Feature

KEY POINTS

- The Law Commission aims to publish a consultation paper in the second half of 2023 on the issue of conflict of laws for cryptocurrency disputes.
- One solution for the *situs* of cryptoassets is a test based on residence of the owner, which was applied in *LMN v Bitflyer*.
- Allocating jurisdiction based on the existing gateways is not without analytical difficulty, and just as with the new gateway 25 for disclosure orders, a gateway specifically tailored for cryptocurrency disputes may be among the Law Commission's possible solutions.
- The existing rules on applicable law could be adapted or clarified with cryptocurrency disputes in mind, or the Law Commission could create bespoke rules.

Author Sophia Hurst

Decrypting conflict of laws

In this article Sophia Hurst considers the various options open to the Law Commission on the issue of conflict of laws for cryptocurrency disputes in advance of its consultation paper to be published in the second half of 2023.

INTRODUCTION

On 18 October 2022 the Law Commission of England and Wales launched a review, commissioned by the government, titled *Digital assets: which law, which court?* It aims to consider how private international law rules can and should apply to international disputes relating to emerging technology, including crypto-assets and distributed ledger technology (DLT). This follows its previous Smart Contracts report, published in November 2021, which concluded that the ever-flexible common law was clearly able to facilitate and support the use of smart legal contracts, without the need for statutory reform. However, it identified the rules on jurisdiction as a key area for future work. Since that project, the issue of conflict of laws for cryptocurrency disputes has already proved ripe for controversy both in and out of the courts and is rapidly gaining the attention of global law-reformers and policy makers. The Law Commission's scope is uncertain; its project is broadly aimed at "ensuring the rules of applicable law and jurisdiction can accommodate an increasingly digitised world". It aims to publish a consultation paper in the second half of 2023. This article considers some of the key issues the project must tackle, and the solutions offered elsewhere.

THE NATURE OF THE PROBLEM

Rules of jurisdiction and applicable law generally look to territorial connecting factors. Broadly, these connecting factors locate the acts, actors and/or assets material to the dispute within jurisdictions and aim to identify the jurisdiction and governing law with which the claim has a real or substantial connection. However, this approach, and the traditional connecting factors upon which it is based, is premised on being able to locate assets, acts and actors within the territory of a particular legal system. There are conceptual and practical difficulties when seeking to apply these rules to assets which exist only or primarily in a virtual environment on DLT, which is deliberately decentralised: cryptoassets sponsored on DLT networks are transacted instantaneously over a distributed ledger that is, often, openly accessible anywhere across the world. Digital assets held on DLT are by design unconnected from any particular jurisdiction or system of law. Further, the pseudonymity within cryptoasset systems makes it difficult to locate the actors responsible for DLT transactions.[1] Put simply, DLT is by definition "distributed", and so any conflict of laws rules anchored in geography are intrinsically problematic.

However, not all situations involving cryptoassets and DLT are homogenous and these difficulties can be overstated. Consider the difference between "on-platform" or "on-chain" assets versus "off-platform" or "tethered" assets. An on-platform cryptoasset is one which exists purely in the ledger. However, on some DLT networks, the on-platform cryptoasset is a digital representation of a real-world asset that exists outside the leger – so-called "tokenisation". The real-world asset can likely be identified within a legal system. Further, some transactions involving cryptoassets will remain purely internal to the DLT (eg a straightforward sale or transfer), whereas others (eg cases of fraudulent interception) will involve actors external to the DLT. The private international law solutions applicable need not be the same for both.

The Law Commission's project presupposes that it is possible to create appropriate private international law rules at a national level. Others have doubted this approach. The Financial Markets Law Committee, for example, has advocated that an international conflict of laws framework for financial transactions and systems using DLT needs to be developed as a matter of priority.[2] One candidate may be UNCITRAL's work on Electronic Commerce.

Nevertheless, and despite the obvious attraction of uniform international rules, recent years have seen an "arms race" to enact national systems of rules attractive to exchanges and crypto-investors. What follows is an analysis of how English law has so far adapted its existing rules and the problems encountered, with which the Law Commission must grapple.

SITUS OF CRYPTOASSETS

There is an emerging consensus in English law that cryptoassets are classified as a type of property, at least for the purposes of private international law and interim remedies.[3]

As such, the traditional approach to governing law for questions regarding rights or entitlement in moveable property is that it should be governed by the law of the place in which the property is situated (*lex situs*). This has historically been justified because, per *Dicey Morris & Collins on Conflict of Laws* 16th ed at 23-025 "first, that the *situs* is an objective and easily ascertainable connecting factor to which third parties might reasonably look to ascertain questions of title and, secondly, that the country of the *situs* has control over the property and a judgment in conflict with the *lex situs* will often be ineffective". It is recognised by *Dicey Morris & Collins* that these justifications less obviously apply in the case of choses in action, and still less for cryptoassets.

When the English courts were first faced with determining the *situs* of choses in action, they tended to look to notions of control; holding that intangibles are situated where they can be effectively dealt with, are properly recoverable or can be enforced:

see eg *New York Life Insurance Co v Public Trustee* [1924] 2 Ch. 101, 109. The notion that an intangible asset is situated where it is effectively controlled has persisted, but even this notion of "control" is difficult to apply in the cryptocurrency context.

One solution is to look to the location of the owner. In *Ion Science* Butcher J relied on the analysis of Professor Andrew Dickinson in *Cryptocurrencies in Public and Private Law* at para 5.108 in holding that the *lex situs* for a cryptoasset was "the place where the person or company who owns it is *domiciled*". HHJ Pelling QC cited *Ion Science* with approval in *Fetch.ai* at [14] and so apparently endorsed the "domicile" test. However, as noted by Falk J in *Tulip Trading Ltd v Bitcoin Association for BSV* [2022] EWHC 667 (Ch) (*Tulip Trading*) the analysis by Professor Dickinson was not based on domicile but "the country where the participant resides or carries on business at the relevant time". There is a distinction between the concepts of domicile and residence in private international law which may produce different results. Residence of an individual is primarily a factual question of where a person resides, whereas domicile is a legal concept which may not coincide with residence.[4] A company is domiciled in its place of incorporation (*Dicey Morris & Collins*, r 173(1) but resident where its central management and control is located, that being where its "real business" is carried on (r 173(2)). Whereas in *Ion Science* the two coincided (and Butcher J appeared to use the concepts interchangeably later in his judgment at [21]), *Tulip Trading* illustrates how the result may differ depending on whether residence or domicile of the owner is used as the test. There, the company TTL was incorporated in the Seychelles but carried on business in England and Wales. Falk J did not conclusively determine the issue but indicated a preference for a residence test (at [148]), which presented difficulties on the facts in that case because TTL had no active business. Falk J ultimately fell back on the residence of TTL's CEO in the jurisdiction as the person with control to deal with the company's assets, even though he had not in fact dealt with the cryptoassets. That conclusion is open to doubt, although it was not challenged on appeal (see [2023] 4 WLR 16 at [7]).

A residence test was applied in *LMN v Bitflyer* [2022] EWHC 2954 (Comm), on an application by the claimant cryptocurrency exchange for *Bankers Trust* and *Norwich Pharmacal* information orders to locate cryptocurrency transferred after a hack and identify the hackers. Butcher J held that the relevant cryptocurrencies were at the time of the hack located in England and Wales on the basis that the claimant company was "resident and carries on its relevant business here", notwithstanding the fact that its servers were located in Romania.

Outside the courts, HMRC, in its Cryptoassets Manual (30 March 2021, last updated 3 November 2022) treats an exchange token as sited by reference to where the beneficial owner is tax resident. That is based not on any control analysis but because it provides "a clear, logical, predictable and objective rule which can be easily applied". For this purpose, HMRC consider an individual to be UK resident if they are tax resident under the statutory residence test.

A different view connected to the idea of control is advanced by the Society of Trust and Estates Practitioners (STEP). In STEP's Guidance Note it argues that, in determining where control is exercised for the purpose of establishing *situs*, the private key is paramount as the cryptocurrency can only be dealt with using that key. Therefore, STEP argues, "its location should be linked to the location of the private key or the person who has control of the private key (who may or may not be the beneficial owner)". This could be because, eg the private key is located with a custodian. The UK Jurisdiction Taskforce's Legal Statement also suggests that the location of control of a digital asset is where its private key is stored (see [99]).

Other candidates for the *situs* of a cryptoasset include the location of the server where an individual or company holds its cryptoassets (as was considered but rejected in *LMN v Bitflyer*, the location of a custodial wallet, or something else altogether.

As such, even if the *situs* of cryptoassets is to be used as the touchstone for establishing jurisdiction and governing law, analyses differ as to exactly how *situs* is to be determined. It is tempting to side with the courts, who have certainly built-up momentum on this topic in the disputes involving fraudulent interception of cryptoassets. But these are first-instance interlocutory decisions establishing only a good arguable case to that effect, and very often without hearing the contrary argument. It is open to the Law Commission to take a different view.

JURISDICTION

Post-Brexit in England and Wales, unless the dispute falls within the 2005 Hague Choice of Court Convention (which is not considered further here), jurisdiction depends on serving the defendant with the proceedings, either within the jurisdiction or, with the court's permission, outside the jurisdiction. To obtain permission, it must be shown that there is a good arguable case that each claim falls within one of the jurisdictional "gateways" at para 3.1 of Practice Direction 6B (PD6B 3.1), that there is a serious issue to be tried on the merits of the claim, and that England and Wales is clearly or distinctly the appropriate forum (see eg Lord Collins of Mapesbury in *AK Investment CJSC v Kyrgyz Mobile Tel Ltd* [2012] 1 W.L.R. 1804 at [81]).

The most common scenario to come before the English courts in recent years has been where cryptoassets have been fraudulently misappropriated. Here, the event giving rise to damage takes place in the real world, not on the DLT, but the pseudonymity of DLT systems may make it extremely difficult to identify a perpetrator, meaning injunctions are sought against "persons unknown". Victims have sought to obtain information from cryptocurrency exchanges located abroad as to the identity of wallet-holders, and onward transfers of the misappropriated assets. Such *Bankers Trust* or *Norwich Pharmacal* relief encountered difficulties with establishing a gateway to serve out of the jurisdiction given the English courts' reluctance to make information or disclosure orders against parties outside of the jurisdiction.

On 1 October 2022, a new gateway PD6B 3.1(25) came into force which was specifically formulated with cryptocurrency disputes in mind. It allows claimants to serve out a claim or application for disclosure against a non-party in order to obtain information regarding the true identity of a defendant or potential defendant, and/or what has become of the claimant's property (25(a)), *and* for the purposes of proceedings which have been or are intended to be commenced in England and Wales (25(b)). The gateway has already

Feature

been successfully relied on in *LMN v Bitflyer*.

However, as 25(b) makes clear, the gateway will only apply if jurisdiction is at least arguably established for the underlying substantive dispute – either because the defendant is in the jurisdiction, or by relying on another gateway. In *LMN v Bitflyer*, the claimant's evidence was that, should the information sought reveal potential defendants outside the jurisdiction, the claimant intended to apply to serve the proceedings out of the jurisdiction (see [27]).

One of the potential gateways identified was PD6B para 3.1(11), which applies where the subject matter of the claim relates wholly or principally to property within the jurisdiction. Thus, the test for determining the *situs* of cryptoassets becomes important to found jurisdiction in England and Wales. It would be open to the Law Commission to suggest a modification to gateway 11 which makes clear how it applies in the case of cryptoassets.

Outside of this scenario, the other potentially applicable gateways will vary depending on the nature of the dispute.

In the case of a purely internal or transactional dispute, the contractual gateways in PD6B 3.1(6) allocate jurisdiction where the contract was made in the jurisdiction (6(a)), by or through an agent residing in the jurisdiction, or is governed by the law of England and Wales (6(c)). Locating the place where a smart contract is made on DLT is a similarly difficult task and unlikely to prove a fruitful gateway absent a default presumption for smart contracts. The contract may, by choice, be governed by English law – this is considered further below.

The other gateway identified in *LMN v Bitflyer* – a fraudulent misappropriation case – was PD6B 3.1(15). Gateway 15 applies where a claim is made against a defendant who is a constructive trustee, or as trustee of a resulting trust, in three circumstances: (i) (15(a)) where the claim arises out of acts committed or events occurring within the jurisdiction; (ii) (15(b)) where the claim relates to assets within the jurisdiction; and, since 1 October 2022; (iii) (15(c)) where the claim is governed by the law of England and Wales. Butcher J considered, at [27], that there was a good arguable case that whoever held the cryptocurrency or traceable substitutes did so as a constructive trustee for the claimant because equity imposed a constructive trust on the fraudulent recipient of fraudulently obtained property.[5] A similar conclusion was reached by Nigel Cooper QC in *Jones v Persons Unknown* [2022] EWHC 2543 (Comm), who consequently ordered a cryptocurrency exchange to deliver up the contents of a wallet holding £1.54m in Bitcoin which the claimant had been fraudulently induced to transfer to a fake crypto-investment platform ([21]).

There is no discussion in either judgment about which limb of gateway 15 applied, but since neither claimant would have been able to establish that fraudulent acts by persons unknown were committed within the jurisdiction to satisfy (15(a)), it can only be (15(b)) or (15(c)). (15(b)), again, leads back to the *situs* of cryptoassets and the caselaw discussed above, but there is an additional problem: the courts have held elsewhere that this gateway does not apply if there are no assets within the jurisdiction *at the time of the application for permission to serve out*, even if the claim relates to assets that were previously in the jurisdiction: *Denisov v Delvecchio* [2022] EWHC 377 (Comm). That precludes reliance on (15(b)) in any misappropriation case and so gateway 15 can only apply where English law governs the claim – (15(c)) – notwithstanding that *Jones* was decided before this limb was introduced.

A perhaps more obvious candidate for misappropriation claims is the "tort" gateway PD6B 3.1(9). Jurisdiction will be founded for claims in tort where damage was, or will be, sustained in the jurisdiction (9(a)), damage has been or will be sustained from an act committed or likely to be committed in the jurisdiction (9(b)), or the claim is governed by English law (9(c)).

The same impossibility persists with locating acts of anonymous bad actors within the jurisdiction. However, given the wide interpretation given to "damage sustained … in the jurisdiction" in *FS Cairo (Nile Plaza) LLC v Lady Brownlie* [2022] AC 995, victims of cryptofraud resident in the jurisdiction may well be able to rely on (9(b)). In *Brownlie*, the claimant had sued in England following the death and serious injury sustained in a car accident during her family's holiday in Egypt. The car journey had been arranged by the defendant Egyptian company. Lady Brownlie argued that although the accident itself (the "harmful event") had occurred in Egypt, the damage for her personal injury, in her capacity as her husband's executrix and damage for her bereavement and loss of dependency were all sustained in England following her return from Egypt. Lord Lloyd-Jones found that damage was indeed sustained in England on the basis that this was where the "actionable harm, direct or indirect, caused by the wrongful act alleged" had been suffered. He rejected an argument that a distinction should be drawn between direct or immediate damage and later or indirect damages.

Following *Brownlie*, the victims of cryptofraud are more likely to be able to argue that "damage was sustained" where they are habitually resident for the purpose of PD6B para 3.1(9)(a) and establish home jurisdiction that way. Lord Lloyd-Jones stressed the requirement under CPR 6.37(3) that claimants must still demonstrate that England and Wales is the proper place (or *forum conveniens*) to bring a claim. This allows the court to refuse jurisdiction if there is another available forum that is clearly and distinctly more appropriate.

PD6B 3.1 (6(c)), (9(c)) and (15(c)) all allocate jurisdiction if the claim is one governed by English law, and so the existing rules as applied to cryptoassets will be considered below. It is nevertheless apparent that allocating jurisdiction based on the existing gateways is not without analytical difficulty and, just as with the new gateway 25 for disclosure orders, a gateway specifically tailored for cryptocurrency disputes may be among the Law Commission's possible solutions. There is also scope for innovation in the method of service, as shown in the recent decision of Lavender J in *Osbourne v Persons* [2023] EWHC 39 (KB) permitting service of proceedings solely by NFT.

GOVERNING LAW

As indicated above, the traditional approach is to look to the *lex situs* to govern questions relating to rights and entitlement to moveable property.

This remains justified in some scenarios. Where the cryptoasset is tethered to an underlying real world asset, the law governing issues of entitlement should most obviously be the *lex situs* of the underlying asset. So, too, where DLT is not dispositive of property rights but merely used as a record keeping device, the

Biog box
Sophia Hurst is a barrister practising from Essex Court Chambers, 24 Lincoln's Inn Fields, London.
Email: shurst@essexcourt.net

traditional *lex situs* approach for the underlying assets should continue to apply (for support of this view, see *Dicey Morris & Collins* at 23-050).

However, where the governing law of a dispute as to the rights and entitlements to an on-chain cryptoasset is concerned, a test for *situs* which looks to the domicile or residence of the owner of the cryptoasset risks becoming entirely circular. In other words, the governing law test should not look to the location of the owner, where ownership is the very point in issue.

The EU legislators took a different approach. Avoiding the difficulty of applying the *lex situs*, the Rome Convention and subsequent Regulation 593/2008 (Rome I), provide that *inter partes* proprietary questions arising from transactions in choses in action are governed by the governing law of the contract giving rise to the claim. This solution too has its limits. It does not apply to proprietary claims where third parties are involved, and it assumes that the governing law of the contract is itself ascertainable. Article 3(1) Rome I recognises that parties may choose the law governing their contractual relations. The UK Taskforces's model Digital Dispute Resolution Rules, aimed for adoption by parties, exchanges, and others, include a default choice of English Law. In the case of permissioned DLT systems, it may be the case that general choices of governing law are or can be written into the terms of permission.

Regulation 864/2007 (Rome II) continues to apply in English law to determine the governing law for non-contractual obligations. In *Fetch.ai*, persons unknown had gained access to the first applicant's trading account holding various cryptocurrencies, traded the assets by adopting undervalues and moved them into third party accounts. HHJ Pelling KC held that the claim for breach of confidence came within the scope of the delict rule under Art 4.1: the law of the country in which the damage occurs irrespective of the country in which the event giving rise to the damage occurred and irrespective of the country or countries in which the indirect consequences of that event occur. Where the underlying claim is in the nature of an equitable proprietary claim, the governing law is difficult to ascertain even in non-cryptocurrency claims (the usual candidates being under Art 10 unjust enrichment or Art 11 negotiorum gestio). These rules could continue to apply for "external" DLT disputes, especially those involving fraud or misappropriation, but guidance as to their applicability in a cryptocurrency context would be welcome.

Another potential solution is presented by examining the governing law principles developed for intermediated securities. The so-called PRIMA principle – which pinpoints the *lex situs* of intermediated securities by looking to the "place of the relevant intermediary account" – was first developed during negotiations for the Hague Securities Convention and is now incorporated into EU law in Directive 2002/47/EC on financial collateral arrangements (FCD) and Directive 98/26/EC on settlement finality in payment and securities settlement systems (SFD).

Article 9(2) of the SFD governs securities "legally recorded on a register, account or centralised deposit system" and submits them to the law of the member state where such register, account or system is "located". This raises questions as to whether a distributed ledger constitutes a relevant "register", whether cryptoassets in the blockchain are "legally recorded" and, perhaps most difficult, where the distributed ledger is "located". Article 9 FCD is similarly problematic. It provides that financial collateral arrangements are governed by the law of the country "in which the relevant account is maintained". DLT does not operate with "accounts" in the traditional sense of the word, though here there may be a closer analogy with cryptocurrencies held in a wallet on a cryptocurrency exchange. Exchanges have identifiable places of incorporation and this could offer a connecting factor, though it is hard to see how governing law should depend on whether cryptoassets are stored in a custodial wallet on an exchange.

The European Commission is consulting on the SFD and FCD and their application to DLT. The issue is pressing, as some member states have pressed ahead with their own reforms. France now allows OTC traded securities to be issued on blockchain networks provided the securities are issued in the French territory and governed by French law: see Art L211-3 *Code monétaire et financier*. Germany has drafted a Bill to allow the issuance of bonds on the blockchain, the governing law being that of the country in which the administrator of the register is supervised. Liechtenstein (an EEA member) has enacted an Act on Token and TT (Trustworthy Technology) Services Providers which applies (under Art 3(2)) where the TT provider is headquartered in Liechtenstein, or where the parties expressly chose its provisions. These all have the potential to clash with the SFD and FCD if it is extended to blockchain networks.

CONCLUSION

There are no shortage of options open to the Law Commission – it could grapple with the above difficulties in adapting the existing English conflict of laws rules to cryptoasset disputes, or could innovate in a new direction. Its consultation paper, to be published in the second half of 2023, will certainly be one to watch. ■

1 See Andrew Dickinson, 'Cryptocurrencies and the Conflict of Laws' in Fox and Green *Cryptocurrencies in Public and Private Law* (OUP 2019) at para 5.08.
2 http://fmlc.org/wp-content/uploads/2018/05/dlt_paper.pdf
3 See paras 71-84 of the UK Jurisdiction Task Force's Legal Statement, applied in *AA v Persons Unknown* [2019] EWHC 3556 (Comm); [2020] 4 WLR 35 at [58]-[61] (*AA*); *Ion Science Limited & Anor v Persons Unknown* (unreported), 21 December 2020 (*Ion Science*) at [11]; *Fetch.AI Limited v Persons Unknown* [2021] EWHC 2254 (Comm) (*Fetch.AI*) at [9].
4 See further *Dicey Morris and Collins*, Chapter 6.
5 See too *Fetch.ai Ltd v Persons Unknown* [2021] EWHC 2254 (Comm); *D'Aloia v Persons Unknown* [2022] EWHC 1723 (Ch).

Further Reading:

- Service, lies and NFTs: litigation and the blockchain (2022) 10 JIBFL 696.
- High Court grants first *Bankers Trust* Order against overseas cryptocurrency exchanges using new "gateway" for service out of the jurisdiction (2023) 2 JIBFL 121.
- LexisPSL: Banking & Finance: Practice Note: Cryptoassets for dispute resolution lawyers – key and illustrative decisions.