Bar Council response to the Law Commission Call for Evidence on Digital Assets and Electronic Trade Documents in Private International Law

1. This is the response of the General Council of the Bar of England and Wales (the Bar Council) to the Law Commission's Call for Evidence on Digital Assets and Electronic Trade Documents ("ETDs") in Private International Law.[1]

2. The Bar Council represents approximately 18,000 barristers in England and Wales. It promotes the Bar's high-quality specialist advocacy and advisory services; fair access to justice for all; the highest standards of ethics, equality and diversity across the profession; and the development of business opportunities for barristers at home and abroad.

3. A strong and independent Bar exists to serve the public and is crucial to the administration of justice. As specialist, independent advocates, barristers enable people to uphold their legal rights and duties, often acting on behalf of the most vulnerable members of society. The Bar makes a vital contribution to the efficient operation of criminal and civil courts. It provides a pool of talented men and women from increasingly diverse backgrounds from which a significant proportion of the judiciary is drawn, on whose independence the Rule of Law and our democratic way of life depend. The Bar Council is the Approved Regulator for the Bar of England and Wales. It discharges its regulatory functions through the independent Bar Standards Board (BSB).

4. This response focuses on key themes raised by the Call for Evidence, with reference to individual questions where possible.

[1] Call for Evidence.

I. Specific Issues on International Jurisdiction

Q1: Consumer Contracts

5. We consider that jurisdiction over consumer contracts with international crypto firms, such as international exchanges, can be accommodated readily by section 15B of the Civil Jurisdiction and Judgements Act 1982. We agree that the test for considering whether a crypto firm has "pursued" or "directed" activities in the UK should be the same as that which applies to other cross-border consumer contracts.

6. However, as set out below (in response to Question 8) it may be helpful if the factors relevant to the determination of this issue by English courts were set out *explicitly* in legislation. A non-exhaustive list of relevant factors would serve the interests of legal certainty and consistency of judicial decision making.

Q2: Contracts Concluded in England and Wales

7. The relevant connecting factor is the person, legal or otherwise, who has undertaken the contractual obligation. That that person has entered into that obligation at some point in the past through a particular mechanism, here a computer, is irrelevant. There is no justification for treating smart contracts differently in this regard from any other contract.

8. The "location" of the real-world actor is not the relevant test for para 3.1(6)(a) but rather whether the contract was either made within the jurisdiction or concluded by the acceptance of an offer, which offer was received within the jurisdiction. Neither of these gateways is necessarily determined by the location of the counterparty, either at the time of contracting or subsequently.

9. It is unlikely that the automatic mechanism by which parties become subject to legal obligations by virtue of smart contracts gives rise to any new difficulties. Although some smart contracts (particularly those based solely on computer code) within DLTs may cause complexities in determining the 'jurisdiction within' which the contract is made or offer received, as the transactions may be between parties located remotely is different jurisdictions (or even in transit), and executed by self-executing code by pre-determined protocols within the DLT network, is it likely to be determined by the courts on the actual facts of the case and the use of analysis tools to determine the proposed claimant's location of where the offer was

received. Further, with the likelihood of future safeguards by regulators, and parties requiring more compliance and trustworthy platforms, governing laws are likely to be agreed within the consensus network and placed in the code.

10. In cases of digital asset claims involving fraud allegations, the main argument may be based on whether the purported contract is genuine or a sham. For instance, in *Mooij v Persons Unknown* (2023)[2], which dealt with cryptocurrency fraud, the primary contention was that the agreements were fraudulent and therefore not valid contracts. Despite this argument, the claimant attempted to rely on contract gateway 6(a). The judge tentatively accepted this reliance, inferring that the contracts were made in England based on English names, language, and some evidence of English telephone numbers. However, since the claimant's main argument was that no valid contract existed due to fraud and lack of consideration, the court allowed the claimant to alternatively rely on gateway 8.

Q3: Damage or Detriment in England and Wales

(1) Approach to Localising Damage or Detriment

11. We consider that the approach of courts to localising damage or detriment under the jurisdictional gateways to have been essentially sound, and that the differences are perhaps not as great as suggested at 5.42 of the Law Commission's Paper. In essence, all cases have taken the starting point for place of damage to be the place where the relevant cryptoassets were "located" through the residence[3] of their owner immediately prior to the tort.[4] Most cases

[2] *Mooij v Persons Unknown* [2023] EWHC 3328 (Comm) at para [20].

[3] We consider that the use of "domicile" has been infelicitous, and that the difference has been resolved correctly in favour of habitual residence: see *Tulip Trading Limited v. Van Der Laan an* Others [2022] EWHC 667 (Ch) at [140]-[148] (which was the only case to date in which the difference appears to have been material). Butcher J seems to have corrected his infelicitous use of the word "domicile" in Ion Science, in LMN v Bitflyer Holdings [2022] EWHC 2954 [20].

[4] *Ion Science* at [13] (as one of a number of alternative options); *Lubin Betancourt* at [11]; *D'Aloia* at [20]; *Jones* at [30]; *Fetch.ai* at [19]. Although the final decision in *TTL* was on the basis of control, this was likely due to the somewhat unusual fact that the cryptoassets had not yet been wrongfully transferred. In any event, this analysis proceeded from the finding already made that the location of the cryptoassets was in England and Wales, as per Professor Dickinson's principle (at [140]-[148]; [159]). *AA* was an exception, as the claimant insurer did not own the relevant cryptoassets prior to the wrongdoing. The identified location of the damage was therefore the bank account from which the purchase pursuant to the ransom demand was made (at [68]), although we suggest that an alternative analysis based on the location of the cryptoassets during their brief period of ownership by the claimant prior to transfer would have produced the same result under the residence test (perhaps similar therefore to the alternatives set out in *Ion Science*).

have referred directly to Professor Dickinson's view to this effect[5] or at least to prior authority which has so done, and there is accordingly some consistency in approach[6].

12. However, the Law Commission is right to note that other locational factors have also been relied upon. These include the locations of misrepresentations, of the cessation of control over a computer, of deprivation of access, and of loss of control of the asset itself. In almost all cases, these features have been coincident with the location of the owner's place of residence prior to the wrongdoing, and there has been no obvious competitor locus. To that extent, we do not consider that reliance on these factors has been central to the decision-making and note that in the one case where all locational elements were not coincident (*Lubin Betancourt*), factors outside the owner's place of residence were regarded by the judge as irrelevant (at [22]).

13. We consider that this is an inconsistency in the jurisprudence to date, and that the approach in *Lubin* should and will likely prevail in future cases where other more tangential factors are in a different location from the habitual residence of the claimant. There is no clear basis in logic or principle for the place of, for example, misrepresentation or of cessation of control of a given device to found the *locus* of any significant, let alone all, damage; certainly not to defeat an otherwise accepted principle for determining the location of the wrongly appropriated asset itself, and therefore the place where loss of that asset will be experienced. Similarly, factors such as the location where any loss of control would be felt are almost invariably likely to be coincident with the geographic "location" of the cryptoassets by reference to the owner's place of residence.

14. It is of course conceivable that technical evidence could challenge Professor Dickinson's proposition, or that unusual facts could require a different analysis. Even these few early cases demonstrate that the modes of fraud and misappropriation in cryptoasset litigation are protean. Overall we are of the view that the law can in most cases do no better than to recognise an essential starting point for *locus damni* based on the location of the

[5] We recognize that the "location" of cryptoassets is a deemed legal fiction, but we consider that the basis of Professor Dickinson's rule accords with common and legal sense. This is consistent with Professor Lutzi's view that the focus should be on the parties rather than the asset, but we disagree with his proposal that the locational anchor should be the place where the party committing the alleged tort was based.

[6] The decided cases so far have all been dealing with urgent without notice applications, and only had to consider whether there was a sufficiently arguable case.

Claimant's habitual residence. We set out below - in our response to question 5 - a proposal for a more open textured approach to the jurisdictional gateway for the cases in which this reasonable starting point might be displaced.

(2) Pure Economic Loss

15. We do not consider that the caution sounded by Lord Lloyd-Jones in *Brownlie II* in relation to pure economic loss is likely to be particularly relevant for the jurisdictional gateway for tort in cryptoasset claims. This is so even though we agree that the facts of cases to date have not alleged damage to the cryptoassets themselves, but deprivation of access to them.[7] We are of the view that the "pure economic" characterisation of the loss does not entail locational remoteness from any "immediate" or "direct" damage in the way seen in the cases cited in Brownlie II, and therefore does not cause comparable issues for the jurisdictional gateways.

16. First, Lord Lloyd-Jones rightly cautions that the cited cases proceed on the "erroneous assumption that the domestic tort gateway should be interpreted in line with the special rule of tort jurisdiction under the Brussels system and fail to appreciate the fundamental differences between the two systems" (at [74]). We agree with this and observe that the effect is that a narrower approach to the definition of damage is adopted in most of these authorities than may in fact appropriate under gateway 9. This is explored further below when considering CJEU cases (which we do not consider to be relevant to the jurisdictional gateway analyses).

17. Secondly, we do not consider that the "pure economic" nature of cryptoasset claims causes issues of geographic remoteness in the ways canvassed in the cases cited in *Brownlie II*. For claimants habitually resident in England and Wales, their cryptoassets will invariably be considered to be "located" in England and Wales, absent any challenge to Professor Dickinson's rule. There is not therefore the tension seen in cases where the investment was made abroad, or where the goods went missing abroad, and the only damage link to England and Wales was the loss to English bank accounts. There seems to be no competitor locus for

[7] Others may be better placed to comment on whether partial damage could conceptually be possible with cryptoassets, but we have seen no convincing evidence or examples of any such scenario (and note the difficulties with such a proposition explored in Hin Liu's "*Interference Torts in the Digital Asset World"*).

more immediate damage, other than the omni-territorial nature of the assets, the effect of which has been effectively neutralised by Professor Dickinson's rule. The analysis in a cryptoasset case would plainly be different, for example, from Bastone v Nasima Enterprises (Nigeria) [1996] CLC 1902, where the locus was held to be Nigeria because that is where the relevant goods were lost, and it was only the financial consequences that were felt in England. In all the cases seen to date, the cryptoassets have gone missing from their English "location", which is the same place that the financial loss is experienced.

18. Overall, unless there is a meaningful legal or technical challenge to Professor Dickinson's principle on the "location" of cryptoassets, we consider that their omni-territorial nature in fact is unlikely to be of significant relevance to any locus analysis. They have, in effect, a deemed legal location by reference to the owner's place of residence, and the analysis can then proceed in the ordinary way.

Q4: Unlawful Act Committed in England and Wales

19. The courts cannot to date be said to have taken a theoretically robust approach to the question of where an unlawful act is committed in the context of crypto litigation.

20. In ***Ion Science v. Persons Unknown*** the Court concluded that the claimants had sustained damage as a result of acts committed in England and Wales. The acts in question were *"the making of representations, the transfer of funds, and the granting of remote access to [the second claimant's] computer in England"*. There is very little reasoning to support this conclusion. It appears that the Court essentially took the view that because the second claimant (and the second claimant's computer) was in England when the relevant acts were committed, it meant that the acts were committed in England. While such an approach appears broadly sensible on the facts of this case (in so far as they are known), it is doubtful that it has the necessary theoretical depth to deal with other, more complicated, scenarios. For example, what would the position be if an individual granted remote access to a computer in England when he was himself outside England, or to a computer outside England when he was in England?

21. In ***Jones v. Persons Unknown*** [2022] EWHC 2543 (Comm.) the Court concluded that the claimant had sustained damage as a result of acts committed in England and Wales: see paragraph [31]. The Court does not appear to have engaged substantively with the question

of where the relevant acts were committed. Rather it simply seems to have asserted that they were committed in England. Contrary to what is suggested at paragraph [5.69] of the Call for Evidence, it is not clear to us that the Court did conclude that the victim's domicile in England was its reason for thinking that the relevant acts occurred in England. But even if that is what the Court decided, it seems to us that the approach of focussing on the victim's domicile (as distinct from place of residence) would have little to recommend it. At least in principle it is possible for a person to be domiciled in England and Wales while being outside the jurisdiction, and potentially having been so for many years. While we understand that the location of the victim could in an appropriate case be relevant to the question of where the unlawful act is committed (or where the object/damage was located), we doubt that it is helpful to use the concept of *domicile* in this regard.

22. Accordingly, our view is that the courts have not so far taken an approach which is theoretically robust in ascertaining where unlawful acts in crypto litigation have occurred. To the extent that the focus in ***Jones*** was on the victim's domicile, consider this may be unhelpful. The approach apparently adopted in ***Ion Science*** has more to recommend it but seems unlikely to be sufficiently sophisticated to deal with the more subtle or complex problems in relation to the issue of where the unlawful act occurred.

Q5: Objects in England and Wales

23. As identified in the Law Commission's paper, the approach of the English courts to Gateway 11 for proprietary claims has not been entirely consistent. However, the essential test that can be distilled from the caselaw is as follows: was the owner of the cryptoassets resident in England and Wales at the time when the cryptoassets were misappropriated?

24. We consider that, on the facts of the reported cases, this approach is not only theoretically sound but practically necessary:

a. Given the "omni-territorial" nature of crypto assets it makes little sense for the Court to enquire as to the location of the property itself (either at the time of misappropriation or the time of the application for service out).

b. Where the asset has a meaningful *corporeal* form, it makes sense to say that the country with jurisdiction is the country in which the asset is presently situated. This is because only

the courts in that country have the necessary sovereign authority to enforce a change in property entitlement. However, this justification for such a rule falls away for cryptoassets that are "omni-territorial".

c. The approach of the courts in England is broadly consistent with the approach suggested by Professor Dickinson[8]. As explained in the Law Commission's papers, Professor Dickinson conceptualizes cryptocurrencies as intangible property arising from the participation of an individual or entity in a DLT system and therefore suggests that the law governing a particular "participation" should be that of the place of residence or business of the relevant participant with which that participation is most closely connected.

d. As demonstrated by the reported cases before the English courts, the owners of the crypto wallets who have misappropriated the claimant's crypto assets will often remain unknown. It may therefore be impossible identify the place of residence of the relevant defendant. It is for that reason that the defendants are referred to as "persons unknown" The practical reality may be that there may be *no practical alternative* to an English court asserting proprietary jurisdiction on the basis of the claimant's place of residence or domicile.

Alternative Basis for Jurisdiction

25. However, the principle applied by the English court may not be appropriate in *all* factual scenarios. Situations in which the principle may be less appropriate might include (for example):

a. Where the misappropriated cryptoassets tokenize or record the ownership "real world assets" that have a physical presence in a third country (other than England and Wales); or

b. Where cryptoassets on a private/permissioned DLT system have some centralized control in a particular third country (other than England and Wales);

26. In these situations, it may be more appropriate for proprietary disputes to be determined by the country in which the physical assets are situated or where centralized control resides. That is because the courts in that country will have the necessary jurisdiction and power to compel return of the property to its rightful owner.

[8] Cryptocurrencies in Public and Private Law, 2019, para. 5.109 – referred to in the Law Commission's own paper at 5.85.

27. Another point is that appropriate account should be given to the various ways in which cryptoassets and interests in them can be held. So, for example, different rules may be appropriate when assets held in trust, and (as is not uncommon) where there are unascertained co-ownership interests in a pooled accounts held on an exchange (cf Re GateCoin Ltd (In Liquidation) [2023] HKCFI 914) (where one might expect that the location of the exchange's register recording the extent of each interest would be significant).

28. It is also the case that the location of the beneficial owner, and the location of the relevant crypto "participant" might not be the same. In *STEP Guidance Note: Location of Cryptocurrencies – an alternative view (2021)* the authors note this and add, "in the case of cryptocurrency, it can only be dealt with by the use of the private key and, arguably, its location should therefore be linked to the location of the private key or of the person who has control of the private key (who may or may not be the beneficial owner)." In other words:

> *there will be situations where cryptocurrency is not held directly by the beneficial owner but, instead, is held on behalf of the beneficial owner by a third party such as a cryptocurrency exchange, trading platform, nominee, trustee or custodian.*
>
> *…*
>
> *It will be the residence of the third party, being the participant in the cryptocurrency system and the holder of the private key that will determine the location of the cryptocurrency. The residence of the beneficial owner will be irrelevant assuming the beneficial owner is not the holder of the public address with which the relevant units of the cryptocurrency are associated and is not the holder of the private key that allows transactions in respect of those units to be authorised.*

29. Accordingly, in propriety disputes concerning cryptoassets we consider there to be an argument for reforming the law in line with the proposals of the UKJT's Legal Statement on Cryptoassets.[9] We propose a new discretionary gateway for proprietary claims involving crypto assets. The factors to be determined by the Court in considering whether to grant leave to serve out of the jurisdiction could include:

a. Whether any relevant off-chain asset is located in England and Wales;

b. Whether there is any centralized control over the cryptoasset in England and Wales;

[9] Paragraph 99, referred to in *Tulip Trading* at para. 148.

c. Whether a particular cryptoasset is controlled by a particular participant in England and Wales (because, for example, a private key is stored here), or was controlled by such a participant before the justiciable act occurred;

d. Whether the law applicable to the relevant transfer (perhaps by reason of the parties' choice) is English law.

30. We consider that such an approach would strike the correct balance between principle, pragmatism and flexibility.

Q6: Types of Claims and Causes of Action

(1) <u>Constructive Trustees</u>

31. Although *Piroozzadeh v Persons Unknown* represents the current law on whether exchanges are constructive trustees, there are reasons to doubt whether it is the final word.

32. The first question is whether cryptoassets are constituted by rights, with correlative duties, capable of being held on trust. The current consensus is that they are, at least for the purposes of freezing orders.

33. Second, and more problematically, are exchanges "*bona fide* purchasers"? When the exchange obtains the cryptoasset, it undertakes to hold equivalent rights for its customer. It was this undertaking that Trower J considered to constitute a purchase, so that a constructive trust would not arise.

34. However, orthodoxy is that a mere promise or undertaking does *not* constitute a good faith purchase so as to give protection from holding rights obtained on trust. The promised consideration in exchange for the right received must not only be paid but paid in full (*Story v Windsor* (1743) 2 Ark 630, 26 ER 776).

35. The rule in relation to cash is quite different. Title to cash is lost if an innocent recipient gives a mere promise in exchange for it (Bills of Exchange Act 1882, s 27(1), 38(2)). This has historically been very important for the protection of banks who have innocently received cash that was held on trust. As cryptoassets are not cash within the meaning of the legislation, a mere promise should not, according to orthodoxy, suffice for purposes of the bona fide

purchase rule. This issue will therefore have to be revisited and must be considered to be in a state of uncertainty.

II. Applicable Law – Non - Consumer Contracts

Q7: Applicable Law and Decentralised Finance

36. We agree that contractual disputes, in the context of DeFi, are not likely to come before the courts with great regularity for the reasons given in paragraph 7.24 of the Law Commission's paper. Resort to litigation will generally be rendered unnecessary because smart contracts execute automatically without the need for human intervention. Moreover, redress is also built into many DeFi protocols. For example, lenders may be protected by automatic liquidation of collateral if a borrower fails to repay or if the value of the borrower's collateral falls beneath a liquidation threshold. Furthermore, even if a party wished to litigate their "counterparties" – other users of the protocol - are likely to be either anonymous or untraceable. In DeFi lending and borrowing typically occur through protocols that create pools of capital. These pools are funded by users who deposit their assets into the protocol.

37. However, it is not impossible – in future – that users of DeFi protocols may wish to resort to litigation. As noted by the Law Commission this could conceivably occur if the underlying code did not perform as intended or where it did not operate as the end user of the protocol expected. Access to decentralized DeFi protocols is often accessed via web interfaces or "frontends" provided by crypto firms. Firms which provide such frontends may charge a fee to users for accessing the underlying smart contract in this way[10]. The use of frontends or web interfaces will usually be subject to detailed terms and conditions of use[11]. Accordingly, there may well be identifiable legal persons against whom actions for breach of contract could be brought.

38. We do not comment here on the viability or merits of contractual claims against companies who provide front-ends or web interfaces to DeFi protocols. Firms that provide

[10] Although, given the decentralized nature of smart contracts on permissionless blockchains it is always possible to access the underlying protocol without using any particular frontend.

[11] See for example: https://aave.com/term-of-use/

such interfaces would be likely to argue that they do not control or own, and are not responsible for, the operation of the code comprising the underlying DeFi protocol. Such code runs in an autonomous and decentralized manner on-chain. We note that the published terms and conditions for using DeFi frontends typically contains explicit disclaimers to that effect and makes it plain that engagement with the protocol is at the user's own risk. However, it is not impossible that in the future, users of DeFi protocols may seek to test the limits of contractual liability in this context.

39. We note the provisional view of the Law Commission (para. 7.26) that in the event that a party were able to litigate the relevant analysis would be that for contracts concerning the exchange of crypto-tokens for crypto-tokens. However, we note that the Law Commission's analysis under this heading (at paras. 7.67 to 7.74) relates to *non-consumer* contracts. We consider it to be arguable that Article 6 for consumer contracts would be a better fit. Those who access DeFi protocols will often be retail consumers. It may also be argued that the defendant (e.g., the company that provides the DeFi "frontend") is pursuing or directing commercial activity in the retail consumer's country of habitual residence. The application of Article 6 would mean that contractual claims by English/Welsh retail consumers would ordinarily be tried in England and Wales (and not, for example, in the country of the company which provides the frontend).

Q8: Applicable Law and Non-Consumer Contracts

40. We consider that further clarity is required in respect of scope of Article 4 (1) (h) of Rome I. In particular, the question arises as to whether and to what extent this applies to online crypto exchanges marketing to UK retail consumers. We note that the Law Commission proceeds on the basis that – under the current law – such exchanges could be within the scope of Article 4 (1) (h)[12]. The consequence would be that choice of law is determined by the exchange itself pursuant to its terms and conditions of use.

41. We consider that this would not necessarily be desirable given that centralized exchanges provide the main "on-ramp" for retail consumers into crypto. Retail consumers are plainly in a weaker bargaining position as compared to centralized exchanges. It may

[12] See para. 7.34 and 8.55.

therefore be more appropriate for the relationship between retail consumers and centralized crypto exchanges to be governed by the law of the England and Wales in accordance with Article 6. We consider that the exclusion of Article 6 in respect of financial instruments should be narrowly construed (see our comments on consumer contracts below).

42. In respect of non-consumer contracts generally, we agree with the Law Commission's overall conclusion that there are no particular problems in applying conventional principles to decide the applicable law for non-consumer contracts involving crypto tokens.

III. Applicable Law – Consumer Contracts

Q9: Applicable Law and Consumer Contracts

General Observations

43. A central issue raised by the Call for Evidence concerns the scope of the protection afforded by Article 6 of Rome I concerning consumer contracts. This gives rise to a general rule (subject to exceptions) that consumer contracts will be governed by the law in the consumer's place of habitual residence.

44. Given the international nature of the crypto industry, issues in respect of Article 6 may well arise in respect of contracts between English consumers and crypto exchanges located outside of England. We consider that the following factors should inform any reform of the law in this area:

45. First, there is a clear public interest in ensuring high standards protection for UK retail consumers entering into contracts with crypto exchanges situated overseas. This is consistent, for example, with the approach to consumer protection under the UK's Financial Promotions Regime for crypto assets[13]. We therefore consider that the protections afforded by Article 6 should be interpreted broadly and the exclusions narrowly.

46. Second, we consider that there is a public interest in ensuring legal certainty and consistency: both for consumers and the crypto industry. It is apparent from the Law

[13] https://www.fca.org.uk/publications/fg23-3-finalised-non-handbook-guidance-cryptoasset-financial-promotions.

Commission's paper that the scope of Article 6 has been interpreted by the CJEU in ways which are not obvious from the language of Rome I. There is therefore scope for further clarification of English law in order to: a) provide greater clarity as to the scope of Rome I; and b) to ensure that it is applied consistently by English Courts.

"Crypto Traders"

47. Further statutory clarification of when "crypto traders" will be treated as consumers for the purposes of Article 6 would be helpful. It is not clear from a natural reading of Article 6 that private individuals that make a living from crypto trading might nonetheless be treated as "consumers" for the purposes of Article 6[14].

48. However, the CJEU's case law suggests that "crypto traders" will not lose the status of consumer merely because (for example) they make large trades, make a significant number of trades or risk significant financial loss. On the other hand, they may lose consumer status if (for example) they incorporate as a company, deal of behalf of others or give the impression that they are acting as "professionals"[15].

49. It may be helpful if the criteria that govern whether "crypto traders" should be treated as consumers for the purpose Article 6 were set out more explicitly in a statutory instrument. This would enhance legal certainty both for crypto traders and for the overseas exchanges with whom they contract. It would also serve the interest of ensuring greater consistency in decision making by English Courts.

When does a firm "pursue" or "direct" activities in England and Wales?

50. Article 6 bites only where a professional is "pursuing" or "directing" their activity in a consumer's country of habitual residence. However, it is not obvious what this means from the language of Article 6. We note that according to the case law of the CJEU, the protections do not apply merely to firms that *market* directly to UK consumers. They go much wider and

[14] We note that there is some English authority on the extent to which wealthy crypto-traders can nevertheless be consumers: Ramona Ang v Reliantco Investments Limited [2019] EWHC 879 (Comm)
[15] See conclusion at 8.33 and 8.34 of the Law Commission's paper.

could include where (for example) a company's website simply 'manifests an intention' to establish relations with UK consumers by accepting payment in sterling[16].

51. It would be in the interests of legal certainty, for both consumers and international firms, if there was greater statutory clarity as to the relevant factors that govern the application of Article 6. This would also help to achieve greater consistency in decision making by English courts.

52. We also consider that consideration should be given to harmonizing the language used in Article 6 with that used in the Financial Promotions regime for crypto assets. For the purpose of section 21 of the Financial Services and Market Act 2000, financial promotions will come within the regime where qualifying communications are "capable of having an effect in the United Kingdom" (s. 21 (3)). One option would be to legislate so as clarify that any firm that comes within the scope of the financial promotions' regime is also within the scope of Article 6 (subject to any relevant exclusions)

Q10: The scope of the exclusion for "financial products"

53. We note the apparent uncertainty and inconsistency arising from the definition of "financial instruments" both by reference to the Regulated Activities Order 2001 (Articles 6(e) and 4 (1)(h)) and also by reference to MiFID (recital 30 and Article 6 (d)). We consider that the interests of consistency and legal certainty would be served by a unified definition of "financial instrument" for the purposes of Article 6. Following the UK's withdrawal from the EU, we suggest that defining financial instruments by reference to the RAO would be most appropriate.

54. We agree with the Law Commission's provisional view that a restrictive approach should be adopted to the financial product exclusion. There is a strong public interest in ensuring that, where security tokens are marketed to UK retail consumers they are able to enforce their consumer rights in UK Courts. If this exclusion is excessively broad in scope it would risk undermining consumer rights. We defer to respondents with specific expertise in financial services regulation on the issue of *precisely* which rights and obligations (if any) should fall within the scope of the exclusion. However, we tentatively suggest that the

[16] Law Commission Paper, paras. 8.46 and 8.47.

exclusion should be narrowly focused upon only those rights and obligations constituting the financial instrument itself.

55. Finally, it is not clear how the financial products exclusion fits with the Financial Promotions Regime for crypto assets. This provides consumer protections in respect of any financial promotion that is capable of having an effect in the UK[17]. The legislation provides consumers with specific rights and remedies where they enter into a "controlled agreement" or "exercise rights conferred by a controlled investment" as a consequence of unlawful crypto promotions (including promotions which may emanate from outside of the UK)[18].

56. There is a strong public interest in ensuring that the consumer rights and remedies arising from the UK's financial promotions regime can be protected in UK courts. That is so even where the relevant firm is based overseas and where the contractual dispute concerns security tokens. The Law Commission may wish to consider whether further legal clarification is required to ensure that nothing in Article 6 undermines the rights of UK consumers to rely, in UK Courts, upon the protections arising from the financial promotions regime.

IV. Applicable Law – Torts and Delicts

Q11: Localising Damage under Applicable Law

57. While it may be desirable to ensure a harmonious approach to localising damage between applicable law and jurisdiction, it is in our view inevitable that the *locus* considerations under the former will be narrower than the latter. We do not consider that any potential tension should be resolved by advocating for a narrower interpretation of the CPR gateway (the ambit of Rome II being beyond the scope of any recommendations, as identified). However, for the reasons given below, we do not consider that there is any obvious reason for

[17] See section21 of the Financial Services and Market Act 2000. With effect from 8 October 2023 the financial promotions regime was extended to "qualifying crypto assets": Financial Services and Markets Act 2000 (Financial Promotion) (Amendment) Order 2023.

[18] See FSMA 2020, section 30 (2) and 30 (3).

a different outcome in cryptoasset claims as between jurisdiction and applicable law, despite these differences in the applicable tests.[19]

58. The relation of the relevant tests to each other can most usefully be reviewed in *Brownlie II*:

a. The question of *locus damni* under art 4 Rome II and the domestic gateway is "distinct and not analogous" (at [45]). Art 4 is more narrowly formulated and makes a distinction between direct and indirect damage which does not feature in the tort gateway.

b. The question of *locus damni* under the Brussels system and the domestic gateway are not the same. Lord Lloyd-Jones rejected the notion that the redrafting of gateway 9 was designed to assimilate the test under the various iterations of the Brussels instruments (at [53ff]). It is observed throughout the judgment that the CJEU decisions under the Brussels instruments have taken a narrower approach to damage consistent with the scheme's overall hostility to adopting the claimant's residence as the relevant *locus*, instead of bringing the claim to the defendant (art 2) (see particularly at [55]), and the conclusion that "*there is, therefore, no sound basis for seeking to assimilate the limited, exceptional jurisdiction under art 5(3)/7(2) of the Brussels system with the tort gateway in our domestic system. In particular, the scope of the exceptional special jurisdiction under the Brussels system cannot be the defining consideration for the scope of the tort gateway in our domestic system"*).

c. While Lord Lloyd-Jones did not specifically consider the differences between the question of *locus damni* in Rome II and the Brussels Convention and Regulations, he did not demur from Lord Sumption's observations in *Brownlie I* to the effect that he was not convinced that "*Rome II has any bearing on…the corresponding provision of the Brussels Convention and Regulations… there is no necessary connection between the two*" (at [22] of *Brownlie*).

[19] Indeed, Trower J in *D'Aloia* decided both applicable law and jurisdiction on the same basis of the *situs* of the cryptoasset (at [11] and [20] respectively).

59. In summary therefore, the tort jurisdictional gateway is wider than the test under the Brussels instruments, which in turn is different from (and likely wider than, given the drafting and the overall scheme) the test under Rome II. The CJEU caselaw is therefore not relevant for the jurisdictional gateway test but will be relevant (within the parameters of the primary legislation scheme) for applicable law.

60. All of the above said, we do not consider these differences between the relevant tests will be particularly significant for cryptoasset claims, nor do we consider that the *CJEU* cases helpfully set out in the Law Commission's paper will obviously lead to a different decision on applicable law to that reached under jurisdiction. For the reasons given above, the omni-territorial and "pure financial" elements of cryptoasset claims have been effectively neutralised by the adopted general rule that cryptoassets are "located" wherever their owner is habitually resident – meaning that both the "direct" and any financial loss will generally be geographically coincident in England and Wales for those resident here. If one considers the facts of *Lubin*, for example, there is no direct or immediate damage in Spain or anywhere else – the online actions of both the claimant and the defendant produce an effect on the cryptoassets in their "location" in England.

Q12: Escape Clause under art 4(3) Rome II

61. We agree with the observations in the Law Commission paper in relation to the general observation made at 9.39 onwards and have nothing further to add, save to note that (as is perhaps obvious) that cases involving elements of fraud and deceit such as those which have come before the courts to date are very unlikely to involve any pre-existing contractual relationship, or any other factors relevant to the escape clause.

V. Applicable Law – Property

Q:19 Law applicable to Property Disputes in Digital Asset and ETD Litigation

62. In relation to sub-question (1), we consider that while contractual principles may provide assistance in many disputes about the ownership of crypto tokens, they do not obviate the need for the *lex situs* rule to be considered. Contractual principles seem most likely to be of assistance in cases (i) involving parties who have dealt with one another; and (ii) cases where a person may be taken as having consented to something akin to a contractual

framework in acquiring the relevant crypto tokens. However, in other scenarios we think that it is difficult to see how contractual principles could provide meaningful assistance. In particular, it is unlikely that they could be helpful in the paradigm case concerning "permissionless" crypto tokens where there has been an "involuntary dispossession" involving parties who have not dealt with one another.

63. In relation to sub-question (4), we think that recourse to the location of the "owner" or "transferor" could be useful in a significant range of cases. Where the parties have voluntarily dealt with one another, such an approach seems reasonably theoretically sound, and would also be pragmatic (in that there should be little scope for dispute about the identity of the parties). The position is certainly more difficult where the parties to the dispute are strangers. This will necessarily be the case where the identity of the person holding the assets is not known, but problems may arise even if this person's identity is known. For instance, it is difficult to see how recourse to the location of the owner or transferor could provide much assistance in a case in which A and B (who have not dealt with one another) both claim that they hold property rights in certain crypto tokens. In such a scenario, resort to the *lex situs* may be necessary.

64. In answer to sub-question (6), we think that it is reasonably likely that the courts will be asked to determine disputes relating to wholly decentralised digital assets held in permissionless DLT networks where the parties have not dealt with one another and there has been an "involuntary dispossession". Such disputes may, however, be rare.

65. In relation to sub-question (7), we appreciate that this does not admit of an easy answer. We think that one approach, which would have the advantage of simplicity, and which would be theoretically sound, would be to take the view that a crypto asset held in a permissionless DLT network is located in England and Wales (on the basis that it is located "everywhere"). On this basis the courts of this jurisdiction would be able to exercise jurisdiction in what may be the relatively rare disputes concerning the ownership of such assets. While we see that such an approach is clearly open to criticism, it does not seem obviously inferior to other potential approaches. Significantly, we envisage that this approach would only be adopted in cases in which assistance cannot be derived from either (i) contractual principles; or (ii) the location of the "owner" or "transferor".

Conclusion

66. We conclude by observing that English law is well placed to provide the necessary legal infrastructure for resolving disputes about crypto assets. The advantage of the common law system is its inherent flexibility and creativity. This means that is capable of evolving and adapting to meet legal questions raised by new technologies such as DLT and crypto. Whilst a principled approach to question of private international law is to be welcomed, undue rigidity is not. The principles should enable English judges to approach the questions of "which court?" and "which law"?" with flexibility, pragmatism and common sense. We also are delighted with the ongoing research and collaborations by the Law Commission with international organisations (such as UNIDROIT, HCCH and ELI) while these legal principles are being discussed to create a proper framework for English Law[20].

Bar Council[21]

16 May 2024

For further information please contact:

Eleanore Lamarque, Policy Manager, Regulatory Issues, Law Reform and Ethics

The General Council of the Bar of England and Wales

289-293 High Holborn, London WC1V 7HZ

Email: ELamarque@barcouncil.org.uk

[20] Including the HCCH proposal for a Normative Project: private International Law Issues Relating to. Digital Tokens: https://assets.hcch.net/docs/d6e2d062-7cd0-4f3d-be96-189c12164ab6.pdf

[21] Prepared by members of the Law Reform Committee who are grateful to Edite Ligere Vice Chair of the Law Reform Committee, Robert Kellar KC, Jessica Elliott and Edward Waldegrave of 1 Crown Office Row Chambers, Shobana Iyer of Swan Chambers and Professor Robert Stevens of Oxford University for their assistance with this response.