Decrypting the *Situs*

Conflicts of Laws Challenges in Cryptoasset Litigation

Chloë Bell and Joshua Cainer

20 October 2020

1 – Introduction

Litigation involving cryptoassets will frequently have a foreign element to it. Conflicts of laws rules will therefore be highly relevant to resolving such disputes.

Traditionally, rules of jurisdiction and applicable law have operated on the basis of territorial connecting factors which ultimately depend on the ability to locate acts and actors within the territory of a particular legal system and establishing the existence of a real and substantial connection of those acts and/or actors to that legal system.[1] Where a thing exists only in a virtual environment and can be commuted instantaneously across the globe, this presents a challenge to the territorial paradigm. Pseudonymity within cryptoasset systems also makes it difficult to locate not only the rights and acts in question but also the actors.[2]

However, these difficulties should not be over-stated. The current authors consider that many conflicts of laws problems can be resolved by a pragmatic application of the traditional rules and by focusing on how cryptoassets are controlled in the real world. This will no doubt be helped along by the developing case-law on the precise classification of these assets, which has picked up pace in the common law world in the last year.

It has not been possible to discuss all conflicts of laws issues which may arise in cryptoasset litigation.[3] The article below focuses on, first, outlining what features of cryptoassets and distributed ledger technology ('DLT'), the technology on which cryptoassets depend for their existence, give rise to difficulties in private international law. Secondly, it gives an overview of the key methodological questions which need to be

[1] Adrian Briggs, *Private International Law in the English Courts* (OUP 2014) at para 1.10.
[2] Andrew Dickinson, 'Cryptocurrencies and the Conflict of Laws' in David Fox and Sarah Green (eds), *Cryptocurrencies in Public and Private Law* (OUP 2019) at para 5.08.
[3] We hope that this article will be followed up by others which explore the full range of conflicts of laws challenges which may arise in this area.

resolved at the outset of an analysis of private international law issues. The third and fourth sections of the article contain the main focus of our analysis, in which we explore existing jurisdiction and applicable law regimes and how they might be applied and/or adapted to apply to so-called 'external disputes', namely disputes which involve engagement with the real world and do not solely concern matters internal to the DLT network . In our view a wholesale re-writing of our conflict of laws regime is not necessary but a pragmatic focus on the "real world" effects of these assets will be required.

A brief note on Brexit: the Law Applicable to Contractual Obligations and Non-Contractual Obligations (Amendment etc.) (EU Exit) Regulations 2019 (SI 2019/834) make clear that both of the Rome Regulations on applicable law[4] will be retained as part of the law of the United Kingdom after the end of the Implementation Period on 31 December 2020 . The discussion below will therefore be the same regardless of Brexit and whether a long-term agreement between the UK and the EU is reached. As regards jurisdiction, this article does not delve into the myriad scenarios which may arise if the Brussels I (recast) Regulation[5] is not mirrored in a deal between the UK and the EU. If a deal is reached between the UK and the EU, the analysis below will likely remain identical. If a deal is not reached, the UK's primary plan is to accede to the Lugano Convention 2007[6] (which in large part reflects the Brussels I Regulation before it was recast), however we do not speculate any further than this. The authors approach jurisdiction issues in the present article on the basis of the law as it stands today, which will at the very least provide a helpful analytical starting point whatever the future legal position turns out to be.

2 – Key difficulties of distributed ledger technology for private international law

From a private international law perspective, there are two main problems created by the distinctive characteristics of DLT.

[4] Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I) and Regulation (EC) No 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations (Rome II).
[5] Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (Brussels I (recast)).
[6] Convention on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (Lugano Convention). The UK applied to join the Convention on 8 April 2020 and is now waiting for the other Contracting Parties to decide whether to agree to the UK's accession: <https://www.gov.uk/government/publications/cross-border-civil-and-commercial-legal-cases-guidance-for-legal-professionals-from-1-january-2021/cross-border-civil-and-commercial-legal-cases-guidance-for-legal-professionals-from-1-january-2021> (last accessed 20 October 2020).

The first problem, which is both conceptual and practical, is the a-national character of DLT and the cryptoassets sponsored on DLT networks.[7] The intangibility of the cryptoasset, combined with the decentralised, distributed nature of the ledger on which they are recorded, and the fact that DLT networks are often openly accessible by members of the public, means that cryptoassets, and the ledgers on which they are recorded, are located everywhere and yet nowhere.[8] This is a challenge both for establishing which state should have jurisdiction over disputes concerning cryptoassets, as well as which state's domestic law is the applicable law that governs such disputes. As we shall see, English law rules of private international law are primarily centred around identifying the key issues in a dispute and establishing which state's jurisdiction and domestic law has the closest connection with those issues raised by the dispute.[9] The application of this conventional methodology to private international law is questionable in the context of cryptoassets, where it is essentially impossible to establish the geographical location of the assets themselves or the transactions of which they are the subject.[10] This has led some, such as Guillaume, to conclude that "only conflict-of-law rules that are independent of any location criterion are able to provide a satisfactory connection to a national legal order".[11] Similarly, Lehmann points out that "It is thus not exaggerated to say that permissionless systems are completely de-nationalized and not connected to any particular country, which makes it impossible to determine the state with the closest connection".[12] By contrast, some, like Dickinson, are more optimistic:

> "Any account of the conflict of laws as it relates to cryptocurrencies must acknowledge and seek to overcome these challenges. Yet, the difficulties arising in this area should not be overstated. Most questions relating to the use of cryptocurrencies and the operation of cryptocurrency systems can be analysed, without undue difficulty, within the existing framework of private international law rules applied by the English courts in civil matters."[13]

The second problem is a practical and evidential one, namely establishing the identity, and thereby location, of the parties to a dispute. Courts will inevitably always know the identity of at least one of the parties, because the claimant in a dispute will make their identity known in the course of bringing proceedings. However, the identity of the other party to a transaction, or a bad faith actor who otherwise interacts with

[7] Matthias Lehmann, 'Who Owns Bitcoin? Private Law Facing the Blockchain' (2019) 21(1) Minn. J.L. Sci. & Tech. 93 at 111-116.
[8] Florence Guillaume, 'Aspects of private international law related to blockchain transactions' in Daniel Kraus, Thierry Obrist and Olivier Hari (eds), *Blockchains, Smart Contracts, Decentralised Autonomous Organisations and the Law* (Edward Elgar Publishing 2019) at 70.
[9] See Lehmann (n 7) at 111.
[10] Guillaume (n 8) at 70.
[11] Guillaume (n 8) at 70.
[12] Lehmann (n 7) at 112.
[13] Dickinson (n 2) at para 5.09.

a cryptoasset, is far harder to determine, either because of the pseudonymity of the DLT network or because of the frequent anonymity of bad faith actors who maliciously attack computer systems. As is discussed below, this renders difficult the application of some private international law rules which depend upon knowing the identity of the parties in order to identify their location.[14] This problem is not one that is unique to the world of cryptoassets and DLT networks – such evidential issues can arise in more usual cases such as hit and run road traffic accidents abroad. However, they arise universally in the context of technology such as cryptoassets, and they arise more acutely because, unlike a car accident where at least one knows where the accident occurred, the second problem compounds with the first problem such that residual indicators of geographical connection are very difficult to identify.

3 – Overarching methodological questions

In addressing how to approach private international law in the context of cryptoassets, there are also three preliminary questions of methodology that need to be addressed.

The first question is whether one adopts an international, national or non-legal approach to the regulation of cryptoassets? There are three broad answers available.

(a) Uniform international rules governing substantive issues: One approach is to establish whether there are any centralised or uniform rules of law at the international level that may be applied in the context of transactions involving cryptoassets.[15] Such an international solution is one of the primary objectives advocated for by the FMLC[16] and the LawTech Delivery Panel UK Jurisdiction Taskforce,[17] and there are already some preliminary efforts by international institutions in proposing model laws and recommendations for regulating internet-based transactions.[18] However, in the absence of adapting some of the existing international rules by way of analogy, it is generally acknowledged that reliance on uniform international rules to govern substantive issues relating to cryptoassets is largely in its infancy, and therefore aspirational at this point. Whilst, from a lawyer's perspective, cryptoasset transactions "might benefit from the uniformization of the rules of private law at the international

[14] See Guillaume (n 8) at 64.
[15] Guillaume (n 8) at 59.
[16] FMLC, *Distributed Ledger Technology and Governing Law: Issues of Legal Uncertainty* (March 2018) at para 6.1.
[17] LawTech Delivery Panel UK Jurisdiction Taskforce, *Legal statement on cryptoassets and smarty contracts* (November 2019) at para 99.
[18] See Guillaume (n 8) at 59-60, who gives the examples such as the work of UNCITRAL on developing the UNCITRAL Model Law on Electronic Commerce, as well as the possible relevance of the United Nations Convention on the Use of Electronic Communications in International Contracts.

level, it must be acknowledged that these rules are still very disparate and insufficient to govern every question of private law raised by the use of these technologies".[19]

(b) Regional/domestic private international law rules: In the absence of any uniform international rules governing substantive issues relating to cryptoassets, it becomes the responsibility of each individual state to apply and develop its own domestic private law so as to determine the legal scope of transactions involving cryptoassets.[20] This then raises the question as to which state's domestic private law applies to any given dispute. Just as there is no real system of uniform international laws governing the relevant substantive issues, there is also a lack of uniform private international law rules adopted at the international level which apply to all states. Accordingly, courts have no choice but to apply regional or domestic rules of private international law in order to determine both jurisdiction and applicable law in cases involving cryptoassets.[21] As we have already indicated, in the European sphere at least, there is scope for applying to cryptoassets the regional conventions concerning issues of private international law, such as the Brussels I (recast) Regulation on jurisdiction and the Rome I and Rome II Regulations on the applicable law to contractual and non-contractual obligations, respectively. In cases that fall outside the scope of those regulations, the courts of England and Wales will have to resort to applying the common law rules of private international law.

(c) *Lex cryptographia* and no governing law: The third alternative is to embrace DLT's resistance to law. For example, as is highlighted by Florence Guillaume, one may question even the premise of whether private international law is able to apprehend Internet-based legal relationships:

> "The traditional approach used for connecting a legal situation to a legal order aims to determine the seat of the legal situation. The rules of private international law are designed to make it possible to determine the State with which the issue at hand has the closest connection. The objective is therefore to establish the geographical location of legal relationships. The method does not appear appropriate, insofar as the Internet – like the blockchain – is an inherently intangible and transnational phenomenon. It is therefore extremely difficult to establish the location of a transaction made on the Internet, let alone the blockchain. This is why States have not yet taken steps to unify the rules of private international law applicable to digital activities via a multilateral international convention."[22]

[19] Guillaume (n 8) at 60.
[20] Guillaume (n 8) at 60.
[21] Guillaume (n 8) at 60-61.
[22] Guillaume (n 8) at 61.

> The philosophical underpinnings of DLT, which was designed as an alternative to legal solutions with an intention to overcome the shortcomings of the trust-based banking system, gives rise to an anti-legalistic tendency.[23] Both philosophically and practically, DLT can appear somewhat 'Teflon coated' when it comes to interacting with law. In that light, one solution is not to apply any law at all to disputes involving DLT, but instead to leave the dispute resolution for the consensus mechanism of the DLT network.[24] Such self-regulation is the goal of those who have advocated for DLT to be governed by a non-state and a-national law called *lex cryptographia*.[25] Both options fundamentally involve the same idea: the consensus mechanisms which provides the foundation for the DLT are what governs each interaction with the cryptoassets, independently of any legal rules.[26] The code replaces the applicability of any real world legal system to those interactions.

We take the view that the way forward, for the moment at least, is to follow the second approach, whereby each state applies its own domestic rules of private international law. Whilst the first approach is one to which we should all aspire in pursuit of legal certainty for participants in DLT systems, it is too aspirational at present to provide a practical solution for the problems which arise with cryptoassets. Furthermore, the third approach is just inherently unrealistic. We agree with those who consider that there are many situations in which cryptoassets come into contact with the real world, and which therefore require real world normative legal frameworks to provide resolution.[27] Problems such as mistake, duress, theft, fraud, inheritance upon death and bankruptcy are all examples where a rational outcome cannot be secured without the application of a real world legal framework.[28] Moreover, it is clear that the absence of an applicable real world legal framework to deal with issues such as misappropriation is not within the reasonable expectations of the majority of participants on a DLT network – many people presuppose that the technology yields binding results.[29] Certainty and predictability of commerce requires that those expectations are met, which ultimately requires the rule of law.

[23] Lehmann (n 7) at 98-99.
[24] Michael Ng, 'Choice of law for property issues regarding Bitcoin under English law' (2019) 15(2) Journal of Private International Law 315 at 335-336.
[25] Lehmann (n 7) at 100, citing: Aaron Wright and Primavera De Filippi, 'Decentralized Blockchain Technology and the Rise of Lex Cryptographia' (10 March 2015) at 48 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664> (last accessed 20 October 2020). See also: Primavera De Filippi and Aaron Wright, *Blockchain and the Law: The Rule of Code* (Harvard University Press 2018) at 52; Guillaume (n 8) at 71-75.
[26] Lehmann (n 7) at 100-101.
[27] See Guillaume (n 8) at 75.
[28] Lehmann (n 7) at 106.
[29] Ng (n 24) at 336; Lehmann (n 7) at 101.

The second question concerns how to categorise cryptoassets, which can be divided generally into two categories. There are 'on-platform' assets, also known as 'native' or 'on-chain' assets, as against 'off-platform' assets, also known as 'tethered', 'exogenous' or 'off-chain' assets.[30] The cryptoasset itself, the purely digital record in the ledger that exists only internally to the DLT system, is classed as an on-platform asset. On some DLT networks, the on-platform asset is a digital representation of a conventional "real world" asset that exists externally to the DLT system. In such cases, in addition to the on-platform asset itself, there will be tethered to it an off-platform asset which is the real-world asset which the on-chain asset represents on the DLT network. The process by which a real world off-platform asset external to the DLT network becomes represented in an on-platform cryptoasset internal to the DLT network is called 'tokenisation'.[31] We will consider the position for purely on-platform assets in the third section of this article, and whether the position should be any different where there are tethered off-platform assets in the fourth section.

The third and final question concerns how to categorise the various different kinds of transactions and interactions that can occur with cryptoassets. Transactions can be divided into, again, two broad categories, although different commentators draw the dividing line in slightly different places.[32] The first category concerns interactions relating to a cryptoasset between two or more participants within a DLT system, in connection with the operation of that system, which some refer to as 'endogenous' or purely internal interactions. The second category concerns interactions relating to a cryptoasset between participants within a DLT system and individuals external to that system, which some refer to as 'exogenous' or external interactions. We agree with Dickinson that internal and external relationships must be analysed separately.[33]

In our view, conflicts of laws questions regarding transactions within a cryptoasset system will be resolved by reference to the system's consensus rules and any rules of law applicable to those relationships. If the DLT system between the participants is regulated by a formal contract between the participants, there will be no difficulty in classifying the relationships between them as contractual for the purposes of applying rules of both jurisdiction and applicable law, namely, the Brussels I (recast) Regulation and the Rome I Regulation, respectively. Where the relationships within a system are not labelled or identified by the

[30] LawTech Delivery Panel UK Jurisdiction Taskforce (n 17) at para 33; FMLC (n 16) at para 3.3(c).
[31] Lehmann (n 7) at 96 and 116, citing Joshua A.T. Fairfield, 'Bitproperty' (2015) 88 S. Cal. L. Rev. 805 at 826-827.
[32] Dickinson (n 2) at paras 5.13, 5.15 and 5.93-5.95. The references to endogenous and exogenous interactions can be found in Lehmann (n 7) at 103-106, citing Primavera De Filippi and Greg McMullen, 'Governance of blockchain Systems: Governance of and by Distributed Infrastructure' (2018) <https://hal.archives-ouvertes.fr/hal-02046787/document> (last accessed 20 October 2020).
[33] Dickinson (n 2) at para 5.15.

system participants as contractual in nature, such as Bitcoin and Ripple, the situation is more complicated. However, in our view, the touchstone for 'matters relating to contract' (for the purposes of the Brussels I (recast) Regulation) and 'contractual obligations' (for the purposes of the Rome I Regulation) are defined widely by the European court by reference to the consensual basis of relationships,[34] such that systems such as Bitcoin and Ripple are likely to be classified as contractual for the purpose of conflicts of laws.[35]

This view is obviously subject to the caveat that the sheer variety of cryptoasset systems means that a single, homogenous analysis is not possible. Rather the analysis must be tailored according to the structures and features of the particular system.

The majority of cryptoasset litigation thus far has arisen out of external interactions or interactions of cryptoassets with the "real world". These interactions form the focus of the remainder of this article in sections three and four, below.

3 – Purely on-platform assets: jurisdiction and applicable law for interactions external to DLT

In this section we explore some of the private international law challenges which arise in external fact patterns in relation to cryptoassets which are not tethered to or representative of a conventional off-platform "real world" asset that exists externally to the DLT system.

3(a) – Jurisdiction

In our view jurisdictional questions are unlikely to raise particularly difficult problems in litigation involving cryptoassets. The rules under the Brussels I (recast) (and the common law regime) are applicable to cryptoasset disputes in the same way as any other dispute. For example, litigation involving tortious conduct (e.g. fraudulent misrepresentation, conversion and misappropriation) involves real persons in the real world such that that it should be no more difficult to locate the event giving rise to the damage and the damage than in similar cases in other contexts.[36]

There may be initial difficulties in identifying a perpetrator where there has been misappropriation or hacking because of the pseudonymity of DLT systems and the general anonymity of bad faith third party

[34] See for example, Joined Cases C-359/4 etc *Ergo Insurance SE v If P&C Insurance AS* [2016] EU:C:2016:40 at para 44 (concerning the Rome I/Rome II Regulations) referring to Case C-373/13 *Kolassa v Barclays Bank plc* [2015] EU:C:2015:37 at para 39 (concerning the Brussels I Regulation).
[35] This view is shared by Dickinson (n 2) at para 5.31. However, this is not the same as concluding that substantive contractual obligations exist between them.
[36] Article 7(2) of the Brussels I (recast) Regulation and Case C-12/15 *Universal Music International Holding BV Schilling* EU:C:2016:449 at paras 30-40.

actors, but the event giving rise to the damage still involves the conduct of the perpetrator which takes place in the real (not virtual world). The perpetrator will be an individual with a domicile ascertainable in the usual way under Article 4 of the Brussels I (recast) Regulation or under the common law. It also seems eminently sensible and pragmatic, as suggested by Dickinson, to apply the existing case law which ascribes the location of tortious damage suffered by a claimant by reference to their habitual residence or relevant place of business, which is where the consequences of the damage will be felt.[37]

The consumer provisions of the Brussels I recast have already been used in cryptoasset-related litigation in England without conceptual difficulty. In *Ramona ANG v Reliantco Investments Ltd*,[38] Andrew Baker J held that the protections afforded to consumers under Articles 17 and 18(1) of the Brussels I (recast) Regulation on jurisdiction applied to individual investors using an online platform to trade cryptocurrencies (in this case Bitcoin futures) where the purpose of the investor's use was as a consumer.[39]

There do remain questions linked to the formal characterisation of cryptoassets which will need to be answered by our courts, such as whether the sale of goods provisions in the Brussels I recast can apply to cryptoasset transactions (e.g. the transfer of tangible goods in exchange for units of a cryptocurrency).[40] However, the conceptual difficulty arising from these cases is not one of private international law. Once the classification issues have been ironed out, the applicable private international law solution will be relatively straightforward.

3(b) – Jurisdiction Challenges in Interim Injunctions

One area where difficulty is yet to be resolved in cryptoasset litigation is in relation to interim disclosure orders sought in order to identify an individual who has perpetrated a fraud or hack. These kinds of orders will inevitably be sought more frequently in cryptoasset litigation due to the pseudonymity of users on DLT systems.

Even with the assistance of asset tracers, all that victims of misappropriation or fraud may know is whether a cryptocurrency exchange or platform has been caught up in the wrongful conduct, after which the trail runs dry. It is common practice then to seek an urgent Norwich Pharmacal or banker's trust order against

[37] Dickinson (n 2) at para 5.12.
[38] *Ramona ANG v Reliantco Investments Ltd* [2019] EWHC 879 (Comm).
[39] *Ramona ANG* (n 38) at [70].
[40] See Article 7(1)(b) of the Brussels I (recast) Regulation.

the exchange or platform so that further information about the perpetrator can be obtained with a view to eventually locating and pursuing them.

However, because of the transnational nature of these assets, it is, and will commonly be, the case that the exchange or platform is neither headquartered nor registered in this jurisdiction or in the EU. They may also have no physical presence or branch[41] in this jurisdiction. This raises an issue about whether an individual can obtain a Norwich Pharmacal or a Banker's Trust order in this jurisdiction against the exchange or platform outside the jurisdiction.

This very issue came up in the now well-known case *AA v Persons Unknown*[42]. Bitfinex was a crypto trading exchange and 96 Bitcoins obtained through a ransom were transferred to an address linked to that exchange. However, Bitfinex was not domiciled in England and Wales. Its headquarters were in Hong Kong and its registered office was in the BVI. Bryan J stated that a complication arose in requiring an institution (such as Bitfinex) out of the jurisdiction to provide information pursuant to a court order of the English court, particularly where the provision of that information might breach the laws of the jurisdiction in which it is headquartered or registered (e.g. the privacy of its accountholders).[43]

Bryan J indicated that the position on that issue had not been definitively determined and mentioned two decisions. One was Waksman J's judgment in the case of *CMOC v Persons Unknown*[44], in which he granted a banker's trust order against banks situated outside England and Wales and the EU because they were a critical source to discover what had happened to the money paid out of the claimant's bank account in London pursuant to the alleged fraud and the case for service out of the jurisdiction was that the banks were a necessary and proper party to the claims which were being brought against the perpetrator defendants.[45]

The second decision referred to was *AB Bank Ltd, Off-Shore Banking Unit (OBU) v Abu Dhabi Commercial Bank PJSC*[46] in which Teare J reached the opposite conclusion. The claimant made an application to serve a claim form out of the jurisdiction where there was a foreign bank innocently mixed up in a fraud. The question was whether Norwich Pharmacal-/Bankers Trust-type relief was a claim for an interim remedy for the purposes of serving out of the jurisdiction, the specific gateway being relied upon that it was a claim for

[41] Cf Article 7(5) of the Brussels I (recast) Regulation.
[42] *AA v Persons Unknown* [2019] EWHC 3556 (Comm), [2020] 4 WLR 35.
[43] *AA v Persons Unknown* (n 42) at [44].
[44] *CMOC v Persons Unknown* [2017] EWHC 3599 (Comm).
[45] *CMOC v Persons Unknown* (n 44) at [10].
[46] *AB Bank Ltd, Off-Shore Banking Unit (OBU) v Abu Dhabi Commercial Bank PJSC* [2016] EWHC 2082.

an interim remedy under section 25(1) of the Civil Jurisdiction and Judgments Act 1982. Teare J concluded that the Norwich Pharmacal/Banker's Trust order was not an interim remedy but a final remedy.[47] He also concluded that it was not an injunction ordering an act within the jurisdiction on the facts of the case nor was the necessary and proper party gateway met either. He therefore concluded that there was no gateway through which the claim for Norwich Pharmacal relief could pass.[48]

It appears that Waksman J was not referred to Teare J's earlier decision and Teare J's judgment is more fully reasoned than Waksman J's on this particular issue. Therefore, it seems to us that a court in the future will be more likely to rely on the judgment of Teare J.

One potential solution to the jurisdictional difficulty identified was canvassed by Teare J in his judgment, namely the 'injunction requiring an act within the jurisdiction' gateway in PD 6B of the Civil Procedure Rules. The order requested by the party before Teare J was an order requiring Abu Dhabi Commercial Bank to "obtain and/or take all reasonable steps to procure the information listed …below and provide to the Applicant a witness statement/affidavit made by a responsible officer which identifies [certain matters] …".[49]

Teare J held that the steps it would take to comply with the injunction would be taken in the UAE not in the UK. If a representative of the claimant was given the witness statement or affidavit in the UAE or in Bangladesh there would be compliance with the order. Teare J, however, went on to say:

> "of course, Abu Dubai could also comply with the order by providing the applicant's solicitors in England with the witness statement or affidavit. But the injunction does not require such action within the jurisdiction. For that reason I consider that the claim also fails the second gateway".[50]

He cited the decision of *Bacon v Automattic Inc and others*[51] which was an *ex parte* decision in which permission to serve an application for Norwich Pharmacal relief out of the jurisdiction was sought and obtained on the basis that the defendants (who were based in California or Colorado) were required to do an act within the jurisdiction, namely, disclose to the solicitors for the Claimant the information sought.[52]

Whilst there is therefore some authority for requesting a Norwich Pharmacal order or Banker's Trust order, and anchoring the jurisdiction of an English court in the fact that the documents be disclosed are to be

[47] *AB Bank Ltd, Off-Shore Banking Unit (OBU)* (n 46) at [16].
[48] *AB Bank Ltd, Off-Shore Banking Unit (OBU)* (n 46) at [17] and [19]-[21].
[49] *AB Bank Ltd, Off-Shore Banking Unit (OBU)* (n 46) at [17].
[50] *AB Bank Ltd, Off-Shore Banking Unit (OBU)* (n 46) at [17].
[51] *Bacon v Automattic Inc and others* [2011] EWHC 1072 (QB).
[52] *AB Bank Ltd, Off-Shore Banking Unit (OBU)* (n 46) at [18].

disclosed to a solicitor in England and Wales, that authority is only *obiter dicta*. Counsel in *AA v Persons Unknown* realised the difficulty of reconciling the two decisions outlined above and invited the judge to adjourn the Norwich Pharmacal/Banker's Trust aspect of his application which Bryan J did.[53] We therefore do not have a definitive view on this issue. The current authors are sceptical that courts will be attracted to the solution canvassed by Teare J as it might be said to be an abuse of process. The solution, whilst neat, essentially amounts to a formalistic circumvention of the limits of the 'requiring an act within the jurisdiction' gateway. A more attractive solution in our view would be a wider interpretation of the PD 6B gateways to avoid severely limiting the jurisdiction of our courts in this area, potentially driving something of a coach and horses through any aspiration of making England and Wales a crypto-litigation centre.

3(c) – Applicable law

More challenging conceptual questions arise as regards the law applicable to a dispute involving cryptoassets.

3(c)(i) – Issues involving property law

Whilst we are yet to get a definitive and fully reasoned judgment on the issue in this jurisdiction, the general direction of travel in the common law world is that cryptoassets are a form of property.[54] In any case, whatever the position of substantive English law, it is clear that the English law rules of private international law have tended to analyse proprietary questions separately and more broadly, particularly where it is evident that a case raises issues relating to the rights of third parties to a transaction.[55] Accordingly, our view is that it is necessary to consider applicable law in the context of issues involving property law. However before getting into a discussion about 'property-law-proper', some have suggested that the Rome I Regulation, specifically Article 14, may provide some solutions to property questions relating to cryptoassets.

Article 14 states as follows:

> "1. The relationship between assignor and assignee under a voluntary assignment or contractual subrogation of a claim against another person (the debtor) shall be governed by the law that applies to the contract between the assignor and assignee under this Regulation.

[53] *AA v Persons Unknown* (n 42) at [49].
[54] For example, *AA v Persons Unknown* (n 42), *B2C2 Ltd v Quoine Pte Ltd* [2019] SGHC(I) 3 and *Ruscoe v Cryptopia Ltd (In Liquidation)* [2020] NZHC 728.
[55] Ng (n 24) at 321-322, citing: T.C. Hartley, *International Commercial Litigation: Text, Cases and Materials on Private International Law* (2nd edn, CUP 2015) at 788; *Re Helbert Wagg & Co Ltd* [1956] Ch 323 at 339-340; *National Bank of Greece and Athens v Metliss* [1958] AC 509 at 526.

2. The law governing the assigned or subrogated claim shall determine its assignability, the relationship between the assignee and the debtor, the conditions under which the assignment or subrogation can be invoked against the debtor and whether the debtor's obligations have been discharged.

3. The concept of assignment in this Article includes outright transfers of claims, transfers of claims by way of security and pledges or other security rights over claims."

One could try to argue that a transaction involving a cryptoasset constitutes an assignment in the sense of being an outright transfer of a claim, because the term 'claim' is considered to more broadly cover any legally enforceable right to a chose in action.[56] If this is the case, then Article 14(2) is capable of being interpreted in such a way that the law applicable to the contract by which the transfer was effected would also govern the underlying questions of proprietary ownership of the cryptoasset as between the transferee/assignee and transferor/assignor. The application of Article 14 to cryptoassets is, however, subject to significant limitations:

(a) First, it is highly doubtful whether most transactions involving a cryptoassets even truly constitute transfers of 'claims' in the sense envisaged by Article 14. Certainly, Dickinson is of the view that cryptoassets frequently will not involve a 'claim', in the sense of a legal right, in order to engage Article 14.[57] Although his analysis focuses on the Bitcoin and Ripple cryptocurrencies, his explanation of the nature of the intangible property rights that accrue are applicable to a range of different cryptoassets which are sponsored via DLT networks:

> "**5.107** In cryptocurrency systems such as the Bitcoin and Ripple systems, the value of the participants' 'entitlements' does not depend on the existence of a legal right to be associated with units of cryptocurrency but instead relies upon a legitimate expectation, founded on technological features of the system, that the consensus rules which underpin the system will be applied and will not be altered fundamentally such as to deprive each participant of the association to particular units within the system and the power to deal with those units. This is a factual and not a legal benefit, but should, nevertheless, be capable of being characterized as a species of intangible property in the same way as (for example) goodwill in a business.
>
> **5.108** Indeed, goodwill provides a potentially valuable analogy for treating such legitimate expectations as a species of intangible property in the English conflict of laws insofar as case law and commentary support the view that the goodwill of a business constitutes a distinct species of intangible property …".[58]

[56] FMLC (n 16) at para 6.12; and Dickinson (n 2) at paras 5.100-5.101, citing Article 2(d) of the European Commission's Proposal for a Regulation of the European Parliament and of the Council on the law applicable to the third-party effects of assignments of claims (Com (2018) 96 final) which defines 'claim' as "the right to claim a debt of whatever nature, whether monetary or non-monetary, and whether arising from a contractual or non-contractual obligation".

[57] Dickinson (n 2) at para 5.106.

[58] Dickinson (n 2) at para 5.107-5.108.

(b) Secondly, whether or not Article 14 applies to cryptoassets, it has limited coverage for issues relating to proprietary ownership. This is because Article 14 does not regulate proprietary issues that arise as against third parties, whether that involves questions about the effectiveness of an assignment of a claim as against third parties where title or interest is in doubt, or questions about the priority of the assignee's right over the right of another person where their title or interest is in competition.[59] Generally, and apart from Rome I, the applicable law to proprietary questions vis-à-vis third parties, arising out of an assignment, is very uncertain in English law and there are divergent approaches across states.[60] In an attempt to harmonize the law on this question, the European Commission launched a consultation in 2017 which offered three different candidate rules for governing the proprietary effects of assigned claims, some of which we will consider below, but no definitive harmonized rule at the European level has yet been adopted as law[61].

In light of this, it is relatively clear that Article 14 currently does not provide a solution to the problem at hand. Furthermore, given that the end of the transition period is likely to pre-date the formal adoption of any EU legislation in relation to third-party effects of assignments, any solutions provided in that legislation will be formally inapplicable in this jurisdiction.

In our view the solutions to these challenges lie in the law applicable to property law as opposed to contractual assignments. Determining the law applicable to property questions private international traditionally relies on the ***lex situs*** of the property – the law of the country where the property is situated.[62] The *lex situs* rule is applied to both immovable[63] and tangible movable property.[64] More pertinently, the *lex situs* rule is also applied by analogy to intangible property.[65] However, the application of the *lex situs* rule to intangible property is made difficult by the fact that intangible property is not truly situated in any particular geographical location. Consequently, special sub-rules have had to be adopted for various forms of intangible property in order to adapt the general *lex situs* rule to the distinctive nature of intangible property.[66]

[59] FMLC (n 16) at para 6.12; and Dickinson (n 2) at para 5.104.
[60] See Dickinson (n 2) at para 5.104.
[61] See European Commission, *Consultation document: conflict of laws rules for third party effects of transactions in securities and claims* (Ares (2017) 1874960, 7 April 2017). However, there has been a Proposal for a Regulation of the European Parliament and of the Council (see n 56).
[62] *Dicey, Morris & Collins on the Conflict of Laws* (15th edn, Sweet & Maxwell, 2012), Rule 128, para 22R-001.
[63] *Dicey, Morris & Collins* (n 62) at para 23R-062, Rule 132.
[64] *Dicey, Morris & Collins* (n 62) at para 24R-001, Rule 133.
[65] *Dicey, Morris & Collins* (n 62) at paras 22-025–22-051.
[66] For criticism of this approach, see Ng (n 24) at 326, citing, among others, Pippa J. Rogerson, 'The Situs of Debts in the Conflict of Laws – Illogical, Unnecessary and Misleading" [1990] 49(3) CLJ 441.

For example, as regards choses in action such as debts, the English common law focuses on the person with control over the asset.[67] Debts are deemed to be situated in the country where the debtor resides.[68] Similarly, the shares in a company are deemed to be situated in the place of incorporation of the company or the place of the register upon which any transfer must be registered to be effective.[69] The EU has taken a different approach to choses in action insofar as they are transferred or securitized: under the Rome I Regulation, Article 14 applies the law of the contract giving rise to the claim.

As regards cryptoassets recorded on DLT systems, the *lex situs* approach (especially the existing special sub-rules) is obviously unworkable. It is helpful to give two broad examples. First, the rules which apply to debts cannot be applied directly or by analogy because most cryptoassets do not represent rights against any particular person such that there is no debtor or obligor.[70] Relatedly, an analogy with payments using bank money is inapposite because, first, there is no third party intermediary like a bank in a disintermediated DLT system and, secondly, the transfer of cryptoassets from being attached to one private key to being attached to another private key is more akin to moving items of property between safety deposit boxes. Secondly, neither can the various rules which can be applied to shares be applied to cryptoassets.[71] The place of incorporation of the issuing company fails as an analogical rule because there is no comparable entity that "issues" cryptoassets to participants in the DLT network in the same way that a company issues shares to its shareholders.[72] The alternative rule, the place where the share register is located, also fails because of the decentralised, distributed and transnational nature of the ledger across each and every node on the network.[73]

[67] See earlier article by OTC barristers Richard Hitchcock QC, Stephen Butler and Chloë Bell highlighting the importance of focusing on 'the person in property' for the purposes of cryptoasset disputes: Richard Hitchcock QC, Stephen Butler and Chloë Bell, 'The Person in Property – OTC on Cryptoassets: a commentary on David Ian Ruscoe and Malcolm Russell Moore v Cryptopia Limited (in liquidation) [2020] NZHC 728' <https://www.outertemple.com/wp-content/uploads/2020/06/Outer-Temple-Chambers_Cryptoassets-The-Person-in-Property1.pdf> (last accessed 20 October 2020).
[68] See *Dicey, Morris & Collins* (n 62) at para 22-026–22-032.
[69] See *Dicey, Morris & Collins* (n 62) at para 22-044–22-045.
[70] Ng (n 24) at 327-328. The LawTech Delivery Panel UK Jurisdiction also dismiss the analogy as inapplicable, at least in the case of fully decentralised DLT networks: LawTech Delivery Panel UK Jurisdiction Taskforce (n 17) at para 96(a).
[71] It should be noted that the law is unsettled as to which rule applies, namely whether the applicable law is the law of the place of incorporation of the issuing company or the law of the place where the share register is located: see *MacMillan Inc v Bishopshate Investment Trust Plc (No. 3)* [1996] 1 WLR 387 (CA); and *Dicey, Morris & Collins* (n 62) at para 22-044–22-045.
[72] Ng (n 24) at 328.
[73] Ng (n 24) at 329.

As the FMLC points out, the identification of a single *situs* for a cryptoasset becomes difficult due to the combination of the asset's intangibility, digital nature and existence on a distributed network.[74] Accordingly, most of those who have examined this issue conclude that there are very good arguments against applying the normal proprietary rules based on *lex situs* to cryptoassets.[75]

Instead, the FMLC has recommended that '**elective *situs***' (i.e. a consensual agreement by which parties choose the law applicable to disputes) should be the starting point for determining the applicable law to property questions arising from cryptoassets. This is effectively to apply, by analogy, contractual choice of law rules as exist under English common law and under Rome I to proprietary issues arising out of the DLT network.[76] The primary variation on this theme would be what we have termed '**direct, systemic elective *situs***': an express contractual agreement between the network participants of the DLT system, adopted via the consensus mechanisms which underpin the network, pursuant to which they collectively choose the applicable law governing proprietary issues such as ownership, transfer and use of cryptoassets.[77] In order to account for the regulatory risks in allowing an unrestricted choice of law by the network's participants, a variation on this theme is what we would call '**direct, systemic modified elective *situs***' – in other words, the same as direct, systemic elective *situs*, but where the participants' choice of applicable law is restricted by regulation.[78]

There are, however, three problems with these variations of elective *situs*:[79]

(a) First, as Ng points out, there is a conceptual objection as to why a contractual choice of applicable law should be applied to property issues vis-à-vis third parties.[80] Why should third parties be bound by a choice of law selected via an agreement to which they were never a party? Such a result might be considered unfair on third parties. Ng's response is that, where a third party's entitlements to the cryptoasset derives from a participant in the DLT network, the third party should have no greater rights than the participants and should, therefore, be bound by the *ex ante* choices made by the participant

[74] FMLC (n 16) at 4.1-4.2.
[75] LawTech Delivery Panel UK Jurisdiction Taskforce (n 17) at para 97; Guillaume (n 8) at 63-64.
[76] Ng (n 24) at 333, citing *Vita Food Products Inc v Unus Shipping Co Ltd* [1939] AC 277 for the common law rule and Article 3(1) of Rome I.
[77] FMLC (n 16) at paras 6.4-6.5; Ng (n 24) at 332-334.
[78] FMLC (n 16) at paras 6.8-6.10; see also para 6.11 where the FMLC briefly discusses the logical extension of this approach, 'deemed elective *situs*', under which there is no consensual agreement at all, rather the election is determined by a state's relevant primary regulatory or competent authority.
[79] See Ng (n 24) at 333 for a fourth problem concerning public policy, which is tangential to the discussion in this article but with which he deals convincingly.
[80] Ng (n 24) at 332-333.

which includes their choice of applicable law.[81] This response has particular force in the context of cryptoassets – the DLT network on which the existence of those cryptoassets depends is itself dependent on the distributed consensus protocol through which any party autonomy would take effect. This means that there is a more powerful rationale, perhaps, for an elective *situs* rule in this particular context. When one characterises the proprietary right in a cryptoasset on the basis of the legitimate expectations one has in the system, as we have already discussed above, the case for applying a contractual choice of law to property issues as against third parties can be made quite powerfully.

(b) Secondly, there are significant practical obstacles to adopting an elective *situs* rule. As a starting point, in many established DLT networks, no express choice has been made by the participants. Neither is there sufficient evidence of an implied choice of law made by the participants of existing networks that can be inferred from their quasi-agreement to sign up to the consensus mechanisms that lie at the foundation of the DLT network – indeed, the anti-legalistic tendencies of such systems would suggest strongly to the contrary.[82] Furthermore, even if there was a desire, moving forward, by participants on existing DLT networks to adopt an elective *situs*, there is the considerable difficulty of obtaining the agreement of the majority of users via the distributed consensus protocol. In this regard, DLT's resilience and resistance to change pose significant obstacles. It is acknowledged, however, that such difficulty might be less problematic for permissioned DLT systems where acceptance of a specified applicable law could be one of the terms on which a user's accession to the DLT system is made conditional.[83]

(c) Thirdly, Dickinson argues that the advantages of uniform applicable law in respect of all cryptoassets for each DLT network are superficial, and outweighed by

> "the cost of greater uncertainty without any obvious advantages for participants in the system or third parties. For example, applying the law governing the relationships between participants in that system … to govern the proprietary effects of a transaction outside the system would, for the affected third parties and in many cases for the participants also, be highly unpredictable and likely to result in their

[81] Ng (n 24) at 333.
[82] Ng (n 24) at 333-334. This is also, implicitly, Dickinson's implicit view: Dickinson (n 2) at para 5.37, citing Rome I, recital (13), *Dicey, Morris & Collins* (n 62) at paras 32-049 and 32-036, and *Halpern v Halpern* [2007] EWCA Civ 291, [2008] QB 195. He considers that the choice of applicable law rule contained in Article 3 of Rome I "has no obvious role to play" in the case of the cryptocurrencies Bitcoin and Ripple because the consensus mechanisms involve a choice of non-state rules and Rome I only validates a choice of applicable law of a national legal system.
[83] FMLC (n 16) at para 6.7.

legal rights being determined according to a law with which neither they nor the transaction(s) in question have a close connection".[84]

One might also consider what, at face value at least, appears to be a more practically straightforward rule which is also effectively another variation of elective *situs*. This rule would hold that the applicable law for third party-proprietary effects would be the same as the applicable law of the assignment – one might refer to this as '**derivative, transactional elective *situs***', based upon the underlying transaction, because the benefit of such a rule allows the parties to the transaction to agree upon not only the law which will govern the transaction, but the law which will govern its proprietary effects as against third parties.[85] To be clear, this form of rule relies upon consensus between the parties to the transaction involving the cryptoasset, as opposed to consensus between the network participants of the DLT network. This kind of rule is one of the three applicable law rules suggested by the European Commission in its 2017 consultation on the applicable law for the proprietary effects of assigned claims.[86] Furthermore, the LawTech Delivery Panel UK Jurisdiction Taskforce, whilst not coming to any firm conclusions, do suggest that the law applicable to the relevant transfer might be a particularly relevant consideration in determining what the applicable law should be.[87]

Whilst this rule has the advantage of simplicity and coherence, it does have significant disadvantages:

(a) First, there is the same conceptual objection as with the two variations of direct elective *situs* we have considered, namely the question why a contractual choice of applicable law should be applied to third parties. However, whilst we have seen that quite a powerful argument can be made in respect of third parties being bound by an applicable law agreed by the DLT network's participants via its consensus mechanisms, the same justification cannot be extended to an applicable law agreed by the parties to an individual transaction.

(b) Secondly, for those such as the FMLC who ideally favour a uniform applicable law in respect of all cryptoassets for each DLT network, there are concerns that such a rule will lead to fragmentation, with different transactions being subject to different applicable laws depending on what the parties to each transaction agree upon.[88]

[84] Dickinson (n 2) at para 5.112.
[85] FMLC (n 16) at para 6.13-14.
[86] See European Commission consultation (n 61) at 24.
[87] LawTech Delivery Panel UK Jurisdiction Taskforce (n 17) at paras 98 and 99(d).
[88] FMLC (n 16) at para 6.15.

On balance, we agree with the FMLC's conclusion that some form of direct systemic elective *situs* rule should be the starting point for fact patterns external to the DLT network involving purely on-platform assets.[89] As they point out, this solution has the benefits of being straightforward, objective and easily ascertainable by all parties involved due to the uniformity of applicable law it produces for each DLT network. It also follows the general pattern of the Rome I and Rome II Regulations which generally give priority to party choice. However, this does not take us very far because this conclusion is very much aspirational. The FMLC themselves admit that elective *situs* is a rule that is appropriate for "DLT systems being designed and built today"[90] and that there will be situations in which elective *situs* "cannot readily or sensibly be implemented".[91] The FMLC fails to give due weight, however, to the fact that there will be significant practical problems with an elective *situs* being agreed on existing DLT networks, especially permissionless systems, as well as to the difficulties of overcoming anti-legalistic tendencies of those actors most likely to be responsible for the creation of new DLT networks.

It is therefore necessary to analyse other rules of private international law which will apply in the absence of an election. Many suggestions have been mooted in the literature. Examples include:

(a) *Lex creationis* is one possible candidate rule, under which the applicable law is the law under which the intangible asset is created.[92] However, whatever the rule's general merits, Ng is right to dismiss the application of this rule to cryptoassets, for the simple reason that, as we have already seen, cryptoassets exist independently of any state's domestic law and so there is no law that is the source of a cryptoasset – there is no *lex creationis*. To that end, Ng suggests that cryptoassets are more akin to a chose in possession than a chose in action, despite their intangibility, because the law is tasked with conferring the protection of property rights on something that exists independently of the law as a matter of fact.[93]

(b) Another suggested approach is to apply the law that governs the code used to create the original DLT network, which would usually be presumed to be the primary residence of the original coder.[94] We agree with the FMLC's primary objection to this, that there is little justification for this rule where the

[89] FMLC (n 16) at para 7.3. This is also the primary conclusion reached by Guillaume (n 8) at 78-79.
[90] FMLC (n 16) at para 7.7.
[91] FMLC (n 16) at para 7.5.
[92] Ng (n 24) at 331-332, citing Maisie Ooi, *Shares and Other Securities in the Conflict of Laws* (OUP 2003).
[93] On the related topic of the law conferring the protection of property rights on cryptoassets, readers will no doubt be familiar with the fact that the Law Commission is aiming to publish a consultation paper on the possibility of recognising the possession of intangible assets in the first half of 2021 as part of its general review of English law in relation to digital assets: <https://www.lawcom.gov.uk/project/digital-assets/> (last accessed 20 October 2020).
[94] Referred to variously as *'lex codicis*' and '*lex digitalis*': FMLC (n 16) at para 6.28.

original coder retains no control over the DLT network or its code because any ongoing developments are determined via the network's consensus mechanism.

(c) Another set of possibilities canvassed by the FMLC is that the applicable law would be: the location of, or determined by, the relevant administrator or operating authority of the DLT network;[95] the location of the private encryption master key/habitual residence of the master key-holder;[96] or the location of the issuer master account.[97] Our main objection to these rules is that these attributes only exist in a minority of DLT systems and it is unnecessarily confusing to demarcate between types of DLT systems in circumstances where there are other, more appropriate rules which are just as capable of identifying suitable connecting factors.

(d) Whilst Guillaume's primary solution is effectively to adopt some form of elective situs, in the event that no agreement on an elective situs is made, she adopts the *lex fori* as the fallback rule, for which she provides the following justification:

> "Attempting to establish such a [fallback] rule again comes up against the intrinsic impossibility of establishing the geographical location of blockchain transactions. In any case, it is not possible to apply a connecting factor that seeks to determine the State with which the issue has the closest connection. In our view, the only option is to provide, in such cases, for the application of lex fori. Any other attempt to establish an objective connection with a State appears bound to fail … This rule does not seek to establish the location of the transaction, but simply to apply lex fori whenever there is a connection of any kind with the forum in question. This example clearly demonstrates that the issue arises more at the level of determining the jurisdiction of the authorities than at that of the applicable law."[98]

Whilst this view is understandable, it is a rather defeatist approach in circumstances where, as we have already seen, various, if imperfect, potential rules to determine connecting factors are capable of being devised. Indeed, we now turn to the rule which we consider to be the most promising candidate for determining the applicable law of property issues for cryptoassets.

<u>Proposed solution – habitual residence of the private key-holder:</u> Having considered all of the alternatives, we conclude that the most promising candidate for a rule of applicable law is a rule based upon the location of the private user encryption key for the DLT system. However, for practical reasons which we will go on to consider, such a rule should take the precise form of a rule that the applicable law is the law of the

[95] Referred to as 'PROPA': FMLC (n 16) at paras 6.16-6.17.
[96] Referred to as 'PREMA': FMLC (n 16) at para 6.18.
[97] FMLC (n 16) at para 6.20.
[98] Guillaume (n 8) at 79.

primary habitual residence/domicile or centre of main interests of the private key-holder.[99] In other words, the law should focus on the location of the person rather than the private key itself.

In concrete terms, this would mean that, in a hacking case, competing ownership claims between the original owner of a cryptoasset and any subsequent recipient from a hacker would be determined by the laws of the primary habitual residence of the subsequent recipient who is the holder of the private key currently registered to that cryptoasset.[100] Alternatively, in the case of an insolvent exchange, this would depend upon the holding structure of the exchange, in particular whether cryptoassets are held in the exchange's own address under the exchange's private key, or whether each client of the exchange has segregated addresses and their own private keys.[101] In the former scenario, proprietary questions would be determined by the laws of the exchange's country of residence/registration; in the latter, the applicable law would be the laws of the primary habitual residences of each client of the exchange.

Such a rule is not dissimilar from the third option presented by the European Commission in its proposal for harmonisation on the law applicable to the third party effects of assignment of claims, which is that the applicable law is the law of the country in which the assignor is habitually resident.[102] Indeed, following its consultation, the Commission went on to adopt this rule (with some exceptions) in its proposal for a harmonised regulation on the law applicable to the third-party effects of assignments of claims.[103]

The 'residence of the private key-holder' rule is also not too dissimilar, in our view, from Dickinson's ultimate solution.[104] As set out above, his view is that the true nature of the intangible property in the context of cryptoassets can be found in the form of the "goodwill" that arises from the legitimate expectations of participants in a DLT network that the consensus mechanisms will be applied. Accordingly, he advocates for a *lex situs* rule that identifies "the country where the premises to which the goodwill is attached are situated".[105] He selects this rule on the following basis:

"**5.109** … Rather than assigning a fictional *situs*, the choice of law rule can be more straightforwardly, and appropriately, expressed in terms that the proprietary effects outside the cryptocurrency system of a transaction relating to cryptocurrency shall in general185 be governed by the law of the country where the participant resides or carries on business at the relevant time or, if the participant resides or carries on

[99] See FMLC (n 16) at paras 6.21-6.24; Ng (n 24) at 334-335.
[100] Ng (n 24) at 334.
[101] Ng (n 24) at 334-335.
[102] European Commission consultation (n 61).
[103] See Article 4(1) of the Proposal for a Regulation of the European Parliament and of the Council (n 56).
[104] Dickinson (n 2) at paras 5.106-5.110.
[105] Dickinson (n 2) at para 5.108.

business in more than one place at that time, by the law of the law of the place of residence or business of the participant with which the participation that is the object of the transaction is most closely connected.

5.110 The rule, so formulated, retains the advantage of being an incremental development of the common law's *lex situs* approach … It also aligns closely, although not exactly, to the European Commission's proposed rule to determine the law applicable to the third-party effects of assignments of claims and may equally be supported on grounds of (relative) predictability and ease of application in comparison with other possible choice of law solutions, suitability for transactions involving more than one type of cryptocurrency, or cryptocurrency alongside claims, or future interests in cryptocurrency and close alignment with the rules that apply in the case of insolvency."[106]

However, we would suggest that this rule is, effectively, no different from a rule based on the location of the habitual residence of the private key-holder. A person only develops the kinds of legitimate expectations described by Dickinson by virtue of being in possession of their unique private key, which is the crucial thing that allows a person to participate in the DLT network and rely upon its consensus mechanisms in the course of making transactions. The criticism may be levelled against us that, by focusing on the private key by way of a rule premised upon the habitual residence of the key holder, we are merely focusing on proxies for the actual form of intangible property. We would counter that criticism by arguing that the results are effectively the same and, moreover, a focus upon the private key-holder is a more objectively ascertainable geographical identifier than the more contestable notion of where goodwill and legitimate expectations might be located. Authors from OTC have also previously written about property being effectively a relationship between a person and a thing and this solution is focused on that relationship.[107]

As one of perhaps the most obvious contenders for a rule of applicable law, it is unsurprising that this rule has proved somewhat divisive amongst commentators. The main proponents of this kind of rule are, in effect, Dickinson and, tentatively, the LawTech Delivery Panel UK Jurisdiction Taskforce who consider that the location where a private key is stored or controlled is a particularly relevant consideration for determining the applicable law.[108] There are, however, valid criticisms of adopting such a rule of applicable law. The following are representative of such criticisms.

Criticism 1 – confusion of jurisdiction with applicable law: Whilst Ng concedes that the rule has the advantage of applying the law of the place which can effectively enforce judgment, he is of the view that this tends to confuse jurisdictional questions with applicable law questions.[109] However, this criticism is

[106] Dickinson (n 2) at para 5.109-5.110.
[107] See Hitchcock, Butler and Bell (n 67).
[108] LawTech Delivery Panel UK Jurisdiction Taskforce (n 17) at para 99(c).
[109] Ng (n 24) at 335.

misguided. There are other well-established rules of private international law which follow this kind of approach, such as the rule that the *lex situs* of bank money is the residence of the bank where the debt obligation can be enforced.[110] In any case, and whatever the coincidental advantages for effective enforcement, there is a distinct substantive justification for applying this kind of rule to cryptoassets by reference to principles of applicable law.

Criticism 2 – unpredictability of the private key-holder's location: Guillaume would dismiss this kind of rule on the basis that the location of the private key "is too random to constitute a useful connecting factor" – it is capable of being stored in a multitude of ways both online and offline that makes the application of such a rule too unpredictable.[111] However, this is merely an evidential concern and a concern which has been adequately dealt with under other legislation such as the Rome Regulations which rely on similar concepts. Moreover, such an evidential concern is misdirected in relation to our particular rule, given that our rule would apply the law of the private key-holder's primary habitual residence. The storage of the key is not necessarily relevant to answering that question and the degree of unpredictability is consequently reduced.

Criticism 3 – lack of uniformity leads to artificially splitting up the ledger: The FMLC point out that this rule has the disadvantage of artificially splitting up the distributed ledger record in such a way that different laws would apply to different transactions involving different participants, given that the location of their private keys will vary widely.[112] However, Dickinson rightly responds to this criticism by emphasising that this rule of applicable law only applies to fact patterns external to the DLT network and, therefore, in no way compromises the integrity of the ledger and the DLT network's consensus mechanisms.[113] Furthermore, as we have already discussed above, Dickinson has a valid point that the advantages of a uniform applicable law in respect of all cryptoassets for each DLT network are superficial in this particular context and that applicable law rules should not pursue uniformity at the expense of producing outcomes with which neither affected parties nor the transactions in question have a close connection.[114]

Criticism 4 – lack of uniformity makes the rule time consuming and costly to apply: Relatedly, Ng criticises the rule as undesirable because it results in a "shifting governing law for property issues depending on the underlying fact pattern, leading to uncertainty and increasing transaction costs".[115] He gives the example

[110] Ng (n 24) at 327, citing *F & K Jabbour v Custodian of Israeli Absentee Property* [1954] 1 WLR 140.
[111] Guillaume (n 8) at 63.
[112] FMLC (n 16) at para 6.22.
[113] Dickinson (n 2) at para 5.112.
[114] Dickinson (n 2) at para 5.112.
[115] Ng (n 24) at 335. The FMLC also raises this concern: FMLC (n 16) at para 6.24.

of a bank taking security over a borrower's cryptoassets having to consider the laws of the borrower's residence, investigate the borrower's exchange's holding structure and also possibly the laws of the exchange's place of incorporation. In the event of the intervention of a third-party bad faith actor in a hacking scenario, the bank would also become subject to the laws of the residence of an unforeseeable third-party recipient from the hacker. We concede that the concerns about increased costs incurred in undertaking investigations and instructing legal opinions will be valid in some cases. However, as Dickinson notes, the most common case will involve transactions to which the relevant litigants are parties, and which will usually be documented in writing.[116] In any case, cost considerations can only ever be subsidiary to the substantive advantages and disadvantages of a rule of private international law and we are of the view that the substantive advantages outweigh issues of cost.

Criticism 5 – change in habitual residence: The FMLC also criticise the rule because it will often give no clear answer to questions of entitlement in circumstances where there is a change of habitual residence between transactions.[117] However, we agree with Dickinson's response that such situations are likely to arise only in a minority of cases and are, in any event, not insurmountable.[118] He suggests the use of either a tie-break rule along the lines proposed by the European Commission in Article 4(1) of its proposal governing the third-party effects of assignments of claims.[119] Alternatively, he recommends "resolving questions of priority by reference to the law of the participant's place of residence etc. at the time of the later of the two transactions (on the basis that no question of priority can have arisen before that time)".

Criticism 6 – joint transferors and chains of transaction: The FMLC's next criticism is that the rule will also often give no clear answer to questions of entitlement in cases involving joint transferors or chains of assignment.[120] Closely related is the FMLC's criticism that one key may be made up of several components held across multiple jurisdictions, potentially by different people.[121] These are admittedly the most difficult problems with which our proposed rule has to contend, however, again, with careful thought there is no reason why these problems are insurmountable. Dickinson suggests that "the proposed rule could be applied to joint transactions involving participants resident or carrying on business in more than one country in the same way as it would apply to a single participant residing or carrying on business in more than one country, by identifying the place of residence or business with which the participation is most

[116] Dickinson (n 2) at para 5.114.
[117] FMLC (n 16) at para 6.22.
[118] Dickinson (n 2) at para 5.115.
[119] Proposal for a Regulation of the European Parliament and of the Council (n 56).
[120] FMLC (n 16) at para 6.22.
[121] FMLC (n 16) at para 6.23.

closely connected".[122] In other words, it is only at this point when the primary rule is stretched to its limits that a court should rely upon a residual fallback "closely connected" rule akin to the fallback position under, for example, Rome I, Article 4(4) where none of the other rules under Rome I are applicable, and also under the English common law rule that applies in the absence of party choice.[123] Such a rule could also conceivably be applied to a private key made up of several components held across multiple jurisdictions, potentially by different people. As for the problems of chains of assignment, Dickinson is right to suggest that any difficulties can be overcome by the parties precisely identifying the factual issues and considering the proprietary effects of each transaction in turn according to the applicable law at each stage.[124]

3(c)(ii) – Issues involving contract law

Compared with issues of property law, the applicable law rules for issues involving contract law are much more straightforward. As Dickinson points out, contractual relationships involving cryptoassets are not fundamentally different from ordinary contracts and the ordinary applicable law rules can be applied relatively straightforwardly.[125] For example, where cryptoassets are kept in an online platform such as an exchange, and the owner of the cryptoassets suffers loss, the extent to which they are entitled to compensation from the company which hosts the exchange will essentially be governed by the applicable law rule which applies to the contractual user agreement.[126] The fact that the subject of the user agreement concerned cryptoassets should not change that analysis.

It remains open to parties to those contracts to agree to a choice of law under Article 3(1) of Rome I. Similarly, many of the special rules provided for under Rome I are likely to apply in similar fashion. There do remain some outstanding questions, such as whether a contract for the transfer of tangible goods in exchange for cryptocurrency is a contract for the sale of goods within Article 4(1)(a).[127] No doubt the currently developing case law on the characteristics of cryptoassets will assist with answering these questions.

[122] Dickinson (n 2) at para 5.116.
[123] See, for example, Ng (n 24) at 336-338. Ng advocates adopting this "closely connected" rule as the primary rule of applicable law for cryptoassets, although we are of the view that such a test is generally adopted as a fallback test for a reason, namely its inherent vagueness, subjectivity and contestability of application, especially in the context of the decentralised, distributed and anonymous nature of DLT networks. Specific, bright line rules such as the one we adopt in this article are preferable.
[124] Dickinson (n 2) at paras 5.117-5.118, where he also provides a worked example of how this might work in practice.
[125] Dickinson (n 2) at para 5.09.
[126] Guillaume (n 8) at 64.
[127] See the discussion by Dickinson (n 2) at para 5.10.

3(c)(iii) – Issues involving tort law

The default rule that applies to torts under the Rome II Regulation can be found in Article 4(1) which provides that the applicable law "shall be 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". Such a rule is often referred to as a rule of *lex damnum*. We are of the view that such a rule is capable of relatively straightforward application to cryptoassets. Such a rule will render a similar outcome in terms of applicable law to our proposed rule for dealing with property law issues. This is because the direct damage will most often take the form of damage to the goodwill generated by the legitimate expectations in the DLT system,[128] the most helpful objective proxy for which is the primary habitual residence of the private key-holder.

Dickinson reaches a similar conclusion by way of analogy with unfair competition cases involving cartels, in which the CJEU has made clear that "the place where the damage occurred is the place where the alleged damage actually manifests itself".[129] Accordingly, he concludes that it is perfectly possible "to ascribe a location to damage suffered by affected participants within the system by reference to their habitual residence or relevant place of business, which is where the consequences for them" of the tort are manifested and felt[130]. In that light, we agree with Dickinson that it should be no more difficult to locate the damage of a tort in cases involving cryptoassets than in other contexts.[131]

To that end, we disagree with Guillaume's pessimism about the applicability of traditional private international law rules to actions in tort and her conclusion that the traditional rules are simply not suited to DLT.[132] She dismisses the adoption of a *lex damnum* rule to cryptoassets on the basis that such a rule essentially equates to identifying the location of the victim's private key, being the part of the DLT system that provides the most individualised link between the cryptoasset and the victim and which represents a helpful proxy for the location of the goodwill generated by the legitimate expectations in the DLT system that will constitute the actual damage suffered.[133] We have already dealt with Guillaume's rejection of rules relating to the private key in the context of issues of property law due to problems of geographical

[128] We use the term legitimate expectation here, as set out above, to mean a legitimate expectation, founded on technological features of the DLT system, that the consensus rules which underpin the system will be applied and will not be altered fundamentally such as to deprive each participant of the association to particular units within the system and the power to deal with those units.
[129] Dickinson (n 2) at para 5.12, citing Case C-352/13, *Cartel Damage Claims Hydrogen Peroxide SA v Evonik Degussa GmbH* [2015] ECLI:EU:C:2015:335 at paras 51-53.
[130] Dickinson (n 2) at para 5.12.
[131] Dickinson (n 2) at para 5.11.
[132] Guillaume (n 8) at 64.
[133] Guillaume (n 8) at 64.

uncertainty and unpredictability. She rejects an approach to tort issues based on *lex damnum* for the same reasons; our arguments in response apply equally here.

4 – On-platform assets with tethered off-platform assets

Where a cryptoasset has been 'tokenised' and tethered to a real or convention asset outside of the DLT a separate analysis is appropriate.

4(a) – Jurisdiction

It seems to us that the analysis regarding the jurisdiction of English courts will be similar to that set out above. Defendants to actions will be individuals with a domicile. Breaches of contract will involve individuals or consumers who will have a domicile. Tortious actions involve real persons who exist in the real world and will give rise to harmful effects in similar fashion to torts not involving cryptoassets.[134] Whatever evidential issues may exist, both the event giving rise to damage and the damage itself will be felt by an individual, most often the private key-holder, with a habitual residence or relevant place of business.

4(b) – Applicable law

The debate regarding on-platform assets with tethered off-platform assets and applicable law is also relatively straightforward. The same conclusions set out above for contract and tort law in respect of purely on-chain assets apply equally to on-platform assets with tethered off-platform assets.

The central question in relation to which a tethered off-platform asset will make a difference concerns proprietary issues and whether it makes sense to adopt the private international law rule that governs the on-platform cryptoasset – such that there is no difference in treatment between purely on-platform assets and on-platform assets with tethered off-chain assets – or whether, instead, to adopt the private international law rule that governs the tethered off-chain asset. The latter approach might perhaps best be coined as '**derivative *lex situs***', given that the applicable law which governs the on-platform asset will be derived from the tethered off-platform asset and the general private international law rule for such proprietary issues is the *lex situs* rule.

This raises the crucial distinction between DLT networks where the ledger/on-platform asset is constitutive of title as against being only dispositive of title. If the ledger/on-platform asset is constitutive this means that it is the DLT system which is determinative of what happens. For example, the transaction between

[134] Dickinson (n 2) at para 5.11.

participants involving the off-platform asset only takes effect by virtue of the transaction between the same participants within the DLT system. Alternatively, title to and interests in the off-platform asset is determined by the transactions that occur within the DLT system. Another example is where the existence of the off-platform asset is itself created by, and only exists by virtue of, transactions that occur within the DLT system, such as a debt. In such cases, the off-platform asset's existence and status is not wholly independent of the DLT system. By contrast, if the ledger/on-platform asset is only dispositive, this means that the DLT system serves purely as a means of recording the transaction – the ledger/on-platform asset is only reflective of transactions, title, interests and assets that have an independent existence in the "real world".[135] In such cases, the off-platform asset has an existence which is wholly independent of the DLT system.[136]

We agree with the FMLC's proposed solution on this issue, or at least what their proposed solution appears to be given that it is not entirely clear what they mean when they refer to the DLT network being dispositive. The FMLC conclude that where the DLT arrangements purport only to be dispositive, then "it appears unlikely that a court will apply any law other than the *lex situs* of the underlying asset".[137] In other words, the applicable law should be governed by the traditional private international law rules that apply to property, which is generally *lex situs*.[138] This is because when an off-platform asset is wholly independent of the DLT system, it is the off-platform asset and the "real world" interactions which are determinative. There is no justification for applying anything other than the normal rules of private international law. However, where the DLT arrangements purport to be constitutive, it is the ledger/on-platform asset which is determinative and the off-platform asset, whilst still important to the participants, is only incidental to the transaction. In such circumstances, there should be no difference in treatment between cases involving a purely on-platform asset and cases involving a tethered off-platform asset.

5 – Conclusion

The above article has sought to demonstrate how existing private international law regimes may be applied to cryptoasset litigation. It is our view that the difficulties, once broken down and analysed using an appropriate methodology, can be overcome. Whilst a single international regime outlining the private

[135] FMLC (n 16) at paras 6.3 and 7.8.
[136] FMLC (n 16) at para 7.8.
[137] FMLC (n 16) at para 4.8
[138] FMLC (n 16) at paras 6.3 and 7.8. The LawTech Delivery Panel UK Jurisdiction Taskforce, whilst not coming to a concluded view on what applicable law rules should apply to cryptoassets, also consider that the location of any relevant off-platform or off-chain asset is a particularly relevant factor to determining what the applicable law should be in any given case: LawTech Delivery Panel UK Jurisdiction Taskforce (n 17) at paras 95 and 99(a).

international law treatment of cryptoassets would be welcome, it is at the present time, aspirational. In the meantime, a pragmatic application of our existing regimes is achievable. The key is not to be unduly distracted by the complexities of unfamiliar technology when most cases still involve real people in real places. When that point is borne in mind, the existing rules can be made fit for purpose so that our courts can apply them to this fast-developing area of the law.

Chloë Bell
Chloe.Bell@outertemple.com

Joshua Cainer
Joshua.Cainer@outertemple.com