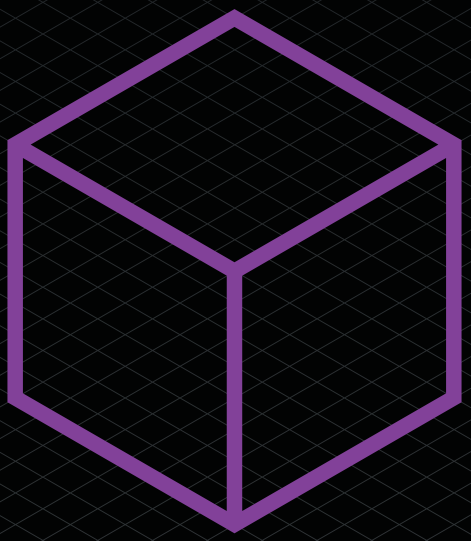
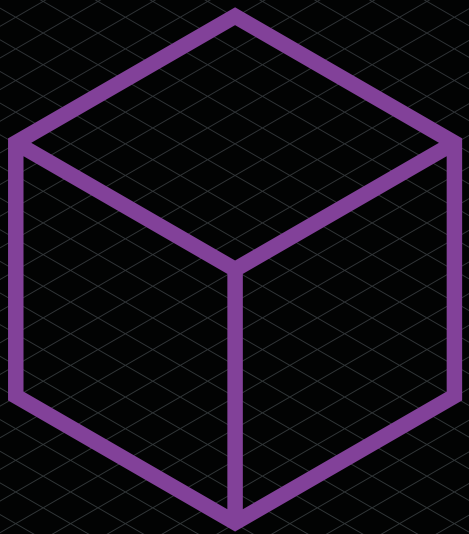
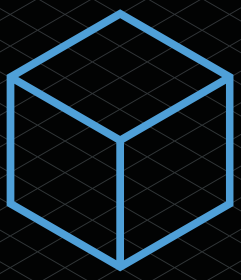
Part 2: Impacts on the Wider Landscape

Section 12 Dispute Resolution







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.clifford-chance.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.