instances. Any NFT purchaser will therefore need clear rights to be able to commercialise an NFT.

Licensing and assignments are also important in the space, where, without these proper terms (as discussed above), one may infringe on rights they thought they had. Without proper licensing or transfer of copyrights in the NFTs one may have purchased they could very well have simply purchased the rights to display the work only and not to use or commercialise it in any way.

The same applies to derivative works and whether any licensing or smart contract terms allow for the creation of those derivative works (e.g. using an NFT character in a TV show/film). It is vital that these terms are clear and understood when any NFTs are transferred, as they will impact the use by any subsequent buyers.
Even established creators can misunderstand these limitations, such as was the case for Quentin Tarantino who was sued by Miramax for breach of contract, unfair competition, copyright, and trade mark infringement, after announcing an NFT auction of seven 'never-before-seen' scenes of his handwritten Pulp Fiction script, discussed below[231].

Miramax v Tarantino USDC CDC 21-CV-8970

In seeking to allege copyright infringement via NFTs, practitioners should keep at the forefront any commercial relationships between the parties. In this case[232], Quentin

[229] Osbourne v Persons Unknown [2022] EWHC 1021
[230] https://serenade.co/terms
[231] Miramax v Tarantino USDC CDC 21-CV-8970
[232] Miramax v Tarantino USDC CDC 21-CV-8970

Tarantino was accused by Miramax LLC of copyright (and trade mark) infringement, as Tarantino granted Miramax "all rights (including all copyrights and trade marks) in and to the film", whilst reserving his rights to specific media (that Miramax argued did not cover NFTs). Tarantino then sought to create NFTs of the Pulp Fiction script, graphics and images as well as scenes with unknown secrets on the basis that NFTs (that didn't exist at the time of the agreement) fell outside its scope. Whilst Tarantino told the court that Miramax had no right to block his NFTs, the parties reached a confidential settlement in order to collaborate and work together on future projects (and, possibly, NFTs).

Design rights in a blockchain backed metaverse: can they subsist?

The question of whether a design right can subsist in a metaverse does not have a straightforward answer, having not yet been properly tested by the Courts. Under UK legislation, the "appearance of the whole or part of a product"[233] can be protected by registration of a design, but there is no clear definition as to whether the virtual recreation of such a design amounts to 'using'[234] of the product in the sense envisioned by legislators. Some commentators have suggested that, without careful contractual protection, rights in the virtual recreation of a physical design might lie with the software licence holder, or virtual designer[235], whilst others argue that the lack of limitation as to a particular class of goods or services when registering a design in the UK suggest that the digital recreation of a design could be covered by a registration in respect of a physical design[236].

UK legislation protects unregistered designs by preventing creation of 'articles', "exactly or substantially" to a design[237]. Whether a digital object can be an 'article' or whether the recreation of a physical design would be considered substantially similar are questions that also remain unanswered.

Lawmakers are certainly alive to this lack of legislative clarity. The UK Intellectual Property Office is in the process of considering how it can "ensure the designs system is flexible enough to support developments in technology"[238]. Similarly, the European Union Intellectual Property Office is updating its own Design Guidelines, clarifying its classification of terms such as 'virtual goods'[239].

This is an area in which much remains to be determined. Nevertheless, areas that practitioners should consider are highlighted below.

Protection of Virtual Assets through Design Rights

It is possible that registration of physical designs could operate to protect digital recreations given the flexibility provided by the lack of restriction of a registration to a particular class of goods. This would be of use to designers in providing long periods of protection (up to 25 years under the UK and EU regimes, subject to renewal[240]). However, the relevance of registered design rights in a metaverse may be limited.

Currently, the use of designs in a metaverse often relates to fashion, with individuals seeking to adorn avatars with digital versions of 'real world' designs. Registration can take up to four months and the costs per application represent a significant financial burden[241]. Considering the rapid fashion cycle, registering a design may

[233] Registered Designs Act 1949, s.1(2)
[234] Ibid. s.7(2)
[235] Brooke Roberts-Islam, Forbes, 3 November 2020, "Digital Fashion: Who Really Owns The IP Rights?" <https://www.forbes.com/sites/brookerobertsislam/2020/11/03/digital-fashion-who-really-owns-the-ip-rights/>
[236] Richard Burton and William Burrell, D. Young & Co, December 2021, "Brand enforcement in the metaverse - time for a re-think?" <https://www.dyoung.com/en/knowledgebank/articles/brand-design-metaverse>
[237] Copyright, Designs and Patents Act 1988, s.226
[238] UKIPO, 12 July 2022, "Consultation outcome, Call for views on designs: Government response" <https://www.gov.uk/government/consultations/reviewing-the-designs-framework-call-for-views/outcome/call-for-views-on-designs-government-response#contents>
[239] Intellectual Property Helpdesk of the European Commission, 29 July 2022, "Intellectual Property in the Metaverse. Episode 5: Enforcement measures and conclusions" <https://intellectual-property-helpdesk.ec.europa.eu/news-events/news/intellectual-property-metaverse-episode-5-enforcement-measures-and-conclusions-2022-07-29_en>
[240] The Registered Designs Act 1949 (as amended) Council Regulation (EC) No 6/2002
[241] Ioanna Lapatoura, 'Fashion Beyond Physical Space: Nfts and Intellectual Property Challenges In The Metaverse' (2022) 33 Entertainment Law Review.

be beneficial only if designers limit registration to the most timeless articles of their collection[242]. This would mean leaving many articles unprotected.

In the 'real world', a high number of designers rely on Unregistered Design Rights (UDR) to secure IP protection for their creations. The Unregistered Designs regime allows for designs to be protected without the need for registration, bridging the gap created by rapid fashion cycles. It follows that UDR might be useful for the IP protection of digital assets in the context of a decentralised metaverse as well[243].

However, whether UDRs apply to digital recreations remains open to debate. To the extent that they might, designers are likely to encounter further difficulties in relying upon UDRs. A blockchain backed metaverse is a borderless space with no territorial boundaries. One of the most important challenges that arise when thinking about the application of UDR in the virtual world is that of territoriality[244].

Art.11 of the Design Regulation allows for unregistered designs to be protected for three years, on the sole condition that the work qualifies[245]. A key requirement for a design right to automatically subsist is for the article to be made available to the public (disclosure) within the territory of the European Union (for the UK following Brexit a "supplementary unregistered design" would be required). Potentially, a design published in a metaverse is published globally, as users from all over the world can access the platform simultaneously. Thus, whether UDR can subsist in the borderless sphere of a metaverse is difficult to determine.

The distinction between an open and a closed metaverse is likely to be a relevant consideration. In an open metaverse the aim is for users to be able to utilise digital assets across different platforms without barriers, whereas a closed metaverse has an 'owner' that is usually able to restrict individuals' access and control available content. Designers might be able to utilise virtual borders in closed metaverses to control the extent of first disclosure by revealing designs to a limited and chosen public.

Enforcement of design rights in a blockchain backed metaverse

Whilst it is possible that design rights subsist in a blockchain backed metaverse, the enforceability of such rights is a different matter. The most obvious potential barrier to enforceability is also one of the key facets of a metaverse, the lack of visibility as to the identity of individual users. Whilst enforcement action might be possible against individuals who have identified themselves in the real world[246], claims against anonymous infringers will be harder to enforce.

Whether infringement takes place in an open or closed metaverse may greatly affect the extent of enforceability. In a closed metaverse, it is conceivable that design rights might be enforceable through the 'owner' of a metaverse, through similar methods to those by which regular social media platforms can be required to take action to remove infringing content[247]. However, this, in and of itself, pulls up important, currently unanswered questions regarding what onus should lie with platform providers in identification as well as in enforcement action.

In an open, blockchain backed metaverse, decentralisation and self-sovereignty are key concepts, neither of which is necessarily conducive to identification by third parties for the purpose of enforcement. Whilst blockchain may enable users to identify themselves, it will likely remain difficult for third parties to do so. Similarly, the existence of a borderless virtual space throws up the potential for jurisdictional enforcement issues[248].

[242] ibid

[243] Ioanna Lapatoura, 'Fashion Beyond Physical Space: Nfts And Intellectual Property Challenges In The Metaverse' (2022) 33 Entertainment Law Review.

[244] Fashion Law and others, 'Design Protection In The Metaverse: How Is It Going To Be?' (Fashion Law Journal, 2022) <https://fashionlawjournal.com/design-protection-in-the-metaverse-how-is-it-going-to-be/> accessed 14 October 2022.

[245] Art.11, Council Regulation (EC) No 6/2002

[246] Hermes International v. Rothschild, U.S. District Court for the Southern District of New York, No. 1:22-cv-00384

[247] Article 14, Directive on Electronic Commerce

[248] Intellectual Property Helpdesk of the European Commission, 29 July 2022, "Intellectual Property in the Metaverse. Episode 5: Enforcement measures and conclusions" <https://intellectual-property-helpdesk.ec.europa.eu/news-events/news/intellectual-property-metaverse-episode-5-enforcement-measures-and-conclusions-2022-07-29_en>

These questions remain to be tested. The answers will be crucial for designers and creators that rely on design rights as it will determine the scope and effectiveness of their rights. Given that the metaverse is only getting larger, with a report by Strategic Market Research anticipating its global market value will surpass $678.80 billion by 2030[249], these uncertainties are likely to become increasingly relevant as time passes.

Patents and DLT

Patents are an intellectual property right which protects technological innovation. They last 20 years and provide a legal monopoly over the scope of the patent (as determined by its claims). That is to say, a granted patent gives its owner the ability to stop others from exploiting an invention as defined in the patent's claims. This is an extremely useful commercial tool and allows any innovator to carve out sections (or implementations) of technology to make it difficult for competitors to compete with them.

While it may seem counter to DLT's open source beginnings, patent filings mentioning blockchain or DLT have increased year on year. Over 20,000 patent applications were published in this space in 2021, up from 17,000 in 2020 and 6,300 in 2019, showing a generally upward trend and a thirst from innovators in this space to seek to protect the unique features of their technology.

Based on data provided by ipQuants[250], blockchain related patent applications are not only being filed in large numbers, but also being granted. Of 837 cases identified at the European Patent Office (EPO) with the terms "blockchain" or "distributed ledger" in the clams, 519 were granted. This gives a grant rate of 62%. Statistics also indicate that the grant rate has increased in recent years.

Currently, granted DLT patent rights can and do already cover many different aspects of DLTs including the core implementation of ledger itself (sometimes called layer 1 technology), protocols built on top of DLTs (sometimes called layer 2 technology), and applications built using either or both layer 1 or layer 2 technologies. More recent patent applications tend to be aimed at protecting further developments of these foundational DLT technologies.

To obtain a patent, an application is first filed at an intellectual property office (IPO). The IPO will then examine the patent application. Patent examiners look at three main things for DLT related applications: novelty, inventive step, and patentable subject matter. When seeking a patent for DLT related technology, the biggest obstacles to overcome, especially in Europe, are typically inventive step and patentable subject matter.

Focusing primarily on the EPO, once they have established that a claim has novelty, they will assess inventive step of subject matter by deciding whether the novel features address a technical problem. That is to say, they will seek to determine whether the novel features relate to patentable subject matter and whether they address a problem which requires technical, rather than commercial, skill to solve. Given the EPO is often regarded as the gold standard for inventive step, especially in the software space, patent applications which can overcome this obstacle will often be granted both at the EPO and most other countries.

The concept of a technical problem has a very broad scope at the EPO and in the context of DLT can encompass everything from problems related to the hardware used to run blockchain nodes through to solutions which improve the security of the use of blockchain to store information relating to public or private cryptographic keys. However, those DLT applications which are focused solely on, say, commercial problems related to cryptocurrency, will find the requirement of a technical problem difficult to satisfy.

[249] Strategic Market Research on the Metaverse Market, June 2022, <https://www.strategicmarketresearch.com/market-report/metaverse-market>
[250] https://ipquants.com/

It is often difficult to judge, at the initial drafting stage of a patent application, exactly which side of the line a patent application will fall on, as a lot of it depends on what else has been disclosed or published (and is therefore prior art) – but experience is teaching us which applications will stand a better chance than others.

Those applications which will stand the most chance of success in demonstrating a technical problem tend to either address problems in the underlying technical architecture or use DLT features (such as the immutability of the blockchain) to address technical problems outside of the architecture.

For example, as the use of the blockchain increases, transaction processing becomes an important problem. Inventions which modify how the underlying nodes process transactions or manage unconfirmed and/or confirmed transactions are more likely to satisfy the requirement for an invention to address a technical problem. However, inventions that involves a generic use of the blockchain to address a commercial problem, such as managing data for a betting application or smoother process of forex transactions, are very likely to struggle. The EPO would likely acknowledge the technicality in the processing but find the novel features related to the betting and financial aspects to lack technical character.

As set out above, the EPO provide what is arguably the 'gold standard' in examining patent applications in this space. However, the UKIPO provide a way of obtaining protection in the UK for much lower filing fees. Aside from the geographical scope of protection which can be obtained, the UKIPO adopt a very different approach for assessing the patentability of subject matter to the EPO. This can sometimes make it difficult to obtain patents using the UKIPO if they relate to DLT technology. The UKIPO appear to assess patentability before they can consider inventive step. By comparison, the EPO acknowledge the differences first, and then determine inventive step and patentability based on these novel features.

A key difference between the approaches is that the UKIPO can often require an applicant to address patentability irrespective of any cited prior art (which can then be cited later if you overcome this objection) which may mean narrowing amendments to the claims without sight or idea of what could be novel or inventive.

The EPO approach has more structure given that the EPO Examiner must demonstrate that some features are known using evidence from the prior art.

For further comparison, the USPTO adopt a different approach again. Recently, it has been indicated that they look more at the practical applications of the invention and, provided the invention is not just limited to the abstract (i.e. difficult maths or a business concept), they will look at novelty and inventive step as the first port of call.

It is clear at this stage that the world of patents is far from harmonised when it comes to assessing the patentability of DLT-based inventions. However, this is not unexpected since it is the way that the above discussed patent offices access all computer implemented inventions. Thus, the differing approaches should not deter applicants from filing a patent application if they are confident that they can demonstrate the merits of their invention beyond just enabling a business method to be implemented. This will provide the most chance of success in most countries. Much of the discussion of patents related to DLT is currently limited to those drafting and prosecuting (applying for) these patent applications. Many patents are, as we stand, not tried before the English Courts as litigation before the higher courts is not yet taking place – although it is expected in the future as interest in the commercial applications of DLT grows.

For this reason, it is key when pursuing patent applications in this space to be as clear as possible in how the features are used and defined to give the best chance of effective protection around your technology.

A particular point of interest will be the extra-territoriality of DLT. Similar to the cloud, DLT does not have a territory of its own and, by its very nature, is multi-jurisdictional. For this reason, it is important to ensure that patent applications are worded to provide flexibility to protection in that the entities involved with the DLT are given individual protection rather than relying on protection for the entire system, as implementations by infringers will often cover multiple jurisdictions. This is not always straightforward but it improves enforceability if your invention is not reliant on activity at more than a single node.

In summary, how the world of patents will treat DLT remains to be determined, but we can say with certainty that patents are being obtained for various aspects of both the application and underlying architecture of this technology.

Trade Secrets and Confidential Information on blockchain

Can a blockchain be used as an escrow for confidential information?

Another use for DLT, given its cryptographic security, is for supply chain management, which would in turn result in the storage (and possible release) of confidential information. In this situation, the DLT would function as a form of escrow between the uploader of the information and any authorised recipient. Given the public nature of some blockchains, and the possibility of reviewing transaction, the question then arises as to whether, once information is added to a blockchain, it can be protected by the common law of confidence.

The three-limb test for whether information could be protected by the common law of confidence was set out in Coco v AN Clark (Engineers) Ltd[251] and is as follows: (i) the information 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. These elements are assessed below in relation to DLT.

Do DLTs have the necessary quality of confidence?

One key question is whether information can retain the necessary quality of confidence if it is placed on DLT. It was held in Saltman Engineering Co Ltd v Campbell Engineering Co Ltd[252] that, outside of contractual provisions, the necessary quality of confidence required that the information was not public property or public knowledge. By comparison, the statutory definition[253] 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.

One relevant question is whether the blockchain is open or closed. An open blockchain can be accessed by anyone, meaning that anyone can attempt to decrypt the information contained on it. While it is difficult to decrypt information held on a sophisticated distributed ledger, especially when salted and peppered hashes are used[254], it is not impossible. It was held in Mars v Teknowledge that the mere fact that information was encrypted did not impart the quality of confidence as “anyone with the skills to decrypt has access to the information”[255]. More recent case law, however, such as Kerry Ingredients v Bakkavor Group[256] has held that information ascertainable by reverse engineering or decryption could still have the necessary quality of confidence if the process of decrypting or reverse engineering would involve significant amounts of work. The courts have yet to determine whether the amount of work required to decrypt information on a DLT is sufficient to give rise to the quality of confidence.

[251] Coco v AN Clark (Engineers) Ltd [1968] F.S.R. 415
[252] Saltman Engineering Co Ltd v Campbell Engineering Co Ltd [1948] 1 WLUK 12
[253] Regulation 2 of the Trade Secrets Regulations
[254] 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.
[255] Mars UK Ltd v Teknowledge Ltd [1999] 6 WLUK 149
[256] Kerry Ingredients (UK) Ltd v Bakkavor Group Ltd [2016] EWHC 2448 (Ch)

Closed blockchains require that a user is authorised before they can access the ledger, and the information is stored on the devices of the trusted intermediary. For an outsider to gain unauthorised access to the information, they would have to overcome the additional (and significant) hurdle of gaining access to the blockchain. It may be that the additional work and complexity involved, combined with the fact that the blockchain was made private in the first place (which may make a court more willing to infer that the information was intended to be confidential), is sufficient for the information to have the quality of confidence. It should be remembered, however, that any dispute in this area will turn on its own facts.

Practitioners should also remember the other steps that can be taken to safeguard the confidentiality of information. While marking information as confidential is not conclusive, it will aid any argument that the information has the quality of confidence, as will any evidence of an agreement between the parties that the information should be treated as confidential.

NFTs and Intellectual Property

NFTs may be considered as a new form of asset but, when considering the IPR related to them, it is unhelpful to distinguish them in this way. Much focus has also been given to what a third party may do with a copy of the asset, which may be in breach of various IPR (such as copy and pasting a digital image). As a result of assumptions people make when acquiring NFTs, the ease of online infringement and relatively limited (albeit growing) understanding of the licences involved, it has become unclear what the purchaser of an NFT owns. Below is a consideration of the IPR that may be acquired when purchasing an NFT, with a review of various NFT collections terms.

<u>NFT Acquisition – who owns the art?</u>

A purchaser of an NFT usually acquires two things:

1. The digital token. This is normally governed under Ethereum’s ERC-721 standard, and it bears a unique address containing metadata stored on a blockchain. The metadata describes (or “points to”) a location that is usually off-chain (for example within The Interplanetary File System, IPFS) where the relevant artwork that you associate with the digital token is stored.

2. A licence or assignment (in the form of a smart contract, but usually set out in natural language terms on the minter’s website). This is issued to the new owner of the NFT from the NFT Project that created the image. This licence or assignment sets out the rights which the new owner has in respect of the intellectual property in the image.

The implication of this is that a purchaser of an NFT is acquiring lines of code written onto a blockchain. More importantly, from an IPR perspective, they are also acquiring rights which prescribe what they may do with the off-chain asset to which the code points.

The IPR in the artwork are separate to the ownership rights in the token. Unless there is a legal instrument transferring them, they will remain with the creator of the art (which may be the minter of the NFT). IPR may be transferred by an assignment or a licence and practitioners should be aware of the formalities related to them and the differences.

It is also necessary for practitioners to consider whether the rights transferred under the initial sale may in turn be transferred in the event the new owner would like to sell or commercialise the artwork. Some platforms facilitate an equivalent to the artist’s resale right, meaning that when an NFT is resold the original seller receives a percentage of the subsequent sale. The purpose of the resale right is to compensate the author for the loss of control over their work by granting them remuneration for each successive sale and therefore seems appropriate in these circumstances. Whether this law applies to digital art is not clear, but the effect can be achieved through contractual terms. This means that the capacity for the seller to benefit from this depends on the terms of the platform they are selling through.

An assignment of IPR with NFT purchases

Under English law, the formalities for an assignment are set out in CDPA 1988 s.90(3). A transfer of IPR must be in writing signed by or on behalf of the assignor. In writing includes any form of notation or code but it is untested as to whether or not a smart contract will fulfil the requirement that the assignment be signed. Practitioners should be aware of this where parties are considering a transfer of IPR in their projects. Minters of the NFT, if attempting to assign the IPR, will likely require a licence back to cover the digital copy and enable authorised continued promotion of the NFT artwork (and project as a whole).

A licence of IPR with NFT purchases

Practitioners should consider if any licence of the NFT art is sole, exclusive or non-exclusive. Each of these are discussed in relation to NFT purchases below.

Under a sole licence, the licensor retains the right to exploit the relevant IPR but may not appoint any other licensees. An exclusive licence differs in that the licensor is itself excluded from using the licensed IP, but it is important to understand that an exclusive licence may not be truly exclusive in the sense that it may be limited by purpose or jurisdiction (for example). A non-exclusive licence entitles the licensor to grant further licences in addition to the one granted as well as continue to exploit the IPR itself. These forms of licences have serious implications when it comes to restricting the use of the IPR in any NFT artwork. As the summary below shows, different projects take different approaches when it comes to IPR in NFT art and practitioners should not ignore this as it has a direct impact on what NFT holders (and unrelated third parties) may and may not do with NFT art.

- The Cryptopunks licence[257] provides that the NFT holder is granted an exclusive, universe-wide, royalty-free, sublicensable licence to reproduce, distribute, preparate derivative works based upon, publicly display, publicly perform, transmit, and otherwise use and exploit the CryptoPunk Art. This licence intends to enable the NFT holder to make both commercial and non-commercial use of the CryptoPunk Art in any and all mediate.

- The NFT License 2.0 (NIFTY) has been created:

  > *"as an open-source resource for the wider community to encourage adoption of the ERC-721 standard. DLI's goal is to positively shape the future of NFTs for creators of blockchain-based art (each, for the purposes of this License, a "Creator") by demystifying the associated user rights while empowering Creators to license their work at scale."* [258]

  Under this licence NFT holders are granted a broad non-exclusive licence relating to non-commercial use as well as a non-exclusive licence relating to commercialising the NFT in merchandise (provided the commercial use does not result in earnings over $100,000).

- Under the Doodles licence[259] the NFT holder is entitled to use the Doodle as their profile picture, sell it and merchandise it up to $100,000 through sales of physical merchandise or by using the Doodle in a piece of art that they create. There are restrictions on minting further NFTs or altering the work and there are limitations on what material the Doodle may be used with.

[257] https://licenseterms.cryptopunks.app/
[258] https://www.nftlicense.org/
[259] https://docs.doodles.app/terms-of-service

- The World of Women digital ownership assignment[260] includes an assignment of IPR to the primary owner of the NFT and there is a "secondary assignment". This agreement appears to be unique, not only because it attempts to assign the IPR in the art, but also because it attempts to impose obligations on subsequent owners of the NFT. Under the secondary assignment, there is an attempt to impose obligations on any future owner of the NFT so that the new owner is under the obligation to assign to any subsequent buyer all rights it has in the art under the same conditions.[261]

The above shows how different projects have attempted to address the transfer of IPR. Practitioners should be aware that there is no correct option when it comes to an assignment, non-exclusive, or exclusive licence. The aims of the project and expectation of the purchasers are the key elements to align with the transfer of IPR.

NFTs sold under Creative Commons licence

One form of licence that is being used by creators of artistic works linked to NFTs is a Creative Commons Licence (also known as CC0). Practitioners should be cautious when considering or having been approached with a CC0 licence. Under a CC0 dedication all rights are released so that the work belongs to the public and the creator is effectively saying that they do not wish to have any control of the copyright in the work. One further complication here is that other intellectual property rights, including trade marks would need to be waived, otherwise they may still be enforced.

This means that any work which has been linked to an NFT and released under a CC0 licence may be copied and reworked as no one owns the exclusive commercial and non-commercial rights. Practitioners should note that these rights are separate from the rights of ownership in the token.

Decentralised autonomous organisation (DAO) ownership of IPR

The issue of ownership is not only important for practitioners so that entities may be able to license rights, which they do in fact own, but it is also important so that it is possible to determine which legal entity owns the relevant IPR. As discussed above in relation to software, where an employee creates a copyright work in the course of their employment, the employing entity will own the copyright in the work (subject to an agreement to the contrary). One question that has been raised in relation to blockchain is: can a DAO own IPR?

This question is, in part, answered by determining the legal status of a DAO which will in turn be influenced by the factual organisational nature of each DAO. If, as suggested in this report, a DAO is considered to be a general partnership, the issue of joint ownership of IPR arises. The DAO's "token holders", being individual investors with a common view of making profit, may well be considered joint owners of any IPR which has been created by or transferred to the DAO.

In the UK, without an express agreement to the contrary, co-owners of IPR may not exploit jointly held IPRs without the consent of the other joint owners. This can stifle commercial exploitation of the IPR, and even management of an IPR portfolio. For example, in respect of patents, all applicants have to agree on any amendments to the specification. Therefore, DAOs would need a mechanism for making decisions around IPR exploitation and portfolio management.

However, practitioners should be aware that not all IPR is treated in the same way. For example, if goodwill is owned by a general partnership, the goodwill attaches to the partnership itself and not to the individual members[262]. This could raise issues if certain token holders ever sought to exploit the goodwill associated with a DAO in a new project, for example.

[260] https://worldofwomen.mypinata.cloud/ipfs/QmRPn2jf3u5tc47Z2PDJRbzKZhBUyi4qBABfSVCDWeUBPz

[261] Disclaimer - all licences are as accessed on 10 October 2022. The above comments should not be considered as legal advice in relation to the enforceability of terms of the licences and assignments (as applicable) but are intended to highlight the issues, using examples, that practitioners should consider when approaching a NFT project.

[262] Gill v Frankie Goes to Hollywood, Decision of Registrar of Trade Marks 0-140-07 of Mr Foley 25 May 2007

Conclusion

As this section has demonstrated, blockchain and related technologies such as NFTs and metaverses pose both potential opportunities and risks for IP rightsholders in every area from registration and ownership to infringement and enforcement. The mapping of intellectual property regulation onto these technologies, as with all new developments, is haphazard at least until the full extent of the technology is realised and its impact for rightsholders is understood.

Guidelines are being developed and the impact of these technologies is being considered by national, regional and international policymakers. Consultations around the extent of IP protection are currently taking place at international level, through WIPO[263], and at national level, for example the UK Digital, Culture, Media and Sport (DCMS) Select Committee announced an inquiry into Non-fungible tokens (NFTs) and the blockchain in November 2022. The call for evidence asks pertinent questions such as "is the UK's light-touch NFT regulation sufficient?" as well as considering the potential benefits and harms posed by NFTs.[264] Practitioners must keep track of these developments and rightsholders should engage with policymakers at this pivotal time to ensure that IP protection is upheld in the future of blockchain and related technologies.

[263] https://www.wipo.int/about-ip/en/frontier_technologies/
[264] https://committees.parliament.uk/work/7038/

Part 2: Impacts on the Wider Landscape

Section 12 Dispute Resolution

12

Section 12: Dispute Resolution

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

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

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

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 8. 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.[265] 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

[265] 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

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 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 10); 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 10)

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 considers issues that are of fundamental importance to the efficient and effective governance of DLT systems, as follows:

— **Jurisdiction and applicable law:** where, how and by what law (or laws) should disputes arising out of DLT systems be resolved?

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

The recent collapse of FTX has highlighted the risks faced by participants in cryptoasset markets.[266] Regulators are becoming increasingly concerned about the absence of consumer and investor protection for those participating in such markets.[267] Illicit use of cryptocurrencies to facilitate money-laundering, cyber crimes and token fraud has compelled regulators in many jurisdictions to bring cryptoassets within the scope of AML

[266] Despite being one of the world's largest cryptoasset trading exchanges, FTX suffered from "a complete failure of corporate controls", "complete absence of trustworthy financial information" and "compromised systems integrity" (according to a Chapter 11 filing by its court-appointed CEO, John J. Ray III: <https://www.documentcloud.org/documents/23310507-ftx-bankruptcy-filing-john-j-ray-iii> Accessed December 2022).

[267] In June 2022, the Bank of England Governor, Andrew Bailey, warned that there were a lot of 'bad actors' in the crypto world and that cryptoasset investors should be prepared to lose all their money: <https://uk.news.yahoo.com/bank-of-england-bailey-crypto-warning-lose-money-162315148.html> Accessed December 2022. The European Parliament's briefing on the EU's proposed regulation on markets in cryptoassets notes that "fraud remains significant and constant" across cryptoasset markets:
<www.europarl.europa.eu/RegData/etudes/BRIE/2022/739221/EPRS_BRI(2022)739221_EN.pdf > Accessed December 2022.

and anti-terrorist financing laws.[268] The increasing use of DLT in financial services has, moreover, 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.[269]

Whilst early progenitors of blockchain technology aimed at creating self-governing and state-remote networks, as epitomised by Bitcoin, experience has demonstrated the need for cryptoassets and other DLT applications to operate within traditional legal and regulatory frameworks. A vision of DLT systems operating in an entirely self-automated manner untouched by traditional law and regulation is not feasible.

1. Jurisdiction and Applicable Law

Notwithstanding the automaticity of smart contracts and the disintermediated nature of DLT systems, there remains considerable scope for disputes to arise out of these systems and their operation. Such disputes may arise between system participants or between participants and outside parties. For example:

— Coding errors or bugs may cause a smart contract to perform in an unintended way;[270]

— 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;[271]

— 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 (e.g. 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 (e.g. by wallet providers failing to keep digital keys secure or misappropriating digital assets in their custody or control);[272] 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 or other property rights.[273]

There clearly is scope for resolving some disputes between participants of a DLT system by encoded on-chain dispute resolution mechanisms. However, such

[268] See e.g. Bermuda's Digital Asset Business Act; Malta's Virtual Financial Assets Act and the AML measures taken by UK and EU regulators discussed below.

[269] 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 December 2022; and the UKJT Legal statement on cryptoassets and smart contracts, published November 2019 <https://resources.lawtechuk.io/files/4.%20Cryptoasset%20and%20Smart%20Contract%20Statement.pdf> Accessed May 2023; 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

[270] The DAO hack exploited vulnerability in ether's computer code which enabled an attacker to drain over $50 million worth of ether in a way that other members of The DAO did not anticipate or intend (as explained by De Filippi and Wright [2018] Blockchain and the Law: the Rule of Code 200).

[271] In B2C2 Ltd v Quoine Pte Ltd [2019] SGCH(I) 3; Quoine Pte Ltd v B2C2 [2020] SGCA(I) 2, the claimant sought unsuccessfully to reverse automatic algorithmic trades on a cryptoasset trading platform that had been concluded at 250 times the going market rate for the cryptoassets in question.

[272] Hacks of cryptoasset exchanges have become increasingly common (e.g. the hack of Coincheck in 2018 resulting in the loss of cryptoassets with a reported value of more than $500 million). The collapse of FTX has been attributed to the misappropriation of billions of dollars of customer funds by or at the behest of its former CEO, Samuel Bankman-Fried.

[273] Such disputes will frequently arise on insolvency of a cryptoasset exchange or other intermediary, as in Ruscoe v Cryptopia Limited (In Liquidation) [2020] NZHC 728.

mechanisms could not resolve disputes involving parties outside the network.[274] It is also unlikely that on-chain dispute resolution mechanisms will displace altogether traditional off-chain dispute resolution mechanisms in disputes between system participants. 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.[275]

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.[276] They should be drafted so as to make clear that they create binding legal relationships not only between each individual user (or node) on the system and the relevant administrator or operating authority (**R(O)A**),[277] 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”.[278] A similar effect can be achieved by the use of master or framework agreements, as are typically used in DLT trading and settlement systems.[279]

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).

[274] Note that the real-world customers of a cryptoasset exchange or cryptoasset trading platform will usually count as outside parties since they will ordinarily not themselves be directly connected to the DLT systems on which their cryptoassets are held or traded.
[275] 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 270) 200-201.
[276] 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, 34 edn, Vol 1, para 2-118.
[277] A term adopted by the FMLC in its report (n 269) para 6.16.
[278] UKJT Legal statement (n 269) para 148
[279] For example, the DLT derivative trading platforms considered in the ISDA / Clifford Chance paper (n 269)

Arbitration

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.[280] 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.[281] Specialist pools of arbitrators with relevant experience of DLT disputes are likely to develop over time.

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

- **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.

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

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

- **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.[282] 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 (i) may not extend to the grant of such remedies against third parties who are not bound by the relevant arbitration agreement; and (ii) generally require the prior consent of the arbitral tribunal or parties (except in urgent cases).[283] This can impede the tracing of misappropriated digital assets, especially given the speed with which such assets can be transferred.

- **Lack of precedent:** unlike court judgments, arbitral awards are not ordinarily reported and have no precedential status in other arbitrations. This requires each tribunal effectively to re-invent the wheel and deprives them of the benefit of decisions in preceding cases. This is potentially problematic in a developing area of law, where it makes sense for adjudicators to 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.[284] 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.

[282] 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.

[283] For example, the English court's power to make orders in support of arbitral proceedings under s.44 of the Arbitration Act 1996 does not allow the court to make orders for the preservation of evidence, or grant freezing injunctions, against a non-party to the arbitration agreement (Cruz City 1 Mauritius Holdings v Unitech Ltd [2014] EWHC 3704 (Comm) [46]–[51], Males J, and DTEK Trading SA v Morozov [2017] EWHC 94 (Comm), Cockerill J).

[284] UKJT Legal Statement (n 269) para 164

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

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

- **Enforcement of remedies:** consideration should be given to providing in the arbitration agreement for awards to be binding on all other participants in the system, so as to avoid the risk of conflicting decisions being rendered on common issues in different disputes (which could have a destabilising impact on the system as a whole).[285] 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.

- **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[286] (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,[287] 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.[288] The Business and Property Courts in England are well-placed for this purpose. They (and other specialist courts in England)

[285] 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.

[286] 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.

[287] 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 Conwvention 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.

[288] 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); Toma v Murray [2020] EWHC 2295 (Ch); and Litecoin Foundation Limited v Inshallah Limited [2021] EWHC 1998 (Ch). The UKJT Legal Statement and AA v Persons Unknown were cited in Ruscoe v Cryptopia [2020] NZHC 728, where the High Court of New Zealand found that cryptoassets held by an insolvent cryptocurrency trading exchange constituted property held by the exchange on trust for its accountholders.

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, Switzerland and New Zealand.[289]

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

Applicable Law

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

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.[290] However, under Regulation 593/2008 on the law applicable to contractual obligations[291] (the **Rome I Regulation**),[292] 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.[293]

- 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"*.[294] 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

[289] In relation to Singapore and New Zealand, see for example the Quoine and Cryptopia cases mentioned above. In Switzerland, the Adoption of Federal Law to Developments in Distributed Ledger Act introduced a concept of DLT rights for digital assets and a licensing system for the trading of such assets (including segregation requirements for cryptoassets held by third party custodians such as wallet providers).

[290] Dicey, Morris & Collins, The Conflict of Laws, (16th edn, Sweet & Maxwell, 2022) para 32R-063 et seq., especially at para 32-072 to 32-074.

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

[292] 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.

[293] 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".

[294] Ibid, para 7.245.

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.[295]

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

Parties should ensure that the chosen law recognises (or is likely to recognise) the legality and enforceability of SLCs. English law is a good candidate, given the conclusion reached by the UKJT that smart contracts are capable of giving rise to binding legal obligations and can be analysed according to "entirely conventional" legal principles.[296] 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".[297] 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 chosen any forum for resolution of disputes or expressly assigned the application of any particular law by which disputes should be resolved. In the case of a permissionless DLT system, jurisdiction and applicable law will typically fall to be determined by application of the relevant conflict of law rules by the national courts seized of a dispute.

In England, the court's jurisdiction generally depends upon the defendant's presence in, or submission to, the jurisdiction or alternatively valid service of legal proceedings (in accordance with the English court's rules) on the defendant outside the jurisdiction.[298]

An English court would apply the rules of the Rome I and Rome II Regulations to ascertain the applicable law.[299] 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

[295] 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.

[296] UKJT Legal Statement (n 269) paras 136-148. Note also the desire expressed by the Law Commission in its current consultation on Digital assets (see footnote [269] 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".

[297] AA v Persons Unknown [57] and [59] (Bryan J), followed and applied in Toma v Murray and Litecoin Foundation Limited v Inshallah Limited (footnote [288] above).

[298] See Dicey, Morris & Collins, The Conflict of Laws (footnote [290]), Chapter 11.

[299] 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.

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 the place where the majority of Bitcoin mining activity is centred (which may e.g. be in the People's Republic of China) was the law applicable to relationships between participants.[300]

Property Aspects

The above addresses issues of applicable law primarily as between system participants. However, digital assets held on a DLT system are a species of property.[301] 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"*.[302]

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 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.[303] 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.[304] 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.[305]

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.[306] 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"*.[307] Another solution must therefore be found. Several have been suggested.

[300] 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.

[301] As noted by the UKJT in its Legal Statement (n 269) paras 15 and 86, and confirmed by Bryan J in AA v Persons Unknown [61]. This analysis was followed and applied in Toma v Murray and Litecoin Foundation Limited v Inshallah Limited, and has been adopted in other common law jurisdictions, including New Zealand (Ruscoe v Cryptopia): see further footnote [288] above. Proprietary freezing and preservation orders over cryptoassets were also made in Vorotyntseva v Money-4 Ltd [2018] EWHC 2596 (Ch), Birss J, and Shair Com Global Digital Services Ltd v Arnold [2018] BCSC 1512 (Supreme Court of British Columbia). Although the Singapore Court of Appeal left open the question of whether cryptoassets constituted property in Quoine v B2C2 (footnote [6]), Menon CJ said that this view had "much to commend" it (at [144]). In its Consultation Paper on Digital Assets (Law Com No 256), the Law Commission agrees with the approach taken by the UKJT in its Legal Statement and provisionally proposes that 'data objects' (which would encompass cryptoassets) be explicitly recognised as a new category of personal property.

[302] UKJT Legal Statement (n 269) para 36

[303] As explained by Dicey, Morris & Collins, The Conflict of Laws (footnote [290]) para 23-025.

[304] 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.

[305] As in Art. 14(1) of the Rome I Regulation.

[306] 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 269) para 6.3.

[307] UKJT Legal Statement (n 269) para 97.

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"*.[308] 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.[309] 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).[310] 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.[311]

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.[312] The need for such international co-operation and co-ordination is clear and compelling. Otherwise uncertainty about the law governing the proprietary effects of the transfer and disposition of digital assets held on DLT systems will undermine trust and confidence in these systems and impede their adoption in the financial services industry and other sectors.

Money Laundering

The Problem Identified

Regulators have become increasingly concerned about the illicit use of cryptocurrencies. Their decentralised, disintermediated and pseudonymous nature makes them ideal vehicles for money-laundering, terrorist financing and other criminal activities, including ransomware attacks, ICO token frauds and transactions

[308] FMLC report (n 269) paras 6.5 and 7.1-7.4.

[309] Ibid para 6.9.

[310] Dickinson in Fox and Green (n 300) para 5.110

[311] 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.

[312] See FMLC report (n 269) paras 5.1-5.2; and UKJT Legal Statement (n 269) 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

on the darkweb.[313] The scale of such criminal activity is difficult to quantify but it is clearly significant and could run into tens of billions of dollars.[314]

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**)[315], 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'"*.[316] The problem is compounded by the increasing use of devices such as tumblers, mixers and private coins to enhance the anonymity of cryptoasset transactions.[317]

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 focused on entities operating at this interface, i.e. cryptoasset exchanges and digital wallet providers. However, it is unclear whether this suffices given the extent to which users can bypass exchanges by using cryptoassets to pay directly for goods and services or transmit value on a peer-to-peer basis.

Regulators have nevertheless been wary of stifling technological innovation. The EU Report explicitly advised against 'throwing the baby out with the bathwater': *"Legislative action should always be proportionate so that it addresses the illicit behaviour while at the same time not strangling technological innovation at birth."* [318] 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.[319]

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".[320] 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"*.[321]

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.[322] 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

[313] 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.

[314] 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%.

[315] Ibid.

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

[317] 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 [313] above) drew attention to the increasing prevalence of ransomware attacks demanding payments in Anonymity-Enhanced Cryptocurrencies, such as Monero.

[318] EU Report (n 314) para 4.1.6

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

[320] EU Report (n 314) para 4.1.2.

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

[322] FATF Guidance (n 95).

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".[323] Nevertheless, progress has been made in the UK (see below), the EU and the United States to improve AML and anti-terrorist financing regulation of cryptoasset markets.[324]

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:[325]

- 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.

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", 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.[326] 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:

[323] FATF, Second 12-Month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers, July 2021 https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfrecommendations/Second-12-month-review-virtual-assets-vasps.html
Accessed October 2021.

[324] In October 2022, the European Council approved the Markets in Crypto-Assets (MiCA) Regulation, which provides not only rules for the prevention of money-laundering and terrorist financing but also rules for consumer protection and prevention of market abuse to ensure the integrity of cryptoasset markets. In December 2022, Senators Warren and Marshall introduced the Digital Asset Anti-Money Laundering Bill in Congress aimed at bringing more of the cryptocurrency market in the US into compliance with Federal money-laundering and terrorist financing laws.

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

[326] FCA, 'Cryptoassets: AML/CTF regime: Register with the FCA' (published 10 January 2020 and updated 1 July 2020). https://www.fca.org.uk/firms/cryptoassets-aml-ctf-regime/registering Accessed June 2020.

— The Cryptoasset Service Provider must register with (and obtain approval from) the FCA before commencing business as a Cryptoasset Service Provider.[327] 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.[328]

— 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.[329]

— 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.[330]

— 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.[331] 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.

— The Cryptoasset Service Provider must in certain circumstances undertake enhanced due diligence measures, including (i) when dealing with high-risk third countries;[332] (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.[333]

— 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.[334]

— 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.[335]

— 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

[327] Regulation 56 of the AML Regulations.

[328] The FCA has refused applications on this ground where e.g. the applicant had deliberately and recklessly published on its website misleading marketing and promotional material: Moneybrain Limited v Financial Conduct Authority [2022] UKUT 00308 (TCC).

[329] Regulation 18 of the AML Regulations.

[330] Regulation 19 of the AML Regulations.

[331] Regulation 27 of the AML Regulations

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

[333] Regulations 33 and 35 of the AML Regulations.

[334] Regulation 40 of the AML Regulations.

[335] Regulation 31 of the AML Regulations.

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 encompass not only cryptocurrencies but also security and utility tokens. 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.[336] 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 could be improved. As at December 2022, 40 firms had been registered but many more were awaiting registration. An even larger number of firms was then 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.[337]

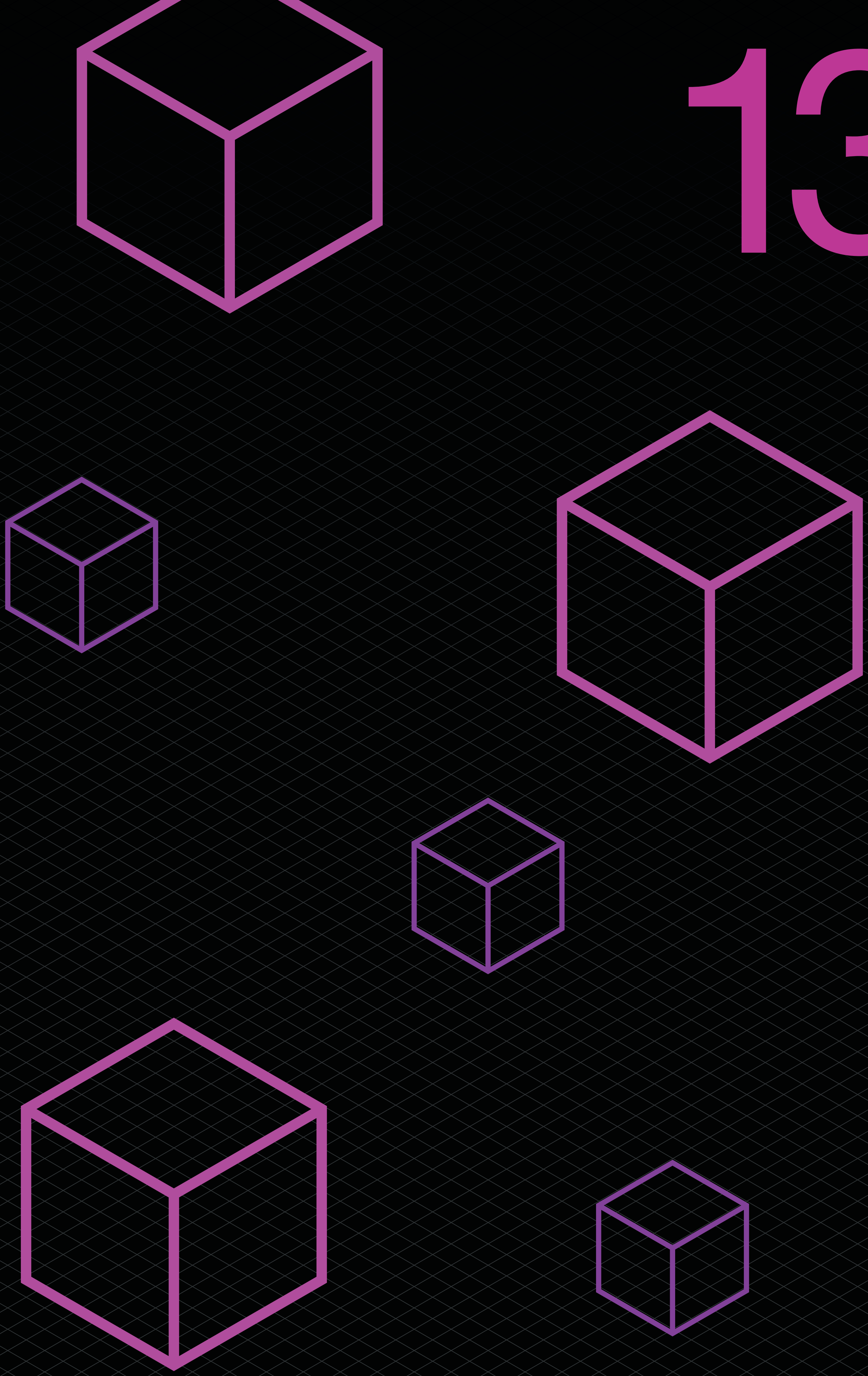
[336] EU Report (n 314) paras 5.3.3 and 5.3.5.

[337] 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. The FCA provides on its website a list of UK businesses that appear to be carrying on cryptoasset activity without being registered with the FCA for AML purposes.

Part 2: Impacts on the Wider Landscape

Section 13 Competition

13



SECTION 13: COMPETITION

Brendan McGurk and Will Perry (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.[338]

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

[338] 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.

with certainty what type of adverts they wish to receive rather than seeking to profile 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."* [339]

Blockchain coupled with the use of smart contracts[340] 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.[341] 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.

Competition law concerns

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"*. [342]In this section, we therefore focus principally on uses of private/permissioned blockchains. [343]

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

[340] 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.

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

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

[343] 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, available here: https://www.cci.gov.in/sites/default/files/whats_newdocument/Blockchain.pdf. For a discussion of the potential interaction

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"*. [344]

— 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.

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.[345]

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

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, available here: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3315182.

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

[345] 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, available here: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3256728.

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[346] 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.[347]

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.[348]

[346] See: Ping Europe Ltd v CMA [2020] EWCA Civ 13; [2020] 4 CMLR 13, ¶¶26-29, 39.

[347] See: Case C-230/16 Coty Germany GmbH v Parfümerie Akzente GmbH [2018] 4 CMLR 9, ¶36.

[348] 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 interoperability).[349]

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).[350] 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.[351] 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.[352]

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.[353]

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)[354] 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

[349] Renato Nazzini, "The Blockchain (R)evolution and the Role of Antitrust", p. 3.
[350] Commission Regulation (EU) No 1217/2010 (14 December 2010), Article 4(2).
[351] 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.
[352] Renato Nazzini, "The Blockchain (R)evolution and the Role of Antitrust", p. 4.
[353] Renato Nazzini, "The Blockchain (R)evolution and the Role of Antitrust", p. 5.
[354] Renato Nazzini, "The Blockchain (R)evolution and the Role of Antitrust", p. 5.

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 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.[355]

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.[356] 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.[357]

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.[358] Different proposals for updates relating to the same chain may compete with one another, i.e. in a "hash war", where the mining servers[359] participating in a blockchain network "vote" on which set of rules

[355] CMA Decision in Case 50233, Online sales of posters and frames (12 August 2016), available here: https://assets.publishing.service.gov.uk/media/57ee7c2740f0b606dc000018/case-50223-final-non-confidential-infringement-decision.pdf.

[356] See in particular: Thibault Schrepel, "Collusion by Blockchain and Smart Contracts", pp. 117-166.

[357] Thibault Schrepel, "Collusion by Blockchain and Smart Contracts", pp. 143-151.

[358] United American Corporation v Bitmain (Case No. 1.18-cv-25106), §I.B.2. The judgment is available here: https://www.courtlistener.com/docket/8382061/united-american-corp-v-bitmain-inc/

[359] 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

or protocol they prefer, and "the rules set mined with the most computer hashing power would prevail and continue the … blockchain going forward.[360] 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 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).[361]

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.[362]

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.[363] 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."[364]

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".[365] 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

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.

[360] 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.

[361] The judgment is available here: https://www.courtlistener.com/docket/8382061/united-american-corp-v-bitmain-inc/

[362] United American Corporation v Bitmain, §II.B.

[363] United American Corporation v Bitmain, §II.B.2, and subsections.

[364] *United American Corporation v Bitmain*, §II.B.2.d.(3)

[365] United American Corporation v Bitmain, §II.B.3.a.(2).

assertions which were capable plausibly of demonstrating whether or not there 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.[366]

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.[367]

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).[368]

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".[369] 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".[370] 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."[371] As regards uses of blockchains that do not amount to cartels or infringements of Article

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

101/the Chapter I Prohibition by object, Nazzini 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."* [372]

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)[373] 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)"*.[374]

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.[375] 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."[376] 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.

[372] Renato Nazzini, "The Blockchain (R)evolution and the Role of Antitrust", pp.8-9, insertion added.

[373] The Chapter II Prohibition and Article 102 both refer to abuse "by one or more undertakings".

[374] Pike and Capobianco, 'Antitrust and the trust machine' (2000), p.8; available at http://www.oecd.org/daf/competition/antitrust-and-the-trust-machine-2020.pdf.

[375] See Opinion 21-A-05 of 29 April 2021 on the sector of new technologies applied to payment activities, p.5; available at https://www.autoritedelaconcurrence.fr/sites/default/files/attachments/2021-06/21-a-05_en.pdf.

[376] 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.[377] 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”.[378] 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.[379] 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.[380]

[377] 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 page 32

[378] Khan, ‘Amazon’s Antitrust Paradox’, Yale Law Journal, 126 (2017), p.44; available at https://ssrn.com/abstract=2911742.

[379] Note that Exclusivity may be contractual or de facto.

[380] 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[381]) 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,[382] cross border payments systems,[383] and intellectual property rights.[384] 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".[385] 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"*.[386] 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.[387] 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.[388] Courts have been willing to set FRAND prices in appropriate cases.[389] There is no reason in principle why this approach could not be applied in the blockchain context. Less clear is the extent to which these principles are

[381] For an example of constructive refusal to supply, see Case T-486/11 Orange Polska v Commission.

[382] See London European-Sabena, OJ [1988] L 317/47.

[383] Commission Notice on the Application of the Competition Rules to Cross-border Credit Transfers, OJ [1995] C 251/3.

[384] Discussed below.

[385] 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.

[386] 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.

[387] See Attheraces v British Horseracing Board [2007] EWCA Civ 38.

[388] See Unwired Planet International Ltd v Huawei Technologies Co. Ltd & Anor [2020] UKSC 37, para 114.

[389] 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.

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.[390] 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."[391]

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".[392] 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.[393]

> *"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".[394] 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

[390] 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/.

[391] 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.

[392] 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.

[393] 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.

[394] Case C-27/76, United Brands v Commission, para 249.

no ability to opt-out of the processing activities.[395] 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."[396]

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[397]? 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 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

[395] 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/.

[396] Schrepel, comments to the European Commission, p.3.

[397] 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.

renders them dominant? Or indeed only those sub-set of users who have market power by reference to the chain's particular applications?[398]

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".[399] 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.

In July 2021, the Government published a consultation on proposals for the new

[398] Shrepel, Is Blockchain the Death of Antitrust Law? P 304
[399] https://www.gov.uk/government/collections/digital-markets-unit

pro-competitive regime that will apply to digital markets.[400] 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.[401] 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.

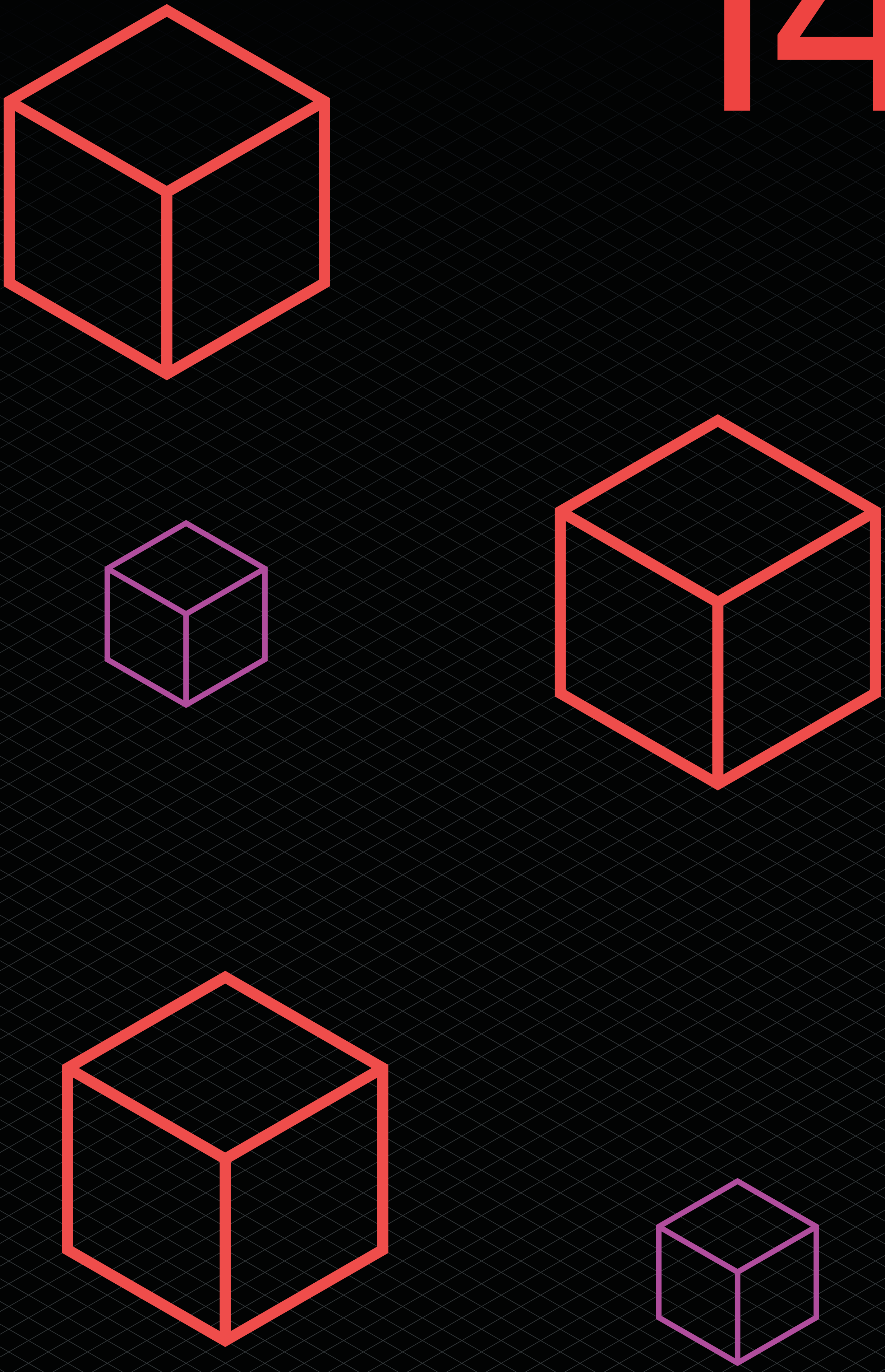
[400] https://www.gov.uk/government/consultations/a-new-pro-competition-regime-for-digital-markets

[401] 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 14 Blockchain and Tax

14



Section 14: Blockchain And Tax

Ceri Stoner, 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 critical 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,[402] the UK government has repeatedly reiterated its claim to be a world leader in this sector. A government taskforce has been established to consider the introduction of a new 'Britcoin' in the form of a central bank digital currency ('CBDC'). Conversations are ongoing between the UK government, the Bank of England and UK businesses to assess the benefits and implications of such a 'Britcoin'.

In 2022, the UK government announced a package of measures to promote the UK as a global cryptoasset technology hub to help ensure that the UK financial services sector continues to grow and attract investment in this sector.[403] Part of this package of measures included exploring ways of enhancing the competitiveness of the UK tax system to encourage further development of the cryptoasset market.

The tax treatment of cryptoassets therefore continues to be under review. As the UK continues to make real-world developments to embed cryptoassets into the financial industry, it is essential that the tax system keeps up. Since 2020, 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, and has since been expanded upon in its continued effort to regulate and provide guidance in this space.[404]

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, examined in this section:

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 Smart Legal Contracts ('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

[402] Kalifa Review of UK fintech, 26 February 2021
[403] https://www.gov.uk/government/news/government-sets-out-plan-to-make-uk-a-global-cryptoasset-technology-hub
[404] https://www.gov.uk/hmrc-internal-manuals/cryptoassets-manual.

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

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

1. Taxation of cryptoassets and blockchain

In the UK at present, there is no specific legislation, nor 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 cryptoasset 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, the 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 13, 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 is 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 as "cryptographically secured digital representations of value or contractual rights that can be transferred, stored and traded electronically".[405] This definition differs subtly but significantly 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 rather the cancellation of one asset and creation of another. The UKJT proposed in its Legal Statement[406] 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'.[407] This provided a global overview of the tax treatments of virtual currencies in different jurisdictions honing-in on the associated policy issues. A more detailed follow up report is expected.

As also explored in Section 3, the UK Government's Cryptoasset Taskforce (comprising HM Treasury, The Financial Conduct Authority ('FCA') and the Bank of England) has recognised three types of cryptoasset since October 2018.[408] In HMRC's March 2021 Cryptoassets Manual,[409] this has been increased to four:

1. **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.

2. **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'.

3. **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.

4. **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, whilst understandable given that they have received most investment, will nonetheless

[405] https://www.gov.uk/hmrc-internal-manuals/cryptoassets-manual/crypto10100

[406] UKJT Legal Statement on cryptoassets and smart contracts, published November 2019 https://resources.lawtechuk.io/files/4.%20Cryptoasset%20and%20Smart%20Contract%20Statement.pdf

[407] https://www.oecd.org/tax/tax-policy/taxing-virtual-currencies-an-overview-of-tax-treatments-and-emerging-tax-policy-issues.htm

[408] 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

[409] https://www.gov.uk/hmrc-internal-manuals/cryptoassets-manual/crypto10100

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 is still silent.

In terms of validation of transactions, HMRC does now recognise proof of stake 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.[410] This 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, that is, crypto derivatives. 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.[411] The area of decentralised finance (DeFi) has been one of particular focus for HMRC in the last year, with update to HMRC's cryptoassets manual to clarify the tax position for parties lending and staking on DeFi transactions and to provide an indication of specific situations where UK tax may become due.[412] In particular, the update suggests that HMRC would not classify earned income (including where a DeFi loan has returns in the form of a cryptoasset or cryptocurrency) or the rate of return as interest.[413] HMRC's published position is that the following would probably be treated as disposals for chargeable gain purposes; (i) lending and borrowing of cryptoassets; (ii) utilising cryptoassets to either provide collateral for debt or as repayment of debt.[414]

The update to HMRC's guidance was followed by an HM Treasury consultation in July-August 2022 to consider the taxation of decentralised financing, in particular in relation to the tax treatment of cryptoasset loans and 'staking'.[415] It therefore seems likely that there will be further refinement to HMRC's position in the near future.

Substance of transaction

The tax treatment of all types of tokens 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.[416] 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 light of HMRC's view that cryptoassets are not currency or money,[417] 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).

[410] https://www.gov.uk/hmrc-internal-manuals/cryptoassets-manual/crypto10300
[411] https://www.gov.uk/hmrc-internal-manuals/cryptoassets-manual/crypto10150
[412] https://www.gov.uk/hmrc-internal-manuals/cryptoassets-manual/crypto60000
[413] https://www.gov.uk/hmrc-internal-manuals/cryptoassets-manual/crypto61110 and https://www.gov.uk/hmrc-internal-manuals/cryptoassets-manual/crypto61412
[414] https://www.gov.uk/hmrc-internal-manuals/cryptoassets-manual/crypto61630 and https://www.gov.uk/hmrc-internal-manuals/cryptoassets-manual/crypto61640
[415] https://www.gov.uk/government/consultations/call-for-evidence-the-taxation-of-decentralised-finance-involving-the-lending-and-staking-of-cryptoassets
[416] https://www.gov.uk/hmrc-internal-manuals/cryptoassets-manual/crypto10100
[417] https://www.gov.uk/hmrc-internal-manuals/cryptoassets-manual/crypto10100

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 (i) income and capital treatment; (ii) application of transfer taxes and VAT; and (iii) operation of 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 individuals receive the cryptoassets from:

i. their employer as a form of non-cash payment; and/or

ii. mining, transaction confirmation or airdrops.[418]

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.[419]

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'). 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."* [420]

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".*[421]

[418] https://www.gov.uk/hmrc-internal-manuals/cryptoassets-manual/crypto20050 and https://www.gov.uk/guidance/non-cash-pay-shares-commodities-you-provide-to-your-employees
[419] https://www.gov.uk/hmrc-internal-manuals/cryptoassets-manual/crypto21100
[420] https://www.gov.uk/hmrc-internal-manuals/cryptoassets-manual/crypto21100
[421] https://www.gov.uk/hmrc-internal-manuals/cryptoassets-manual/crypto42250

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.[422] If an airdrop is received in exchange for the 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.[423] 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.[424]

Capital Gains Tax

As noted above, HMRC considers that cryptoassets are typically held as personal investments and, as such, will attract capital gains tax on disposal on any gains realised. While intangible assets, 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:[425]

- selling cryptoassets for money;
- exchanging cryptoassets for a different type of cryptoasset;
- using cryptoassets to pay for goods or services; and
- giving away cryptoassets to another person.

It should, however, be noted that HMRC states that 'disposal' is a broad concept and therefore this is a non-exhaustive 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."[426] The application of these rules also applies in a corporate context.

Corporation Tax

As noted above, HMRC does not consider cryptoassets to be money or currency. As such, any corporation tax legislation relating exclusively to money or currency does not apply to cryptoassets.[427] 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.

[422] https://www.gov.uk/hmrc-internal-manuals/cryptoassets-manual/crypto21250
[423] https://www.gov.uk/hmrc-internal-manuals/cryptoassets-manual/crypto20050
[424] https://www.gov.uk/hmrc-internal-manuals/cryptoassets-manual/crypto20250
[425] https://www.gov.uk/hmrc-internal-manuals/cryptoassets-manual/crypto22100
[426] s.104(3)(ii) TCGA 1992
[427] https://www.gov.uk/hmrc-internal-manuals/cryptoassets-manual/crypto41050

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"*.[428]

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[429] have priority over the chargeable gains rules".[430] 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,[431] however, such losses must be reported to HMRC first. Also, in the same way as 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.[432] 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.[433] Where a person owns a variety of types of token, such as Bitcoin, Ether and Litecoin, that individual will need to have three separate pools for each type of token.[434]

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.[435]

[428] Ibid
[429] Corporation Tax Act 2009, Part 8
[430] https://www.gov.uk/hmrc-internal-manuals/cryptoassets-manual/crypto41150
[431] https://www.gov.uk/hmrc-internal-manuals/cryptoassets-manual/crypto41300
[432] https://www.gov.uk/hmrc-internal-manuals/cryptoassets-manual/crypto41450
[433] Ibid
[434] https://www.gov.uk/hmrc-internal-manuals/cryptoassets-manual/crypto22200
[435] https://www.gov.uk/hmrc-internal-manuals/cryptoassets-manual/crypto44100

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.”*[436]

This logic could potentially extend to all cryptoassets, depending on their specific terms.

The same is considered true if exchange tokens were given as consideration for a land transaction, in which instance they would be deemed to be ‘money or money’s worth’ and therefore chargeable to stamp duty land tax.

The position in respect of stamp duty differs, however. HMRC guidance suggests that exchange tokens – and therefore by extension all cryptoassets – are not considered to meet the definition of ‘money’ in the context of stamp duty consideration. This is the logical conclusion to HMRC’s position that cryptoassets are neither money nor currency.

VAT

HMRC guidance provides that:

> *“VAT is due in the normal way on any goods or services sold in exchange for cryptoasset exchange tokens. The value of the supply of goods or services on which VAT is due will be the pound sterling value of the exchange tokens at the point the transaction takes place.”*[437]

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,[438] have 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:*
   ii. the activity does not constitute an economic activity for VAT purposes because there is an insufficient link between any services provided and any consideration; and
   iii. 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 the VAT Finance Manual (VATFIN7200), will be exempt from VAT under Item 5, Schedule 9, Group 5 of the Value Added Tax Act 1994.”*[439]

However, it should be noted 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.

[436] https://www.gov.uk/hmrc-internal-manuals/cryptoassets-manual/crypto44150
[437] https://www.gov.uk/hmrc-internal-manuals/cryptoassets-manual/crypto45000
[438] For example, CJEU case, Skatteverket v David Hedqvist C-264/14 (22 October 2015) and First National Bank of Chicago (C-172/96) (14 July 1998). https://www.gov.uk/hmrc-internal-manuals/cryptoassets-manual/crypto45000
[439] https://www.gov.uk/hmrc-internal-manuals/cryptoassets-manual/crypto45000

1. 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.[440]

This was confirmed in the Court of Justice of the EU (CJEU) in the Swedish case, *David Hedqvist (C-264/14)*.[441]

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.

2. Impact of blockchain on tax authorities

The impact of blockchain on tax policy and tax evasion has 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, which 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, or ‘CARF’ (the Crypto-Asset Reporting Framework) to increase transparency surrounding the (tax) treatment of crypto-assets. Following a public consultation on the topic in 2021-22, CARF was approved by the G20 in August 2022, and reviewed by the Finance Ministers and Central Bank Governors. Whilst this new standard has not yet been published, it is expected soon in the first half of 2023.

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 of cryptoassets and virtual currencies.[442] 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 enter into force on 1 January 2026 and will be enforced by virtue of significant new penalties. In addition, the European Parliament, Council and Commission agreed on the Markets in crypto-assets (MiCA) Regulation in June 2022, which will take effect in 2024. MiCA will act as a mechanism to regulate the issuance, offer to the public and trading of crypto-assets and is expected to be adopted by various European jurisdictions as a unified licensing regime. Whilst changes in European statute will not, from a legal perspective, have direct effect in the UK, as a non-European jurisdiction, this is expected to influence UK policy changes and will of course impact UK operators active in European markets.

[440] https://www.gov.uk/hmrc-internal-manuals/cryptoassets-manual/crypto45000

[441] Skatteverket v David Hedqvist C-264/14 (22 October 2015)

[442] 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

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.

— **Futureproofing:** proofing against changes in technical capabilities and standards will be crucial in order to validate the initial investment to adopt such technology in the first place and for it to remain relevant.

— **Mission creep:** as the digital goals are broken down into steps, and developments in the sphere of cryptoassets continues, there is a risk that unplanned and unsustainable long-term commitments may be made.

— **Limitations of digitalisation:** in certain cases digitalisation will not be appropriate, nuances may be missed, and a digitised approach may not be capable of facilitating certain judgement calls.

— **Legislative basis:** it will be vital to establish a proper legal basis for the collection and use of data.

3. 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 internally and externally (in respect of 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 at an organisation, rather than at the periphery.

Part 2: Impacts on the Wider Landscape

Section 15

Blockchain and ESG

15

Section 15: 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 China[443], 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

[443] https://cbeci.org/mining_map

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 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.[444]

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[445]). Blockchain analysis has been recognised as an

[444] https://cryptoclimate.org/

[445] 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.

important tool for cryptoasset service providers to consider when dealing with assets that have originated from anonymous or private sources.[446] Still, important questions remain as to how AML/KYC requirements should be adjusted to take into 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.

[446] See the Joint Money Laundering Steering Group's Sectoral Guidance on Cryptoasset Exchange Providers and custodian wallet providers.

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.

Part 2: Impacts on the Wider Landscape

Section 16

Blockchain and Family Law

16

Section 16: Blockchain and Family Law

Victoria Clarke, Elite Law Solicitors

Introduction

When the Bitcoin white paper was published on 31 October 2008 it envisaged a world with a digital decentralised currency that would fall outside the control of governments and banks. It was a utopian ideal of individuals working together with a currency safe from the centralised currencies so badly affected by the financial crash of 2008. It also allowed users to obtain goods and services anonymously, and became the currency of choice on the dark web.

This anonymity has continued to be one of the most inviting features of cryptoassets within family law proceedings. Individuals can hold cryptoassets without a record anywhere of what they own, when it was obtained, or where it is being held. Arguably it is the latest in a history of tools to obstruct the Family Court from enabling a fair division of assets.

The history of illegality of some cryptoassets can cause concern to people who separate from a partner who owns such assets. It can lead to the belief that those who hold cryptoassets are also hiding other assets within proceedings. Because of this, those who hold cryptoassets are often treated with suspicion and distrust within family law proceedings leading to extensive questioning during disclosure, or a general mistrust of evidence that is provided, even if that evidence is completely accurate and detailed.

Cryptoassets in family law have not received a great deal of testing within the Court arena. This is mainly because family law cases are encouraged to settle, and the majority are unreported. Cryptoassets are also a relatively new asset, so those with significant wealth in cryptoassets may not actually be at the point of a marital breakdown. It is anticipated that more cases with cryptoassets will appear over time, through a combination of it becoming more mainstream and long-term relationships coming to an end where cryptoassets were obtained some time ago.

The majority of this chapter will therefore consider the issues arising within the voluntary settlement process, things for new couples to be aware of, and what should be considered when attempting to reach an agreement or inviting a Court to become involved.

Pre-Nuptial / Cohabitant Agreements

For those going into a new marriage, or beginning a cohabiting relationship, there is benefit to entering into an agreement setting out what would happen at the termination of that relationship. And as younger generations increasingly see the value in these documents, there needs to be consideration for how cryptoassets would be treated within these agreements.

Rather than using a generic “cryptoassets” definition, any agreement should have clear definitions of the different types of cryptoasset that are part of the agreement. If there are any identifiable wallets such as a specific cold wallet, for example a Ledger, Trezor, or other model, these should be specified within the definitions.

The public keys for any shared access wallets, or wallets containing shared cryptoassets, should also be set out in the definitions. This will avoid any future dispute over which wallets were considered shared.

If there is to be a division of any shared cryptoassets on separation, the parties could also consider a nominated wallet for cryptoassets to be transferred into, prior to division. The parties will however need to be aware that the wallets are asset-specific – for example a Bitcoin Wallet, or an Ethereum Wallet. They may therefore have to nominate a wallet per asset.

Disclosure of any separate cryptoassets should be provided in the same manner as any other disclosure within the preparation of a pre-nuptial agreement or cohabitant agreement. This can take the form of a transaction history for a trading account that holds cryptoassets, or the history of a wallet, which is often easy to download within the interface for managing that wallet.

Financial Disclosure on Separation

There is now a Cohabitant Separation Agreement precedents book provided by Resolution, the body of family lawyers who promote the constructive resolution of family disputes.

Whilst cryptoassets are not raised within this version of the precedents, it illustrates that there are many more couples cohabiting in today's society than before. This social structure is growing in popularity, particularly with younger generations. This, together with the fact that obtaining cryptoassets is most popular amongst younger generations, makes it a fair assumption that any division of cryptoassets is likely to occur where couple are cohabitees, rather than married or in a civil partnership. There are no statutory laws to give guidance to cohabitees in England and Wales. Any agreement would effectively be a contract between the parties, with enforceability through the civil courts. It is therefore imperative to ensure that any agreement is clear and accurate.

The provisions for the split of any cryptoassets upon separation can be addressed in the same way as above. Clear definitions of the various relevant wallets will be required, with the public key where it is appropriate.

On separation, the provision of public keys will need to be considered carefully. A public key gives an individual the ability to view the balance and movement of transactions, and that degree of access following a separation may be considered excessive. Practitioners may therefore need to consider whether it is onerous to request or provide this information.

If a party is reluctant to provide their public key, this should be explained clearly to the opposing party to avoid any suggestion of withholding information or frustrating the disclosure process. It should also be recorded in any separation agreement to avoid any suggestion of failure to provide disclosure at a later date.

Financial Settlements within the Court system

The current judicial system is still working to understand cryptoassets and blockchain technology within the family courts. Things are slightly further advanced in the civil courts as there are more cases brought through civil claims between cryptoasset companies, blockchain providers, and trading platforms. The only two reported cases regarding the recognition of cryptoassets as property are both civil cases, and the only other reported case regarding cryptoassets, specifically serving an Order via NFT, was also a civil case.

It is therefore necessary for family lawyers and barristers to explain these assets to a Judge in a clear and precise manner. If not, the risk is that the importance of cryptoassets will be dismissed when considering a Final Order. Judges have been known to ignore tokens that are about to be released through an Initial Coin Offering or accepting that tokens have a nil value because they are not currently listed on a trading exchange, despite there being evidence of their value. Judges have also made Freezing Orders incorrectly, at one point freezing the UK business bank account for a global training platform because the applicant did not correctly explain that they were trying to freeze a user's trading account rather than the bank account itself. There are also professionals advertising order templates that are wrong. Some encourage practitioners to request private keys, which in itself is incorrect and could create significant harm for those that either refuse to provide these keys or provide them and have their wallets affected.

Issues for Solicitors to consider

Practitioners should ensure that clients do not consider taking purely cryptoassets by way of a financial settlement. The explosiveness and volatility of cryptoassets means that a party cannot rely solely on these assets to meet their needs. There should be a balance of centralised and decentralised assets to ensure that even at the bottom of the market, a party can meet their reasonable needs.

Clients must also investigate their tax liabilities as a part of the disclosure process. It is likely that clients will not have made any tax declarations during their trading or mining years, mainly because HMRC did not declare that these were taxable events until 2018. Practitioners should ensure that their clients accurately ascertain their tax liability as part of the disclosure exercise, to ensure they are accounting for what could be quite a large tax bill depending on how long they have held their cryptoassets.

Conclusion

Cryptoassets are here to stay, and they will form part of our society for the foreseeable future. Younger generations have grown up in a digital world, and a digital currency is one step closer to the Metaverse that is becoming more and more accessible.

Whether cryptoassets are used as a currency, or as a traded asset, they will continue to grow and develop. NFTs have had an initial peak but their intrinsic value is still appealing to many. There are those who value digital artwork, and they do not need to hold a tangible object in order for it to retain value.

These views will result in the adoption of cryptoassets increasing, and we as family law practitioners will be exposed to it more frequently. The unpredictability and complexity of these assets means that they should be respected, and understood, before being advised upon. There are practitioners who consider them on the same level as a car or artwork, but they should not be overlooked as this could cause problems for family lawyers in the future, especially if it appears that a client was not properly advised. They should be approached with caution from those with minimal experience, and expert advice be sought if a practitioner is not confident in their own knowledge of the asset.

Part 2: Impacts on the Wider Landscape

Section 17
The Legal and Regulatory Impacts of Non-Centralisation

17

Section 17: The Legal and Regulatory Impacts of Non-Centralisation

Marcus Bagnall, Gabrielle Tanner, Nicholas Crossland and Ben Towell, (Wiggin LLP)

Introduction: network topologies – non-centralised networks

A network can be defined as a system of connections and interconnections that facilitate exchanges. Networks traditionally are ‘centralised’, meaning they have a central authority controlling network decision-making and information-processing. Any peer-to-peer (**P2P**) interactions that occur over a network are only those permitted by the network’s central authority.

As an alternative to centralised networks, disaggregated, decentralised and distributed networks have arisen (each being a **non-centralised network**). Each network type describes distinct architectures, with the distinguishing characteristic between these networks being the locus of network control:

- **Disaggregated networks** are centralised networks with interoperable functional components separately provided and operated by multiple vendors.

- **Decentralised networks** comprise multiple independent control authorities that share network control and maintain independent decision-making and information processing. P2P interactions again only occur as permitted by the decentralised control authorities.

- **Distributed networks** have no central control authority, where instead decision-making and information-processing is shared across independent nodes in accordance with a common network protocol. P2P interactions may occur as is permitted by this protocol.

Blockchain has rapidly realised the potential for non-centralised networks by facilitating network decision-making without a centralised locus of control. Even in a distributed network, without a ‘consensus mechanism’ there is still someone ultimately responsible for the network’s governing protocol.

This chapter focuses on how non-centralised networks can disrupt P2P platforms by helping to solve their unique challenges, and the potential legal and regulatory hurdles arising from this disruption.

1. Creators and consumers – realising non-centralised content

Centralised vs. non-centralised content platforms

Non-centralisation, enabled by blockchain technology, is expected to disrupt the way that content is currently created, consumed, monetised and distributed. Content platforms with a non-centralised backend offer alternative solutions to issues faced by traditional platforms while also providing novel commercial opportunities for content creators, consumers and advertisers.

Traditional streaming models generally rely on centralised content delivery networks (**CDNs**) to obtain, store and distribute content. This centralised approach makes platform owners susceptible to high operational costs, as storage, administration and hardware fees increase with user growth. A centralised model is also by its nature, more vulnerable to hacking compared to platforms built using a non-centralised architecture. The storage structure of a non-centralised platform can enable faster and more reliable streaming by improved content transit.

Platform operators traditionally retain most of the revenue created within a platform’s ecosystem.[447] Blockchain-powered platforms using a non-centralised model provide options for alternative revenue sharing structures, where content creators exert

[447] Chainflix White Paper, Version 2.0, October 2020 https://www.chainflix.biz/assets/pdf/whitepaper.pdf

greater control over the price of their content and consumers can be rewarded for viewing content.

Chainflix – the use case

Chainflix is a distributed P2P content streaming platform, with features similar to popular video-sharing platforms (**VSPs**) such as YouTube and Reddit. A user-centric platform, Chainflix utilises blockchain and AI technology combined with a P2P structure, to create multi-level efficiency in a monetised, ad-based content platform. Whilst the platform's revenue still comes from advertising, the model is disruptive due to its revenue structure and who controls it. The native utility coin (**CFX)** powers the Chainflix ecosystem by rewarding participants in the following ways:[448]

- Consumers can earn or 'mine' CFX coins by viewing content or advertisements through a 'proof-of-view' (**POV**) consensus mechanism that enables advertisement monetisation while protecting against bot manipulation.
- Content creators can set the CFX mining ratio between themselves, viewers and 'enhancers'.
- Enhancers can earn CFX by 'adding value' to a video, for example by providing subtitles or dubbing.
- Users can also earn CFX for hosting platform content.

Distributed storage

Peers across the Chainflix network contribute to a P2P storage pool in a meshed overlay structure, allowing creators to store content in a distributed system for viewers to access and stream. Using this system, Chainflix can provide faster streaming speeds compared to a centralised network whilst avoiding high infrastructure costs.

A distributed storage network, while a commercially favourable alternative to a centralised network, paints a complex legal picture. Who would be liable for any illegal or harmful content hosted or made available through a distributed peer hosted network? How can illegal content be removed and who should be responsible for removing it? How would this liability assessment change if illegal content is distributed across a storage network in fragments?

As the technology evolves, it remains an ongoing question whether software protocol developers should hold fiduciary duties to network users. In *Tulip Trading v Bitcoin Association for BSV and others*,[449] the claimant's private key was stolen from being hacked, leading to billions of dollars' worth of Bitcoin taken from his wallet without his authorisation. The claimant asserted that the Bitcoin software protocol developers owed him a duty to patch the software and restore his stolen Bitcoin[450] on the basis that he had entrusted the care of his tokens to the Bitcoin software protocol developers, who exercised "complete power over the [blockchain] system". The Court initially rejected this argument, finding that the Bitcoin network software developers did not owe a fiduciary duty to the claimant. The judgment highlighted that the distinguishing characteristic of a fiduciary relationship, the obligation of "undivided loyalty" to its beneficiaries, was not present as the claimant's request benefited the claimant alone, and not the rest of the network. The Court, however, did not rule out whether such duties might be owed in other circumstances.[451]

[448] Chainflix White Paper, Version 2.0, October 2020 https://www.chainflix.biz/assets/pdf/whitepaper.pdf

[449] Tulip Trading v Bitcoin Association for BSV and others [2022] EWHC 667 (Ch).

[450] The Dao, an early decentralised autonomous organisation, was hacked in 2016 leading to a loss of over $60m of Ether. The Ethereum blockchain was forked to restore funds stolen from tokenholders as if the hack never occurred.

[451] At the time of writing, the case in on appeal before the Court of Appeal for which judgment is due to be handed down in H1 2023.

P2P advertising

The structure of the content network at Chainflix is built across multiple layers:[452] (1) The first layer is responsible for streaming original content, (2) the second for any on-chain acts that enhance content (such as dubbing or special effects) and (3) the third layer upon which advertisements are displayed. Incentives relating directly to that advertisement are provided according to the relevant smart contract terms once the consumer interacts with the advertisement. The POV consensus mechanism also gives the consumer the option to decide whether they want to see advertisements (and therefore obtain any rewards for doing so).

This advertising model creates greater transparency for consumers compared to centralised models and from this perspective aligns with the Advertising Standards Authority (**ASA**) focus on transparent advertising. A key rule within the UK Code of Non-broadcast Advertising and Direct & Promotional Marketing (**CAP Code**) is that marketing communications must be obviously identifiable as such.[453] In the Chainflix ecosystem, advertisements are technologically distinguished from content within the content network, giving consumers greater awareness and control over what they view.

Influencer marketing, which has in recent years fallen foul of advertising regulations in the UK,[454] raises further complexities for distributed P2P platforms. Whilst influencer marketing can look and feel like content, its actual purpose is to endorse a product or brand. The CAP Code requires influencers to clearly identify advertisements to ensure consumer transparency.[455] UK-established video-sharing platforms must also include terms and conditions regarding any advertising on their platform and provide technical functionality for content creators to declare whether their video contains advertising.[456] Distributed P2P platforms could immutably address these requirements through their embedded smart contracts for advertisements on their platform. There remains however room for human error and creators could incorrectly or fail to categorise their content as containing advertising, meaning distributed P2P platforms would need to retain some form of centralised technical functionality to ensure ongoing compliance.

Limits to decentralisation?

Video-sharing platforms will soon be regulated under the Online Safety Bill and subject to more stringent requirements designed to improve the safety of these platforms for users, particularly children.[457] Platforms that fail to protect their users from harmful content face fines of up to 10% of their revenue or, in the most severe cases, could be blocked.[458] Platforms must implement measures to proactively tackle and erase or remove illegal material shared or stored on their platform.[459] Platforms likely to be accessed by children will also need to maintain sufficient age assurance mechanisms to prevent children from viewing harmful content.[460] Regulators will expect platforms to maintain comprehensive 'Community Guidelines' setting out terms and conditions for use and regulation of their platform.[461] Platforms must prominently communicate these guidelines to consumers and demonstrate enforcement of any non-compliance.[462] Platforms will need to ensure their terms are readily accessible and notified to users before streaming or contributing content.[463]

[452] Chainflix White Paper, Version 2.0, October 2020 https://www.chainflix.biz/assets/pdf/whitepaper.pdf
[453] CAP Code, Rule 2.1
[454] ASA escalates sanctions against influencers who repeatedly break the rules, ASA, 18 January 202
[455] CAP Code, Rule 2.4
[456] Ofcom's video-sharing platform framework: a guide for industry, Ofcom, 25 July 2022 (https://www.ofcom.org.uk/online-safety/information-for-industry/vsp-regulation/guide)
[457] Online Safety Bill: Ofcom's roadmap to regulation, Ofcom, 6 July 2022
[458] Online Safety Bill: Ofcom's roadmap to regulation, p.10, Ofcom, 6 July 2022
[459] Online Safety Bill: factsheet, Online Safety, Gov.uk (https://www.gov.uk/government/publications/online-safety-bill-supporting-documents/online-safety-bill-factsheet#key-points-the-bill-covers)
[460] Ofcom's first year of video-sharing platform regulation, What we found, Ofcom, 20 October 2022 (https://www.ofcom.org.uk/__data/assets/pdf_file/0032/245579/2022-vsp-report.pdf)
[461] Ibid.
[462] Ibid.
[463] Online Safety Bill: factsheet, Online Safety, Gov.uk (https://www.gov.uk/government/publications/online-safety-bill-supporting-documents/online-safety-bill-factsheet#key-points-the-bill-covers).

Chainflix proposes a ‘content supervisor’ within its decentralised ecosystem responsible for assessing the eligibility of content, preventing illegal content from entering the platform and imposing restrictions against harmful content.[464] The content supervisor would be a “public organisation or government institution” whose decisions would be recorded on-chain.[465] While purists will baulk at limits being applied to full network decentralisation, it demonstrates the necessary and increasingly implemented trade-off to enable decentralised platform growth in the context of a regulated real-world ecosystem.

2. Efficiency and governance in two-sided markets

Somewhat ironically, when considering an industry susceptible to disruption by non-centralisation, a good place to start may well be an industry recently disrupted by web 2.0. The traditional taxi market has since been disrupted by several (now global) ride-sharing platforms offering services centred around a mobile app connecting riders with drivers. They were disruptive by solving the problems for ride market supply and demand, specifically (1) riders being unable to find a taxi when needed, where needed and with a suitable payment method and (2) drivers being unable to find riders when and where needed facing ‘dead time’ between rides.

While this may *feel* P2P, it isn’t P2P in the same way as a P2P crypto DEX or a file-sharing protocol.[466] A ride-sharing platform regulates the interface between the network’s value creators and value extractors, and itself extracts value in the form of a percentage of the ride value from drivers and subscription or management fees from riders. Without consensus mechanisms, such networks need control authorities.

A ride-sharing platform’s primary interest therefore is in extracting value typically achieved through:[467] (1) imposing commissions; (2) dictating pricing (using a proprietary, undisclosed algorithm); and (3) excluding riders and drivers from participating in platform governance. Ride-sharing platform are not incentivised to allow supply and demand to set the pricing since its revenue depends on commission. Further, regulators have so far intervened mainly to set caps on fares to respond to perceived market distortions, without addressing how to balance the interests of the ride-sharing platform against consumer or policy goals.

Improving the quality or decision making of the network’s ‘central node’ is not enough when a misaligned incentive structure persists. A decentralised network provides a solution by setting ride fares with a real-time auction model allowing riders to choose a driver based on price, timing, and rating. The platform meanwhile charges a flat fee to drivers for using the platform instead of commission on each fare.

DRIFE – the use case

DRIFE uses blockchain technology to drive efficiency by using smart contracts to transparently and immutably compute ride prices, transfer payments, resolve simple disputes, handle ratings, and carry out other basic operations.[468]

A thematic legal challenge for non-centralised networks is that, particularly in regulated industries such as ride-sharing, regulators expect a person of substance to remain responsible for compliance and holding legal responsibility for the network. Centralised ride-sharing platforms retain such responsibility, including for vetting drivers, upholding consumer standards, and providing legal recourse for grievances. If a network fully relinquishes its authority to network participants (riders and drivers in this case), it can neither functionally nor practically carry this legal burden.

[464] Chainflix White Paper, Version 2.0, October 2020 https://www.chainflix.biz/assets/pdf/whitepaper.pdf.

[465] Ibid.

[466] Early examples of decentralised web infrastructure include file sharing protocol BitTorrent through which a network shares the infrastructure burden of file transfer. A protocol can be fully P2P (as some decentralised crypto exchanges (DEX) are) because it is simply a set of rules by which a network operates internally and there is no need for a single authority.

[467] DRIFE, discussed below, identifies these value extraction points as potential areas for further disruption.

[468] DRIFE White Paper (http://whitepaper.drife.io/).

DRIFE proposes a solution to this by using a ‘franchise NFT’ model. Key platform operations (including compliance with local laws) are assigned to franchise NFT holders each covering a distinct geographic area.[469] NFT holders are chosen using an auction format where potential franchisee operators can bid DRIFE tokens.[470] Franchise NFT holders are granted powers by the network’s central node (hence only a decentralised rather than a distributed network) to choose smart contract parameters and ultimately extract some value of their own from rider subscription fees in exchange for handling local compliance. The platform shares in this value as well as benefiting from its own token allocation.[471]

There isn’t yet a widely accepted model to operate a decentralised network in a regulated environment without some form of centralised structure apportioning legal responsibility to specific legal or natural persons.[472] DRIFE’s model is, in some ways, no different from a traditional franchise model. For example, in a franchised food chain, the central operating burden (including regulatory burden) is obviated and in return franchisees benefit from the brand’s reputation and ubiquity.[473] However, using blockchain technology, local franchisees benefit not only from the global brand but from the efficient operational technology and tokenomics of the wider network.[474]

This use case demonstrates that governance is a key consideration for resolving the unique legal issues arising from network decentralisation. The absence of a central authority is both the precise benefit as well as a critical challenge of decentralised networks, creating an inherent tension between full decentralisation and the need to maintain legal and regulatory accountability.

3. Decentralised governance in telecommunications networks

While decentralised franchise models governed by smart contracts is one model for addressing governance challenges arising for non-centralised networks, decentralised telecommunications networks provide us with further blockchain use cases.

Pollen is a mobile network comprised of multiple P2P individuals hosting small cells placed in a host’s window, roof or garden, with backhaul provided through the host’s broadband connection.[475] The network was established as an alternative to centralised wireless communications offering the alternative of a “privacy focused, anonymous, decentralized, 4G /5G, open-source mobile network enabled by a crypto economy… owned and operated by its users”.

Decentralised networks promise: (1) increased network resilience, by providing alternative network solutions for both consumer use and to bolster vendors’ existing offerings; and (2) a solution to the last mile issue,[476] where centralised infrastructure expansion such as establishing new cell sites in urban environments is often prohibitively expensive or not possible due to the presence of legacy equipment. In a decentralised network, individual hosts instead make micro-infrastructure investments to expand network footprint.

PollenCoin (**PCN**) drives incentive arrangements underpinning the Pollen ecosystem, by providing benefits to participants for network roll-out, maintaining network

[469] This has the additional purported benefit of allowing franchisees to capitalise on local market understanding

[470] This is not dissimilar to a validator in a proof-of-state network consensus mechanism.

[471] The DRIFE foundation proposes to retain 20% of tokens. Tokens are then used throughout the DRIFE ecosystem, with their value potentially being driven by increased service uptake.

[472] Some jurisdictions have taken steps to recognise decentralised autonomous organisations, but the UK is yet to do so. Potential regulatory responses to decentralised networks include minimum code, audit and transparency requirements to ensure the network protocols meet required consumer protection and policy requirements.

[473] Many fast food chains benefit from a franchise model since a local operator can set up an outlet locally, take on responsibility for standards at the outlet while having a household name brand from day one. Two examples of global franchise models are Domino’s and McDonald’s.

[474] For example, payments and refunds can be processed by smart contract, and tokens allocated to franchisees may increase in value as activity on the network (and therefore reliance on its native token) increases.

[475] The small cells available to purchase vary in size, signal strength and cost.

[476] Government Guidance: Telecoms resilience - https://www.gov.uk/guidance/telecoms-resilience

connections and completing validation tests.[477] The Pollen network also incentivises deployment in areas where there is coverage demand by increasing the amount of earnable PCN in target locations.

Decentralised mobile networks do however give rise to challenges similar to those faced in other regulated industries,[478] throwing up novel issues in spectrum access[479], telecoms regulatory compliance[480] and back-haul[481], as the existing regulatory structures naturally assume there to be centralised network ownership or control.

Pollen has devised a potential solution to the central authority issue, showing an alternative to the 'franchise NFT' approach taken by DRIFE. The network has developed what it calls an enhanced DAO (eDAO) model. Once fully implemented, all PCN token-holders will be entitled to vote on strategic decisions of the eDAO, which includes appointing Pollen's governing board and the management team responsible for day-to-day operations. Authority and accountability for the Pollen network will be placed on these bodies, who will be responsible for ensuring legal and regulatory compliance.[482]

A key challenge facing these decentralised mobile networks is incentivising adoption. Helium Mobile[483] is a prime example of this. Helium is a similar concept to Pollen, though it began with providing connectivity to IoT devices via similar small cells installed by the Helium community, who, again, are incentivised by earning Helium's native cryptocurrency (**HNT**).

Helium's pivot to a crypto tokenomics structure initially solved many of its decentralised network incentivisation issues. Early adopters reported high initial earnings and began investing heavily in setting up hotspots to earn HNT. However, some issues soon arose: (1) participants were able to game the system into making it appear that their cells were spread across a location, when they were in fact only in one location, therefore generating a larger amount of tokens due to the clarity of signal. (2) it was reported that a small number of insiders held 70% of the mined tokens during Helium's lucrative start, with only 30% going to the rest of the Helium community, which, while not illegal, effectively centralised control of what was supposed to be a decentralised network.[484] (3) Helium's tokenomics model makes network demand have a direct impact on HNT's value, allowing all those involved in creating the network to earn HNT and share any gains. However, flagging demand,[485] initial difficulties sourcing compatible costly small cells and urban area oversaturation have all combined to adversely affect the take-up required to effectively propagate the network and provide HNT incentives to participants.[486]

[477] Portable mobile devices that carry out the network coverage validation tests when passing by the small cells can also be purchased, through which PCN is also earned. Pollen also plans to implement a level of gamification to the network, via methods such as loot boxes or geographic multiplier boosts that provide additional PCN to those who provide coverage in those areas. (Pollen White Paper: Payments - https://docs.pollenmobile.io/pollen-mobile-docs/white-paper/payments)

[478] See further discussion above regarding non-centralised content or ride-sharing networks.

[479] In the US, the Federal Communication Commission has created the Citizens Broadband Radio Service (CBRS), which enables the use of the frequency bands from 3.55 GHz to 3.70 GHz without purchasing a spectrum licence. Previously only large corporations realistically had access to such bands, as allocation would be decided through an expensive auction process. However, access to these bands is not so widely available in other jurisdictions, including in the UK (FCC - 3.5 GHz Band Overview - https://www.fcc.gov/wireless/bureau-divisions/mobility-division/35-ghz-band/35-ghz-band-overview) .

[480] For example, both Electronic Communications Networks and Electronic Communications Services providers in the UK must comply with Ofcom's General Conditions (GCEs). How these would apply to someone attaching a mobile small cell to their window and using their broadband connection for backhaul to establish a publicly available network is yet to be seen. Compliance with many GCEs as they stand would also be cumbersome, difficult to maintain or just outright impossible on a decentralised basis. (Ofcom's General Conditions - https://www.ofcom.org.uk/phones-telecoms-and-internet/information-for-industry/telecoms-competition-regulation/general-conditions-of-entitlement)

[481] Networks like Pollen rely on back-haul connectivity to each individual users' broadband internet connection. While there is no issue with this in functionality, it remains to be seen if such a network were to become mainstream whether internet providers would be so willing to allow for such uses.

[482] White Paper: Key Pollen Network Actors - https://docs.pollenmobile.io/pollen-mobile-docs/white-paper/key-pollen-network-actors

[483] Helium - https://www.helium.com/

[484] Forbes: Crypto Darling Helium Promised A 'People's Network.' Instead, Its Executives Got Rich - https://www.forbes.com/sites/sarahemerson/2022/09/23/helium-crypto-tokens-peoples-network/?sh=8edaecc73166.

[485] Helium users fret as revenue fails to keep pace with network growth - https://coingeek.com/helium-users-fret-as-revenue-fails-to-keep-pace-with-network-growth/

[486] Unsuccessful deployments in IoT – a furore about failure c/o NB-IoT, Sigfox, Helium (LoRaWAN) - https://enterpriseiotinsights.com/20220929/internet-of-things-4/unsuccessful-iot-deployments-on-nb-iot-sigfox-helium-lorawan-a-furore-about-failure

This is not to say that Pollen will suffer the same fate, and indeed Helium may rally, but as will all new technologies and services they key for a decentralised platform's success is to maintain user appeal.

4. Conclusion: governance is the central challenge

While we are yet to see the full scope of the legal and regulatory challenges that decentralisation will face, the lack of a central governing body is one of the greatest legal hurdles at present to non-centralised networks. This is in no small part due to the current legal and regulatory ecosystem built to assume a centralised model of network ownership and accountability.

Where non-centralised networks do not offer alternative options for legal accountability (such as DRIFE's franchise NFT model or Helium's network-elected governing body) to replace the traditional centralised structures structure in their centralised competitors, they will struggle succeed particularly in regulated sectors.

While the blockchain space remains innovative in the area of network governance and compliance protocols, market participants watch with interest as to whether these proposed alternatives stand up against regulatory scrutiny and potentially judicial treatment.

Annex 1
Specialist Consultees

Annex 2
Smart Legal Contracts

Annex 1:
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

Ciaran McGonagle,
ISDA

Gary Chu,
General Counsel, Fnality International

Professor Michael Mainelli,
Executive Chairman, Z/Yen Group

Dr Michèle Finck,
Max Planck Institution for Innovation and Competition

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

Nick West,
Chief Strategy Officer, Mishcon de Reya LLP

Peter Brown,
Group Manager Officer, ICO

Sarah Green,
Law Commissioner for commercial and common law, Law Commission

Annex 2: Smart Legal Contracts

Rowena Wisniewska Sethi, 4-5 Gray’s Inn Square

This Appendix has been created further to the UK Law Commission’s advice to the government on smart contracts published on 25 November 2021. The focus of this supplementary Appendix is on the interaction between Smart Legal Contracts (**SLCs**) and the existing UK legal framework and common law. The Commission’s overarching conclusion is that the current legal framework is clearly able to support and facilitate the utilisation of SLCs. It also concludes that the flexibility of the common law means that the jurisdiction of England and Wales already provides an ideal platform for business and innovation through the medium of SLCs, without the need for any additional statutory law reform. Equally, the Law Commission also identifies particular issues that parties may wish to consider and address in negotiating and finalising smart legal contracts so as to mitigate, as far as possible, against the risk of disputes arising as a result of uncertainties arising from lack of clarity in the contract terms. It is hoped that as Smart Legal Contracts become more mainstream, established practices and models will emerge and so will become a routine part of the process of SLC negotiation and drafting.

What are the key functions of smart contracts more generally?

- They can perform transactions on decentralised exchanges

- They can facilitate games on a distributed ledger and run online gambling programmes

- They can facilitate the exchange of collectibles on a distributed ledger

What is a Smart Legal Contract?

An SLC is a legally binding contract in which some or all of the contractual obligations are defined in and/or automatically performed by code in a computer programme. This means that the code is designed to automatically execute certain actions in the event that certain pre-agreed and pre-defined conditions are met (this is known as automaticity). The other key feature is that an SLC is legally enforceable. The code may be designed to give effect to legal provisions or have legal consequences, however, it may also be the case that the code is utilised to facilitate the internal functioning of an SLC, or the interaction between two contracts, for example.

There are three key forms of SLCs:

- Natural language contract with automatic performance by code: This is the most commonly used form of SLC at present and generally is unlikely to raise any novel legal issues;

- Hybrid contract: This is a contract in which some contractual obligations are defined in natural language and others are defined in the code of a computer programme. Accordingly, some, or all, of the contractual obligations are performed automatically by the code. There is a spectrum in respect of the range of options, for example the terms of a hybrid contract could be primarily written in code with a few natural language terms or they could be primarily written in natural language and include just one or two terms written in code; and

- A contract recorded wholly in code: all the contractual terms are defined in, and performed automatically by, the code of a computer programme.

Digitising legal contracts and/or transactions may use any combination of SLCs, Smart Contract Code (SCC) and the three models described above. However, there are also certain features of the negotiations of SLCs which are unique, for example it may be the case that the parties do not ever meet each other due to the pseudonymous nature of DLT. This in itself may cause challenges if there is a dispute over jurisdiction, for example, or one of the parties seeks to obtain a remedy against the other.

The Interaction between SLCs and Distributed Ledger Technology (DLT)

As outlined already, DLT exists in decentralised locations and unlike traditional centralised databases, is not maintained or controlled by a central administrator or entity. Network participants do not have to reconcile their local databases with a ledger maintained by a central administrator, rather participants approve and eventually synchronise additions to the ledger through an agreed "consensus mechanism". Generally, this mechanism requires some (or all) of the participants to determine the validity of a proposed data entry and is usually designed so that once data is added to the ledger, it is immutable and cannot be amended.

DLT also has additional functions in relation to the storage of smart contracts (and the digitised portions of hybrid smart contracts). However, smart contracts are not defined as SLCs solely by reference to DLT: they can be performed automatically by computer programmes without the use of DLT. Nevertheless, DLT systems have specific benefits and distinctive features which lend themselves well to storing smart contracts and therefore also SLCs. For example, as DLT has become increasingly sophisticated, computer programmes can be recorded on a distributed ledger and performed by the computers on the network. Therefore, an SLC may be drafted primarily or solely in code and deployed on a distributed ledger system so as to bring about automatic performance as conditions of the contract are fulfilled. However, it may be the case that automation of an SLC leads to novel legal issues arising. It is the intersection between these issues and the UK legal framework and common law that the UK Law Commission has explored in its 25 November 2021 advice paper.

The interaction between smart contracts and the common law/current UK legal framework

In compiling its advice, the UK Law Commission considered the usual key steps in the formation of a contract and then considered how the sometimes novel features of SLCs may give rise to complexities and issues and how the current framework may aid practitioners in identifying solutions and mitigating against risks. For example, if issues arise regarding the certainty and completeness of an SLC, conflicts between the code and natural language could potentially be resolved through the process of interpretation. Therefore, in examining the question of whether the parties intended to create legal relations, the Court may look at the nature and purpose of the platform on which the code is deployed and the nature of the transactions executed by the code.

Formation

This could be particularly complicated if an agreement is reached on a DLT system and the UK Law Commission has advised that parties who do intend such transactions to create legal relations would be well advised to make this clear in natural language beforehand to mitigate against the risk of disputes arising further down the line. The other key question the Commission has posed on the formation of such contracts is whether they can satisfy the "in writing requirement" under the Interpretation Act 1978[487] given that the definition of "writing" is an inclusive one and could be interpreted to accommodate new technologies providing they involve "representing or reproducing words in a visible form". In the view of the Law Commission source code can constitute "writing" for the purposes of the Act, however, if the terms of such a contract are said to reside in machine code or a lower level of code than source code, then it will be more difficult to argue that the contract is "in writing".

[487] Pursuant to Schedule 1 to the Interpretation Act 1978, "Writing" includes typing, printing, lithography, photography and other modes of representing or reproducing words in a visible form, and expressions referring to writing are construed accordingly.

Signature

In more novel scenarios where an SLC consists entirely of code, the parties could sign the contract electronically by means of a digital signature to authenticate a piece of code deployed on a DLT system. This is on the basis that a digital signature is generally capable of satisfying the statutory requirement. The position regarding deeds is more complex and the Law Commission is of the view that the current law does not support the creation of deeds which are wholly or partly defined by code, given the legal requirement that a deed must be signed in the presence of a witness who then formally attests the signature. In the view of the Commission there therefore remains some uncertainty as to whether the technology pertaining to Smart Legal contracts can meet the various formalities that apply to deeds.

Interpretation

Although the principles of interpretation of contracts have evolved in response to the Courts seeking to interpret natural language terms, coded terms can still be subject to contractual interpretation in the usual way. The Commission has proposed that one approach could be to examine how the coded term would be understood by a functioning computer. The other test proposed is to ask what a person with knowledge and understanding of code, “the reasonable coder”, would understand the coded term to mean. The benefit of applying this test is that it potentially provides an
insight into how the parties intended the code to function, irrespective of how the computer ultimately performs.

Remedies

Given the immutable nature of DLT, Courts may face practical difficulties in rectifying coded terms. However, rectification is likely to be more relevant where the contract is ongoing, or requires continuous performance, and where the code may have partially, as opposed to fully, performed. It may be more difficult where the code has fully executed and cannot be unwound. The Commission has suggested that an expert coder could be instructed to translate the bargain reached by the parties in code.

With regard to vitiating factors that may render a contract void or voidable, such as mistake, misrepresentation, duress and undue influence, the Law Commission is of the view that the existing law suffices. However, the key area for reform identified by the Commission is unilateral mistake. Whilst it recognises that a fundamental change to the existing principles in the context of SLCs concluded by computer programmes is not needed, the test as to whether a non-mistaken party has knowledge of the mistaken party’s mistake requires adaption. Such a test would need to encompass questions as to whose knowledge of the mistake is relevant, the time frame for assessing that person’s knowledge, and the type of knowledge that is required.

Breach of contract

A party may be liable for breach of contract if the code fails to perform obligations under a contract correctly. The Law Commission considers that the existing principles for awarding damages for breach of contract should not create difficulties where the terms of a natural language contract are performed by computer code and also why such a contract could not be terminated for breach in the usual way. There are, however, practical considerations at play, given that the party who elects to terminate may not in practice have such a power if for example the code is recorded on an immutable distributed ledger. With regard to the doctrine of frustration, parties are advised to draft detailed provisions that mitigate as far as possible against the risk of external events beyond their control from affecting or interfering with performance of the code.

Consumer considerations

The Consumer Rights Act 2015 (CRA 2015) requires that a trader must ensure that the written terms of a consumer contract are transparent. With the advent of more complicated SLCs in a business-to-customer context, it may be challenging for businesses to meet this statutory requirement. It will therefore be critical to provide unequivocal and informative pre-contractual literature to consumers up front, which explains clearly the various terms and how these operate in practice. Clarity and simplicity are therefore key.

Jurisdiction

A further area of challenge may be in the area of jurisdiction given the pseudonymous nature of some DLT systems which means that parties may enter into SLCs without knowing the real identity of counterparties. A challenge may therefore arise in determining whether a court's jurisdiction can be based on the defendant's presence within England and Wales, or whether a claimant must obtain the Court's permission to serve outside the jurisdiction. Clarity at the outset is again critical and the Law Commission advises that parties should consider designating the law applicable to their contractual relationship and therefore the terms of their contract.

Conclusion

Overall, dealing directly with anticipated issues in contractual terms before they arise should go mitigate to some extent the risk of uncertainties regarding the legal treatment of an SLC and potentially reduce the likelihood of disputes arising. Further, Appendix 1 to the Law Commission's report provides a helpful list of 10 key issues parties may wish to provide for in designing and agreeing their SLC.

Ultimately, the resounding message from the Commission is that the existing legal framework and the common law in the UK provide a suitable environment to facilitate SLC formation and execution. However, the key lies in the planning stages, including making clear the role of the code in the contract, the relationship between natural language and coded terms and considering whether the code can be designed to terminate performance if required. It therefore seems that the greater the human engagement at the outset, the more smoothly the contract is likely to function once automaticity is triggered.