



**Law
Commission**
Reforming the law

Digital assets and ETDs in private international law: which court, which law?

Responses to call for evidence

Contents

| | |
|---|-----|
| Aave Labs | 1 |
| Andreessen Horowitz (a16z) | 6 |
| Ashurst LLP | 29 |
| Bar Council | 44 |
| Professor Janeen Carruthers | 64 |
| Ian Clements and Alexander Hewitt | 67 |
| City of London Law Society's Financial Law Committee | 71 |
| Commercial Bar Association (COMBAR) and Chancery Bar Association (ChBA) | 88 |
| Marina Comninos | 136 |
| D2 Legal Technology (D2LT) | 139 |
| Sean Edwards | 147 |
| Enigio AB | 149 |
| Financial Markets Law Committee (FMLC) | 153 |
| Dr Lorna Gillies | 175 |
| Professor Uglješa Grušić | 180 |
| Denis Jude Haughton | 206 |
| Associate Professor Benjamin Hayward | 207 |
| Herbert Smith Freehills LLP | 210 |
| Hogan Lovells LLP | 215 |
| Dr Sara Hourani | 223 |
| International Swaps and Derivatives Association (ISDA) | 226 |
| Kennedys Law LLP | 235 |
| Dr Israel Cedillo Lazcano | 245 |
| Linklaters LLP | 246 |

| | |
|--|-----|
| Norton Rose Fulbright | 250 |
| Associate Professor Sagi Peari | 260 |
| Luminita Procopie | 264 |
| Camilla Slater | 265 |
| Society of Scrivener Notaries | 266 |
| Society of Trust and Estate Practitioners (STEP) | 271 |
| Göker Tataroğlu | 278 |
| Assistant Professor Jasper Verstappen | 282 |
| W Legal | 284 |
| Wave BL | 312 |

Network Frontiers Limited

[REDACTED]

[REDACTED]

[REDACTED]

16 May 2024

By email to: conflictoflaws@lawcommission.gov.uk

Dear Law Commission,

Call for evidence - Digital assets and ETDs in private international law: which court, which law?

Network Frontiers Limited, a company registered in the UK respectfully submits feedback to the Law Commission's call for evidence entitled "Digital assets and ETDs in private international law: which court, which law?", which was published in February 2024.

Aave Labs is software development company that builds blockchain-based software for Web 3.0, the next generation of the Internet, which refers to the system of applications built on top of blockchains that allows users to have control over their own assets, data and virtual interactions. Aave Labs are, to date, best known for the creation of the Aave Protocol, a decentralised, non-custodial liquidity protocol that allows users to supply or borrow cryptoassets and earn interest on any supplied assets.

We acknowledge the commentary on the Aave Protocol within the Commission's report and recognize the necessity of clarifying certain key aspects to enhance understanding of decentralized finance (DeFi) from a legal perspective. While we have not addressed every question posed by the Commission, we are keen to correct specific statements and provide detailed clarifications regarding the Aave Protocol.

Please let us know if you wish to explore any of these topics in more depth. We are eager to engage in dialogue and offer additional information to support the Commission's efforts.

Yours faithfully,

[REDACTED]

Stani Kulechov

Founder and CEO of Aave Labs

Responses

1. Blockchain pseudonymity

We clarify that blockchain transactions are pseudonymous rather than anonymous. Transactions are linked to digital addresses that do not directly reveal personal identity yet provide a consistent identifier on the blockchain.

In reference to section 3.121: *"Anonymous lenders deposit their crypto-tokens in a lending smart contract, which deposits them in a lending asset pool."*

- Blockchain transactions are often described as pseudonymous rather than anonymous due to the nature of how transactions are recorded and traced on the blockchain. In a blockchain, transactions are recorded on a public ledger. When someone makes a transaction, it is tied to their digital address, a string of numbers and letters. This address acts as a pseudonym. While it does not directly reveal the person's real-world identity (such as their name or physical address), it is a consistent identifier that represents them on the blockchain. Furthermore, these transactions are highly traceable given that often the traces lead to a centralised exchange. Centralised exchanges generally require users to undergo Know Your Customer (KYC) procedures, which link their digital addresses to real-world identities. As a result, while blockchain transactions provide a level of pseudonymity, the involvement of centralised exchanges means that it is possible to trace these transactions back to individuals.

2. Peer-to-protocol Transactions

We explain that transactions in DeFi do not follow a traditional peer-to-peer model but rather a "peer-to-protocol" model. This means transactions occur between an individual and a set of smart contracts making up the protocol.

In reference to section 7.21: *"Herbert Smith Freehills gave Aave (a DeFi lending platform) as an example of a use case for "peer to peer" smart legal contracts (whilst also acknowledging that non-legal smart contracts could also be concluded on the platform)."*

- We understand that the underlying concept behind saying that "transactions are peer-to-peer transactions," usually aims to highlight that transactions occur directly between two parties without the need for an intermediary, such as a bank or a traditional financial institution. However, when discussing decentralised networks and liquidity protocols like Aave, the nature of transactions shifts from a peer-to-peer model to a "peer-to-protocol" model because transactions do not occur directly between two parties. Instead, they happen between an individual and a set of smart contracts that make up the protocol. These smart contracts are automated, self-executing contracts with the terms of the agreement directly written into

auditable code. They function as the "intermediary" but in a decentralized and automatic manner.

- Additionally, many (however not all) DeFi liquidity protocols operate on a pool-based model. Users supply their assets to a liquidity pool from which other users can take loans against their collateral. The terms, interest rates, and repayments are managed by the smart contracts. Thus, suppliers and borrowers interact with the protocol (or the pool) rather than directly with each other. This setup enables more flexibility and accessibility in supply and borrowing but shifts the interaction from individual to protocol.

3. Absence of Direct Legal Relationships Amongst Participants of a Liquidity Protocol

Participants in a liquidity protocol like Aave engage with smart contracts according to preset rules, without establishing direct legal relationships with other participants. Thus, the nature of the legal relationship among participants of these protocols deviates markedly from that found between lenders and borrowers in the conventional financial sphere.

In reference to section 7.21 *"Users who transact on DeFi protocols may, therefore, enter into smart legal contracts."*

- Building on the previous point on the peer-to-protocol dynamic within liquidity protocols (as explained in section 2 above), it is important to consider the distinct legal framework governing user interactions within a smart contract liquidity pool. The nature of the legal relationship among participants in a liquidity protocol deviates markedly from that found between lenders and borrowers in the conventional financial sphere. Attempting to shoehorn these novel interactions into the traditional lending paradigm would not only be inaccurate but also overlook the fundamental differences underpinning them. Notably, there's an absence of a direct legal relationship between participants who supply liquidity and those who borrow from the pool.
- To characterise the activity, we suggest the following analogy of liquidity protocols with liquidity pools like the Aave and a transportation system. In a transportation system, passengers use roads, buses, trains, or subways to reach their destinations. While all are using the same infrastructure, there is no direct or legal relationship between one passenger and another; their interaction with the system and each other is mediated through the infrastructure itself—the roads, vehicles, and schedules. Passengers agree to the rules and regulations of the transportation system (buying tickets, following schedules, adhering to safety protocols) but do not enter into agreements directly with other passengers. Similarly, in DeFi lending protocols with liquidity pools, participants supply, borrow, or provide liquidity according to the rules set by smart contracts. These smart contracts govern how

transactions are executed, interest rates are determined, and collateral is managed. Participants interact with the protocol (the smart contracts and the blockchain infrastructure) rather than directly with each other. This structure ensures that while participants are contributing to and benefiting from the shared liquidity pool, they do not have to establish legal relationships with one another. Their agreements are with the protocol itself, not with individual lenders or borrowers. In essence, the term "peer-to-protocol" underscores that while individuals are acting in a common ecosystem and their actions impact each other indirectly through changing conditions (like liquidity levels and interest rates), they are not entering into transactions directly with one another. Instead, their interactions are mediated by the underlying technology, which acts as an intermediary that dictates the terms of engagement, much like a transportation system facilitates the movement of people without requiring them to have direct agreements with one another. This structure simplifies the process, reduces the need for trust between individuals, and leverages blockchain technology to ensure transparency, security, and compliance with the rules encoded in smart contracts.

- In our view the characterisation of "legal smart contracts" does not accurately describe the operation of liquidity protocols like Aave. These networks facilitate a unique kind of interaction that is not well-represented by the traditional notion of legal agreements. Instead, they create an environment where transactions and relationships are defined and managed through code, reflecting a significant departure from established legal and financial models. The following sections will explore some of these areas.

4. Liquidation vs. Default

We also wish to highlight that in DeFi protocols like Aave, liquidation differs fundamentally from traditional lending defaults; it occurs when a borrower's collateral falls below a specified threshold, enabling a third party to act as a liquidator by repaying part of the debt and acquiring the collateral at a discount. This process is not connected to a traditional default by the borrower.

Section 3.121 *"If the crypto-tokens offered as collateral drop below a certain value, or the borrower defaults, then the collateral will liquidate in favour of the lender."*

- In our view, the description of the liquidation processes in protocols like Aave lacks precision. Specifically, when the value of a borrower's collateral falls below the designated liquidation threshold in DeFi platforms, it does not initiate a traditional default as seen in conventional lending, but instead, this decrease in value triggers an opportunity for a new participant, any third party, to act as a liquidator. This liquidator repays part of the outstanding debt and, in return, acquires the collateral at a discounted price. This process is automated and impersonal, based purely on the state of the collateral and market conditions, without any direct legal claims against any of the

liquidity pool borrowers. This process underscores the unique risks and lack of traditional legal recourse in liquidity protocols, contrasting sharply with traditional lending where legal avenues exist for recourse.

5. Legal Nature of the Collateral in Liquidity Protocols

The legal nature of collateral differs significantly in traditional lending and liquidity protocols like Aave. In traditional lending, collateral is secondary to the borrower's obligation to repay the loan and interest. In liquidity protocols like Aave, there is no legal obligation to repay. At the same time collateral in liquidity protocols like Aave is central to the solvency of the liquidity pool (and not an accessory to a debt repayment obligation).

Section 3.121 *"If the crypto-tokens offered as collateral drop below a certain value, or the borrower defaults, then the collateral will liquidate in favour of the lender."*

- This nuanced understanding of liquidation in DeFi — where there is no direct legal relationship between the participants of a liquidity pool (as explained in section 3 above), and where liquidation serves more as a market mechanism rather than a punitive measure against default (as explained in section 4 above) — underscores why it is critical to comprehend the distinct legal nature of collateral within the protocols.
- In traditional lending collateral is primarily an accessory to the main debt obligation. It secures the loan by providing a safety net for the lender if the borrower fails to meet the repayment terms. Although crucial for risk mitigation, collateral is not the primary focus of the legal agreement. The borrower's core obligation remains the repayment of the borrowed sum and any interest due, making the collateral secondary in the legal structure of the loan. Unlike traditional lending where the borrower has a clear legal obligation to repay the loan irrespective of changes in collateral value, liquidity protocols operate differently. In DeFi, there is no primary obligation to repay. While users often choose to repay to reclaim their collateral and avoid liquidation, this repayment is not legally mandated. Positions in DeFi can be perpetual, existing indefinitely as long as the conditions of the smart contract are met and the collateral remains above the required thresholds. In DeFi environments, the collateral does not secure a position but is integral to the viability of the entire liquidity pool. If the value of collateral in a liquidity protocol drops rapidly, outpacing the rate at which liquidations can occur, this leads to the economic inviability of liquidating positions, thus accumulating bad debt within the pool. As a result, the liquidity pool may become insolvent.

1. INTRODUCTION

- 1.1 We greatly appreciate this opportunity to reply to the consultation and call for evidence, entitled “Digital assets and ETDs in private international law: which court, which law?” (the “**Consultation**”), issued by the Law Commission on February 22, 2024. Andreessen Horowitz (“**a16z**”) is committed to working with international officials, regulators, and public bodies to address the specific risks and opportunities in the blockchain ecosystem, and we commend the Law Commission for its commitment to soliciting information from a diverse body of stakeholders and a wide range of perspectives in the course of conducting its assessment of the law of England and Wales in this area.
- 1.2 A16z is a venture capital firm that invests in seed, venture, and late-stage technology companies, focused on bio and healthcare, consumer, crypto, enterprise, fintech, and games. A16z currently has more than \$42 billion in committed capital under management across multiple funds, with more than \$7.6 billion in crypto funds. In crypto, we primarily invest in companies using blockchain technology to develop protocols that people will be able to build upon to launch Internet businesses. Our funds typically have a 10-year time horizon, as we take a long-term view of our investments, and we do not speculate in short-term crypto-asset price fluctuations.
- 1.3 We believe that blockchain technology is a momentous achievement in the development of the Internet. Since it was first developed in 2008, the blockchain ecosystem has grown rapidly, and our firm has been at the forefront of advancing the industry through investments in companies that develop protocols and applications relating to decentralised social networks, identity management, enterprise solutions, financial services, content creation, environmental protection, data storage, and many other sectors. As an industry leader, we have also assisted domestic and international regulators and officials with education around the unique attributes of decentralised systems, as well as the development of clear and robust frameworks that are appropriately calibrated to those attributes. We hope to channel our industry observations in providing helpful feedback to the Consultation.
- 1.4 In our responses, we focus on what we see as the key considerations to effectively characterise and capture the blockchain ecosystem within the law in a way that preserves the benefits of blockchain technology and protects the future of the Internet, while reducing the risks of uncertain or unwelcome legal outcomes. In particular, we focus on our experience of how decentralisation works from a technical and practical perspective and, therefore, how it should interact with contract and other areas of private law.
- 1.5 Our responses are divided by reference to three sets of questions from the Consultation, as follows:
 - (a) In section 2, we begin by providing an outline of decentralisation and decentralised finance (“**DeFi**”) to frame our responses to questions 7(1) – (3) and to support our view that: (i) legal contracts are not necessary when interacting directly with DeFi Protocols (defined below at 2.2(b)(iii)); (ii) legal contracts will not be formed when interacting directly with DeFi Protocols; and (iii) legal contracts will also, in general, not be formed in relation to DeFi Apps when no account relationships exist between users and application providers, which means that users do not provide DeFi Apps with private information or custodial assets;
 - (b) In section 3, we set forth our view as to the appropriate way to characterise cryptoassets from a regulatory perspective before providing responses to questions 10(1) – (3) and explaining why we believe following the current UK regulatory approach is the correct way for English and Welsh courts to characterise cryptoassets under the Rome I Regulation; and

- (c) In section 4, we consider questions 19(4), (6), and (7) and the Law Commission's suggestions as to how to determine applicable law to cryptoassets and explain why it is important to follow a case-by-case, principles-based approach.

2. QUESTIONS 7(1) – (3)

2.1 In order for us to provide informed responses to these questions 7(1) – (3), it is first necessary to establish what the term decentralisation means and, in turn, DeFi. Once we have provided our definitions of those terms based on our extensive market experience, we will move on to discuss why: (i) legal contracts are not necessary when interacting directly with DeFi Protocols (defined below at 2.2(b)(iii)); and (ii) legal contracts will not be formed when interacting directly with DeFi Protocols. We will discuss other aspects of DeFi, like DeFi Apps (defined at 2.2(b)(iv)), in the sections that follow. Provided the foundations of how DeFi Protocols work are understood, in our view there is no need for clarification as to how contract law applies to DeFi.

2.2 DeFi

(a) Decentralisation

- (i) Decentralisation is a broad term that refers to multiple aspects of a blockchain. Emerging decentralisation use-cases include decentralised social media, gaming, and identity management, among many others. To determine if a system is decentralised, stakeholders can evaluate it using the following technical and operational considerations.
- (ii) To ascertain if a system is technically decentralised, stakeholders can use two tests:
 - (A) Can any single person or group of persons control or fundamentally alter a system's purpose or code, control user funds, reverse transactions, or restrict access to the system? If the answer is no, then the system is decentralised. Otherwise, the system is not decentralised.
 - (B) Is the system built on top of a public and Permissionless Blockchain?¹ If not, then the private and permissioned features of the base blockchain could curtail its decentralisation.
- (iii) Operational decentralisation ensures that insiders cannot exploit information asymmetries to harm consumers. To assess if a system is operationally decentralised, evaluators can consider:
 - (A) How much of a protocol's value (or tokens) do insiders own?
 - (B) How much influence do insiders have on governance processes?
 - (C) How recently insiders or developers have added new functionality to a project?
- (iv) As many regulators and other authorities have noted, and as we have noted previously, decentralisation is a spectrum, with some blockchain networks

¹ A permissionless blockchain, is a network in which users have equal permission to utilise and interact with the network, and in which users' permission to utilise and interact with the network is not set by the network itself or any central person or institution (a "**Permissionless Blockchain**" and each such blockchain would be "**Permissionless**"). Accordingly, a Permissionless DeFi Protocol would be a DeFi Protocol that users have equal permission to utilise and interact with, with there being no central person or institution which could control interaction with the DeFi Protocol.

and related businesses starting off centralised and transitioning toward a decentralised model. Roadmaps for decentralisation can differ significantly depending on the characteristics of a project. In the context of a DeFi Protocol, we suggest that a “sufficiently” decentralised system exists where: (i) information regarding its operation is transparent and available to all; (ii) the protocol is composed of open-source code and no single person or group of persons acting pursuant to an express or implied agreement can materially alter its primary purpose, and whose design prevents any such person or persons from amending or reversing transactions executed and recorded on the blockchain; and (iii) public participants have the ability to access the protocols and execute digital asset transactions through them in accordance with predetermined, non-discretionary automated rules and algorithms.

(b) DeFi and CeFi

- (i) DeFi systems are important emerging technologies in the blockchain ecosystem that provide the functionality for peer-to-peer lending, borrowing, and other financial transactions. However, DeFi does not readily lend itself to existing financial regulatory frameworks or the legal relationships that exist in relation to traditional financial (“**TradFi**”) services. For the most part, this is because DeFi applications are an alternative to trusted financial intermediaries – the primary targets of traditional regulatory frameworks and the centralised counterparties to which legal obligations attach in respect of their clients. Traditional regulatory frameworks do not take into consideration the transparency of blockchains, the reduced barriers to entry that open-source code provides, and other advantages of Permissionless Blockchains.
- (ii) Decentralisation mitigates many legacy financial services risks in a number of ways, including by ensuring that no single person or group of persons can: (i) control or fundamentally alter a protocol’s purpose or code; (ii) control user funds or assets; (iii) reverse transactions; or (iv) restrict access to a protocol. Furthermore, given that full decentralisation requires a protocol to be built on an open and Permissionless Blockchain, users are able to interact with and inspect the open-source code of protocols themselves. Taking these factors together, many of the risks associated with legacy models of finance, which existing private laws and financial regulations typically address, do not arise once sufficient decentralisation has been achieved, given the absence of trusted central actors from whom users need protection, and that users have full visibility of the protocol’s workings. In a DeFi context, this allows users to engage in peer-to-peer transactions without relying on third parties and maintain more control over their assets relative to traditional finance.
- (iii) DeFi protocols (“**DeFi Protocols**”) are software programs consisting of smart contracts that provide the functionality for peer-to-peer lending, borrowing, and other financial transactions. Protocols are hosted on or integrated in public blockchain networks, such as Ethereum,² and tend to be open-source,³

² See Lindsay X. Lin, *Deconstructing Decentralised Exchanges*, Stan. J. Blockchain L. & Pol’y (Jan. 05, 2019), <https://stanford-jblp.pubpub.org/pub/deconstructing-dex>; see also Fred Ehrsam, *Why Decentralised Exchange Protocols Matter*, Medium (Sept. 27, 2017), <https://medium.com/@FEhrsam/why-decentralised-exchange-protocols-matter-58fb5e08b320>.

³ Open-source software enables the public to view, contribute to, and learn from a protocol’s underlying technology. This avoids vendor lock-in, helps to quickly identify and fix errors, and fosters network effects through community engagement.

decentralised, autonomous,⁴ and censorship resistant.⁵ It is important to clarify that DeFi Protocols are separate from the foundations that initially deploy protocols at the early stages of decentralising and issuing and distributing native tokens. Once a system becomes a protocol, it operates independently from its foundation, and a diverse set of stakeholders governs it. Per the decentralisation tests included above, no single party or group of parties controls the protocol, and therefore, there is no legal person responsible for its ongoing functioning.

- (iv) DeFi applications (“**DeFi Apps**”) are programs built on top of DeFi Protocols that allow users to access protocols. In general, DeFi Apps provide a graphic user interface or APIs or both.⁶ In contrast to the protocol layer, businesses and developers of DeFi Apps are centralised entities or individuals that provide their application to users often in return for some form of remuneration or other consideration. However, unlike traditional internet applications, in general, DeFi Apps do not have account relationships with users, take custody of user assets, or hold proprietary user information.
- (v) Consideration of other protocols that are widely used on the Internet helps illustrate the distinction. For example, consider SMTP, which is the protocol underlying email technology, versus webmail applications, such as Gmail, that provide users with a simple interface for sending emails using the protocol. In order to send an email using SMTP, it is not necessary to interact directly with the protocol, and a person does not otherwise have a legal relationship with the creators of the protocol (or the protocol itself) by virtue of sending an email. As we will discuss below, to use an application like Gmail, it is necessary to create an account with Google, as the centralised business providing the Gmail application. DeFi Apps are similar to webmail applications like Gmail in that they provide simple interfaces for interacting with protocols, but with a crucial distinction: DeFi Apps, in general, do not require users to set up accounts with them and do not hold proprietary user information or assets. This is a significant difference that obviates the need for private contractual relations in most cases, as we will discuss further below.
- (vi) The below diagram provides a visual comparison between web1 and web3 protocols and apps and the technology layers in which these arise.⁷

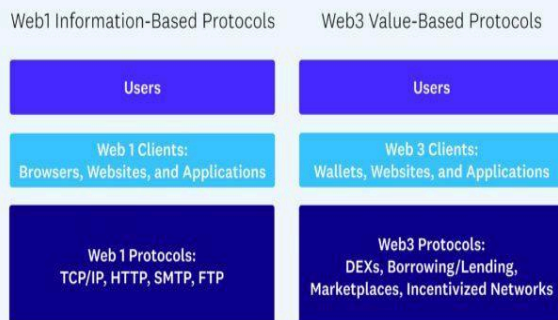
⁴ The DeFi Protocol’s smart contracts should be self-executing, meaning the rules and actions are predetermined. The autonomous nature of the DeFi Protocol’s smart contracts ensures the DeFi Protocol’s credible neutrality (i.e. that the DeFi Protocol will not discriminate against individuals or types of transactions).

⁵ Censorship resistance, like decentralisation, is a similarly broad term that describes the ability of almost anyone to use Permissionless Blockchains, as well as the fact that no one can be kicked off of a Permissionless Blockchain. It also describes the fact that no one interacting with the blockchain is powerful enough to block transactions or prevent others who wish to validate blockchain transactions from joining the consensus network. DeFi Protocols must not have the ability to censor individuals or transactions.

⁶ n[2].

⁷ See Miles Jennings, *Regulate Web3 Apps, Not Protocols*, a16z, <https://a16zcrypto.com/posts/article/web3-regulation-apps-not-protocols/> (Sept. 29, 2022).

Web1 to Web3: Improving Internet Functionality



Source: Miles Jennings/ a16z crypto



- (vii) Our responses to these questions 7(1) – (3) distinguish between DeFi Protocols and DeFi Apps and the principles of decentralisation set forth above, but note that despite these differences, private contractual law should generally not apply to either. As we discuss, DeFi Protocols are a new iteration of trustless and transparent digital public goods on the Internet that do not involve the same kinds of legal relationships as those that arise between intermediaries and their clients in traditional financial services. We also discuss DeFi Apps, which include certain centralised elements that resemble traditional finance, but do not involve traditional relationships between providers and users because there is no account relationship and the providers do not hold customer information or assets. While the Consultation, and therefore our response, is focussed on DeFi as opposed to other web3 considerations, the regulation and application of private law to DeFi Protocols and DeFi Apps will have a broader effect on web3 as a whole. Of course, the most immediate outcome is that the application of private law to web3 actors outside of DeFi is likely to be interpreted in accordance with its application to DeFi. Therefore, any significant restrictions or improper legal approaches for DeFi could have broader implications on the rest of the web3 ecosystem, affecting use-cases ranging from gaming to social media to identity management.
- (viii) Centralised finance (“CeFi”) institutions, as the name implies, are “centralised” operations, complete with management teams and conflicts of interest, where users interact with third-party intermediaries, enter into account relationships, seek custodial services, and provide proprietary information to access crypto markets.⁸ The intermediaries are typically traditional private businesses, where users are customers of the business, and decisions about how to run the business are made behind closed doors.
- (ix) We note that the Law Commission includes a definition of DeFi applications (the “**LC DeFi Definition**”) at paragraph 7.17 of the Consultation, as follows:

⁸ See *What Is CeFi (Centralized Finance)?*, WorldCoin, <https://web.archive.org/web/20230522165246/https://worldcoin.org/articles/what-is-cefi> (May 22, 2023); see also Ekin Genç, *DeFi vs. CeFi in Crypto*, CoinDesk (Apr. 10, 2024), <https://www.coindesk.com/learn/defi-vs-cefi-in-crypto/>.

- (1) *They purport to have a decentralised ownership and governance structure.*
- (2) *They operate through smart contracts that execute the terms and conditions of a transaction in an automated manner.*
- (3) *DeFi relies on “open source” technology, where anyone can read the underlying source code that operates the applications and performs financial activities.*
- (4) *Anyone can use the DeFi applications, so long as they fulfil the application’s technical requirements for participation (such as ownership of a crypto wallet).*

- (x) The first point that we would note on this definition is that it defines DeFi “*applications*”, rather than protocols. We question whether this was the intention of the Law Commission, and if its understanding of applications and protocols aligns with the one set out above in paragraphs 2.2(b)(iii) and 2.2(b)(iv).
- (xi) On limb (1) of the LC DeFi Definition, we do not think it is helpful to include applications that “*purport*” to be decentralised. An application or protocol can purport to be decentralised, without having characteristics that constitute sufficient technical and operational decentralisation. When assessing DeFi Protocols, and the application of law in relation to them, it is important to ensure that true DeFi Protocols are assessed, as otherwise the scope of operations will be too broad to draw meaningful conclusions. A DeFi App on the other hand, could purport to be decentralised; however, as already set out, DeFi Apps are operated by centralised parties. To that end, we provide the tests of decentralisation outlined in section 2.2.
- (xii) While limb (1) of the LC DeFi Definition does not fully engage with the notion of decentralisation, it is still informative to apply limbs (2) – (4) of the LC DeFi Definition to our definition of decentralisation in the context of a DeFi Protocol at 2.2(a)(iv) in order to understand any differences.
 - (A) Broadly, the LC DeFi Definition aligns with our definition of decentralisation (in that it mentions operation of smart contracts through automated rules (limb (iii) of our definition), the use of open source code (limb (ii) of our definition), and that decentralisation allows for the use of protocols or code by anyone (limb (iii) of our definition)).
 - (B) One notable difference is that the LC DeFi Definition does not include wording to the effect that “*no single person or group of persons acting pursuant to an express or implied agreement can materially alter its [the DeFi Protocol’s] primary purpose, and whose design prevents any such person or persons from amending or reversing transactions executed and recorded on the blockchain*”, which is included in limb (ii) of our definition. This is key to the notion of decentralisation because it goes to the argument that no legal person controls the smart contracts and is therefore something that should be factored into the LC DeFi Definition.
 - (C) Finally, the LC DeFi Definition makes no reference to distributed ledger technology/Permissionless Blockchains which enable the

operation of a DeFi Protocol and allow it to be transparent (which also goes to limb (i) of our definition of decentralisation at 2.2(a)(iv)) and is the technology that underpins DeFi Protocols and therefore should be mentioned.

2.3 **Question 7(1): Do you agree that contractual disputes in the context of DeFi are not likely to come before the courts?**

Contractual Principles

- (a) In our view, it is helpful to start with the principles upon which contracts, and contract law, are built when considering the extent to which contractual disputes will arise in the context of DeFi. *Chitty on Contracts* notes that the binding force of contracts has been long recognised as a principle of English law “*which suits the needs of commerce as well as the expectations of parties to contracts more generally.*”⁹ As set out above at paragraph 2.2(b)(iii), true decentralisation and DeFi Protocols are “*open-source, decentralised, autonomous and censorship resistant*”. As a result, we would question the extent to which the needs of commerce and the expectation of parties require the binding force of contract when interacting with DeFi Protocols and DeFi Apps.
- (b) Contracts are a means of risk allocation between parties. Parties to a contract evaluate what they are trying to achieve, what each party undertakes to perform, and allocate risks of non-performance, partial performance, or some other form of breach between themselves. In the context of a DeFi Protocol, smart contracts perform as programmed and can be inspected by anyone. Therefore, the typical risk allocation function of contract law is less relevant in this context, given that the DeFi Protocol model is trustless and transparent. Notwithstanding this point, and as addressed below, there are practical risks inherent to the technology of smart contracts. In particular, the risk that a smart contract does not function as intended, which could result in a number of bad outcomes, including that hackers could exploit unidentified smart contract deficiencies to make a gain at the detriment of other users. These risks are important, and we advocate for a number of regulatory solutions to address them, including: (i) smart contract disclosures, which set out the risks associated with a protocol’s smart contracts; and (ii) smart contract audits, which involve analysing a protocol’s smart contracts to identify vulnerabilities or poor coding. But, as discussed below, we stress that these risks need not be addressed through private contract law.
- (c) Taking these arguments in paragraphs 2.3(a) and 2.3(b) together, our view is that decentralisation at the protocol level mitigates the issues and risks that private contract law arose to address and, therefore, user interactions with DeFi Protocols should not give rise to claims based on private contract law. As we will also discuss, DeFi Apps should also not give rise to private contractual claims where there is no account relationship between DeFi Apps and users, but this should not impact the need for *regulatory* requirements relating to smart contract disclosures, security audits, and other issues, which we have elaborated elsewhere.¹⁰

⁹ H Beale (ed), *Chitty on Contracts* (35th ed 2023), Volume 1, Part 1, Chapter 2, Section 3.

¹⁰ See Miles Jennings & Brian Quintenz, *Regulate Web3 Apps, Not Protocols Part IV: Practical Application*, a16z (Feb. 17, 2023), <https://a16zcrypto.com/posts/article/regulate-web3-apps-not-protocols-practical-application/>.

Requirements for a Contract

- (d) In addition to our arguments in paragraphs 2.3(a) – 2.3(c) above, we recognise that the law of England and Wales has a well-defined test for what constitutes a legally binding contract, which we first consider in the context of DeFi Protocols. Taking the definition used by the Law Commission, which reflects the position in common law and statute, the requisite elements to a contract are:
 - (i) agreement;
 - (ii) consideration;
 - (iii) certainty and completeness;
 - (iv) intention to create legal relations; and
 - (v) formality requirements.¹¹

Agreement

- (e) Starting with limb (i) of the Law Commission’s definition, there must be an agreement in order to form a legal contract. For an agreement to exist under English and Welsh contract law, there must be both offer and acceptance.¹²
- (f) To assist us in discussing the applicability of contract law to DeFi, it would be helpful to first establish how a typical DeFi Protocol works.
- (g) The hypothetical protocol (the “**Exchange Protocol**”) in this example is a decentralised exchange that operates on the Ethereum blockchain and allows for peer-to-peer exchanges of crypto tokens through the use of smart contracts. Unlike centralised exchanges that use a traditional order book system to facilitate trading – where a buy order is matched with a sell order for the same amount and price of an asset – the Exchange Protocol uses an automated liquidity protocol. This protocol allows users to pool their cryptoassets together in “liquidity pools,” which allows trading. Users that want to sell or purchase a certain cryptoasset can “swap” the cryptoasset with other tokens in the liquidity pools, and an algorithm calculates the price of each cryptoasset depending on the composition of the pool. The Exchange Protocol, like other similar DeFi Protocols, once deployed, functions in perpetuity as originally programmed, since their design parameters often severely limit functionality updates. In addition to the Exchange Protocol, there is also an Exchange App (the “**Exchange App**”). Like many DeFi Apps, the Exchange App is a front-end application that allows users to interact with the Exchange Protocol, but unlike traditional webmail interfaces, it neither has an account relationship with users nor holds proprietary user information or custodies assets.
- (h) While we note the Law Commission’s discussion in its Smart Contract Paper (the “**Smart Contract Paper**”)¹³ regarding binding agreements between computers, we note that a key element of the discussion is that computers must run code “*deployed by or on behalf of legal persons*.”¹⁴ As explained above, the nature of a decentralised platform means that once decentralisation is achieved, there is no legal person who

¹¹ Law Commission, *Smart legal contracts: Advice to Government* (2021), para 3.2.

¹² n[9] *Volume 1, Part 2, Chapter 4*.

¹³ n[11], Chapter 3.

¹⁴ *Ibid*, para 3.27.

deploys a DeFi Protocol or on whose behalf one is deployed. It is not possible for “*a single person or group of persons*” to materially alter the DeFi Protocol or to reverse or block transactions that take place on it. Therefore, from the point at which decentralisation is achieved, a DeFi Protocol cannot be said to be deployed by or on behalf of legal persons, such that it can satisfy the contractual requirements for offer and acceptance. We also note that the Law Commission does not seem to consider that a person will enter into a contract with a DeFi Protocol in its considerations at paragraph 7.24 of the Consultation (and in particular, 7.24(3) where it notes there is often no intermediary in the DeFi context).

- (i) Having discounted that a DeFi Protocol can satisfy the requirements for offer and acceptance, we consider the possibility of offer and acceptance with counterparties to transactions on the protocol. Given that many DeFi Protocols operate in the same way as the Exchange Protocol, often there will not be a counterparty to a transaction (whether anonymous, pseudonymous, or identifiable). This is because, as explained above, these exchange protocols operate through liquidity pools rather than with a centralised order book to match trades directly between parties. Because there are no counterparties when users interact with liquidity pools, there are no legal persons who can meet the requirements of offer and acceptance.

Intention to create legal relations

- (j) If for any reason, or owing to a particular set of circumstances, the requirements for offer and acceptance are met, there would still be no contract in our view, as there is no intention to create legal relations. We acknowledge that, where a contract is made in a commercial context, rather than a personal one, there is a presumption in law of an intention to create legal relations.¹⁵ However, given the discussions at paragraphs 2.3(a) – 2.3(c) above, we contend that parties do not intend to create legal relations with DeFi Protocols. In this sense, we agree with the views of the Chancery Bar Association and Commercial Bar Association set out at paragraph 3.73 of the Smart Contracts Paper: (i) there is a distinction between an intention to create legal relations with respect to transactions performed by code and an intention to make use of the functionality of the code; and (ii) if performance of the code is guaranteed, the transacting parties may not consider legally enforceable rights of use to them or intend to create such rights. For these reasons, we would also argue that no contract is formed when interacting with a DeFi Protocol because there is no intention to create legal relations. When interacting with a DeFi Protocol, a person is simply making use of the DeFi Protocol’s code (in the same way that a person would interact with any protocol (such as SMTP) that is equally automated and Permissionless, thus allowing any member of the public to make use of it without making it scarcer for others).
- (k) We note that the Law Commission also recommended that, given the complexity in assessing intentions to enter into a legally binding agreement in a smart contract context, parties that have the requisite intention should make this clear in natural language.¹⁶ This argument suggests that the Law Commission thinks the rule in *Edwards v Skyways* may not be sufficient to presume that there was an intention to create legal relations when interacting directly with a DeFi Protocol. We would agree with the Law Commission that this is the right approach, and it further supports our argument that there is no intention to create legal relations in relation to interactions with DeFi Protocols and therefore no legal contract will be formed.

¹⁵ *Edwards v Skyways Ltd* [1964] 1 WLR 349.

¹⁶ n[11], para 3.75.

Law Commission Views

- (l) We note that the Law Commission is of the view that, even if private contracts are created, they are unlikely to be enforced, and therefore ultimately the conclusion of both of our sets of reasoning are the same (i.e., there will be very limited contractual disputes brought before the courts in relation to DeFi Protocols). However, we wish to comment on two points included in the Law Commission's arguments at paragraph 7.24 of the Consultation:

(i) *...there may be instances where code does not perform as intended, or where it does not operate as one party expects. These and other scenarios may give rise to contractual disputes.*

(A) We dispute this line of reasoning for the following reasons. As an initial matter, we accept that there may be instances where code does not perform as developers and users expect. The potential for code to operate other than as intended is why we advocate for regulatory requirements like smart contract disclosures and audits (see paragraph 2.3(b)) to ensure that code is tested, and that users are aware of potential risks. However, because the open-source code will function as programmed, whether intended or not, we disagree that private contractual law is appropriate for raising claims. We acknowledge the discussions in the Smart Contracts Paper regarding interpreting code in accordance with what it would mean to “*a reasonable person with knowledge and understanding of code*”;¹⁷ however, in the context of DeFi Protocols, persons have the opportunity to inspect and interpret the code prior to any transaction being undertaken given that it is open source.

(B) Secondly, and as a more fundamental issue which we have already set out above, there is no contract to be disputed where users interact with DeFi Protocols. Therefore, no contractual disputes should arise, even where the code does not perform as expected.

(ii) *Even if a party wished to litigate, their counterparty may be anonymous.*

(A) As explained in the context of the Exchange Protocol hypothetical in paragraph 2.3(g), often DeFi Protocols do not function so as to directly match counterparties. Instead, liquidity may be sourced from comingled liquidity pools, such that there are no identifiable counterparties. Therefore, the issue of an anonymous counterparty is not what obviates contractual litigation, but rather that there is no counterparty to litigate against.

DeFi Apps

- (m) As already discussed in this response, and throughout our publications and consultation responses, the law should recognise DeFi Apps as distinct from DeFi Protocols. DeFi Apps are operated by centralised parties, have a business plan, a place of business, and there may be user terms provided in relation to the provision of such software services. However, despite the presence of identifiable legal person(s) and provisions such as terms of business, we do not believe that private contractual obligations will arise in the case of DeFi Apps with which users do not have an

¹⁷ n[11], paras 4.40 – 4.61.

account relationship; these Apps neither hold customer assets (i.e., they are non-custodial) nor proprietary user information. We acknowledge that it is possible that the DeFi App layer is the layer of DeFi at which contract law could become applicable, if the DeFi App holds user assets or proprietary user information, or otherwise engages in activities that satisfy the requisite elements for forming contractual relations. However, we note that this will be a heavily fact dependent inquiry on the DeFi App at issue, and that in most cases, contractual relations will not form. Moreover, the DeFi App, as noted above, may have agreements and duties vis-a-vis its customer that create a conventional contractual relationship and which do not implicate the need for any special treatment.

Case law and market practice

- (n) Recent case law also supports the position that legal contracts do not arise in relation to decentralised arrangements. For example, we note that in *Tulip Trading Limited v Bitcoin Association For BSV & Ors* [2022] EWHC 667 (Ch), arguments were made on the basis of fiduciary duties, rather than any contractual relationship between parties. In fact, at several points contractual relations were expressly accepted as not existing, for example “*the Defendants’ alleged control of the Networks and their alleged ability to make a change to the software, irrespective of whether they are actually engaged in making changes, and in the absence of any more general contractual or other obligation to make changes in the future.*”¹⁸ Indeed, it is telling that no attempt was made as part of the case to argue that an obligation arose in contract, and it instead seemed to be an uncontroversial statement that there is “*certainly no contractual relationship.*”¹⁹ As a good example of decentralisation, the Bitcoin network is a strong comparison to DeFi Protocols, and consequently the fact that no contracts were found to arise in this context also suggests contractual claims should not arise in relation to DeFi Protocols.
- (o) We accept that the positions set out in this response, and in DeFi more generally, are not risk free. We would also accept that while some of the risks of TradFi and CeFi are solved in DeFi through the decentralised nature of DeFi Protocols, there are different risks that apply instead and these need to be considered differently from a legal perspective.
- (p) In practice, market participants in DeFi seek to mitigate these risks, not by reliance on contracts with various parties but instead through: (i) transparent open-source code that the public can inspect, such that issues can be identified and addressed; (ii) smart contract disclosures; and/or (iii) code audits that can be arranged to ensure no unidentified issues with code. Even though code can operate in a way that was not intended, market participants who transact through DeFi Protocols generally accept that they are relying on the immutability of code, rather than external factors (including legal recourse in contract or other private law causes of action), to enforce their transaction. Of course, while market participants understand these risks and that private contractual law recourse is not required, this does not obviate the need for criminal law in relation to DeFi, where bad actors commit the same crimes in the DeFi space that are widely accepted to be illegal outside of it (such as fraud). Accordingly, the typical means of criminal recourse and requirements for forfeiture of assets are still relevant to DeFi Protocols and Apps. We also reiterate our support for bespoke regulatory requirements that mitigate risks unique to DeFi as well.

¹⁸ Para 75, [2022] EWHC 667 (Ch).

¹⁹ *Ibid*, para 67.

- (q) To summarise our response to this question 7(1), we agree that contractual disputes are not likely to come before the courts in relation to DeFi Protocols because people that interact with DeFi Protocols will not form legal contracts. Similarly, we do not believe that, in general, contracts will be formed in other aspects of the DeFi space, like DeFi Apps. Of course, this is a heavily facts and circumstances dependent question that for DeFi Protocols depends on the extent of decentralisation of the network, and for DeFi Apps depends on factors including the presence of account relationships.

2.4 Question 7(2): Do you agree that, as a result, these disputes will not be resolved with reference to private international law and the question of applicable law?

- (a) While we note that this question refers to “*disputes*”, rather than specifically contractual disputes, we assume that it is only concerned with contractual disputes given the context of the question and the surrounding discussion in part 7 of the Consultation.
- (b) Given the arguments that we have already set out in response to question 7(1), we would dispute the underlying assumption of this question 7(2) (of contractual disputes in DeFi). As set out at paragraphs 2.3(e) – 2.3(l), where someone interacts with a DeFi Protocol, the requirements for establishing a legal contract are not met and so, contractual disputes will not arise.
- (c) We would caveat our response at paragraph 2.4(b) above with the acknowledgement that it is not the case that no contracts are formed at all in the crypto or DeFi space. As set out at paragraph 2.3(m), the response to this question will differ where decentralisation has not been fully achieved or where interactions are with DeFi Apps that function like traditional centralised intermediaries (i.e., requiring account relationships, holding proprietary user information, custodial user assets, etc.). In such cases, we see no reason why these disputes will not be resolved with reference to private international law and the question of applicable law.

2.5 Question 7(3): Would the law applicable to these kinds of disputes benefit from further clarification?

- (a) In our view, no clarification is required. English common law has refined the definition of a contract for hundreds of years, and it is sufficiently clear to us if and when contract law would apply to disputes in relation to DeFi.
- (b) It is important to ensure clarity regarding any guidance or recommendations that the Law Commission ultimately issues as a result of this Consultation. This is essential to ensure that, if any changes to law or guidance are made for DeFi, the changes are based on solid foundations. Based on our reading of the Law Commission’s considerations in the Consultation, we view it as particularly important that the Law Commission’s understanding of DeFi Protocols and Apps is clear and reflects how such DeFi Protocols and Apps operate technically and in practice.

3. QUESTIONS 10(1) – (3)

- 3.1 The characterisation of cryptoassets has been subject to significant discussion in the UK and globally and, given the advanced nature of such discussions, we think that framing our responses to these questions 10(1) – (3) by reference to the regulatory characterisation of cryptoassets is useful.
- 3.2 The FCA takes a case-by-case approach to determining the regulatory characterisation of cryptoassets, which is set out in the FCA’s Guidance on Cryptoassets (the “FCA

Guidance).²⁰ For example, paragraph 30 of the FCA Guidance includes a list of factors that should be considered as part of an analysis to determine whether a cryptoasset would be deemed a security, given that not all cryptoassets are automatically deemed securities. In essence, the approach in the FCA Guidance is that the UK’s current laws and regulation will be applied to cryptoassets in the same way that they would any other asset to determine regulatory characterisation.

- 3.3 This same case-by-case approach is also the basis on which HMT’s proposals for a new cryptoasset regime would operate (the “**UK Crypto Regime**”).²¹ While the UK Crypto Regime expands the existing regulatory position for crypto, it does not change the fundamental approach to characterising cryptoassets, such that whether the UK Crypto Regime will apply to a cryptoasset depends on the characteristics of the individual cryptoasset. The UK Crypto Regime will not apply a block approach whereby any cryptoasset is regulated in the same way as all other cryptoassets. In particular, the UK Crypto Regime will distinguish between cryptoassets that fall within the existing definitions of “traditional” financial instruments and those that do not.
- 3.4 The EU also takes a case-by-case approach to the regulation of cryptoassets both through the upcoming MiCAR²² regime and the EU’s existing regime. Given the complex nature of MiCAR and existing regimes, ESMA was given a mandate to provide guidance on determining the regulatory classification of cryptoassets, which it has published a consultation on, namely the *Consultation paper On the draft Guidelines on the conditions and criteria for the qualification of crypto-assets as financial instruments* (the “**ESMA Consultation**”). We have provided our views on the ESMA Consultation as a whole elsewhere; however, we note that it does make clear that cryptoassets should be characterised through a case-by-case approach in the EU.²³ For example, at paragraph 20 ESMA states “*ESMA is of the opinion that the circumstances must be considered on a case-by-case basis in order to legally qualify crypto-assets. For this purpose, a “substance over form” approach in determining what constitutes a financial instrument should be followed.*”
- 3.5 Without commenting on the actual drafting or outcome of regulation in the UK and the EU (including the outcomes of any related consultations, such as the ESMA Consultation), at a principles level, we agree that the approach taken in both jurisdictions – of assessing cryptoassets on their own particular characteristics – is the right approach.
- 3.6 **Question 10(1): Do the exclusions of financial instruments and transferable securities, as set out in Articles 6(4)(d) and (e) of the Rome I Regulation, apply to crypto-tokens?**
 - (a) Yes, in our view, it is clear that the relevant exclusions will apply to cryptoassets (or crypto-tokens per the wording of the question), to the extent that such cryptoassets constitute financial instruments or transferable securities. As set out above, whether a cryptoasset qualifies as a financial instrument or transferable security will require a case-by-case analysis of the particular characteristics of that cryptoasset; however, a cryptoasset could theoretically fall within the scope of these terms.

²⁰ FCA, *PS19/22, Guidance on Cryptoassets Feedback and Final Guidance to CP 19/3*.

²¹ HM Treasury, *Future financial services regulatory regime for cryptoassets Response to the consultation and call for evidence* (October 2023).

²² Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 (“**MiCAR**”).

²³ We disagree with ESMA’s characterization of non-fungible token series, and as noted above, regulators should take a principles-based case-by-case approach to the classification of all cryptoassets.

3.7 Question 10(2): What would be the positives and negatives of interpreting these provisions in an international way, bearing in mind guidance from the European Securities and Markets Authority?

- (a) Generally, we think that seeking to harmonise rules internationally is a positive step. This is particularly the case given that decentralisation, by nature, lends itself to assets being global, and the Permissionless nature of DeFi Protocols allows users to interact with them from anywhere in the world. Therefore, a globally agreed set of standards for regulating cryptoassets would better equip operators in the space (including providers of crypto services and end-users) and provide important protections for users.
- (b) With that said, we do not think that unilaterally adopting an interpretation for the purpose of a particular regime (such as the Rome I Regulation,²⁴ in this case) that differs from the position that otherwise applies in determining whether something is a financial instrument or transferable security is the right approach. The downside to this approach is that it would be a move away from a well-developed regime in which there is a significant degree of certainty as to whether a cryptoasset would fall under the scope of regulatory regimes and towards another (as yet unclear) regime.
- (c) With regards to the Law Commission's reference to Recital (30) of the retained Rome I Regulations, and question regarding whether courts should look to ESMA guidance in relation to its interpretation for the purposes of Rome I Regulations (we presume because Recital (30) refers to MiFID),²⁵ such an approach would not be correct in our view. Even if it is accepted that retaining a reference to MiFID in Recital (30) was not an oversight, how ESMA or EU member states understand or implement MiFID does not change or impact its text. There is divergence across the EU, as set out in the ESMA guidance referenced at paragraph 8.75 of the Consultation, which showed member state competent authorities taking differing views as to whether certain assets constitute financial instruments. Therefore, taking any approach that looks towards the EU (or other countries) for guidance would not be in accordance with the Rome I Regulations, because the regulations point to definitions in MiFID and not in other states' national laws that have implemented MiFID. This also highlights a further issue with taking an international approach to interpretation, which is that it is ultimately a compromise on all fronts, because it does not deliver an optimal outcome. MiFID and ESMA guidance provides the framework for an outcome, but it is the decision of member states to arrive at the actual outcome, and the states will not necessarily arrive at the same place. Such a divergence in outcomes is not helpful to market participants and highlights that following an international approach (even that of the EU, to which we are closely aligned) does not mean that outcomes will be the same.
- (d) Therefore, this again supports the position that the standard means of interpretation and characterisation of cryptoassets for the purpose of the UK financial regulatory regime (as set out at paragraph 3.8 below) should be followed in the UK.

3.8 Question 10(3): Should the courts simply apply the Financial Services and Markets Act 2000 (Regulated Activities) Order 2001 in line with Financial Conduct Authority guidance?

- (a) In practice, for the purposes of determining whether UK financial services regulatory requirements relating to financial instruments, including prospectus requirements, are

²⁴ Rome I Regulation (EC) No 593/2008 ("Rome I Regulation").

²⁵ Directive 2004/39/EC ("MiFID").

triggered in relation to a cryptoasset, a UK lawyer would consider the relevant definitions of specified investments set out in the Financial Services and Markets Act 2000 (Regulated Activities) Order 2001 (“**RAO**”) in relation to the cryptoasset in question. This is the case, notwithstanding the fact that; for example, UK prospectus requirements are (currently) expressed to be triggered only in relation to certain offers of “transferable securities” to the public in the UK.

- (b) Practically, this approach works because the RAO provides the vehicle to implement the definitions of MiFID “financial instruments” (including “transferable securities”) into the UK financial regulatory regime. Accordingly, in our view, while it may be technically possible to query whether the specified investments set out in the RAO accurately capture the MiFID notion of a “financial instrument,” there is very little risk of any such divergence arising in practice whilst the UK continues to maintain alignment with the current approach to defining regulated investments for the purposes of the UK financial regulatory perimeter. Indeed, from a UK perspective it would be highly unusual to assess the regulatory characterisation of a cryptoasset under the RAO and come to the conclusion that the cryptoasset in question was not a specified investment, but still go on to consider whether it was a “financial instrument” under MiFID and then come to a different conclusion. To do so would be to suggest that the UK did not implement MiFID properly.
- (c) Given that there is pre-existing guidance on this issue that has been subject to comment and review by those familiar with the market, the RAO (and accompanying guidance) is what the courts should apply when determining whether cryptoassets fall under the definitions of financial instrument and transferable security. It would be unhelpful if a separate interpretation of the relevant definitions was introduced, which was only relevant in the specific Rome I Regulation context and would create uncertainty and confusion in the market. Particularly given that the Rome I Regulation is relevant to consumer contracts, this would not be the optimal outcome.

4. QUESTION 19 (4), (6) & (7)

- 4.1 As with our responses to the questions above, and particularly questions 7(1) – (3), it is useful to consider these questions 19(4), (6) and (7) with a focus on DeFi, as distinct from the position that may apply to these questions in a CeFi context. We agree with the overarching theme of the Law Commission’s discussions in part 12 of the Consultation, which is that the nature of decentralisation, DeFi, and cryptoassets results in difficult questions regarding the correct approach to determining where cryptoassets are located and therefore what applicable law should apply to them. We appreciate the Law Commission’s efforts to bring together a variety of suggestions that have been made to address these complexities. However, we believe that some of the relevant ideas mentioned in the Consultation would be an inappropriate basis from which applicable law or jurisdiction should be applied to cryptoassets and sometimes involve strained attempts to draw connections between decentralised cryptoassets or protocols and particular entities, individuals, or territories. On the other hand, certain suggestions in the Consultation have merit as potential frameworks through which applicable law can be decided going forwards. Ultimately, our view is that a principles-based approach is most appropriate, and courts should focus on achieving appropriate outcomes for parties involved in disputes, rather than trying to find novel ways of applying existing legal constructs (such as *lex situs*) that do not necessarily work for new types of assets. Furthermore, as set out throughout our responses it is important to consider that, in some cases (such as in relation to DeFi Protocols), the nature of the technology, being open-source and autonomous, will significantly mitigate the risks that existing private international law addresses and therefore may diminish the need for these private law principles to be applied.

4.2 **Question 19(4): To what extent would recourse to a distinct rule based on the connecting factor of the “owner” or “transferor” for cases where parties have voluntarily dealt with one another obviate the need for us to consider further the application of the *lex situs* rule to cases where the parties to the dispute are strangers?**

- (a) We take this question as an opportunity to consider the suggested approaches in the Consultation to determining applicable law, and give our views as to the appropriateness of these tests, as well as our preferred approach to determining applicable law going forwards. In summary, we do not think that the factors of “owner” or “transferor” should be used to determine applicable law and that the continued application of *lex situs* to cryptoassets should be reconsidered, in favour of a principles-based approach.

(i) **Original Coder²⁶**

- (A) The Law Commission raised the possibility in the Consultation that the law applicable to a cryptoasset could be the place where the original coder had their primary residence (the “**Original Coder Approach**”), based on a suggestion previously put forward by the Financial Markets Law Committee (“**FMLC**”).²⁷ We could see merits to the Original Coder Approach where the original coder is still completely in control of the network and runs the relevant computing hardware from within their jurisdiction, but importantly, this would clearly signify that the network is not decentralised, as per the tests outlined in Section 2.2(a). In that case, reasonable arguments could be made that the cryptoassets are all in the same jurisdiction. This scenario will evidently not occur where decentralisation (as set out in paragraph 2.2(a) above) has been achieved and is therefore not an appropriate approach to take to determining applicable law.
- (B) In addition, relying on the Original Coder Approach means a cryptoasset would be linked to the country of its original coder indefinitely. This is conceptually challenging in relation to a decentralised network for a number of reasons, including: (i) the original coder could have gone on to other projects years before a decision is made on applicable law; (ii) the network may have no nexus to the coder’s jurisdiction at the point in time when the decision is made on applicable law; and (iii) the network nodes may be distributed across the globe, making any one of a number of countries potentially more relevant to the network than that of the original coder. Such an approach would also be difficult practically, in terms of locating original coders and deciding upon the applicable law based on this. For example, taking the example of bitcoin, the most widely traded and capitalised cryptoasset, the Original Coder Approach would not result in a clear outcome given that the original developer of bitcoin remains unknown. In the absence of being able to locate the original coder, it is unclear what the appropriate next step would be, and there is no clear line of reasoning that follows from the Original Coder Approach that would lead to an outcome in this scenario.

²⁶ Para 12.76 of the Consultation.

²⁷ FMLC, *Distributed Ledger Technology and Governing Law: Issues of Uncertainty* (March 2018), para 6.28.

- (C) As is clear from our arguments above, the Original Coder Approach gives too much attention to the original coder in determining applicable law to cryptoassets. If the Original Coder Approach is adopted in any way, our concern is that it gives credence and legitimacy to the incorrect idea that the original coder is of significant importance to the functioning of a decentralised network on an ongoing basis. It would not require a large misstep in reasoning to then conclude that the original coder has some form of responsibility for the network on an ongoing basis, simply because of their initial involvement with the protocol. Such a conclusion would not only be objectively unfair from a principles perspective (given that the original coder may no longer have any control or input in the functioning of the protocol), but deeply problematic from a commercial and policy perspective, in that being a founder and original coder would entail potentially unlimited and uncontrollable risk if their control over a network was ever relinquished (therefore disincentivising decentralisation, which would be a great disadvantage to innovation globally in our view). This outcome is not the direction that English and Welsh law should move towards.
- (D) We note that the FMLC themselves raised issues with this approach, noting it would be *“difficult to explain why the original coder should impact the ongoing life of the distributed ledger where s/he is not also the system administrator.”*²⁸ We strongly agree with this comment and thus, as the Law Commission itself has noted this difficulty with the Original Coder Approach, would hope that it is given no further consideration going forwards.

(ii) **The closest and most real connection**²⁹

- (A) The Law Commission suggested that courts could look towards the place that has the closest and most real connection to a blockchain network, in order to determine the law that applies (the **“Closest Connection Approach”**). It then also set out arguments from Michael Ng (the proponent of the Closest Connection Approach) that this results in a conclusion that the law of Massachusetts applies to bitcoin because of various linking factors. We believe that each of the factors is incomplete and unworkable, and we address them in turn:

- (I) **An initial developer of the Bitcoin network is resident in Massachusetts:** Such an argument is similar to the Original Coder Approach discussed above, which we disagree with. Addressing the bitcoin example set out in the Consultation, it is not clear how much of an ongoing connection the initial developers or participants in the Bitcoin network have with the network. For example, Gavin Andresen has not contributed to the Bitcoin github since 2016.³⁰ Consequently, our arguments made in paragraph 4.2(a)(i) above again become relevant, given that he appears to have no direct ongoing connection to the functioning of the network, which

²⁸ *Ibid.*

²⁹ Para 12.74 and 12.75 of the Consultation.

³⁰ See Bitcoin Github, <https://github.com/bitcoin/bitcoin/commits/master?author=gavinandresen>.

suggests limited importance of a network's previous developers. Accordingly, there is no reason why Massachusetts should be more relevant to the location of bitcoin than any other jurisdiction, and presumably the only reason Gavin Andresen was mentioned at all is because the identity of Satoshi Nakamoto is unknown, which again highlights the flaws with this approach. This unknown also has the potential to cause more issues for the Closest Connection Approach going forward. For example, if Massachusetts was considered the applicable jurisdiction for a number of years and disputes were settled on this basis, only for Satoshi Nakamoto to then be identified as someone resident in England or Wales, the correct jurisdictional outcome would be unclear, i.e., whether the applicable law to the Bitcoin network would need to change to the law of England and Wales.

- (II) **Funding for bitcoin was received from MIT, further linking the network to Massachusetts:** We do not agree that the place from which funding originates should dictate applicable jurisdictional law. In the context of bitcoin, and all decentralised networks, funding of the network does not result in legal ownership rights over the network in the way that it typically would with funding of a legal company, so the network cannot be said to closely relate to the jurisdiction of its funders in that way. While funding may result in cryptoasset issuance (and associated governance and economic rights), we note that the Closest Connection Approach does not seem to consider that when assessing connections, presumably because looking at global cryptoasset ownership to understand the applicable law for a decentralised network would give rise to significant difficulties. In addition, looking at cryptoasset ownership is more aligned with an approach of deciding law on an individual, rather than network-wide basis.
- (III) **Network participants are all connected through an MIT open-source licence:** This factor touches on what could theoretically be a relevant consideration, namely the network participants, but then ignores this group to focus on the software that connects them. It is unclear why the use of an MIT open-source licence suggests proximity to Massachusetts, given that such a licence could be used anywhere in the world and does not require any sort of physical proximity or connection to Massachusetts.

- (B) While we addressed each of the factors used in the Closest Connection Approach in turn to make clear why they are not an appropriate basis upon which to characterise the location of a decentralised network, our broader argument is that this general approach is incompatible with the way in which a decentralised network functions.
- (C) It is enlightening that Michael Ng himself "*accepts that these factors do not suggest that the Bitcoin network is "particularly closely*

*connected” to Massachusetts in “absolute terms.”*³¹ It is a logical leap of reasoning to accept his statement, but still suggest that Massachusetts is the appropriate jurisdiction to base the applicable law of the whole network, although Ng does suggest *“that Bitcoin, which is by design disconnected from any legal system, is “more closely connected” to Massachusetts than any other system* [our emphasis].”³² Because the Bitcoin network (and by extrapolation other decentralised networks) are by design disconnected from any particular jurisdiction, we suggest that trying to develop new approaches to determining the physical location of bitcoins, which seeks to categorise a whole network of assets that are owned on a dispersed and global basis in a uniform manner, is not appropriate.

- (b) Having discussed the issues with some of the approaches raised in the Consultation, we explore other meritorious suggestions below.

(i) **Relevant participant**³³

- (A) We note the Law Commission’s reference to Professor Andrew Dickinson, who presents interesting arguments that are worth further consideration. It is important to note that his suggested approach (the **“Participant Approach”**) is only intended to apply in relation to transactions outside of a cryptocurrency system, so essentially transactions that occur off-chain. Examples of transactions that he considers relevant for framing this approach include transfers of interests in cryptoassets (such as by way of security), attachments by judgement creditors, or governmental expropriation.³⁴
- (B) In his arguments, Professor Dickinson raises similar points to those that we have raised throughout our responses. Namely, that transactions involving cryptoassets will *“frequently not involve a ‘claim’ in the sense of a legal right.”*³⁵ Rather, on networks such as the Bitcoin network, the value of participants’ ‘entitlements’ generally does not depend on legal rights but on legitimate user expectations that consensus rules underpinning the network will function consistently and not be used to deprive them of their assets, which is a *“factual and not a legal benefit.”*³⁶
- (C) Professor Dickinson compares cryptoassets to the concept of goodwill in a business, given that both are intangible assets. While we do not question the merits of this analogy on a legal basis, from a commercial or common-sense perspective, the concept of goodwill and cryptoassets are distinct. Cryptoassets, as Professor Dickinson points out, are grounded in fact and code. A person who holds a cryptoasset in a wallet knows that he or she has ownership of the

³¹ Para 12.75 of the Consultation.

³² *Ibid.*

³³ Para 12.73 of the Consultation.

³⁴ A Dickinson, “Cryptocurrencies and the Conflict of Laws” in D Fox and S Green (eds) *Cryptocurrencies in Public and Private Law* (2019) para 5.93.

³⁵ *Ibid* para 5.106.

³⁶ *Ibid* para 5.107.

cryptoasset. Goodwill, on the other hand, is “*the benefit and advantage of the good name, reputation and connection of a business*”³⁷ and a more difficult concept to identify and quantify.

- (D) Disregarding these conceptual differences, it is still useful to understand how Professor Dickinson arrives at the conclusion that participation is the appropriate lens through which to assess applicable law. His argument is essentially that as the intangible property in a cryptoasset arises from participation in that cryptoasset network, the location of the participant is the appropriate way to determine applicable law. This concept of network participation as a key factor grounds this approach in the facts of how a decentralised network operates and so is a more convincing argument than the Original Coder Approach and Closest Connection Approach discussed above.
- (E) While Professor Dickinson also addressed this criticism, we would like to address one of the criticisms raised with this approach by FMLC. It notes that this approach “*artificially splits up the distributed ledger record, leading to the application of different laws to transactions involving different participations.*”³⁸ Firstly, as Professor Dickinson points out, the Participant Approach is only intended to apply to transactions outside the cryptoasset network and so does not affect the distributed ledger. Secondly, we do not see the suggestion that different laws will apply to different transactions as an argument against this approach, or that the distinction is “*artificial.*” As we have already set out in our arguments above, it is more artificial to uniformly apply the law of a jurisdiction to a whole network that by its nature will not have a close link to that jurisdiction. The nature of cryptoassets is that the law that applies to them should be determined on a case-by-case basis, rather than on a wholesale basis. We note that Professor Dickinson makes similar points, noting that trying to identify a single law for all transactions in a cryptoasset would “*come at the cost of greater uncertainty without any obvious advantages for participants in the system or third parties.*”³⁹

(ii) Principles-based approach⁴⁰

- (A) In our view, the arguments put forward by Amy Held are also convincing. We agree that the omniterritorial nature of cryptoassets makes it difficult to uniformly apply existing legal concepts to ascertain their location for the purposes of applicable law. We also agree that a well-considered supranational approach to such matters may be helpful. However, we recognise that practically, this may not be forthcoming and given the growing nature of cryptoassets and DeFi globally, each jurisdiction should consider their approaches to this issue in lieu of broader agreements.

³⁷ *Muller & Co's Margarine Ltd v Inland Revenue Commissioners* [1901] A.C. 217.

³⁸ n[34], para 5.111.

³⁹ *Ibid*, para 5.112.

⁴⁰ Para 12.82 and 12.83 of the Consultation.

- (B) In the absence of an agreement, the suggestion for courts to take an internationalist approach reflecting commercial practices around omniterritorial assets (the “**Principles-based Approach**”) is the most sensible option. We find the following suggestions by Amy Held to be particularly convincing: *“courts should do this in a way that ‘recognises the differences between national systems of property law; does justice in the immediate case; gives effect to the parties legitimate expectations, especially those relating to market practice and conventions; takes into account the decisions of other national courts and international developments; and most, importantly, anticipates that such approach will eventually lead to global principles that may inform a future convention.’”*⁴¹
 - (C) Of all the approaches set out in the Consultation, this approach seems to most readily accept that decentralised cryptoassets will not necessarily fit within existing legal principles. Ultimately, the law needs to be flexible and adaptive to the novel nature of these assets, and there is not one particular legal principle that can be referred to at the moment which addresses all of the issues that are currently in question. Therefore, there must be some degree of deference to courts to adopt positions that achieve principles-based outcomes. The Principles-based Approach is a positive step in that it embraces the inherently global nature of decentralised networks and assets.
- (c) In conclusion, we recognise the complexity that is involved in seeking to decide on jurisdictional rules relating to cryptoassets and appreciate the Law Commission’s efforts to bring these suggestions together, but we respectfully suggest that some of the Law Commission’s suggestions are not appropriate and should not be taken further. We presented our concerns with the Original Coder Approach and the Closest Connection Approach, and we think neither of these are suitable for further development. The Original Coder Approach and Closest Connection Approach do not adequately capture the decentralised nature of blockchain networks. As set out, we recognise that these approaches attempt to categorise whole networks as located in one jurisdiction for the purposes of applicable law, but it is clear from the issues with these arguments that such an approach does not work for decentralised, global, and distributed networks.
- (d) In our view, it is important to take a practical and principles-based approach to this matter going forwards, which recognises that there may be no single existing legal principle which can be applied to cryptoassets in order to produce an appropriate outcome. Amy Held’s arguments are most convincing because they accept the complex realities of decentralised cryptoassets and allow for flexibility to achieve sensible outcomes.
- 4.3 **Question 19(6): To what extent is it 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”?**
- (a) We would argue that there is an important distinction to be made when answering this question, which is whether claims are being made in a CeFi or DeFi context. We set

⁴¹ Para 12.83 of the Consultation. A Held, “Crypto Assets and Decentralised Ledgers: Does Situs Actually Matter?” in A Bonomi, M Lehmann and S Lalani (eds), *Blockchain and Private International Law* (2023) p 257.

out the differences in these contexts below and explain why, in our view, such disputes will continue in a CeFi context but are likely to be rare in a DeFi context.

- (b) For the purpose of this question 19(6), we will consider a common form of involuntary dispossession, in which someone (the “**Owner**”) is tricked into giving away the private keys to their wallet. Once they have given away their private key to a bad actor (the “**Bad Actor**”), the Bad Actor is able to transfer cryptoassets out of the Owner’s wallet and into their own wallet or account (through one transfer or a number of different transfers). This could be a wallet held on-chain, or a wallet held with a CeFi custody provider. In the vast majority of such cases, the Owner does not know the identity of the Bad Actor but may attempt to trace their cryptoassets through the blockchain.

(c) **CeFi**

- (i) In some cases, the Owner will trace their cryptoassets to centralised exchanges or custody providers.⁴² The Owners can then seek an injunction against the centralised exchange, freezing the relevant cryptoassets, despite the fact that they ultimately do not know the identities of the Bad Actors. The Owner can also request the CeFi intermediary to provide any information they have on the identity of the Bad Actors to further assist with the claim.

(d) **DeFi**

- (i) In other cases, the Owner may trace their cryptoassets to an on-chain wallet with an unidentified owner. In this case, given that the nature of DeFi allows direct peer-to-peer transactions and custody of cryptoassets without intermediaries, there may be no identifiable third-party actor to seek recourse from.
- (e) Therefore, we consider it likely that cases brought in relation to decentralised cryptoassets held on Permissionless Blockchains but via centralised intermediaries, such as centralised exchanges or custody providers will continue to come before the courts. Owners may recognise that the possibility of direct recourse against anonymous Bad Actors is low, but the existence of centralised intermediaries makes bringing the dispute worthwhile because there is at least a possibility of useful recourse.
- (f) In a DeFi context, there is no third-party intermediary. Therefore, where an Owner concludes that there is no reasonable chance of identifying the Bad Actor, it is unclear what the Owner would gain by bringing their claim before a court, as there is no realistic prospect of recourse (unless the Bad Actor has moved the ill-gained assets from a DeFi ecosystem to a centralised entity). This again highlights the point that we have made throughout our responses, which is that the nature of DeFi results in its own unique risks.

4.4 **Question 19(7): How should courts approach the question of applicable law in such disputes relating to decentralised digital assets held in permissionless DLT networks where the parties have not dealt with one another and there has been an “involuntary dispossession”?**

- (a) As with question 19(6) above, to answer this question a distinction needs to be made between CeFi and DeFi contexts. Ultimately, the principles that are applied should be the same (namely the Principles-based Approach we advocated for in our response to

⁴² See *AA v Persons Unknown & Ors Re Bitcoin* [2019], for example.

question 19(4)). However, as discussed in response to question 19(6), the likelihood of: (i) these disputes coming before courts in a DeFi context is low; and (ii) there being any legitimate recourse that courts can offer to Owners is also low. We see no issue in applying the Principles-based Approach in the CeFi context, as such an approach should result in the most appropriate outcomes that are also consistent internationally with other jurisdictions that take reasonable approaches to such issues.

Ashurst LLP
London Fruit & Wool
Exchange
1 Duval Square
London E1 6PW

Tel +44 (0)20 7638 1111
Fax +44 (0)20 7638 1112
DX 639 London/City
www.ashurst.com

23 May 2024

By email

conflictoflaws@lawcommission.gov.uk

Commercial and Common Law Team
Law Commission
1st Floor, Tower
52 Queen Anne's Gate
London SW1H 9AG

Dear Team,

Call for Evidence: Digital Assets and ETDs in Private International Law: Which Court, Which Law?

On behalf of Ashurst LLP, I have the pleasure to provide this response to the Law Commission's Call for Evidence.

Ashurst LLP is a leading international law firm, and our global, multi-disciplinary team of experts provides innovative advice to local and global corporates, financial institutions, and governments on all areas of commercial law. Our practitioners have deep experience and are involved across the cryptoasset and Digital Asset industry on some of the most strategic and innovative projects to date.

Our response contains our own views based on our general knowledge of Digital Assets and our experience of advising clients in respect of specific examples of Digital Assets. Our response is not made on behalf of any of Ashurst's clients. We have responded to a number of the questions in the Call for Evidence in the Annex to this note.

We welcome the work of the Law Commission to develop the issues that arise from the cross-border nature of many digital assets undertakings. Although the use of digital ledger technology (DLT) does not always involve such considerations, the range of operating models with cross-border elements does create a need to address potential conflicts of laws from property, contract, and tort/delict perspectives.

To this end, we have also welcomed the work of UNIDROIT, reflected in the "Principles on Digital Assets and Private Law" ("UNIDROIT Principles"). The approach taken in the UNIDROIT Principles to the determination of applicable law has merit, in so far as it focusses on proprietary issues. We have sympathy with the commentary, under Principle 5 of the UNIDROIT Principles, that it would be "incoherent and futile" to make a list of connecting factors for choice of law purposes that could have universal application.

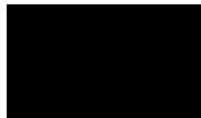
At the same time, it could seem a peculiar outcome if a buyer and seller in different jurisdictions than the issuer of a digital asset were to have a dispute between them resolved under, for example, the applicable law of the domestic law of the state of the issuer, where the relevant asset or system on which it is found does not specify the applicable law, following Principle 5(1)(c). Although this could be entirely appropriate, in some cases, it is not difficult to conceive of

cases which would be better addressed in other ways. For this reason, we would suggest that the preferred position in the UK is to develop the Rome I and Rome II approaches on a case-by-case basis. The choice of law rules in private international law are notoriously difficult to narrow, due to the variety of facts that arise in particular cases. In our view, the waterfalls in the Rome I and Rome II Regulations, as assimilated into UK law, provide a stable and tested starting point for the development of the law in this area.

The novel features of digital assets ought to be addressed thoughtfully, but they should not be given undue weight. At their most basic level, digital assets represent entries in databases. Generally, it is not difficult to expand the rules applicable to, for example, cases involving intermediation (including commercial agency and trust concepts) to take account of the specific features of digital assets. The questions that arise in tort cases with cross-border elements (eg, the localisation of losses) ought to be addressable, in most cases, through consideration of the facts of particular cases, rather than through *ex ante* specifications.

We hope that our comments are of assistance. We are available to discuss any of the points in this response.

Yours faithfully,



Etay Katz, Partner
ASHURST LLP

ANNEX

QUESTION 1

In this question, we seek views and evidence on jurisdiction over consumer contracts.

(1) To what extent can the issue of jurisdiction over consumer contracts in the digital and decentralised contexts be accommodated by section 15B of the Civil Jurisdiction and Judgments Act 1982?

In our view, s. 15B of the Civil Jurisdiction and Judgments Act 1982 (the "1982 Act") provides a broad basis for a consumer domiciled in the UK to seek relief. Where a consumer has engaged a service provider outside of the UK for digital assets or uses decentralised technologies to enter into the transactions, then the position is essentially the same as for cross-border e-commerce. Consumers domiciled in the UK, entering into transactions for digital assets or using decentralised technologies to enter into transactions, should have the same rights and remedies as for other consumer contracts, including the availability of s. 15B of the 1982 Act.

This does not mean, however, that, in transactions for or involving digital assets, a consumer contract will always be found with the same readiness as for other contracts made at a distance (eg, by e-commerce). One challenge is that s. 15E(1)(c) of the 1982 Act defines one of the parties to a "consumer contract" as a person who:

- "(i) pursues commercial or professional activities in the part of the United Kingdom in which the consumer is domiciled, or
 - (ii) by any means, directs such activities to that part or to other parts of the United Kingdom including that part,
- and which falls within the scope of such activities [...]"

The challenge for a claimant will be to identify the person who can be shown to "pursue commercial or professional activities" when entering into the relevant contract. Even where such a person can be found, a second challenge will be to show that their participation in a distributed network meets either of the limbs in this part of the definition; ie, that their activities are in or directed to the relevant part of the United Kingdom.

In the case of *Bitar v Banque Libano-Francaise SAL*, [2021] EWHC 2787 (QB), the claimant was able to demonstrate that a Lebanese bank which maintained a Web site aimed at the Lebanese diaspora generally was directing its commercial or professional activities to the United Kingdom. A question that will have to be answered by the courts, in due course, is whether the same result obtains when a

person is, for example, operating an offshore node of a distributed network and engaging in transactions with other participants who are domiciled in the UK.

(2) Does the fact that the business is a crypto-business, as opposed to any other business, change the analysis of whether a business has directed its services to consumers located in the UK?

No. The situation with cryptoassets and e-commerce is fundamentally the same. A firm which does not wish to expose itself to consumer claims in the UK can exclude UK-domiciled consumers from accessing its services. There are KYC, AML and other checks, along with technical means available to support a policy of exclusion.

(3) Are there any changes or clarifications that are needed in respect of the issue of jurisdiction over consumer contracts?

An amendment could be made to s. 15B(7) of the 1982 Act with the object and effect of granting the consumer a right to treat its home jurisdiction as the forum for pursuit of claims against the issuer of digital assets.

(4) To what extent does this issue cause problems in practice (or is likely to in future)?

QUESTION 2

In this question, we seek views and evidence on jurisdiction founded on the basis that a contract was concluded in England and Wales.

(1) How should the courts apply gateway 6(a) to a smart contract? Should the relevant connecting factor be the participating computer, or the real-world actor?

In our view, the courts should apply gateway 6(a) to a smart contract on the basis of the real-world actor, rather than the participating computer. The location of IT systems at offshore locations is a matter of commercial convenience which can have little bearing on the making of contracts. If we take an example where the parties to a contract are in England and France, while the IT systems they are using to communicate offers and acceptances are in different third countries, it would seem peculiar if the law of one of the third countries was selected to resolve questions of applicable law because of the locations of system components.

(2) If gateway 6(a) should use a connecting factor based on the real-world actor, how should their location be determined? Should it be by their habitual residence, their domicile, or at the place where they happen to be at the time the contract was formed?

The habitual residence test is the most appropriate test. The test can be found in the Rome I Regulation and is assimilated into UK law by The Law Applicable to Contractual Obligations and Non-Contractual Obligations (Amendment etc.) (UK Exit) Regulation 2019 and the Jurisdiction, Judgments and Applicable Law (Amendment) (EU Exit) Regulations 2020.

(3) Has the question of where a smart contract is made arisen in legal and commercial practice? If so, please provide details.

(4) To what extent is it likely that the question of where a smart contract is made will become prevalent in practice?

We would hope this is unlikely. It would be undesirable for a rule to develop that links the applicable law to the location of a system component on which a smart contract is executed. Were that the case, then it is possible that the participants in the relevant system or the users of the relevant service could be unaware of the applicable law or become subject to the applicable laws of jurisdictions they had not anticipated when they joined the system or signed up to the service.

The relevant factor is the habitual residences of the parties to the dispute, who are responsible for the relevant smart contract or for interacting with it. In cases where the smart contract is operated within, for example, a trading platform, then the rules of the trading platform and the law applicable to the trading platform would also be relevant considerations; but the place where the trading platform operator locates their servers ought not to be determinative.

QUESTION 3

In this question, we seek views and evidence on jurisdiction founded on the basis that damage or detriment was suffered in England and Wales.

(1) Do you consider the approach of the courts of England and Wales so far in the crypto litigation when localising damage or detriment for the purposes of jurisdiction to be theoretically sound?

(2) To what extent can it be said that the tortious damage pleaded in the cryptotoken litigation are not cases of pure economic loss? How else could tortious damage in the crypto-token context be conceptualised?

(3) If the crypto-token cases are cases of pure economic loss, to what extent would it be desirable that a consistent approach is taken in England and Wales to localising pure economic loss as between jurisdiction and applicable law?

QUESTION 4

In this question, we seek views and evidence on jurisdiction founded on the basis that an unlawful act was committed in England and Wales.

(1) To what extent is the approach of the courts of England and Wales so far in the crypto litigation when localising where an unlawful act was committed for the purposes of jurisdiction theoretically sound?

(2) To what extent does the question of where an unlawful act is committed or event occurs for the purpose of jurisdiction arise in practice?

QUESTION 5

In this question, we seek views and evidence on jurisdiction founded on the basis that the claim relates to objects within England and Wales.

(1) To what extent is the approach so far of the courts of England and Wales in localising a crypto-token for the purposes of jurisdiction theoretically sound? What would be the relative merits and demerits of any alternatives?

(2) What point in time is relevant for gateways 11 and 15(b)? Do these gateways require that a crypto-token is within England and Wales: at the time of proceedings, at the time of misappropriation, or some other time?

(3) To what extent does the question of where a crypto-token is located for the purpose of jurisdiction raise issues in practice?

QUESTION 6

In this question, we seek views and evidence on the types of claims and causes of action relied upon in applications to serve proceedings relating to crypto-tokens out of the jurisdiction.

(1) To what extent can it be said that there is a serious issue to be tried where claimants allege that exchanges are constructive trustees in the circumstances pleaded in Piroozzadeh v Persons Unknown and comparable cases?

We would not rule out the possibility that an exchange might be found to be a constructive trustee of digital assets which have been delivered to it by a person other than the rightful owner. It will depend on the circumstances of the case whether a constructive trust could be found to exist.

Although the court in *Piroozzadeh* did not need to establish whether the requirements for a constructive trust had been met, the case turned on the exchange being a bona fide purchaser for value without notice. In a case where the exchange is on notice that another person has a superior claim to ownership, then it would not be able to rely on the bona fide purchase for value without notice defence. If it acquired the relevant cryptoassets in those circumstances, then a constructive trust claim could have merit.

The other possibility is that ownership does not transfer to the exchange when assets are placed with it. Many exchanges offer custody services for digital assets. Increasingly, in light of MiCAR in the EU and forthcoming rules in the UK, these are going to take the form of segregated (ie, insolvency remote) holdings. Where this model is applied, the claim that the deposit of a cryptoasset is a purchase for value by the exchange/custodian is less likely to be given force. Finding a constructive trust in a jurisdiction outside of the UK is, however, likely to be problematic – it seems to us that the reverse case (where the constructive trust is imputed to an exchange in the UK in relation to a holder elsewhere) is more likely.

(2) Is there any further practical evidence we could consider in relation to the ways in which exchanges defend or intend to defend applications and/or claims alleging they are constructive trustees at the return date of these applications?

(3) Are there similar problems with causes of action under any of the other gateways?

(4) Are these cases indicative of a need to consider more carefully the “serious issue to be tried” limb of the three-stage test for service out of the jurisdiction?

QUESTION 7

In this question, we seek views on applicable law and decentralised finance (DeFi).

(1) Do you agree that contractual disputes in the context of DeFi are not likely to come before the courts?

No. In any situation that involves competing rights and interests, controversies may arise which will likely require the assistance of the courts to resolve. DeFi arrangements present novel problems. Unless the parties to any dispute agree to resolve them by other means, then we anticipate that issues will be brought before the courts.

DeFi arrangements take many forms. There are some which reflect attempts to "democratise" ownership and governance. There are others which are, in fact, heavily reliant on an inner circle of coders or participants; sometimes, to such an extent that it is questionable whether they ought to be described as DeFi.

Each case has to be assessed on its own facts. However, in our view, there is often a basis for looking at DeFi arrangements as multilateral contracts between the participants in the relevant system. Wherever a participant experiences harm, we would expect claims to arise. The novel technical features of DeFi systems raise questions about the applicability of existing rules. We would, therefore, expect, in the absence of ADR, that such claims will be submitted to the courts for resolution.

(2) Do you agree that, as a result, these disputes will not be resolved with reference to private international law and the question of applicable law?

We do not agree that, as a result, these disputes will not be resolved with reference to private international law and the question of applicable law. Where the parties to a dispute are in different states, then the steps to identify the applicable law will still be relevant. Party autonomy, though important, is not always used in order to specify applicable law in clear ways; and, accordingly, questions are expected to arise.

(3) Would the law applicable to these kinds of disputes benefit from further clarification?

Yes, it would be beneficial for the law applicable to these kinds of disputes to be further clarified. We would suggest that the waterfall used in the Rome I and Rome II approaches, as assimilated into UK law, should be the starting point for any analysis.

QUESTION 8

This question concerns the applicable law for non-consumer contracts.

(1) Can the provisions of the Rome I Regulation for identifying the applicable law for non-consumer contracts be applied to contracts involving cryptocurrencies without undue difficulty?

Broadly, yes, the provisions of the Rome I Regulation for identifying the applicable law for non-consumer contracts can be applied to contracts involving cryptocurrencies without undue difficulty.

(2) If the provisions cannot be applied, or can only be applied with significant difficulty, what are the possible solutions?

(3) If the provisions can be applied easily or without undue difficulty, are there any areas that would benefit from further clarification?

Notwithstanding our view that the provisions of the Rome I Regulation for identifying the applicable law for non-consumer contracts can be applied to contracts involving cryptocurrencies without undue difficulty, the waterfall used to identify the applicable law in the absence of choice, in Art 4 of the Regulation, does not align completely to the markets for cryptoassets.

Digital securities traded on a multilateral system under MiFID (ie, MTFs) will fall within Art 4(1)(h); meaning that the "single law" that governs the system will also apply to contracts concluded within it. However, a transaction executed on a trading platform operated by an unregulated firm (or, in the EU, regulated as a crypto-asset service provider under the Markets in Crypto-Assets Regulation) would, pursuant to Art 4(2) of the Regulation, be governed by the law of the country where the party required to effect the characteristic performance of the contract has their habitual residence. Although the markets for native crypto-assets and digital securities are distinct, it ought to be considered further whether there is merit in aligning these arrangements.

The provisions of Art 4(3) and 4(4) of the Rome I Regulation remain important to address the determination of applicable law appropriately. The issue we would flag here is whether accommodation for trading platforms ought to be introduced on par with MTFs.

(4) To what extent is the application of these provisions problematic in practice?

The provisions of the Rome I Regulation have not proved problematic, generally.

(5) If the issue is prevalent in practice, what would be the consequences if it were not resolved adequately as a matter of law?

QUESTION 9

This question concerns the applicable law for consumer contracts.

(1) Can the provisions of the Rome I Regulation for identifying the applicable law for consumer contracts be applied to contracts involving crypto-tokens without undue difficulty?

(2) If the provisions cannot be applied, or can only be applied with significant difficulty, what are the possible solutions?

(3) If the provisions can be applied easily or without undue difficulty, are there any areas that would benefit from further clarification?

(4) To what extent is the application of these provisions problematic in practice?

(5) If the issue is prevalent in practice, what would be the consequences if it were not resolved adequately as a matter of law?

(6) We seek views on whether the provisions of the Rome I Regulation for identifying the applicable law for consumer contracts can be applied to contracts involving crypto-tokens without undue difficulty.

QUESTION 10

This question concerns the exclusions in Articles 6(4)(d) and (e) of the Rome I Regulation.

(1) Do the exclusions of financial instruments and transferable securities, as set out in Articles 6(4)(d) and (e) of the Rome I Regulation, apply to cryptotokens?

The exclusions only apply to crypto-assets which represent "financial instruments" and "transferable securities"; eg, digital bonds.

(2) What would be the positives and negatives of interpreting these provisions in an international way, bearing in mind guidance from the European Securities and Markets Authority?

(3) Should the courts simply apply the Financial Services and Markets Act 2000 (Regulated Activities) Order 2001 in line with Financial Conduct Authority guidance?

(4) To what extent do these exclusions cause problems in practice (now or in the future)?

(5) If these exclusions are problematic in practice, what would be the consequences if they were not addressed as a matter of law?

(6) What kind of reform is needed?

QUESTION 11

We seek views and evidence on localising damage arising in tortious claims relating to crypto-tokens for the purposes of applicable law.

(1) To what extent is it likely that claims in tort, such as those pleaded in the crypto-token litigation for the purposes of service out of the jurisdiction, will proceed to trial before the courts of England and Wales? Is it likely that the question of applicable law will be in dispute between the parties?

We anticipate that claims sounding in tort will be advanced in the courts of England and Wales; particularly where contractual privity is difficult to evidence. Given the cross-border nature of cryptoasset businesses, generally, with many arrangements basing themselves in offshore locations, disputes may be complex and require recourse to the courts to a greater degree than is the case in traditional finance.

(2) If it becomes necessary for the courts of England and Wales to determine the question of applicable law, how could the courts approach the question of localising tortious damage in the broader digital asset and electronic trade documents context? Please indicate whether your response should be considered in the context of the CJEU jurisprudence or in the context of a potential common law approach.

Locating the place where tortious damage has occurred can be challenging; particularly if it is looked at from the perspectives of technical acts that could have

taken place in multiple locations. It is also problematic to look at factors like the locations of accounts in which losses might be evidenced. We would suggest that the courts ought to be able to develop the law on the basis of cases brought before them. The CJEU jurisprudence could be relevant for certain legacy cases, but divergence between the EU and UK is to be expected.

QUESTION 12

We seek views and evidence on recourse to the “escape clause” in Article 4(3) of the Rome II Regulation.

(1) In what circumstances in the digital assets and electronic trade documents contexts would it be appropriate for the courts of England and Wales to have recourse to the escape clause on the basis of a pre-existing contractual relationship?

Where Article 14(1) applies, because the parties have agreed to be governed in their affairs by a particular set of laws, then the courts of England and Wales should continue to give effect to their accord.

In other cases, where there is a pre-existing contractual relationship that is closely connected to the tort/delict, it is open to the courts to apply English law.

(2) To what extent would the parties in a tort claim involving digital assets and electronic trade documents have a pre-existing contractual relationship? Would these represent the vast majority of cases?

We expect that there will be a pre-existing contractual relationship in the majority of cases where a tort claim is made involving digital assets and electronic trade documents. This is because the provision of crypto-asset services typically follows models derived from traditional financial markets, in which contracts are standard practice in order to manage the allocation of risks between the parties.

There is a potential gap where there is no contractual privity between the participants in an open network. For example, it would be difficult to establish privity between the holder of a Bitcoin and the pseudonymous creator of the Bitcoin system, Satoshi Nakamoto. A claim in tort against Nakamoto (if "he" can be found) would not be subject to the conditions of a pre-existing contractual relationship for these purposes.

We would expect the same situation to prevail where a developer in an open network arrangement, who has made no promises and does not stand in privity to the owner of a digital asset, is charged with responsibility for losses incurred by

the owner due to, eg, negligence in the coding of the relevant system or failure to address a security breach.

In these cases, the choice of law should follow the principles in Article 4(1) or (2). It is, of course, still possible for Article 4(3) to apply, based on a close connection to another country, where there is no pre-existing contract.

(3) If the parties to a tort claim do not have a pre-existing contractual relationship, when else would it be appropriate for the courts of England and Wales to have recourse to the escape clause? What factors should the courts consider when identifying the country “manifestly more closely connected” to the tort?

QUESTION 13

We seek evidence, particularly from market participants, on how market practice in respect of bills of lading has been affected, or how it is likely to be affected, by the introduction of the Electronic Trade Documents Act 2023

QUESTION 14

We seek evidence on market sentiment relating to use of DLT platforms for electronic bills of lading.

(1) Is it likely that market participants will move towards a wholly decentralised DLT platform for bills of lading?

(2) To what extent can we assume that market participants will be reluctant to join a DLT platform that does not at least offer a user agreement setting out the terms on which the DLT platform will operate, and the rights and obligations of all users of the platform?

(3) Other than wholly decentralised DLT platforms, how else might DLT be used to issue and transact with electronic bills of lading (under the 2023 Act or otherwise)?

QUESTION 15

We seek evidence on the difficulties, if any, of incorporating the Hague-Visby Rules where an electronic bill of lading has been used.

(1) How often do disputes arise as to incorporation of the Hague-Visby Rules, specifically because an electronic bill of lading has been used, and how likely are they to in future?

(2) Are there concerns in the market, both in the marine insurance and shipping sectors, regarding the incorporation of the Hague-Visby Rules in electronic bills of lading? Please provide detailed examples in your answer and, where possible, distinguish between electronic bills under the Electronic Trade Documents Act 2023 and electronic bills held within contractual “approved systems.”

QUESTION 16

We seek evidence on market practice to help us identify where it could be said that an electronic bill of lading is “issued” for the purpose of the Hague-Visby Rules, as implemented in the UK by the Carriage of Goods Act 1971.

(1) How, in practical terms, does a carrier wishing to issue an electronic or tokenised bill of lading do so within the respective electronic “approved” system or DLT system? What steps must a carrier take within the system?

(2) How, in practical terms, does a shipper “receive” an electronic or tokenised bill of lading within an “approved” system or DLT system? What steps must a shipper take within the system?

(3) Does the issue of an electronic or tokenised bill of lading between carrier and shipper involve the platform provider, or do the systems allow for electronic or tokenised bills to be sent directly from carrier to shipper? (4) What are the market standards or best practices relating to existing electronic or DLT systems on the “issue” of a bill of lading?

QUESTION 17

We seek views on the most appropriate connecting factor for determining where an electronic bill of exchange is “delivered to a first holder” for the purposes of section 72(1) of the Bills of Exchange Act 1882.

(1) As the connecting factor for determining where an electronic bill of exchange is “delivered to a first holder”, what are the relative merits and demerits of recourse to: (i) the reliable system, and (ii) a relevant person?

(2) If the reliable system were used as the connecting factor, should it make a difference whether the reliable system is a central registry or a DLT system? Is it desirable for a single connecting factor to be used for all types of reliable systems?

(3) Can we assume that the “reliable systems” that are or will be used in the context of bills of exchange will largely be comparable to those used in the context of bills of lading?

(4) If a relevant person were used as the connecting factor, what are the relative merits and demerits of recourse to (i) the transferor; and (ii) the transferee?

(5) To what extent does the question of the formal validity of a paper bill of exchange arise in practice? How likely is it that the question of the formal validity of an electronic bill of exchange will arise in practice?

(6) Do electronic bills of exchange pose any other issues for section 72 of the Bills of Exchange Act 1882 that we have not considered here?

QUESTION 18

We seek views on whether it would be desirable to have a single conflict of laws regime to cover all types of electronic trade documents that fall within the scope of the Electronic Trade Documents Act 2023.

(1) Would it be preferable for electronic bills of exchange, cheques, and promissory notes to continue to be governed by the Bills of Exchange Act 1882 through an extended application of section 72; or for them to fall within new rule for all electronic trade documents under the 2023 Act?

(2) If a single conflict of laws regime for all electronic trade documents under the 2023 Act is preferable, what should be its scope? Should it cover contractual obligations only, or both contractual and proprietary obligations arising within the reliable system?

(3) If a single conflict of laws regime for all electronic trade documents under the 2023 Act is preferable, what approach should we take to any new regime and what broader objectives of the conflict of laws should we keep in mind? Stakeholders may wish to refer back to Chapter 6 from paragraph 6.103.



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 in different jurisdictions (or even in transit), and executed by self-executing code by pre-determined protocols within the DLT network, it is 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 residence³ of their owner immediately prior to the tort⁴ 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 effect⁵ or at least to prior authority which has so done, and there is accordingly some consistency in approach⁶.

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 Dickinson⁸. 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) Constructive Trustees

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 way¹⁰. The use of frontends or web interfaces will usually be subject to detailed terms and conditions of use¹¹. 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 assets¹³. 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 6¹⁴.

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 sterling¹⁶.

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 UK¹⁷. 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 section 21 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 2000, 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 it is capable of evolving and adapting to meet legal questions raised by new technologies such as DLT and crypto. Whilst a principled approach to questions 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 Law²⁰.

Bar Council²¹

16 May 2024

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.

Submitted to Law Commission Call for Evidence on digital assets and ETDs in private international law
Submitted on 2024-05-15 16:10:35

About you

What is your name?

Name:
Professor J M Carruthers

What is your email address?

Email:
[REDACTED]

What is your telephone number?

Telephone number:
[REDACTED]

Questions on international jurisdiction - specific issues (Chapter 5)

Question 1: In this question, we seek views and evidence on jurisdiction over consumer contracts.

Please share your views and evidence below::

Section 15B should be capable of being interpreted in such a way as to accommodate most consumer contracts in the digital/decentralised contexts, and the analytical approach should not differ markedly merely because the business in question is a crypto-business.

Question 2: In this question, we seek views and evidence on jurisdiction founded on the basis that a contract was concluded in England and Wales.

Please share your views and evidence below::

I have no strong view on whether the connecting factor should pertain to the participating computer or the real-world actor, but if it should be decided that the real-world actor is a more appropriate localising factor, it would be important to settle on a connection that does not introduce yet more uncertainty or scope for debate - as, for example, might be the case with domicile or habitual residence. The place where the real-world actor was to be found at the time when the contract was formed may be fortuitous, but at least should be capable of being readily ascertained.

Question 3: In this question, we seek views and evidence on jurisdiction founded on the basis that damage or detriment was suffered in England and Wales.

Please share your views and evidence below::

The approach and reasoning, on the face of things, are not consistent. Consistency in approach as between jurisdiction and applicable law is much to be preferred.

Question 4: In this question, we seek views and evidence on jurisdiction founded on the basis that an unlawful act was committed in England and Wales.

Please share your views and jurisdiction::

As above, the approach and reasoning, on the face of things, do not appear to be consistent.

Question 5: In this question, we seek views and evidence on jurisdiction founded on the basis that the claim relates to objects within England and Wales.

Please share your views and evidence below::

Discrepancies between application of domicile and application of place of residence/business need to be ironed out.

With regard to tempus inspiciendum, the time of the application is relevant for the purposes of gateway 11.

Question 6: In this question, we seek views and evidence on the types of claims and causes of action relied upon in applications to serve proceedings relating to crypto-tokens out of the jurisdiction.

Please share your views and evidence below::

-

Questions on applicable law - non-consumer contracts (Chapter 7)

Question 7: In this question, we seek views on applicable law and decentralised finance (DeFi).

Please share your views and evidence below::

Not known.

Question 8: This question concerns the applicable law for non-consumer contracts.

Please share your views and evidence below::

The general rules set out in the assimilated Rome I Regulation are apt to cover contracts involving crypto-tokens.

Questions on applicable law - non-consumer contracts (Chapter 8)

Question 9: This question concerns the applicable law for consumer contracts.

Please share your views and evidence below::

The consumer contract provisions of the assimilated Rome I Regulation should be capable of being applied to consumer crypto-token contracts. The current framework of rules should be adequate. Occasional difficulties in ascertaining, e.g. if a frequent crypto-trader is a consumer, or if activities have been pursued in or directed to a particular country, should not undermine the general effectiveness and operability of the consumer rules in Rome I. However, clarification will be needed from as to the extent of the financial exclusions in art 6.4(d) and (e).

Question 10: This question concerns the exclusions in Articles 6(4)(d) and (e) of the Rome I Regulation.

Please share your views and evidence below::

-

Questions on applicable law - torts and delicts (Chapter 9)

Question 11: We seek views and evidence on localising damage arising in tortious claims relating to crypto-tokens for the purposes of applicable law.

Please share your views and evidence below::

1. Too speculative to say.
2. The courts would take account of the CJEU jurisprudence, but clearly would not be fettered by it if the view should be taken that the EU case law restricts the proper development of domestic law (eg in light of jurisdictional developments in *Brownlie II*). It is a matter of conjecture how the courts of England & Wales would act with regard to applicable law in any case where the damage suffered is by way of deprivation.

Question 12: We seek views and evidence on recourse to the “escape clause” in Article 4(3) of the Rome II Regulation.

Please share your views and evidence below::

Article 4.3 is likely to be a very useful device in any applicable law dispute arising in the DLT/crypto-token context. The 'exceptionality' of the provision should not be over-stated (particularly in a DLT/crypto-context, where art 4.1 may not provide genuine certainty): *Owen v Galgey* [2020] EWHC 3546 (QB), per Linden J at 60-61.

Questions on applicable law - negotiable instruments, bills of lading, and the exclusions from the Rome Regulations (Chapter 10)

Question 13: We seek evidence, particularly from market participants, on how market practice in respect of bills of lading has been affected, or how it is likely to be affected, by the introduction of the Electronic Trade Documents Act 2023.

Please share your views and evidence below::

-

Question 14: We seek evidence on market sentiment relating to use of DLT platforms for electronic bills of lading.

Please share your views and evidence below::

-

Question 15: We seek evidence on the difficulties, if any, of incorporating the Hague-Visby Rules where an electronic bill of lading has been used.

Please share your views and evidence below::

-

Question 16: We seek evidence on market practice to help us identify where it could be said that an electronic bill of lading is "issued" for the purpose of the Hague-Visby Rules, as implemented in the UK by the Carriage of Goods Act 1971

Please share your views and evidence below::

-

Questions on applicable law - section 72 of the Bills of Exchange Act 1882 (Chapter 11)

Question 17: We seek views on the most appropriate connecting factor for determining where an electronic bill of exchange is "delivered to a first holder" for the purposes of section 72(1) of the Bills of Exchange Act 1882.

Please share your views and evidence below::

-

Question 18: We seek views on whether it would be desirable to have a single conflict of laws regime to cover all types of electronic trade documents that fall within the scope of the Electronic Trade Documents Act 2023.

Please share your views and evidence below::

-

Question on applicable law - property (Chapter 12)

Question 19: We seek views on the law applicable to property disputes in relation to digital assets and ETDs. Where possible, we ask that stakeholders contextualise their responses, for example, give details as to whether it relates to a pledge over an ETD or property entitlements in crypto-token litigation.

Please share your views and evidence below::

The identity of the disputing parties is very significant. Where a dispute occurs between the parties to the transfer of an asset (an 'original-parties dispute'), there is scope for applying a law other than the *lex situs*. Where the basis of the transfer between the original parties is contractual, it would be appropriate, for the purposes of applicable law, to have recourse to contractual principles, obviating the need to consider the *lex situs* rule. Where, however, a dispute occurs between one of the 'original parties' and a third party claiming otherwise to have acquired or derived title to the property in question (a 'remote-parties dispute'), the *lex situs* is the classic connecting factor and so consideration of how this factor should be construed in the crypto-tokens context would be necessary.

Likewise, it is appropriate in my view to make a distinction in applicable law terms between cases where a party has been voluntarily dispossessed of an asset and those cases where there has been involuntary dispossession.

Irrespective of what rules may be drafted in relation to party autonomy and recourse to contractual principles, it will be necessary to have - at least as a fallback, applicable law provision - a rule that 'localises' a crypto-token, albeit not necessarily *sub nom. lex situs*.

MEMORANDUM

To: The Law Commission cc: [Ian Clements](#), Partner, Dentons
conflictoflaws@lawcommission.gov.uk

From: [Alexander Hewitt](#)

Date: 9 May 2024

Matter No:

Subject: **"Digital assets and ETDs in private international law: which court, which law?"
Response to questions 17, 18 and 19 from the Commission's February 2024 call for
evidence regarding electronic trade documents (ETDs)**

Question 17

We seek views on the most appropriate connecting factor for determining where an electronic bill of exchange is "delivered to a first holder" for the purposes of section 72(1) of the Bills of Exchange Act 1882.

(1) As the connecting factor for determining where an electronic bill of exchange is "delivered to a first holder", what are the relative merits and demerits of recourse to: (i) the reliable system, and (ii) a relevant person?

Answer: We would favour the location of the holder over that of the reliable system, which may have no connection with the original or later parties to a bill or note, or their transactions. However, our strong preference would be for the original parties to a bill or note to be able to choose the governing law for all issues relating to their bill or note by including a choice of law clause on the face of the bill or note – and for this choice to bind all parties to the bill or note from time to time.

(2) If the reliable system were used as the connecting factor, should it make a difference whether the reliable system is a central registry or a DLT system? Is it desirable for a single connecting factor to be used for all types of reliable systems?

Answer: Use of the location of the reliable system will tend to be more or less arbitrary, as that location may be temporary or have no commercial or other practical connection with the bill or note or its original or later parties or any related transactions. However, if the location of the reliable system is to be used as a connecting factor, this would be more defensible for a central registry than for a DLT system.

(3) Can we assume that the "reliable systems" that are or will be used in the context of bills of exchange will largely be comparable to those used in the context of bills of lading?

Answer: This would sometimes be a safe assumption. However, the requirements for a reliable system under the 2023 Act are not excessively demanding and not all bills or notes are issued in connection cross border trade, or where traded goods are carried by sea. Notes, for example, are frequently used to pay for service deliveries (such as under construction contracts) in many countries and, in the UK, for certain types of land sale

(4) If a relevant person were used as the connecting factor, what are the relative merits and demerits of recourse to (i) the transferor; and (ii) the transferee?

[Puyat Jacinto & Santos](#) ► [Link Legal](#) ► [Zaanouni Law Firm & Associates](#) ► [LuatViet](#) ► [For more information on the firms that have come together to form Dentons, go to \[dentons.com/legacyfirms\]\(https://www.dentons.com/legacyfirms\)](#)

Dentons is a global legal practice providing client services worldwide through its member firms and affiliates. Dentons UK and Middle East LLP is a limited liability partnership registered in England and Wales under no. OC322045. It is authorised and regulated by the Solicitors Regulation Authority, SRA Number 447523 and the Law Society of Scotland. A list of its members is open for inspection at its registered office: One Fleet Place, London EC4M 7WS. Any reference to a "partner" means a person who is a partner, member, consultant or employee with equivalent standing and qualifications in one of Dentons' affiliates. Please see [dentons.com](https://www.dentons.com) for Legal Notices.
96334905.2

Answer: Use of the transferee as a connecting factor would, to some extent, be consistent with the existing conflict of laws rules for paper bills and notes. Having the opposite rule for electronic bills and notes might lead to confusion, even among market participants taking sophisticated legal advice. We would favour giving the original parties to bills and notes the ability to choose the law which governs the formal validity of those documents via an express choice of law clause on the face of the bill or note – and for the chosen law also to bind later parties to the bill or note, including later transferees and transferors.

(5) To what extent does the question of the formal validity of a paper bill of exchange arise in practice? How likely is it that the question of the formal validity of an electronic bill of exchange will arise in practice?

Answer: This issue does not often come up in practice. However, it could arise on a high-value or structured transaction, or where parties to a bill contracted from states whose laws emanated from different legal cultures.

(6) Do electronic bills of exchange pose any other issues for section 72 of the Bills of Exchange Act 1882 that we have not considered here?

Answer: One problem with section 72 is that it does not provide a complete set of conflict of laws rules for bills and notes. In addition, few market participants would be able accurately to decode section 72 without specialist advice, which may not always be readily available, or which they might not realise they require. Presumably, section 72's complexity and lack of clarity were not major problems when the 1882 Act came into force as, at that time, bills and notes were more regularly used in daily life. However, if trade and trade finance transactions are to be digitised in the present it would seem sub-optimal for the conflict of laws rules relating to ETDs to be as complex, uncertain, incomplete as section 72.

Question 18

We seek views on whether it would be desirable to have a single conflict of laws regime to cover all types of electronic trade documents that fall within the scope of the Electronic Trade Documents Act 2023.

(1) Would it be preferable for electronic bills of exchange, cheques, and promissory notes to continue to be governed by the Bills of Exchange Act 1882 through an extended application of section 72; or for them to fall within new rule for all electronic trade documents under the 2023 Act?

Answer: We would favour a single rule for all 2023 Act ETDs, including bills, notes and cheques. Among other considerations, section 72 is not easy for traders or financiers to work with and many market participants would routinely deal with batches of documents consisting of multiple types of ETD in any given trading or finance transaction. In such (normal) cases, it would promote digitisation, clarity and certainty in markets if a single conflicts regime applied to all types of ETD.

(2) If a single conflict of laws regime for all electronic trade documents under the 2023 Act is preferable, what should be its scope? Should it cover contractual obligations only, or both contractual and proprietary obligations arising within the reliable system?

Answer: We would favour a single regime that covered both contractual and proprietary rights and obligations arising within or outside the reliable system, but also covered wider issues such as formal validity.

(3) If a single conflict of laws regime for all electronic trade documents under the 2023 Act is preferable, what approach should we take to any new regime and what broader objectives of the conflict of laws should we keep in mind? Stakeholders may wish to refer back to Chapter 6 from paragraph 6.103.

Answer: We would strongly favour a regime based upon UNIDROIT Principle 5(1) and which gave that principle wide application. One advantage of Principle 5(1) in this context is that ETDs will usually be relatively ephemeral (e.g. when compared with crypto-currency), voluntarily produced for specific trading transactions by the parties to those transactions and only sold or delivered to later parties who voluntarily purchase or take security over those ETDs or underlying goods or rights. In this sort of fact pattern, party autonomy seems most likely to produce results which are certain, practical, useful and promote trade digitisation. We also note that, in the context of another UNIDROIT project, party autonomy on the conflict of laws rules relating to contract, property, possession and security law issues has worked extremely well under the Cape Town Convention and its Aircraft Equipment Protocol – often (rightly) referred to as the most successful commercial law treaties in history.

We would also suggest that it would be worth, for the avoidance of doubt, considering whether any new rule for 2023 Act ETDs should address the effects of conversion, under section 4 of the 2023 Act, of an ETD to a paper trade document or vice versa.

Question 19

We seek views on the law applicable to property disputes in relation to digital assets and ETDs. Where possible, we ask that stakeholders contextualise their responses, for example, give details as to whether it relates to a pledge over an ETD or property entitlements in crypto-token litigation.

*(1) To what extent would recourse to contractual principles obviate the need for us to consider the *lex situs* rule?*

Answer: In relation to ETDs, we consider that a conflict of laws rule based on UNIDROIT'S principle 5(1) would greatly reduce the need to consider the *lex situs* and we would favour wide use of party autonomy over issuer-based rules.

(2) Do permissioned networks and/or cases where there is clearly a contractual or hierarchical relationship between the parties represent the vast majority of DLT applications for digital assets and ETDs?

Answer: No response.

(3) Should we need to consider a new conflict of laws regime for property rights in digital assets and ETDs, what approach should we take to any new regime and what broader objectives of the conflict of laws should we keep in mind? Stakeholders may wish to refer back to Chapter 6 from paragraph 6.103.

Answer: In relation to ETDs, please see our answers to questions 19(1) and 18.

*(4) To what extent would recourse to a distinct rule based on the connecting factor of the "owner" or "transferor" for cases where parties have voluntarily dealt with one another obviate the need for us to consider further the application of the *lex situs* rule to cases where the parties to the dispute are strangers?*

Answer: In relation to ETDs, use of an "owner" or "transferor" connecting factor would tend to reduce the utility of the 2023 Act as it would tend to increase the cases where an ETD might be governed as to contractual matters by the laws of a part of the UK, but where property and security law questions were (for no obvious practical benefit) governed by the laws of a non-UK state.

(5) In what circumstances could a rule based on the "owner" or "transferor" be satisfactorily used? Do creditors taking security over ETDs typically require, as a matter of contract, that the debtor warrants their title to grant the security interest?

Answer: We do not see there is an obvious case for use of this rule. Warranties as to title are very common when security is taken over trade documents, or where trade documents are purchased at a discount. However, these warranties are often only of limited value. If a transferor sells an ETD, or offers it as security, its warranty as to title is only as good as its solvency, or the purchaser or security taker's ability to enforce the warranty in legal proceedings. For this reason, most purchasers or security takers would rather have good title to the purchased or secured asset than have to sue on a warranty. If they acquire good title they can be more confident the purchased or secured asset is outside the insolvency estate of the transferor (and is thus unavailable to the transferor's other creditors). If they were happy merely to have a contractual claim against their seller or security provider they would not have sought outright ownership of an asset, or security over that asset.

(6) To what extent is it 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"?

Answer: No response.

(7) How should courts approach the question of applicable law in such disputes relating to decentralised digital assets held in permissionless DLT networks where the parties have not dealt with one another and there has been an "involuntary dispossession"?

Answer: No response.

Ian Clements and Alexander Hewitt



The City of London Law Society

THE LAW COMMISSION: CALL FOR EVIDENCE ON DIGITAL ASSETS AND ETDS IN PRIVATE INTERNATIONAL LAW: WHICH COURT, WHICH LAW

CLLS FINANCIAL LAW COMMITTEE RESPONSE

INTRODUCTION

The City of London Law Society ("**CLLS**") represents approximately 15,000 City lawyers through individual and corporate membership including some of the largest international law firms in the world. These law firms advise a variety of clients from multinational companies and financial institutions to Government departments, often in relation to complex, multijurisdictional legal issues.

This response to the Law Commission's Call for Evidence on its paper entitled, "Digital assets and ETDs in private international law: which court, which law?" (the "**Call for Evidence**") (this "**Response**") has been prepared by the Financial Law Committee ("**FLC**") of the CLLS, whose members specialise in major financings involving obligors incorporated in multiple jurisdictions, creditors incorporated or doing business in multiple jurisdictions, and assets located, or deemed by principles of private international law to be located, in multiple jurisdictions. Concepts of English law and other laws relating to digital assets and the development of these concepts are increasingly critical to the transactions and advisory matters on which members of the FLC advise. Full details of the members of the FLC appear on the CLLS website. We understand that Linklaters LLP is making its own submission to the Call for Evidence and we wish to note that the Linklaters LLP has not been involved in the preparation of this Response. We note also that Clifford Chance LLP has not been involved in the preparation of this Response.

The FLC continues to appreciate greatly the thorough work and detailed analysis undertaken by the Law Commission with regard to the legal issues that arise in the context of digital assets, including the private international law issues the subject of the Call for Evidence. As the FLC noted in its response dated 4 November 2022 to the Law Commission's Consultation Paper on Digital Assets issued in July 2022 (the "**July 2022 Consultation Paper**"), and as has also been recognised by the UK Jurisdictional Taskforce (the "**UKJT**"), the very nature of most types of digital assets has given rise to, and will continue to give rise to, complex cross-border legal issues, and we fully support the Law Commission's ongoing work in this area.

We set out below the FLC's responses to those questions listed in the Call for Evidence to which we had a substantive response. In doing so, we have sought to retain the terminology used in the Call for Evidence, notably the terms defined in the Glossary to the Call for Evidence. A number of the questions included in the Call for Evidence fall outwith the experience of or specialisms in law practised by the members of the FLC; we have either not responded to these questions or have included only limited responses. Before setting out specific responses to specific questions, we set out below a summary of the points we would like to raise generally with some of the concepts and proposals set out in the Call for Evidence, in particular with regard to financial products which are or may in the future be evidenced by or created on distributed ledgers ("**DLs**") or on exchanges or other systems which utilise distributed ledger technology ("**DLT**").

We appreciate that the Call for Evidence seeks input on a broad range of digital assets and potential issues arising under principles of private international law: it is not focused solely on financial assets or financial products, and it raises questions in the context of both consumers and commercial parties. This Response primarily addresses voluntary commercial dealings; questions arising in the context of consumers and criminal law raise points of policy beyond the remit of the members represented on the FLC, including in the context of the regulation of financial services and financial products in the UK. On the other hand, the development of financial products, the proper functioning of the international capital markets and maintaining the core role in which English law has played in developing and sustaining these products and markets are key areas of interest for the FLC.

SUMMARY

1. English law has developed over the centuries as a dominant legal system in terms of both international trade and international finance; two significant reasons why English law continues to maintain its dominance in these areas are (a) the flexibility of the common law and principles of equity and, thus, their ability to evolve over time, and (b) the relative certainty of the outcome of a dispute arising under English law, because of the relative certainty of the law and the expertise of the judiciary of the English courts. As the Call for Evidence notes, the English courts are very adept and skilled in determining international disputes, but litigation is a competitive arena. We are concerned to ensure that the English legal system maintains its pre-eminence in financial law, and in financial services regulation, by developing in a manner that embraces digital technology, maintaining and enforcing clear principles so that parties have confidence in their dealings and clarity as to the rights and obligations arising from those dealings.
2. In our view, in the context of intangible financial products and financial assets which are or are capable of being transferable, traded or settled across national borders, English law principles of private international law should recognise and give effect to the existing English law principle of party autonomy, or (in the context of clearing, settlement and payment systems) participant autonomy, and not seek to apply concepts such as *lex situs*. We consider that, given that digital assets may be anywhere or nowhere, or in many places at the same time, the application of the existing English law principle of party autonomy or participant autonomy to allow persons dealing with digital assets to choose the law to govern their rights and contractual obligations will provide the most robust, practical and internationally-recognised solution to determining the rights and obligations of those parties. In addition, where there are sound public policy reasons to do so, the principle of party autonomy should also apply to determine and govern the circumstances in which rights, interests and obligations may affect and be binding on third parties, so as to derogate from mandatory laws that might otherwise apply to a participant in a system. It is critical that English principles of private international law in this area are not unnecessarily subsumed in or confused by principles of property law developed over the centuries primarily to deal with tangible property, or with claims or other intangible proprietary rights realisable against a person or persons located in a single sovereign state.
3. English law already recognises principles of participant autonomy in the context of financial market infrastructure and has done so for twenty five years in the form of legislation. Regulation 24 of the Financial Markets and Insolvency (Settlement Finality) Regulations 1999 (the "**Settlement Finality Regulations**") implemented Article 8 of the (then) EC Settlement Finality Directive. Regulation 24 of the Settlement Finality Regulations provides that, in the event of an insolvency of a participant in an applicable securities settlement, clearing or payment system, the governing law of the system (defined to mean the law "chosen by the participants" in the system) determines any question relating to the rights and obligations arising from, or in connection with, that insolvent participant's participation in the system. The primacy of the system's governing law will give third party effects to the contractual and other provisions of the system's default rules or other arrangements (including

netting, porting and collateral) in priority to the rights, claims and interests of third parties, e.g. the relevant insolvency office-holder or non-participant creditors of the insolvent participant, in relation to the same assets the subject of the rules or other arrangements.

4. The same Directive and the Settlement Finality Regulations implementing it in the UK include further provisions which are intended to ensure the continuing smooth operation of securities settlement, clearing and payment systems notwithstanding the insolvency of a participant, including, for example, giving primacy to the rules of the system over provisions of national insolvency law applicable to an insolvent participant which would otherwise prevent or inhibit agreed trades or other obligations from settling. It seems to us that there is no obvious reason why similar laws applicable to digital assets may not be enacted in the United Kingdom, where required. Financial market counterparties in the UK and the European Union (and in other sophisticated jurisdictions) are already familiar with and accepting of the principles of participant autonomy in the context of dealings with financial assets, including in the context of dealing with associated proprietary rights. Indeed, it would be a retrograde step to move away from this already established, legally robust and commercially accepted means of dealing with cross-border financial products and payments issued, transferred and/or settled through a consensual system, towards a system based on solutions developed for tangible assets which will not result in the necessary certainty or commercial or international acceptance.
5. The FLC is keen to assist the critical work which the Law Commission is undertaking with respect to digital assets so as to encourage the development of an appropriate and internationally recognised new applicable law rule to govern proprietary issues affecting native crypto-tokens, i.e. tokens that are not constitutively linked to another asset, such as a share or other security, and which may be recorded in a permissionless or permissioned DLT-based system. International acceptance and recognition of the applicable law is a fundamental criterion, and for this reason, we consider that the correct approach to the applicable law issues for "linked" assets should be one based upon Principles 4 and 5 of the UNIDROIT Principles on Digital Assets and Private Law (the "**UNIDROIT Principles**"), namely that the "normal" conflict of laws rules determining the applicable law for proprietary issues affecting the underlying linked asset (and not that of the crypto-token) should have primacy and will govern (see paragraph 5.24 of the UNIDROIT Principles). The application of the relevant conflict of law rule for the underlying asset (e.g. the place of the relevant register in the case of a linked share) should not itself be affected by the fact that the underlying share is recorded on a DL or is constitutively linked to a crypto-token recorded in a DLT system. In consequence, no new or different conflict of law rule will need to be developed for linked assets.
6. Where we refer in this Response to the principle of party autonomy, or participant autonomy, allowing the participants in a system to choose a single governing law, we mean that governing law without reference to its conflicts of law, i.e. without admission of concepts such as renvoi, which could muddy the waters by taking one to a different system of law. The necessity of avoiding this outcome is reflected in Principle 5 of the UNIDROIT Principles and in Regulation 19 of The Financial Collateral Arrangements (No.2) Regulations 2003¹ (the "**FCARs**"). Regulation 19 of the FCARs states that any question relating to the matters specified in paragraph (4) of Regulation 19² which arises in relation to book entry securities collateral which is provided under a financial collateral arrangement shall be governed by "the domestic law of the country in which the relevant

¹ UKSI 2003 No. 3226.

² These matters include the legal nature and proprietary effect of book entry securities collateral and the requirements for rendering a financial collateral arrangement which relates to book entry securities collateral effective against third parties.

account is maintained"; paragraph (3) of Regulation 19 further provides that "domestic law" excludes any rule under which, in deciding the relevant question, reference should be made to the law of another country.

7. Adopting, where possible, the principle of party autonomy or participant autonomy should also facilitate an appropriate and internationally-agreed approach to financial services and markets regulation in a number of different ways. For example, the current BIS³ -based capital adequacy regime applicable to banks and other financial institutions is based primarily first on the risk-weighting of assets by reference to counterparty risk, modified where appropriate by credit risk mitigation factors such as valid security interests supported by appropriate legal opinions; and secondly on market risks. It is almost certainly the case that the current capital adequacy regime will need to adapt over time to reflect the manner in which financial exposures (bonds, loans, derivatives, shares, etc) are created, evidenced, settled or secured or used as collateral for other exposures, but it is axiomatic that if these exposures are created based on DLT technology or the like, the recognition of participant autonomy will greatly facilitate determining the risks that arise, where those risks are likely to fall, and the potential magnitude of those risks; and, therefore, will enable financial services and markets regulation to be appropriately focused (including, for example, requiring any operator or administrator of a DLT-based system to be regulated) and, thus, foster confidence in the system⁴. This is critical in a world in which financial assets now move in an instant across national borders, all the time.
8. We believe it would be helpful for the Law Commission to analyse and determine how, in practice, the conflict of law rule for determination of the applicable law for proprietary issues affecting a share or other registered security, by reference to the location of the relevant register, is to be applied where the register is a DL register. The same practical considerations will arise in relation to any underlying asset that is linked to a token recorded in a DL, where the DLT-based system performs functions in relation to the token (e.g. to support issuance, transfer or payment of the digital asset) and where the relevant conflict of laws rule points to the location of the performance of the relevant act in determining the applicable law for the relevant legal issue to be decided by the court.
9. Unlike tangible assets, an intangible asset has no existence other than by and under the arrangement (typically but not necessarily consensual) under which it arises, is created or is "instantiated" and that allows it to be enjoyed; for example, by its transfer or by the receipt of rights, privileges or benefits attached to or arising from the intangible asset. As a consequence, English law has long recognised that consensual arrangements⁵ may give rise to "conditions", "burdens" or "obligations" which are inextricably linked to and form part of the intangible assets and, are, therefore, capable of third party effects and are exercisable *erga omnes*. Those conditions, while rooted in contract or

³ The Bank for International Settlements, aka in this context, the Basel Committee.

⁴ Another example of the key importance of legal certainty in the regulation or supervision of participants in the financial markets can be found in the internationally-recognised standards for financial market infrastructures set out in the CPMI-IOSCO Principles for financial market infrastructures (April 2012) (the "**PFMIs**"). The recognition of a single, clear conflict of laws rule for proprietary issues, based on the applicable law chosen by the participants in a systemically important system (securities settlement system, CCP or payment system) using DLT-based functionality, will enable or facilitate observation of Principle 1: "An FMI should have a well-founded, clear, transparent and enforceable legal basis for each material aspect of its activities in all relevant jurisdictions". Such a clear, certain and pragmatic approach to relevant conflict of laws issues, readily manageable by the participants in the system, will allow for the obtaining of "well-reasoned and independent legal opinions or analyses" on proprietary and collateral-related issues (as contemplated by paragraph 3.1.3 of the PFMIs); as well as the mitigation of the risks arising from the potential conflict of laws across the jurisdictions in which such systemically important systems operate (as contemplated by Principle 1, Key Consideration 5 and paragraphs 3.1.1, 3.14.5 and 3.18.5 of the PFMIs).

⁵ These arrangements may include trusts as well as contracts.

another consensual arrangement, may be said to be intrinsic to the arrangement and impressed upon the intangible asset so as to travel with it upon any transfer, and to be binding upon and effective against third parties, including any third party asserting a proprietary interest in the asset. The intangible asset is, therefore, capable of being governed by the same law (in determining its proprietary or third party effects) as the parties decide should govern the consensual terms of the arrangement. This is particularly so in the case for consensus-based DLT-based systems, where the participants in the consensus have agreed to apply a specific law to govern proprietary matters in relation to the digital asset and as impacting upon status changes to the DL; and where the majority of the consensus required to validate a transaction and effect an update to the DL are not located in a single country or territory.

10. In our view, therefore, English law principles of private international law would and should respect party autonomy or participant autonomy in the context of determining the appropriate law to govern the proprietary aspects of a contractual or other consensual arrangement involving the creation, issuance and transfer of rights in and to the digital asset, including the creation, attachment, priority and perfection of security interests over such assets. English law already recognises this approach, both in the common law and, in the context of the clearing and settlement of securities, through specific legislation. Parties dealing with digital assets evidenced by entries on a DL (whether or not maintained by an exchange) may prefer to choose the law that governs the issuance and transfer of digital assets on the DL, as well as the nature of the security interests that may be created over the digital assets and the manner by which the security interests may be enforced and the forum in which disputes should be settled; so their choice of applicable law includes both the law of obligations and the law of property, insofar as that pertains to proprietary rights to the digital assets represented on the DL.
11. Equally, it is not necessarily the case that the law chosen to determine the contractual provisions of a digital asset must be the same governing law as the law that determines whether the asset has been transferred, or whether security has been created over the asset. For example, bonds governed by English law, New York law and the laws of many other jurisdictions are, if issued in the European capital markets, typically held (through an established legal mechanism) in one or both of the two principal European clearing systems, Euroclear and Clearstream. If the bonds are held in the international central securities depository ("ICSD") operated by Euroclear, the terms on which interests in the bonds are transferred by participants in Euroclear are governed by the rules binding on participants in the Euroclear system; these rules are governed by Belgian law, because Euroclear Bank S.A./N.V. is a Belgian company operating the ICSD under Belgian law as the governing law of the system. A similar analysis applies to bonds held in Clearstream Banking S.A., where Luxembourg law applies to the terms on which the bonds held in that system are cleared and settled. The arrangements for clearing and settlement do not, however, prevent or preclude the terms and conditions of the bonds themselves from having a different governing law from the law applicable to the relevant clearing system. The same result is possible, in our view, where digital assets are cleared and settled using DLT-based systems rather than an ICSD using legacy systems, albeit it may be necessary to enact specific legislation in order to ensure the primacy of the clearing and settlement regime over other laws that may be relevant, for example in the context of an insolvency of a participant and the impact upon any rights and obligations arising from or in connection with its participation in the system (see our comments above on the Settlement Finality Regulations). We are concerned that although the Call for Evidence clearly and correctly, in our view, states that the principles used to determine the key "connecting factors" relevant to determining the "right" law or forum for a dispute involving digital assets must be pragmatic, practical and based on sound policy grounds (crucially, respected in other relevant jurisdictions), there is an emphasis on connecting factors based on *situs* which the FLC considers will not foster a workable solution in

the context of financial assets and financial products, held in DLT-based systems and, worse, may undermine the intentions of users, developers and operators of DLT-based financial products.

12. Reliance on principles of *situs* developed for tangible assets will give rise to complications where digital assets are recorded on a DLT-based system such as blockchain, where the system is built on consensus, i.e., the DL can only be updated, rectified, amended or (generally) maintained by a qualified majority of validating node operators ("VNOs"). The VNOs operating a particular blockchain are likely to be resident or domiciled in many different jurisdictions, so basing the question of which court should have jurisdiction over a dispute on whichever court has *in personam* jurisdiction over the VNOs is very unlikely to work; likewise, there is likely to be no single law, aside from the governing law of the system chosen by the VNOs and other participants, based on *situs* or otherwise, that can provide a suitable "connecting factor" to determine proprietary issues affecting digital assets recorded in the system. Any attempt by a court to impose upon the consensus majority a solution to a proprietary dispute affecting such a digital asset, e.g., by reference to the location of the transferor at the time of transfer, by issuing an order to rectify the DL under and in accordance with a law different from that chosen by the consensus majority, is likely to be futile.
13. For example, there is clearly commercial appetite to decentralise dealings through (and associated credit and other risks arising from) clearing and settlement systems for securities, whether debt or equity, as assets "constitutively linked" to a crypto-token recorded on a DL and for "native" (or "endogenous") digital assets that are not linked to an underlying "real world" asset. If, however, principles of *situs* are attempted to be applied to, for example, the issuance and then subsequent transfer or settlement of bonds or other digital assets recorded in a DLT-based system, there will be multiple potential governing laws for those digital assets recorded in the same DLT-based system, depending on the *situs* of the issuer of the bond (or, if there is an issuer, other digital asset) and the *situs* of any transferor or subsequent holder of the bond or other digital asset, or the *situs* of the nodes that form part of the DL maintained by the system. This is clearly not a workable or sustainable approach. The same concern would apply to syndicated loans where participations are recorded in the same DLT-based system and, indeed to any intangible financial asset, including an electronic trade document ("ETD") that is capable of transfer, assignment, novation or other disposition, whether absolutely or by way of security, on-chain or off-chain.
14. In our response to questions relating to matters of jurisdiction, we are commenting strictly from the point of view of when the English courts should take or refuse jurisdiction, not on the substantive law that should be applied to the particular case.
15. As with previous responses made by the FLC to the Law Commission's work on digital assets, we wish to note, also, that the law applicable to digital assets cannot be viewed without also considering the regulatory environment in which numerous persons operate, including investors in and users of digital assets and those providing finance for the acquisition of, or secured by, digital assets. We appreciate that not all persons who deal with digital assets operate in a regulated environment, but many do (and some may argue, as a policy matter, that more should), and it is critical that the regulatory environment reflects, so far as possible (noting again that principles of private international law are almost invariably engaged when dealing with digital assets), accepted legal characteristics of these types of asset and the rights, obligations and restrictions to which these characteristics give rise. Another aspect of regulation relevant to digital assets is the legal and regulatory regime which many sovereign nations have enacted to protect consumers ordinarily resident in those nations. Legislation protecting consumers differs from jurisdiction to jurisdiction, depending on the policies adopted by the relevant sovereign state, and for that reason, achieving international consensus in the context of digital assets held by consumers is likely to be more difficult than achieving international consensus when dealing with other persons and entities. As

we have noted above, we do not comment on policy matters pertaining to the protection of consumers' rights or related questions as to the extent to which UK financial services regulations should apply to businesses with no nexus to the UK.

RESPONSES

Our responses to the questions raised in the Call for Evidence are set out below.

1. Question 1, Paragraph 5.11 and Paragraph 13.1 of the Call for Evidence: views and evidence on jurisdiction over consumer contracts.

- 1.1 We have no comment on this question other than to note that if consumers in the UK are permitted to invest in and/or trade digital assets on an exchange or on a native DL, the views we set out below regarding the appropriate law and jurisdiction applicable to such assets should apply also in the context of consumer contracts; and the applicable choice of law may result in a UK regulator determining that a UK-based consumer does not have the necessary knowledge or expertise to invest in or trade in the applicable digital assets (or, at least, not on an exchange or DL which is based outside the UK) and, therefore, that they may not be offered to consumers in the UK. There is a separate question as to how a UK regulator may enforce that restriction against non-UK entities seeking to promote their activities to UK consumers, but that appears to us to be beyond the remit of the Call for Evidence.
- 1.2 For avoidance of doubt, any digital asset which may be created in the future that deals with land or title to land in England and Wales, including the taking of security over land or interests in land and whether the interest in land is held by a consumer or any other person, must be subject to English law and the jurisdiction of the English courts. In other words, for land and interests in land, the *lex situs* should continue to determine the applicable law and jurisdiction. This is consistent with the view we express in the Summary above that, where an underlying asset is constitutively linked to a crypto-token, it should be the relevant applicable law for the underlying asset that governs proprietary issues affecting the crypto-asset (in line with Principles 4 and 5 of the UNIDROIT Principles).

2. Question 2, Paragraph 5.20 and Paragraph 13.2 of the Call for Evidence: views and evidence sought on jurisdiction founded on the basis that a contract was concluded in England and Wales.

- 2.1 We think that a distinction should be made between smart contracts concluded within a participant-based system, and other smart contracts. In the case of the former, participant autonomy should apply; in the case of the latter, particularly for consumer contracts, it seems to us that the relevant connecting factor should be the real-world (consumer) actor, based on his/her/its habitual residence; otherwise, it is difficult to see how statutory protections for consumers will apply.
- 2.2 We believe that the question of where a smart contract is made will become prevalent in practice particularly in the context of consumer contracts, where policy reasons in the jurisdiction in which the relevant consumer is habitually resident will be dominant; and in the context of DLT-based systems used in international finance and international trade, where legal certainty as to the applicable law and its effects, including in the context of an insolvency of a participant in the system, is critical.

3. Question 3: Paragraph 5.56 and Paragraph 13.3 of the Call for Evidence: views and evidence sought on jurisdiction founded on the basis of damage or detriment suffered in England and Wales.

3.1 The FLC has no particular views or evidence on this question other than to note that where any claim relates to a digital asset held or evidenced in a DLT-based system, the rules and governing law of the system should prevail over and otherwise determine any tortious claims; to do otherwise would be to undermine the safety and soundness of the system and could undermine participant or wider confidence in the integrity of the system's governance and operational arrangements. We agree with the Law Commission's point that the issues raised here are more difficult, not least because the actions giving rise to the damage or detriment suffered frequently involve criminal acts, which give rise to different and difficult policy considerations.

4. Question 4: Paragraph 5.76 and Paragraph 13.4 of the Call for Evidence: views and evidence sought on jurisdiction founded on the basis that an unlawful act was committed in England and Wales.

4.1 The FLC has no particular views or evidence on this question, which we view as a policy matter.

5. Question 5: Paragraph 5.116 and Paragraph 13.4 of the Call for Evidence: views and evidence sought on jurisdiction founded on the basis that the claim relates to objects within England and Wales.

5.1 The FLC has no particular views or evidence on this question other than to note that if where any claim relates to a digital asset held or evidenced in a DLT-based system, the rules and governing law of the system should prevail and otherwise determine the relevant claim; to do otherwise would be to undermine the safety and soundness of the system and could undermine participant or wider confidence in the integrity of the system's governance and operational arrangements.

6. Question 6: Paragraph 5.133 of the Call for Evidence: views and evidence sought on the types of claims and causes of action relied upon in applications to serve proceedings relating to crypto-tokens out of the jurisdiction.

6.1 The FLC has no particular views or evidence on this question other than to note that if where any claim relates to a digital asset held or evidenced in a DLT-based system, the rules and governing of the system should prevail; to do otherwise would be to undermine the safety and soundness of the system and could undermine participant or wider confidence in the integrity of the system's governance and operational arrangements.

6.2 Specifically in the context of crypto-exchanges, the question whether a crypto-exchange should be deemed to hold crypto-tokens, or otherwise be liable, as a constructive trustee appears to us to be a question that should be determined by the rules of the exchange applied in accordance with the relevant principles of the governing law of the system and, specifically, by reference to the person who the operator of the exchange determines, by applying the rules of the exchange in accordance with the governing law of the system, is the true beneficial owner of the assets held in the exchange. It may be that it is necessary to develop the rules of crypto-exchanges so that they capture situations in which there is a dispute as to who the true beneficial owner of the digital assets is, and provide for a means of determining that dispute. We have considerable sympathy for the argument that the operator of a crypto-exchange should not be held to the standards of, and subject to the liabilities of, a

manager/discretionary trustee or other fiduciary under English law simply by reason of its operating the exchange – which is largely a mechanical, administrative function intended to ensure smooth settlement of transfers of instruments traded on or through the exchange. We note, also, that typically under current operating models⁶ for financial instruments (as distinct from crypto-tokens), it is not the exchange that holds legal title to assets traded on or through the exchange; legal title tends to be held by a depositary institution or other custodian. It is equally important, however, that systems are developed which protect the assets of beneficial owners of digital assets from criminal or tortious acts or acts otherwise in breach of equitable duties owed to the beneficial owner; these will likely be matters determined, for a particular exchange, by domestic law and regulation in the jurisdiction in or under which that exchange is incorporated or operates the exchange and principles of participant autonomy should then apply.

7. Question 7: Paragraph 7.28 and Paragraph 13.7 of the Call for Evidence: views on applicable law and DeFi.

- 7.1 We agree that contractual disputes in the context of DeFi are not likely to come before the courts and as a result, they are not likely to be resolved by reference to English law principles of private international law and the question of applicable law.

8. Question 8: Paragraph 7.84 and Paragraph 13.8 of the Call for Evidence - questions on the law applicable to non-consumer contracts; Question 10: Paragraph 8.93 and Paragraph 13.10 of the Call for Evidence – questions concerning the exclusions in Articles 6(4)(d) and (e) of the Rome I Regulation.

- 8.1 We are setting out our views on these three questions combined because they raise similar points and concerns.
- 8.2 We do not agree with the conclusion in paragraph 12.35 of the Call for Evidence that "there is a general consensus that property law remains a mandatory form of law from which parties cannot derogate using the principle of party autonomy and freedom of contract", at least insofar as that statement purports to apply to transactions involving financial assets held, cleared and settled via a DLT-based system where the participants in the system have agreed to abide by the rules of that system in accordance with the governing law of that system. The rules and chosen governing law of the system should, in our view, trump the concept of "factual control"; factual control is a concept suited to tangible assets, but is strained beyond any efficacy when attempted to be applied to intangible assets held in a DLT-based system in which the participants, and specifically the VNOs participating in the consensus mechanism, have agreed to apply the chosen governing law to determine proprietary and other issues affecting digital assets held or recorded in the system. In our view, it is not sensible to seek to apply possession-type characteristics to assets that are incapable of being possessed, as that concept is formulated and understood in English law, nor is it necessary to force an unhappy analogy with possession on intangible assets. As we have noted in our

⁶ It is possible that, going forward, this position will change as DLT-based systems allow exchanges for linked financial instruments to act additionally as a "digital securities depository". These operating models are likely to be the subject of FMI sandbox arrangements governed by the Financial Services and Markets Act 2023 (Digital Securities Sandbox) Regulations 2023 and related rules made by the Financial Conduct Authority and the Bank of England.

Summary, the Settlement Finality Regulations demonstrate that the statement in paragraph 12.35 of the Call for Evidence is disproved in the context of securities, settlement, clearing and payment systems; these Regulations derive from an EC Directive and are reflected in the domestic laws of the member states of the European Union as well as in UK law.

- 8.3 We consider that it is also not necessary to adopt, for the purposes of English law principles of private international law, the "user consent" principles summarised in paragraphs 12.50 to 12.63 of the Call for Evidence (which also considers Principle 5 of the UNIDROIT Principles). The "user consent" principle posits that, as a matter of the law of obligations, a non-user or a non-participant in a system cannot be bound by an obligation unless it has agreed or consented to be so bound and that, therefore, in the absence of this agreement or consent, the choice of law agreed by the users or participants of the system (including as to the transfer of proprietary rights) cannot bind any such non-user or non-participant and, thus, the choice of law will not be effective *erga omnes*. We do not consider that it is necessary to analyse the participant autonomy principle, as it may apply to digital assets held or recorded in a DLT-based system, in this way. The better analysis is that the law that the participants in the system have agreed shall apply to proprietary disputes will also bind third parties seeking to deal with digital assets held or recorded in that system, even if they have not actively agreed or consented to that law, because that agreement is an inherent and intrinsic part of the digital asset over which that third party seeks to take a proprietary interest. English law has developed the "conditional benefit" principle; this dictates that where a right assigned or transferred to a third party is itself conditional or qualified so that its exercise is subject to a restriction or burden, the assignee or transferee must comply with that restriction or burden: see *Chitty on Contracts*, at paras. 23-082 and 23-083. Thus, we would qualify the observation made in paragraph 12.33 of the Call for Evidence that contractual rights "are only valid and enforceable against a particular person [the contractual counterparty]".
- 8.4 Accordingly, a third party who seeks to acquire a proprietary interest or right in or to a digital asset held or recorded in a DLT-based system must take that interest or right subject to the intrinsic restrictions or burdens associated with that interest or right, including that it may only exercise its rights, or certain of its rights (notably with respect to transfers of title), with respect to the asset in question subject to the law chosen by the participants in that system (and, in particular, by the VNOs of the DLT-based system). The "right", authority or power of the system itself (or the operator of and participants in the system), as against any third party acquiring the benefit of a digital asset held or recorded in the system, to determine proprietary issues affecting that asset by reference to applicable law is not a contractual construct but is, rather, an intrinsic feature of the digital asset. We do not consider there to be any material policy reason why this approach should not apply to digital assets: it is consistent with established principles of English law that an intangible proprietary right is inevitably subject to a framework within which the right arises, exists or is instantiated and by which it may be transferred or the other rights of ownership otherwise enjoyed, including the ability to grant a security interest over the proprietary right and the rights of the holder of that security interest. To take a more simple example, a beneficial interest in a trust exists upon and subject to the terms of that trust and any third party who seeks to take a proprietary interest in that beneficial interest, e.g. a person taking security over the interest, takes subject to the regime that created that interest.

- 8.5 By way of further example, let us assume that the owner with legal title to a digital asset held or recorded on a DL, with factual control through possession of the private key, is Party A. Party A effects, or purports to effect, off-chain equitable assignments to the same digital asset to both Party B and Party C and, thus, there is a title dispute between Party B and Party C. If Party A is physically located in country X and a court in country X (applying its domestic law) determines that Party B has priority and title to the digital asset, the court might consider making an order declaring Party B to be the true owner and that the private key should be passed by Party A to Party B. However, the court in country X also knows that the consensus mechanism in the system in which the digital asset in dispute is recorded has agreed to resolve proprietary disputes by reference to the laws of country Y. Under the laws of country Y, Party C rather than Party B has good title to the digital asset.
- 8.6 If the court in country X were to declare in favour of Party B, it would need to recognise that its order may be futile and in vain, and would not prevent Party C from obtaining an order from a court in country Y declaring that it has title to the asset under country Y's proprietary laws, and notify the system's participants of the correct priority position under which it, and not Party B, has good title to the digital asset. In such a case, Party C could reasonably argue that if the consensus mechanism were to update the ledger in response to a transaction input by Party B (applying the laws of country X), it would be acting contrary to its agreement to operate the consensus mechanism solely in accordance with the laws of country Y – with the resulting adverse reputational and other effects on the integrity and predictability of the system so as to vitiate public confidence in the system. This would be contrary to the economic self-interests of the VNOs and other participants, as the continuing financial value of the digital assets they hold in the system will be directly affected by the wider market confidence in the integrity and predictability of the system's governance and operational arrangements. Further, Party C could reasonably assert that any legal title vested in Party B in execution of the court order made in country X would (under the applicable law governing the system) in fact be impressed with Party C's continuing, subsisting prior equitable interest. Party B could not take the legal title to the digital asset, by the passing of control of the private key to it in compliance with an order of the court of country X, free and clear of Party C's equitable interest. If English law applied, Party B would hold the legal title to the digital asset on trust for Party C. In such a case, Party C could maintain that any action the VNOs might take to execute and complete a transaction input by Party B without the consent of Party C would be a breach of trust and would, therefore, potentially put all VNOs verifying that transaction and effecting a consequential change to the DL at risk of constructive trust accessory liability.
- 8.7 The result would be that any legal title passed to Party B by order of the court in country X would potentially render the digital asset valueless. It would no longer be capable of an effective transfer through the system in which it exists. In principle, Party B might be able to make onward "off-ledger" transfers of the legal title by passing the private key to a new transferee and so on. However, any such onward transfer is likely to be effected subject to the continuing, subsisting prior equitable interest of Party C from transferee to transferee. One of the key economic features of the digital asset, its transferability through the DLT-based system in which it is recorded, is lost. In practice, this is likely to mean that there will be a fork in the blockchain. The consensus mechanism will only respond to a transaction input by Party C and its successors in title.

- 8.8 Faced by this practical reality – evidencing that the true "root of title" to a digital asset is the consensus mechanism applicable to the DLT-based system in which the digital asset is held or recorded and not factual control alone – the courts in country X (seeking to avoid making a futile order) are likely to apply the laws of country Y, and not their own domestic law, to make an order instructing Party B to pass control of the digital asset in dispute to Party C. Party C can then input a transaction into the system requiring it to enter on the ledger its system address (under its private key), or that of its nominee, agent or custodian or that of a third party transferee (as Party C's successor in title).
- 8.9 We noted in paragraph 8.2 above that we do not agree with the statement in paragraph 12.35 of the Call for Evidence, that "property law remains a mandatory form of law from which parties cannot derogate using the principle of party autonomy and freedom of contract". In our view, in the context of a DLT-based system where the participants may be domiciled or resident in many different jurisdictions, but have agreed a consensus mechanism for the operation of the system and transfers of digital assets through the system by way of a status change to the DL, any principle of private international law applicable to this arrangement must recognise that no particular jurisdiction will have coercive authority to enforce its principles of personal property law against the consensus agreed by the participants. To put it another way, the transfer mechanism for digital assets held or recorded on a DLT-based system, and the entities which operate that mechanism through the consensus, are not within the "sphere of sovereignty" of any particular country or territory. Therefore, the "nature of property law" referred to in paragraph 12.34 of the Call for Evidence cannot apply to the digital asset and in our view, and recognising the operation of a DLT-based system independently of any particular legal system, where a person takes or purports to take a proprietary interest in a digital asset held or recorded in a DLT-based system, that person must be taken to have accepted that, to ensure the validity of that transaction as against third parties, it has no choice but to invoke the authority of the consensus operating in the DLT-based system in applying the prescriptive sovereignty of the jurisdiction whose laws have been chosen to determine proprietary issues affecting the digital asset.
- 8.10 As we indicated in the Summary, where we indicate our support for recognition of the principle of party autonomy, or participant autonomy, to allow the participants in a system to choose a single governing law, we mean that governing law without reference to its conflicts of law, i.e. without admission of concepts such as renvoi, which could undermine the desire to achieve legal certainty by taking one to a different system of law from that intended by the participants in the system and understood by third parties who take subject to the rules and governing law of the system. The necessity of avoiding this outcome is reflected in Principle 5 of the UNIDROIT Principles and in Regulation 19 of the FCARs.
- 8.11 In the context of financial assets in particular, therefore, we believe that attempts to apply the *lex situs* of a digital asset held or recorded in a DLT-based system will be impractical and ineffective. It is critical to the effectiveness, stability and utility of cross-border international finance transactions that the principles of private international law applied to dealings with digital financial assets should provide legal certainty; absent that, systemic risks are inevitable. This outcome may be achieved if the principle of participant autonomy is applied to systems which operate a consensus mechanism. There is support for this approach in *Dicey & Morris*, Rule 143; this

approach is already recognised in the Settlement Finality Regulations, in the context of clearing, settlement and payment systems, and is at least implicit in the assumptions as to the risks inherent in financial systems and dealings in financial assets made by financial services regulators in multiple jurisdictions. There are strong public policy reasons to support the "participant autonomy" approach and, thus, to support the objectives of the efficacy of court action and public confidence in a safe, efficient and predictable mechanism for the treatment of rights associated with digital assets, including the taking of collateral over digital assets held in a consensus-based system.

- 8.12 As is implicit in the comments we have made in this Response on the policy benefits of protecting the primacy of the governing law chosen by the participants of a DLT-based system to determine proprietary and non-proprietary claims or other issues, we would also strongly favour a review (and amendment) process to the Rome I Regulation and the Rome II Regulation (as applicable in the UK) so as to ensure that relevant consumer, mandatory and locational rules are subordinated to the governing law of the system, or, as appropriate, the country or territory whose law governs the system, so that participants have certainty as to the law that will govern any claim or other issue arising out of, or in connection with, their participation in the system as affecting relevant digital assets held in the system. For similar reasons, we would also favour consideration as to whether the common law rule in *Ralli Bros. -v- Compania Naviera Sota y Aznar*⁷, which as a matter of English private international law may require that a contract is not enforced or is invalid insofar as its performance is unlawful by the law of the country where the obligations arising out of it are to be performed, should be modified in its application to contracts executed on, or to be performed by the functions provided by, an exchange, clearing or settlement system operating with DLT-based functionality. Specifically, it might be clarified that the place of performance of any such contract, for the purpose of the common law rule, should be deemed to be the country or territory whose law governs the system. Any relevant modifications made to the relevant provisions of the Rome I Regulation and the Rome II Regulation and the relevant common law principle for "simple" contracts should be applied equally to the corresponding conflict of laws rules adopted and applied to contracts made on bills of exchange, promissory notes or other negotiable instruments held in a reliable system, including ETDs.

9. Question 9: Paragraph 8.92 and Paragraph 13.9 of the Call for Evidence - questions concerning the applicable law for consumer contracts.

- 9.1 The FLC has no particular views or evidence on this question other than to note (a) that much will depend on consumer protection legislation, which raise questions of policy beyond the competence of the FLC, and (b) where any claim relates to a digital asset held or evidenced in a DLT-based system, the rules and governing law of the system should prevail for the reasons set out above.

10. Question 11: Paragraph 9.38 and Paragraph 13.11 of the Call for Evidence – views and evidence on localising damage arising in tortious claims relating to crypto-tokens for the purposes of applicable law; and Question 12: Paragraph 9.54 and Paragraph 13.12 of the

⁷ [1920] 1 KB 614.

Call for Evidence – views and evidence on the "escape clause" in Article 4(3) of the Rome II Regulation.

- 10.1 In our view, the key policy objective of obtaining legal certainty with respect to dealings with digital assets, and thus assuring confidence in those dealings, may be achieved in part through the common law (the principle of participant autonomy), and in part by legislation which enables those dealing with digital assets, and in particular participants in a DLT-based system, to choose a law to govern both their contractual rights and their non-contractual rights arising with respect to the system, including enabling contracts to be performed or settled through that system. The chosen law should govern both the relationships between participants in the system and third parties in dealings in digital assets issued, held, recorded or transferred within the system.
- 10.2 We think a more certain result would be obtained, including in the context of non-contractual claims, if the first option in any waterfall of options provided by English law principles of private international law (and, ideally, in any supranational treaty or convention to which the UK may come to adhere) is the law chosen by the participants in the relevant system which, as we have noted above, we consider would also bind third parties, including in the context of proprietary rights arising with respect to the digital assets held or recorded in the system.
- 10.3 In those cases where participants in a system have not expressly chosen the applicable law to govern proprietary issues affecting digital assets recorded in the system, we consider that (without affecting the primacy of the chosen law, where specified) the relevant conflict of laws rule will need to provide a "waterfall" of options to determine the applicable law to govern proprietary issues. This could include application of the law of the country or territory in which the operator or administrator (if there is one) of the system has its registered office or "statutory seat" (as provided by Principle 5 of the UNIDROIT Principles); or, failing that, the law of the country or territory in which the owner or controller of the digital assets in dispute is domiciled, has its habitual residence or is located as at the time of the transaction. We would favour priority (where available) for the location of the administrator of the system, especially where it has access to "master node" functionality to update the DL, over the location of the issuer of a digital asset recorded in the system.
- 10.4 We agree that a "default position" is likely to be needed in the absence of an express choice of law or satisfaction of the other "higher priority" tests in the waterfall, for the location of the controller or transferor of the digital asset the subject of the particular dispute or transaction. This may be of particular relevance for permissionless DLT systems. It would, though, be fundamental to the concept of a waterfall of options that there would be no "escape clause" that would override the participant autonomy rule.
- 10.5 We note that anonymity, or the inability to identify holders, transferors or transferees of digital assets, has been a problem in the tortious cases thus far considered by the English courts. Any rule of private international law that is based on the location or the transferor or current holder of a digital asset means (particularly for digital assets recorded or held in a permissionless system) that the applicable law may be incapable of being ascertained, which in turn may cast doubt on the question whether the courts of any particular sovereign country could or should accept jurisdiction in the applicable dispute.

11. Questions 13 to and including Question 19 on electronic bills of lading, electronic bills of exchange/negotiable instruments and the Electronic Trade Documents Act 2023.

- 11.1 We note the comments made by members of trade associations during the industry/practitioners roundtable events held by the Law Commission in April 2024, that (a) English law is invariably included as the governing law of bills of lading; (b) section 72 of the Bills of Exchange Act 1882 (the "**1882 Act**") does not apply to bills of lading; (c) local law matters typically arise only in the context of fraud and insolvency, and (d) there was and is a very well understood and consistent approach to trade documents recognised in multiple legal systems around the world, based principally either on the 1882 Act or the French civil law approach. We agree that in the experience of the members of the FLC, UK and European banks use bills of exchange less, these days, than banks in the Middle East and the Far East. Finally, we note the comments made by practitioners at the roundtable events that there is growing use of ETDs and the Electronic Trade Documents Act 2023 has been a catalyst for legislation in other jurisdictions. Our comments on these questions are, therefore, primarily limited to the concerns arising from section 72 of the 1882 Act, in the context of bills of exchange and promissory notes.
- 11.2 We agree with the comments made by participants at the roundtable events that the policy objectives should be to foster and ensure transparency, cost-efficiency and effective cash management in the context of international trade and, therefore, an approach which provided for a single system of law as data/ETDs move through the inevitable multiple platforms for the submission of ETDs will be a critical objective; the key is developing "reliable systems.
- 11.3 We do not agree with those who would argue that there should be movement away from reliable systems towards relevant participants; this seems to us to be likely to undermine the need for certainty.
- 11.4 Where a bill of exchange or promissory note is issued as an ETD, the functions of the relevant reliable system will or may operate on the ETD to perform the acts of issuance, drawing, acceptance, indorsement, presentment and payment (and to make the related contracts on the instrument) that are the subject of the conflict of laws rules of section 72 of the 1882 Act. As the performance of those functions will be governed by the law of the reliable system and section 72 is primarily concerned with legal issues (formal validity of instruments/contracts, contract interpretation and duties), it would be logical and consistent with legal policy for the country whose law governs the system to be identified as the relevant "place" for the purposes of s. 72. This would provide a coherent, certain and readily ascertainable conflict of laws solution for s. 72 in its application to bills of exchange and promissory notes issued, held and negotiated as ETDs in a reliable system; and relevant stakeholders could readily assess and analyse the validity and effectiveness of the reliable system's functions as operating in relation to an ETD, under the applicable law, to support the formal validity of the ETD held and negotiated through the system, as well the other legal matters the subject of section 72.
- 11.5 It is conceivable that a negotiable instrument, which is not a bill of exchange or promissory note, may be issued, held and transferred as an ETD by means of a reliable system. It seems likely that such an instrument would not fall within the scope of the

conflict of laws rules set out in section 72. In order to provide legal certainty for the corresponding conflict of laws rules that would apply to such an instrument, a suitable statutory provision is likely to be needed to extend like rules to those set out in section 72, as modified above for bills of exchange and promissory notes recorded in a reliable system, to other types of negotiable instrument recorded in the reliable system.

- 11.6 Separately, as a general observation and although not strictly a private international law issue relevant to bills of exchange, promissory notes and other negotiable instruments recorded in a reliable system, in order to allow for the effective presentment for payment or acceptance of such instruments as ETDs by means of a reliable system, substantive amendments would also need to be made to the rules for due presentment for payment (section 45 of the 1882 Act) and due presentment for acceptance (section 41) to the extent they require presentment "at a reasonable hour on a business day" and/or presentment "at the proper place". Presentment is a process under which the bill of exchange itself is physically delivered to the payer: see *Barclays Bank plc -v- Bank of England*⁸; see also s. 52(4) of the 1882 Act. These substantive provisions would need to be expressed to apply to any instrument constituted as an ETD which requires the instrument to be presented (as a matter of the 1882 Act or common law) with reference to temporal or locational requirements that are inapposite for the DLT-based system or similar operation of a reliable system. As it is likely that a legislative instrument will be required to set out the conflict of laws rules for ETDs that are negotiable instruments (and to make amendments to the provisions of section 72 to govern how the relevant conflict of laws rules are intended to apply to bills of exchange or promissory notes issued as ETDs), it would be reasonable to take the opportunity to make appropriate modifications to the rules for presentment for payment/acceptance (both under the 1882 Act and at common law) to support the presentment for payment/acceptance of ETDs, as negotiable instruments, by means of a reliable system.
- 11.7 Please note on this point that the statement in paragraph 11.36 of the Call for Evidence that "... the place where a bill is payable, where an act relating to presentment is done, or where the bill is dishonoured do not seem to relate to the location of the bill of exchange itself", is not correct. A bill is payable at the location of the "proper place" where the bill itself must be duly presented for payment in accordance with section 45 of the 1882 Act and it will be dishonoured by non-payment at that place where payment is refused or cannot be obtained in accordance with section 47 of the 1882 Act.
- 11.8 Consideration should also be given as to whether the safety and integrity of the operation of reliable systems, and public confidence in such systems, might be further enhanced by establishing in legislation conflict of laws rules for ETDs recorded in reliable systems, but which are not within scope of the limited rules set out in section 72 of the 1882 Act, for example, material validity, effect of illegality, mandatory provisions and other matters that are governed by the Rome I Regulation for "simple" contracts, i.e. those that are not made in the form of a negotiable instrument.

16 May 2024

⁸ [1985] 1 All ER 385 at 394



**JOINT RESPONSE OF THE COMMERCIAL BAR ASSOCIATION AND THE
CHANCERY BAR ASSOCIATION TO THE LAW COMMISSION'S
*DIGITAL ASSETS AND ETDs IN PRIVATE INTERNATIONAL LAW:
WHICH COURT, WHICH LAW? CALL FOR EVIDENCE***

30 May 2024

Contributors

Chloë Bell (3 Verulam Buildings)
Anca Bunda (3 Verulam Buildings)
Joshua Cainer (Outer Temple Chambers)
Anson Cheung (Outer Temple Chambers)
Rumen Cholakov (3 Verulam Buildings)
William Day (3 Verulam Buildings)
Peter Dodge (Radcliffe Chambers)
Charlotte Eborall (3 Verulam Buildings)
Matthew Hoyle (One Essex Court)
Sophia Hurst (Essex Court Chambers)
Luka Krsljanin (Blackstone Chambers)
Sarah O'Keefe (Brick Court Chambers)
James Potts (3 Verulam Buildings)
Nik Yeo (Fountain Court Chambers)

This is the joint response of the Commercial Bar Association (“COMBAR”) and the Chancery Bar Association (“ChBA”) and is confined to those questions concerning digital assets. Where the same question asks about both ETDs and digital assets, the response is confined to digital assets, save where otherwise expressly stated.

References to “paras” or “fns” are (unless otherwise indicated) to paragraphs or footnotes in the Law Commission of England and Wales’ *Digital Assets and ETDs in Private International Law: Call for Evidence* (2024).

Consultation Question 1

1. In this question, we seek views and evidence on jurisdiction over consumer contracts.

(1) To what extent can the issue of jurisdiction over op and decentralised contexts be accommodated by section 15B of the Civil Jurisdiction and Judgments Act 1982?

(2) Does the fact that the business is a crypto-business, as opposed to any other business, change the analysis of whether a business has directed its services to consumers located in the UK?

(3) Are there any changes or clarifications that are needed in respect of the issue of jurisdiction over consumer contracts?

(4) To what extent does this issue cause problems in practice (or is likely to in future)?

1.1. We agree with the Law Commission that consumer contracts in the digital and decentralised contexts do not pose any significant new difficulties compared to other cross-border consumer contracts that are well-established in the jurisprudence. We consider that the issue of jurisdiction over consumer contracts in the digital and decentralised contexts can be accommodated comfortably by section 15B of the Civil Jurisdiction and Judgments Act 1982 (“CJJA 1982”). This is consistent with the approach taken by the courts in *Soleymani v Nifty Gateway LLC*,¹ but also in *Chechetkin v Payward*,² where Mr Justice Miles found that the claimant fell within the definition of consumer under section 15E of the CJJA 1982.

¹ [2021] EWCA Civ 1297 (CA) (cited by the Law Commission at fn 240).

² [2022] EWHC 3057 (Ch).

1.2. We do not consider that the fact that the business is a crypto-business, as opposed to any other business, changes the analysis of whether the business has directed its services to consumers located in the UK. A particular feature of some crypto- businesses (including large exchanges) is their opaque corporate structure and the fact that it is difficult to ascertain from which country the business is providing services. This issue is less often encountered with distance-selling or other businesses providing goods or services over the internet outside the crypto sphere. However, this still does not change the analysis of whether a business has directed its services to consumers located in the UK. As explained Rby the Law Commission, for an internet business to be directing its activities to a particular country, it must, in addition to allowing the customers from the country to access the website, manifest an intention to establish commercial relations with consumers from one or more other countries. The application of this test (as well as the other aspects of the test set out in the CJEU jurisprudence) is fairly straightforward when crypto-businesses advertise to consumers in the UK (for example by placing online advertisements or even advertisements in public transport). It is likely that the application of the test will be less straightforward when crypto-businesses, for example large exchanges, use a general “.com” domain and include statements on their websites to the effect that they are not operating in the UK, but in reality allow customers domiciled in the UK to open an account and trade, including sometimes allowing them to trade in sterling by using UK bank accounts. Notwithstanding these challenges, we are of the view that courts will be able to deal with these situations on a case by case basis. As such, we do not consider that there any changes or clarifications that are needed in respect of the issue of jurisdiction over consumer contracts.

1.3. We also do not foresee that the issue of jurisdiction over consumer contracts is likely to cause significant issues in practice. A consumer is defined in section 15E of the CJJA 1982 as “*a person who concludes the contract for a purpose which can be regarded as being outside the person's trade or profession.*” The limits of this definition have been tested in a number of CJEU cases cited by the Law Commission. As pointed out by the Law Commission, the fact that someone is placing large and risky bets with apparent sophistication does not undermine their status as a consumer. As such, it is likely that a vast number of individuals buying or selling cryptoassets will fall under the definition. Issues may arise in practice if individuals who would have otherwise been classified as consumers choose to trade through, for example, limited companies and are therefore

unlikely to fall under the CJJA 1982 (although we note that this is a point implicit, not explicit, under the CJJA 1982, in contrast to Article 6 of the Rome I Regulation³). However, this is an issue of general application that was considered by the drafters of the legislation and the courts when striking a balance between the need to protect consumers and the need to protect businesses/ensure certainty and, in any event, it is something that has already been considered by the courts previously (in contexts outside cryptoassets).

- 1.4. More specific issues may arise in practice where UK customers use virtual private networks to trade on crypto-exchanges (or access other crypto businesses) that do not advertise to UK customers but allow those with an obvious UK domicile or residence to open an account. In any event, this too is an issue that the courts are likely to be able to resolve on a case by case basis.

³ Regulation on the law applicable to contractual obligations (EC) No 593/2008, Official Journal L 177 of 04.07.2008.

2. In this question, we seek views and evidence on jurisdiction founded on the basis that a contract was concluded in England and Wales.

(1) How should the courts apply gateway 6(a) to a smart contract? Should the relevant connecting factor be the participating computer, or the real-world actor?

2.1. Gateway 6(a) requires that the contract is made within the jurisdiction or that an offer was at least received within the jurisdiction. The gateway was widened to address concerns that jurisdiction may otherwise be determined by the happenstance as to the sequencing of offer and acceptance, given the general rule under English law that a contract is formed where the acceptance is communicated. Those concerns were misplaced because, prior to that reform, courts had shown themselves willing to construe gateway 6(a) liberally and recognise the possibility that cross-border contracts can be made simultaneously in two places.⁴ This approach should continue even after that reform since it is consistent with the general approach taken to the gateways, i.e., that a broad approach is appropriate because claims with tenuous connections to the jurisdiction will then be ‘filtered out’ at the stage of assessing *forum conveniens*.⁵

2.2. COMBAR and ChBA previously suggested, in responding to the Law Commission’s call for evidence in respect of smart contracts,⁶ that the general rule requiring communication of acceptance in the *lex fori* should be applied by the Court in respect of gateway 6(a) by focusing on the place where the real-world actor (i.e., human) is when acceptance is communicated rather than on the place where computer programs or codes interact with each other autonomously of the real-world actor. This was broadly the same response as other consultees.⁷ However, the Law Commission’s response was that “*it is difficult to see how this approach would apply to smart legal contracts where acceptance does not need*

⁴ See, e.g., *Apple Corps Ltd v Apple Computer Inc* [2004] EWHC 768 (Ch) and *Conductive Inkjet Technology Ltd v Uni-Pixel Displays Inc* [2013] EWHC 2968 (Ch).

⁵ See, e.g., *FS Cairo (Nile Plaza) LLC v Lady Brownlie* [2022] AC 995 at [79] and [82], albeit on gateway 9.

⁶ Law Commission, *Smart Contracts: Call for Evidence* (December 2020); Joint ChBA and COMBAR Response (16 April 2021) p 23 (response to question 47).

⁷ Law Commission, *Smart Legal Contracts: Advice to Government* (November 2021, Law Com No 401) paras.7.31-7.35.

to be communicated to the offeror, and therefore does not occur”, and suggested that there might be “a bespoke principle that identified a smart legal contract’s place of formation”.⁸

2.3. The first point is a good one (which we accept poses a problem for its previous proposal, though see the next paragraph) but the second, with respect, is not. There is nothing unusual about contracts formed in circumstances where the offeror has waived the right to receive communication of acceptance: it simply reflects that the communication requirement for acceptance is a default not a mandatory rule.⁹ There is also nothing new about contracts being formed autonomously of human actors. The classic example is the ticket machine in the car park,¹⁰ where it must be the case that the relevant human actor whose offer was made through the ticket machine has waived any right to receive communication of the acceptance before the contract is made with the customer. We therefore doubt that a special rule needs to be created for smart contracts (just as no special jurisdictional rule needs to be created for car parking machines).

2.4. We suggest that question 2(1) offers a false dichotomy. It asks whether the relevant connecting factor is the participating computer or the real-world actor. However, the overriding question for gateway 6(b) is where the contract is made and, once it is recognised that there is no “conceptual barrier”¹¹ to treating a contract as concluded in multiple places, the contract can fairly be characterised as having been concluded both in the place of the participating computer (if it can be identified)¹² and in the place of the real-world actor (even where they have waived their right to communication of the acceptance)¹³ and choosing between them (if that is the choice) would then be a matter to be addressed at the *forum conveniens* stage.

⁸ Ibid, paras 7.35-7.36. See also para 5.14 of the present *Call for Evidence*.

⁹ See, e.g., *Carlill v Carbolic Smoke Ball Co* [1893] 1 QB 256 (CA) and *Argo Fund Ltd v Essar Steel Ltd* [2005] EWHC 600 (Comm).

¹⁰ *Thornton v Shoe Lane Parking* [1971] 2 QB 163 (CA) referring to a “ticket which is issued by an automatic machine” at 169: “It can be translated into offer and acceptance in this way: the offer is made when the proprietor of the machine holds it out as being ready to receive the money. The acceptance takes place when the customer puts his money into the slot. The terms of the offer are contained in the notice placed on or near the machine stating what is offered for the money.”

¹¹ *Apple Corps Ltd v Apple Computer Inc* [2004] EWHC 768 (Ch) at [37].

¹² An exercise which is easier for car parks than code.

¹³ Here, the approach of the majority in *Quoine Pte Ltd v B2C2 Ltd* [2020] SCGA(I) 02 in looking (albeit when applying the substantive law of unilateral contracts, not a question of jurisdiction) at the last point at which the (human) B2C2 programmer had input into the code provides an example of where relevant human involvement can predate by some period the actual formation of the contract.

(2) If gateway 6(a) should use a connecting factor based on the real-world actor, how should their location be determined? Should it be by their habitual residence, their domicile, or at the place where they happen to be at the time the contract was formed?

2.5. It would be orthodox to treat the real-world actor as being in the place where they are actually located at the time that the contract is formed. We note the language adopted by the Law Commission (“*happen to be*”) implies some dissatisfaction with this rule. We consider that to be misplaced: it means that the operation of this gateway will turn on objective primary fact which should then reduce the scope for extended jurisdictional arguments. It would be a rare case for there to be a dispute about where someone physically was located at the relevant time. That makes it attractive in practice (as well as in line with first principles).

2.6. In contrast, concepts of domicile (largely used in the common law) and habitual residence (largely used in European legislation) involve a broader dichotomy

(4) To what extent is it likely that the question of where a smart contract is made will become prevalent in practice?

2.7. We doubt the place(s) in which a smart contract is formed will matter other than in the private international law context. We add that it may be relevant to governing law not just jurisdictional questions. In contrast, it may well be relevant in practice to ask when a smart contract is formed (and so when the contracting party was bound). In that context, the question of where the contract is formed may arise as an ancillary issue.

Consultation Question 3

3. In this question, we seek views and evidence on jurisdiction founded on the basis that damage or detriment was suffered in England and Wales.

- (1) Do you consider the approach of the courts of England and Wales so far in the crypto litigation when localising damage or detriment for the purposes of jurisdiction to be theoretically sound?**
- (2) To what extent can it be said that tortious damage pleaded in the crypto-token litigation are not cases of pure economic loss? How else could tortious damage in the crypto-token context be conceptualised?**
- (3) If the crypto-token cases are cases of pure economic loss, to what extent would it be desirable that a consistent approach is taken in England and Wales to localising pure economic loss as between jurisdiction and applicable law?**

3.1. We consider that the difficulties in localising damage or detriment for the purposes of jurisdiction in crypto litigation to be generally reflective of locating damage or detriment in cases without physical damage or detriment. We do not think that there is anything theoretically problematic in the case-law to date other than the fact that most of the decisions have arisen in contexts with only one party being represented such that the Court has not necessarily had the advantage of considered arguments from both sides, and in an interim relief or jurisdictional context where the threshold is one of a good arguable case or serious issue to be tried.

3.2. However, we do not agree that the case-law cited is remarkably inconsistent or more difficult to interpret than other case-law in the context of pure economic loss and jurisdiction:

3.2.1. *AA v Persons Unknown* – the damage (i.e., the loss of money by paying the ransom) was directly suffered in England in the Claimant company's bank account.

3.2.2. *Ion Science v Persons Unknown* – the damage was held to have been suffered in England because the direct damage was suffered by the Claimants in England

(i.e., where the company (C1) was incorporated and where C2 was domiciled). This is where both Claimants directly felt the losses.

3.2.3. *Lubin Betancourt Reyes v Persons Unknown* – the direct damage was felt in England (i.e., where C1 was domiciled and where C2 was incorporated). The bank accounts of the Claimants were English and the USDT and Binance accounts were registered to an address in England. C1 was acting in the course of business when the spear-phishing attack took place. The reason C1 was in Spain was not because he had relocated the centre of his business interests but due to being there because of the travel restrictions of the Covid-19 pandemic.

3.2.4. *D'Aloia v Persons Unknown* – the Claimant felt the direct loss in England where he was located when the transfer of crypto-tokens was made. The same analysis is applicable to *Jones v Persons Unknown* and *Fetch.ai*.

3.3. We can see that *Tulip Trading* is the one case that does not fall within the kind of analysis that can be applied to the other cases. Specifically, the Claimant company was incorporated in the Seychelles. Therefore the loss would have been directly felt in the place of incorporation. Whilst the company's agent was in England, the basis for relocating the company's damage to the place of the agent is unclear as it erodes the concept of having a separate corporate personality for companies.

3.4. We can see the argument that the tortious damage pleaded (thus far) in crypto cases can be classified as pure economic loss because what the claimants are complaining about is their deprivation of access to a thing of value that they would otherwise be able to trade, spent or exchange. Some of us agree with the way this is put in para 5.49. Others are cautious about classifying these cases as “pure economic loss” cases because of the inconsistency with the Supreme Court's recent description of pure economic loss as “*economic loss that is not consequent on damage to, or loss of, the claimant's property (or on personal injury to the claimant)*”.¹⁴

3.5. We think it would be desirable to have consistency between jurisdiction and applicable law in crypto-token cases. It is obviously desirable for a court with jurisdiction to be applying its own laws. This ultimately comes down to a robust application of the relevant

¹⁴ *Armstead v Royal & Sun Alliance* [2024] 2 WLR 632, [21].

legal tests and we consider that to be beyond issues of jurisdiction and applicable law in respect of crypto-tokens. However, it is something we would welcome were it possible for the Law Commission to address in this project.

Consultation Question 4

4. In this question, we seek views and evidence on jurisdiction founded on the basis that an unlawful act was committed in England and Wales.

(1) To what extent is the approach of the courts in England and Wales so far in the crypto litigation when localising where an unlawful act was committed for the purposes of jurisdiction theoretically sound?

(2) To what extent does the question of where an unlawful act is committed or even occurs for the purpose of jurisdiction arise in practice?

4.1. The answer to question 4(2) is that this question can arise in practice – but largely at the interim stage of proceedings and typically without notice (exceptions being where there are uncontested applications for summary judgment¹⁵ but these are too have so far been uncontested) – and the answer to question 4(1) therefore is that the existing case law should be treated with caution and not treated as having definitively settled the relevant principles. An example of this is Trower J’s comments in *Piroozzadeh v Persons Unknown*¹⁶ which made clear that too much weight should not be placed on his *ex tempore* judgment on a without notice application in *D’Aloia v Persons Unknown*¹⁷ in respect of whether a cryptocurrency exchange was a constructive trustee.

4.2. In the particular context of identifying whether an unlawful act has been committed in England, we consider that the Law Commission has correctly identified the relevant cases to date: *Ion Science v Persons Unknown*;¹⁸ *Jones v Persons Unknown*;¹⁹ and *D’Aloia v Persons Unknown*.²⁰ However, we suggest that the Law Commission risks overstating the importance of these authorities:²¹

4.2.1. In *Ion Science*, Butcher J held (*ex tempore* on a without notice application) no more than that there was a good arguable case that gateway 9 was available either on the basis of the damage having been sustained in England or on the basis that

¹⁵ *Jones v Persons Unknown* [2022] EWHC 2543 (Comm); *Boonyaem v Persons Unknown* [2023] EWHC 1380 (Comm); *Mooij v Persons Unknown* [2024] EWHC 814 (Comm).

¹⁶ [2023] EWHC 1024 (Ch) at [28].

¹⁷ [2022] EWHC 1723 (Ch).

¹⁸ Unreported, 21 December 2020.

¹⁹ [2022] EWHC 2543 (Comm).

²⁰ [2022] EWHC 1723 (Ch).

²¹ Paras 5.64-5.73.

the unlawful acts had been in England. This was a case where the (English-domiciled) Claimant was tricked into allowing remote access to their computer (in England), following which the Defendant and/or their associates executed transactions that extracted the Claimant's bitcoin. It is difficult to see how at least one of those limbs of gateway 9 was not satisfied on that fact pattern, but likewise hard in the circumstances to treat *Ion Science* as authoritative as to where unlawful acts are committed or occur for jurisdiction purposes in cryptoasset disputes.²²

4.2.2. In *Jones*, Nigel Cooper KC (sitting as a Deputy High Court Judge) held, in the context of an uncontested summary judgment, that gateway 16 was satisfied for an unjust enrichment claim on the basis of acts committed in the jurisdiction but without explanation. The Court appeared to regard this as obvious since the Claimant was domiciled in England (and, it can be inferred from the judgment, physically located in England)²³ at the time of the cyber-attack. The Law Commission notes that it is “*surprising*” that Russia was not seriously considered as the place in which the unlawful acts were committed, given the evidence that the cyber-attack may have emanated from Russia.²⁴ But this is likely to turn on the strength of that evidence as to that connection: on the face of the judgment it was only “*a suggestion*” that the attack came from Russia.²⁵ In those circumstances, and especially given the uncontested nature of the hearing, it is not surprising that the Court did not decide that the unlawful acts were committed in Russia. (And see also paragraph 4.4 below.)

4.2.3. Lastly, in *D'Aloia* itself, the Court (even at the without notice hearing) declined to state a view on this point, being both a complex question and unnecessary on the facts of that case.

4.3. Although these cases cannot be treated as having settled definitively the relevant principles, they do show that this issue does arise in practice. However, it arises less often

²² The fact that Butcher J did not even assign a neutral citation number to the transcript of his judgment underlines that the Court likely did not think the judgment was of any particular precedential value – the finding that the points were arguable was subject to being persuaded otherwise on a return date. So the Law Commission should be cautious in treating *Jones* as articulating some form of domicile rule. Cf Para 5.72(1).

²⁴ Para 5.73.

²⁵ See *Jones* at [19]: “*Mr Jones is the victim of a large scale cyber fraud perpetrated by a group of online cyber criminals located overseas. There is a suggestion that they are based in Russia*”. Typically, such suggestions are the result of internet chatter rather than any specific tracing expert report.

than might initially be thought. This is because it is almost invariably the case that the perpetrators are unknown or operate from an unknown jurisdiction (even if there are suspicions that they are in a particular place, such as in *Jones*, as discussed in paragraph 4.2.2 above). Further, most of the cases have arisen out of situations where the damage was arguably quite clearly suffered in England and Wales (which is true in both *Ion Science* and *Jones*) such that any consideration of where the unlawful acts were committed or occur is not necessary.²⁶ As such, we expect that the jurisprudence on the location of the unlawful acts in cryptoasset disputes will take longer to develop with the parties using the damage gateway (which is broadly construed to include consequential loss)²⁷ where possible. Of course, in situations where all damage is suffered elsewhere, the location of unlawful acts will gain greater significance.

- 4.4. As with our response to certain other questions we address, it is also important that the Law Commission does not assume that this question yields a single jurisdictional answer. Gateways 9(b), 15(a), 16(a)-(b) and 21(b) are all phrased slightly differently but none of them require all juridically-relevant acts to be within the jurisdiction. It is well established in the context of gateway 9(b) – which can be applied by analogy to the other gateways – that it suffices that some substantial and efficacious acts are committed in the jurisdiction, even if there are other substantial and efficacious acts elsewhere.²⁸ In the case of an unlawful means conspiracy, for example, the tort can be regarded as being committed both in the place where the combination was formed and the place where it was implemented (and so the answer in *Jones* may well be that there were relevant acts in both England and Russia). As under gateway 6(a) choosing between those locations (if that is the choice) would then be resolved at the *forum conveniens* stage of the analysis.

²⁶ In a case, such as *Piroozzadeh v Persons Unknown*, where the claimant is not domiciled, resident or present in the UK, the point might be more complex, but that case was discontinued after the interim injunction was discharged at [2023] EWHC 1024 (Ch).

²⁷ *FS Cairo (Nile Plaza) LLC v Lady Brownlie* [2022] AC 995.

²⁸ *Metall und Rohstoff v Donaldson* [1990] 1 QB 391 (CA) at 437. See also *FS Cairo (Nile Plaza) LLC v Lady Brownlie* [2022] AC 995.

Consultation Question 5

5. **In this question, we seek views and evidence on jurisdiction founded on the basis that the claim relates to objects within England and Wales.**

(1) To what extent is the approach so far of the courts of England and Wales in localising a crypto-token for the purposes of jurisdiction theoretically sound? What would be the relative merits and demerits of any alternatives?

5.1. As noted above, we are cautious about drawing too much from many of the authorities, which are often first-instance interlocutory decisions establishing only a good arguable case that a gateway applies, and very often without hearing the contrary argument. The precedential value of such authorities is therefore limited.

5.2. The Law Commission has identified five cases in which jurisdiction was addressed. Additionally:

5.2.1. A ‘residence of the beneficial owner’ test also was applied in *LMN v Bitflyer*,²⁹ on an application by the claimant cryptocurrency exchange for Bankers Trust and Norwich Pharmacal information orders to locate cryptoasset transferred after a hack, and identify the hackers. Butcher J held that the relevant cryptocurrencies were at the time of the hack located in England and Wales on the basis that the claimant company was “resident and carries on its relevant business here”, notwithstanding the fact that its servers were located in Romania, which was briefly considered as an alternative situs.

5.2.2. Implicitly, this is also the approach taken by HMRC when it comes to whether cryptoassets fall within its purview. In its policy paper ‘Cryptoassets: tax for individual’ confirms that cryptoassets are liable to inheritance tax on the death of the holder and capital gains tax on a valid disposal, where the beneficial owner is UK resident. However, the choice is made for a ‘convenient, bright line rule’ (and somewhat self-serving...) rather than based on any theoretical analysis.

²⁹ [2022] EWHC 2954 (Comm), [20(2)].

5.3. We agree with the point made at para 5.97 and are also cautious about the degree of reliance placed on Professor Dickinson's analysis. "Participant" does not mean the same as beneficial owner, not least because the person controlling the private key and therefore 'participating' may be doing so on someone else's behalf (e.g., a trustee).

5.4. It is hard to conclude that the current test - residence (or maybe domicile) of the owner - is theoretically sound because it is out of step with the approach taken for other intangibles and is no more than a proxy, or a convenient fiction:

5.4.1. It carries none of the justification for the original gateway – e.g., per *Dicey Morris & Collins on Conflict of Laws* 16th ed. at para 23-025 (albeit in the context of the *lex situs* rule, rather than jurisdiction): "*first, that the situs is an objective and easily ascertainable connecting factor to which third parties might reasonably look to ascertain questions of title and, secondly, that the country of the situs has control over the property and a judgment in conflict with the lex situs will often be ineffective.*"

5.4.2. It is also inconsistent with the English law approach to other intangibles, i.e., for choses in action they are situated where they can be effectively dealt with, are properly recoverable or can be enforced (so effectively, where they are 'controlled'): see, e.g., *New York Life Insurance Co v Public Trustee*.³⁰

5.4.3. If that is right, it is not clear that a cryptoasset is controlled where its beneficial owner is resident (or domiciled). The UK Jurisdiction Taskforce's *Legal Statement* suggests that the location of control of a digital asset is where its private key is stored (see [99]). Society of Trust and Estates Practitioners (STEP) has also taken the view that locating cryptoassets for trusts and estates purposes, location should be linked to the location of the private key.

5.4.4. By way of example, see the case of James Howells, who accidentally threw away a USB drive containing the access information for bitcoin valued at over £200m. He obtained private equity backing to try to retrieve it from Newport local council landfill site but Newport council are denying permission to search.³¹

³⁰ [1924] 2 Ch 101, 109.

³¹ <https://www.bbc.co.uk/news/uk-wales-67297013>

Imagine James Howells was resident/domiciled in the U.S. Are the bitcoin more obviously located in the U.S. or Wales?

5.4.5. On the other hand, if a private key is kept encrypted on line (as Dr Wright said he did in relation to the cryptoassets in question in *Tulip Trading*), then even physical location of the private key is problematic. Perhaps then ‘control’ over the private key (and, to borrow from *Tulip Trading*, where any corporate controller exercises its central management and control) should be the touchstone.

5.4.6. Finally, not all digital assets are alike and some may more easily and more directly be identified within a jurisdiction, i.e., if a digital asset is tethered, the location of the off-chain asset may be thought to provide a closer connection.

5.5. We agree with the concern identified at para 5.98 as to the enforceability of a judgment where jurisdiction has been established on the purported basis of situs of the asset, where in fact residence of the beneficial owner has been used as a proxy. Although we do not have any direct examples, we think such an approach may well clash with other jurisdictional rules for locating the situs of a cryptoasset. In these cases, which are almost uniformly cross-border, there is a concern that judgments will not be capable of being enforced or will be subject to enforcement challenges.

5.6. As the Law Commission acknowledges, the case law has mainly been developed in the context of crypto-fraud cases, where the courts display a ready willingness to take jurisdiction and to assist victims using the arsenal of interim remedies available. See also *Joseph Keen Shing Law v Persons Unknown & Huobi Global Limited*,³² in which the High Court, having previously imposed a worldwide freezing order, ordered a crypto-exchange to transfer cryptoassets (which were not traceable by the Claimant) into this jurisdiction, convert them into fiat currency and pay them into the Court Funds Office, to enable enforcement of any personal claim against the Defendant, mirroring the rarely-invoked historical jurisdiction invoked in fraud cases discussed in *Derby v Weldon (No. 6)*³³ and *United Norwest Co-Operatives Ltd v Johnstone (No. 2)*.³⁴ Whilst counter-fraud policy may

³² [2023] 1 WLUK 577.

³³ [1990] 1 WLR 1139.

³⁴ Unreported, 6 December 1994. In the former case, the Court declined to order that money be transferred from one jurisdiction to another; instead ordering that the money remain in the account in which it was held and a receiver appointed.

provide a justification for adopting a peculiar approach in fraud cases (especially ‘hot pursuit’ scenarios), civil fraud is not the only scenario in which the gateway could or would apply:

- 5.6.1. A test based on residence or domicile of the (beneficial) owner effectively collapses into a test of residence of the claimant, subject to the claimant being able to show a good arguable case/plausible evidential basis that it is the beneficial owner. However that is not an internationally recognised way to found jurisdiction (the default position is usually defendant’s home court – see paragraph 19.4.3 below).
- 5.6.2. Wills and estates – in the context of cross-border probate disputes, the location of an asset may impact on whether and if so how it falls within the terms of a will governed by English law, and the validity of any bequest. There is clear scope for jurisdiction clash here.
- 5.6.3. Insolvency. Insolvency disputes will not often need to have direct recourse to the jurisdictional gateways, because jurisdiction is allocated under the Insolvency Act and Rules on the basis of debtor’s centre of main interests (COMI). That said, the situs of cryptoassets may be relevant for the purposes of allocating insolvency jurisdiction otherwise than on the basis of COMI, e.g., for establishing the English Court’s jurisdiction to open ancillary proceedings on the basis that some of the debtor’s assets (including digital assets) are situate in England and Wales, and whether they are ‘property’ falling within section 436 of the Insolvency Act 1986. Current consensus is that this will be established where any relevant off-chain asset is located in England & Wales, where there is any centralised control in the jurisdiction, or where a participant exercises control. This was applied in *Zipmex*,³⁵ a Singaporean case concerning the insolvency of a cryptoasset exchange incorporated in Singapore and a number of its subsidiaries. In establishing the group’s COMI, the Singaporean court was concerned with the practicalities of where the assets were held and administered using a hot wallet facility, as insolvency office holders would likewise need to be able to administer the assets.

³⁵ *Re Zipmex Pte Ltd and other matters* [2022] SGHC 196
https://www.elitigation.sg/gd/s/2022_SGHC_196.

5.7. In addition to specific points that we address in relation to constructive trust analyses conducted by courts, in the context of the timing question, a more general potential difficulty with the constructive trust analysis in the context of jurisdiction is that in the fraud context assets are often traded or transmitted onwards by the fraudster. If they end up in the hands of a bona fide purchaser for value without notice (Equity's darling) then there would be a complete defence to the claim, which may undercut the asserted basis for jurisdiction. The failure to raise this potential defence at a without notice hearing for interim relief was referred to by Trower J in *Piroozzadeh v Persons Unknown*.³⁶ Further, even without the need to make full and frank disclosure about potential defences available to the particular defendant before the Court, the claimant would need to show (to the relevant standard of proof, depending on the stage at which this issue arises) that any interim hands through which the cryptoassets passed before reaching the defendant were not hands of an innocent purchaser.

(2) What point in time is relevant for gateways 11 and 15(b)? Do these gateways require that a crypto-token is within England and Wales: at the time of proceedings, at the time of misappropriation, or some other time?

5.8. We agree with the Law Commission's view that the property gateway is intended to apply only to property within the jurisdiction at the time of the application for permission to serve out of the jurisdiction. If the relevant property was formerly, but is no longer in the jurisdiction, the underlying rationale for the gateway falls away. The *D'Aloia* approach – that the property was in the jurisdiction at the time of the misappropriation – is effectively looking at the point in time of the act of misappropriation as the relevant point, but that is more obviously catered for by gateway 15(a) (or the tort gateway, paragraph 9). We think the Law Commission is right that gateways 15(a) and (b) were intended to be disjunctive, and look to different points in time.

5.9. If *Denisov v Delvecchio*³⁷ is right, then gateway 15(b) is unlikely to be applicable in many misappropriation cases as a claimant is unlikely to be able to show that dissipated assets remain in England & Wales, unless resort is had to the fiction that *situs* is simply where the beneficial owner is (see above). But that feels illogical where the case involves a

³⁶ [2023] EWHC 1024 (Ch) at [28].
³⁷ [2022] EWHC 377 (Comm).

complaint that assets have been transferred away. It also sits oddly with the fact that the courts are also using notions of control elsewhere in the analysis, i.e., in *D'Aloia* in considering whether the cryptocurrency exchange was arguably subject to a constructive trust, Trower J's analysis looked at whether it had sufficient control over the relevant wallets.

- 5.10. If the better answer is that the property must be in the jurisdiction at the time of the application to serve out, a consequence is that the reliance on gateway 15 in *Jones* was probably wrong. In that case there was no discussion about which limb of gateway 15 applied, but since the Claimant would not have been able to establish that fraudulent acts by persons unknown were committed within the jurisdiction to satisfy 15(a), it can only be 15(b) – *Jones* being decided before 15(c) was introduced into the rules. Whether and on what basis it can be determined that English law applies so as to fall within gateway 15(c) is considered elsewhere in our responses.

(3) To what extent does the question of where a crypto-token is located for the purpose of jurisdiction raise issues in practice?

- 5.11. So far, the cases have largely³⁸ been one-sided in that the applicant for injunctive relief has only had to establish an applicable gateway to a good arguable case standard, and often more than one gateway is relied upon. As such, it has not been a prominent issue in the crypto-fraud cases but in other scenarios, such as those identified above, there is a risk that situs will have more direct consequences.

³⁸ A notable exception where the question of jurisdiction was subject to a contested hearing was *Tulip Trading Limited v Bitcoin Association for BSV* [2022] EWHC 667 (Ch).

Consultation Question 6

6. **In this question, we seek views and evidence on types of claims and causes of actions relied upon in applications to serve proceedings relating to crypto-tokens out of the jurisdiction.**

(1) To what extent can it be said that there is a serious issue to be tried where claimants allege that exchanges are constructive trustees in the circumstances pleaded in *Piroozzadeh v Persons Unknown* and comparable cases?

- 6.1. *Piroozzadeh*³⁹ concerned the discharge of an injunction on grounds that there had been a failure by the applicant at the without notice hearing to make a fair presentation, particularly of the defence of bona fide purchaser in circumstances where the cryptocurrency exchange's intended defence had been known to the applicant. While Trower J seriously doubted that there was a serious issue to be tried on this proprietary issue, he refused to determine the issue in light of his other conclusions and the fact that another exchange defendant had already listed a strike out application which would address the question of whether there was a serious issue to be tried.⁴⁰
- 6.2. The existence of a constructive trust as against cryptocurrency exchanges is obviously fact sensitive. Different cryptocurrency exchanges operate in different ways that can affect whether a constructive trust arises. In *Piroozzadeh* the relevant exchange was Binance. At the return date, Binance produced evidence which showed that, upon receipt of a cryptoasset, Binance would transfer the received assets into a 'pool' with the cryptoassets of other account-holders and then use those assets as its own. In exchange, users were then credited the amount of the value which they had deposited and which were swept into Binance's pool, with no segregated asset but a right to withdraw on request. Hence, Binance was in a similar position to a conventional bank. So cryptoassets were not held on an express or implied trust for Binance's users. If it was then in practice the only question is whether the Claimant can trace into the relevant Binance's user's rights against Binance as a beneficiary. If it was not, then the question of whether, nevertheless, cryptoassets of a third party victim of fraud were held on a constructive trust depended on

³⁹ [2023] EWHC 1024 (Ch).

⁴⁰ Ibid, [42]. As noted in response to question 4 above, the claimant in *Piroozzadeh* discontinued proceedings before that strike out application could be heard.

whether the Claimant could show that it could trace through all previous blockchain wallet addresses and so whether Binance received the Claimant's traceable assets in law or equity. Although not fully brought out in that judgment, the former requires that there be no mixing in any of those previous blockchain addresses, while the latter requires showing that the owners (or controllers) of those previous blockchain addresses were not themselves bona fide purchasers for value without notice. Even then, Binance would have a defence if it was itself a bona fide purchaser for value without notice – for instance, in that case, Binance had (prior to being notified of the Claimant's claim) paid away the allegedly traceable cryptoassets on the instructions of its user, and hence had given good consideration.

6.3. It should be noted that in other interim applications, courts have concluded that claimants have a good arguable case based on a constructive trust analysis.⁴¹ However, to make a similar point to the answer to question 4 above, because such cases have been interim *ex parte* applications, there has been limited argument and/or evidence from the exchanges as to their holding patterns for cryptoassets (and thereby the proper application of a constructive trust analysis). Further in a number of these cases, the cryptocurrency exchanges were joined not as constructive trustees but rather as respondents under the *Bankers Trust* and/or *Norwich Pharmacal* jurisdiction. *Piroozzadeh* was different in seeking to establish liability on the exchange for cryptoassets that had been paid away on the instructions of the account-holder before any proceedings had been notified to the exchange. *D'Aloia* is similar, and a trial in that case is listed for June 2024.

6.4. Further, as a matter of trust law, the question of when and whether a constructive trust arises in the context of theft or fraud is still “*a matter of some controversy*”.⁴² The central authority for the proposition that a thief or person who obtains property by fraud (in circumstances where the theft or fraud involved no breach of trust or other fiduciary duty) arose is *Westdeutsche Landesbank Girozentrale v Islington LBC*.⁴³ However, academic debate exists as to (among other things) (i) the nature of any right held on constructive trust by the defendant; (ii) whether, where the claimant is the victim of a theft, superior legal title remains with the victim; and (iii) whether, where the victim is defrauded under

⁴¹ *AA v Persons Unknown* [2020] EWHC 3556 (Comm) at [62]-[63], *Fetch.AI Limited v Persons Unknown* [2021] EWHC 2254 (Comm) at [15] and *Osbourne v Other Persons* [2023] EWHC 340 at [24]

⁴² *Lewin on Trusts* 20th ed (2020), para.8.029.

⁴³ [1996] AC 669.

a fraudulent misrepresentation, the legal transfer is unencumbered by any trust interest and would only arise at the point where the victim exercises their equitable right to rescind.⁴⁴

6.5. Amidst all of this uncertainty, in emerging asset classes and new technology, “*the common law is there is now one clear point that is now probably beyond argument in practice, which is that cryptocurrencies are property that can be the subject matter of a trust. A constructive trust analysis was applied in *Armstrong DLW GmbH v Winnington Networks Ltd* in relation to intangible European Union Allowances, although the nature of the title that the fraudster held was unclear, and described as “some form of *de facto legal title*”.*⁴⁵ As the Law Commission concluded in its *Digital Assets Final Report*, this matter is not unique to digital assets and, while inevitably there will be some interpretive difficulties *perfectly able to evolve in a logical and clear way where the facts at hand are described clearly and in full, and where legal principles are logically and consistently applied to distinct causes of action*”.⁴⁶

6.6. Subject to that caveat, the extent to which there is a serious issue to be tried where claimants allege cryptocurrency exchanges are constructive trustees in a similar way as in *Piroozzadeh* is contingent on a number of factors including the particular holding pattern and arrangement that an individual cryptocurrency exchange has implemented (which may be different from Binance) and the broader content of trust law (which is itself uncertain). That makes it impossible to give any generalised answer to this question.

(2) Is there any further practical evidence we could consider in relation to the ways in which exchanges defend or intend to defend applications and/or claims alleging they are constructive trustees at the return date of these applications?

6.7. As above, the result in *Piroozzadeh* was significantly affected by evidence produced on behalf of the Binance cryptocurrency exchange as to how the exchange itself operated and dealt with cryptoassets. Similarly, the question as to whether a constructive trust arose in *Ruscoe v Cryptopia*⁴⁷ and *Quoine Pte Ltd v B2C2 Ltd*⁴⁸ depended significantly on evidence

⁴⁴ There is a vast amount of literature on this but for the views of one author of this COMBAR response, see W Day and S Worthington, ‘Proprietary Restitution’ in W Day and S Worthington (eds), *Challenging Private Law: Lord Sumption on the Supreme Court* (Hart 2020).

⁴⁵ [2012] EWHC 10 (Ch) at [276].

⁴⁶ Law Commission, *Digital Assets: Final Report* (June 2023, Law Com No 412) para 9.42.

⁴⁷ [2020] NZHC 782.

⁴⁸ [2020] SCGA(I) 02.

by the relevant exchanges in those cases as to how they held cryptoassets (including the terms of contract with their users).

6.8. In practice, it is difficult for potential claimants and their legal advisors to anticipate how exchanges will defend applications or claims without *ex ante* information as to their operations and structure, because that information will dictate whether there could be a seriously arguable case that the exchange in question operated as a constructive trustee and/or what defences they might have. While Binance operates as a non-custodial holding intermediary, there may be other cryptocurrency exchanges who do have custodial intermediated holding arrangements (i.e., they hold cryptoassets received from account-holders on trust for those account-holders). For example, the New Zealand High Court held that on the facts (and particularly in light of the fact that the terms of use were replete with reference to “trust” in a technical trustee sense) Cryptopia held cryptoassets in its wallets on an express trust (actually, one trust for each type of cryptoasset) on behalf of the exchange’s account-holders.⁴⁹

(3) Are there similar problems with causes of action under any of the other gateways?

6.9. Other causes of action relied upon in applications to serve proceedings relating to crypto-tokens out of the jurisdiction include breach of confidence and unjust enrichment.⁵⁰ As noted in Law Commission’s *Digital Assets Final Report*, existing principles of unjust enrichment can be applied to disputes involving digital assets without conceptual difficulty.⁵¹ While there may be evidential challenges in establishing whether an enrichment was ‘at the claimant’s expense’ and/or questions of timing when establishing the value of digital objects, we agree that the existing common law principles of unjust enrichment are sufficient.

6.10. As to breach of confidence or misuse of private information, we note that the Law Commission has picked up on suggestions by academics that breach of confidence claims are inapposite in cryptoasset disputes.⁵² The criticism is that *Fetch.ai Ltd v*

⁴⁹ *Ruscoe v Cryptopia Ltd* [2020] NZHC 728.

⁵⁰ See, e.g., *Fetch.ai Ltd v Persons Unknown* [2021] EWHC 2254.

⁵¹ Law Commission, *Digital Assets: Final Report* (June 2023, Law Com No 412) para 9.56.

⁵² Law Commission, *Digital Assets and ETDs in Private International Law: Call for Evidence* (2024) para 5.132 citing A Held and M Lehmann, ‘Hacked Crypto-Accounts, the English Tort of Breach of Confidence, and Localising Financial Loss under Rome II’ (2021) 10 *Butterworths Journal of International Banking and Financial Law* 708.

Persons Unknown was wrong in law on the basis that, in a claim for breach of confidence, “the information must have been imparted in circumstances importing an obligation of confidence [...] It cannot be said that the Applicants imparted the confidential information to the *Persons Unknown* in circumstances importing an obligation of confidence; if anything, it was *Binance* who, having imparted the confidential information to the Applicants, might plausibly bring an action for breach of confidence.”

6.11. This seems like an oversimplification. As *Clerk and Lindsell on Torts* notes, “the use of the word “imparted”, however, is now clearly too limited for the modern action, it now being established there is no need for an initial confidential relationship”.⁵³ The editors go on to note that there are a wide range of circumstances which may give rise to an obligation of confidence, including where confidential information is obtained deliberately or accidentally, including where “confidential information comes to the knowledge of a person ... in circumstances where he has notice ... that the information is confidential, with the effect that he should be precluded from disclosing the information to others”.⁵⁴

6.12. Where the fraudster in *Fetch.ai* had come by the private keys clearly without the consent of the claimant, and it being obvious that the private key of a crypto wallet is confidential, it is difficult to see how the information was not imparted in circumstances importing an obligation of confidence. At the very least it is difficult to see how it was not seriously arguable and so a serious issue to be tried.

(4) Are these cases indicative of a need to consider more carefully the ‘serious issue to be tried’ limb of the three-stage test for service out of the jurisdiction?

6.13. We do not consider that there is any problem with the present application of the ‘serious issue to be tried’ limb of the three-stage test for service out of the jurisdiction. *Piroozzadeh* itself turned on an improper presentation of the case at the without notice hearing. It should also be recalled that many without notice applications never become public knowledge, especially those where the relief is refused (which is, in fact, what

⁵³ *Clerk and Lindsell on Torts* 24th ed (2023) para 25.06.

⁵⁴ *Ibid*, paras.25.12 and 25.16. Also *Attorney General v Guardian Newspapers Ltd* (No 2) [1990] 1 AC 109 (HL) at 281-282.

almost happened in *Piroozzadeh*). Further, while *ex tempore* judgments (and those written judgments given to date) are necessarily short, there is no suggestion in them that the Courts have not been careful when approaching the question of serious issue to be tried.

6.14. The test for a serious issue to be tried was recently considered in *Richards v Kulczyk* (a non-cryptoasset case) where it was emphasised that “[w]hile the court should grasp the nettle on points of law, where they are narrow short points of apparently settled law, a court is much less likely to consider it appropriate to reject a claim at an early stage when the arguments turn on novel, unsettled or developing areas of law”.⁵⁵ There is obviously a need for balance in this context. Cryptoasset claims should be properly scrutinised on a jurisdiction application, and those that are obviously bad in law should be dismissed at that stage, the Courts must also allow the substantive principles governing emerging assets like digital assets to be developed where possible at trial (if possible) rather than at a jurisdictional hearing. *Piroozzadeh* also demonstrates the need, in a novel, unsettled or developing area of law, for an applicant’s full and frank disclosure to be appropriately detailed, and so Courts may have significantly more material to consider at a without notice hearing than would be the case in a more settled area. We have no reason to consider that proper scrutiny is not happening; the absence of trial judgments in this area is primarily a result of nearly all claims to date being undefended (or being discontinued⁵⁶).

6.15. By way of example (only), HHJ Pelling KC in *Fetch.ai Ltd v Persons Unknown*⁵⁷ was careful to set out three categories of persons (“those who were involved in the fraud against whom it is appropriate to seek both heads of relief (subject to the points I am going to mention in a moment); secondly, a class designed to capture those who have received assets, I think, without having paid a full price for them, or something of that nature; and, third, and most importantly, those who fall within the category of innocent receivers”) and to qualify the scope of proprietary relief in respect of the third category of persons unknown, such that proprietary relief was available only to those who knew, or ought reasonably to have known that the assets belonged to the claimant and/or did not belong to them. There are other instances of where the Court,

⁵⁵ [2022] EWHC 863 (Ch) at [59].

⁵⁶ Which has now been the fate of *Tulip Trading Limited v Bitcoin Association for BSV*.

⁵⁷ [2021] EWHC 2254 (Comm).

even at a without notice hearing, has not been willing to grant what has been sought by the Claimant.⁵⁸

⁵⁸ E.g., *Boonyaem v Persons Unknown* [2023] EWHC 1380 (Comm).

Question 7.

7. In this question, we seek views on applicable law and decentralised finance (DeFi).

(1) Do you agree that contractual disputes in the context of DeFi are not likely to come before the courts?

7.1. No.

7.2. The Law Commission defines “defi” by reference to there being no “intermediary” (e.g., cryptocurrency exchange) between the two contracting parties, contracting through the defi code (para 7.16), where transactions are only recorded “on chain” (para 7.18). At para 7.16 the Law Commission states: “*our tentative view is that any contractual disputes that may arise in this context are not likely to come before the courts*”. At para 7.19, a distinction is drawn between smart contracts and smart legal contracts.

7.3. However, there may well be disputes over whether what on its face appears to be a ‘smart contract’ *simpliciter* is in fact a smart legal contract – e.g., a disgruntled ‘party’⁵⁹ may seek to argue that there is an intention to create legal relations evidenced by the code (as is recognised in paras 7.20-7.21).

7.4. The mere fact that performance risk is ameliorated by automatic execution does not remove the potential for dispute over the myriad of other fact patterns that give rise to disputes over contracts – including, alleged misdescriptions and mistake. There will clearly be questions of whether any alleged unintended consequences give rise to any cause of action (as in *Quoine v B2C2*) where such consequences lead to a loss being suffered by one of the parties. If so, that is likely to trigger disputes which may well come before the Courts. The potential for technical glitches cannot be ignored.

7.5. Moreover, the potential for contractual disputes can arise where one party argues that (for example) the code has not performed as expected. (This is acknowledged in para 7.24(1), but we wonder whether it is somewhat underplayed.) What is ‘expected’ may well turn on how the functionality of the code is described, and if it is described by an identifiable person who has not fully excluded their liability, disputes may arise that there is either a

⁵⁹ Using this term simply to describe a participant in the DeFi code, not a contractual party.

collateral contract with that person (especially if that person is, or is associated with, the guardians of the code) or for misrepresentation (as noted in para 7.27).

7.6. Over-collateralisation (referred to in para 7.24(2)) is unlikely to be any greater bulwark against contractual disputes ending up in court than in the secured or margin lending market. The fact that in a defi protocol the quantity of collateral required may well be assessed and valued purely objectively (rather than subjectively by a lending officer) cannot be assumed to mean that the lender necessarily has greater protection than in the ‘trad-fi’ market and hence that contractual disputes are less likely to arise.

7.7. The anonymity restraint on litigation cited in para 7.24(3) is also potentially overstated. As *Boonyaem v Persons Unknown*⁶⁰ shows, English courts can quite readily grant proprietary remedies against ‘persons unknown’; and as *Mooij v Persons Unknown*⁶¹ and *Persons Unknown v Wright*⁶² show, any supposed restraint on granting personal remedies against ‘persons unknown’ (as was held in *Boonyaem*) is probably unfounded, so long as jurisdiction can be asserted over them in the first place.

7.8. So far as jurisdiction is concerned, gateway 8 (applicable to negative declarations that no contract exists) may well be relied upon just as much as gateways 6 or 7. However the disgruntled party may even seek to impose liability on guardians⁶³ of the code itself, e.g., for the tort of procuring breach of contractual covered by gateway 8A.

7.9. However such jurisdictional issues raise problems over where the contract is made, broken and what its governing law is. (Note even a negative declaration that there is no contract under gateway 8 would have to show that the contract which is alleged to be binding fulfils gateway 6.)

⁶⁰ [2023] EWHC 1380 (Comm).

⁶¹ [2024] EWHC 814 (Comm).

⁶² [2023] EWHC 2292 (Ch).

⁶³ The term is used to attempt to be neutral between those who may (*pace Tulip Trading*) have fiduciary or other obligations to users of the code, and those who simply happen to have a certain influence over the code or its security.

(2) Do you agree that, as a result, these disputes will not be resolved with reference to private international law and the question of applicable law?

7.10. No. We think that there remains a potential for a significant number of disputes over whether smart legal contracts have been created, and that therefore questions of private international law and applicable law will be relevant.

(3) Would the law applicable to these kinds of disputes benefit from further clarification?

7.11. See our response to question 8. Where there is a smart legal contract then there necessarily must be identifiable contracting (human or corporate) parties, and so the application of the Rome I Regulation ought to be possible. Difficulties for conflict of laws that might arise were the law to recognise the code as a legal entity itself are, we suggest, better addressed when considering that (much more significant) development, which feeds into the question of responsibility for AI, and is therefore, we expect, beyond the scope of the Law Commission's present project.

Consultation Question 8

8. This question concerns the applicable law for non-consumer contracts.

(1) Can the provisions of the Rome I Regulation for identifying the applicable law for non-consumer contracts be applied to contracts involving crypto-tokens without undue difficulty?

(2) If the provisions cannot be applied, or can only be applied with significant difficulty, what are the possible solutions?

(3) If the provisions can be applied easily or without undue difficulty, are there any areas that would benefit from further clarification?

(4) To what extent is the application of these provisions problematic in practice?

(5) If the issue is prevalent in practice, what would be the consequences if it were not resolved adequately as a matter of law?

8.1. As we have observed above in relation to question 1, we anticipate that the provisions of the Rome I Regulation for identifying the applicable law for non-consumer contracts can be applied to contracts involving crypto-tokens without undue difficulty. Notwithstanding this general conclusion, we explore below some of the areas that are likely to cause some difficulty in practice.

8.2. At paras 7.9 and 7.10, the Law Commission highlights the fact that direct participants on the blockchain pose a particular problem for conflict of laws, but that this problem is less common in practice given that most people rely on intermediaries, such as cryptocurrency exchanges. Based on our experience, this is accurate. However, in particular in the context of multi-jurisdictional crypto-fraud it is likely that fraudsters will seek to avoid using intermediaries and resort to direct participation on the blockchain. We agree that the focus of the Law Commission should be upon the majority of participants who will have a contractual relationship with an intermediary.

8.3. We also agree with the Law Commission's conclusion at para 7.59 that the 'escape clause' in Article 4(3) is unlikely to be used for the types of contracts discussed in the call for evidence. However, we anticipate that some difficulty may arise in relation to the application of the 'catch-all' provisions in Article 4(4), i.e., in order to ascertain the law of the country with which the contract is most closely connected. This issue is likely to arise

in cases of multi-jurisdictional crypto-fraud where there is a contractual claim. In practice, the majority of these situations are likely to involve exchanges, which as the Law Commission pointed out are akin to ‘multilateral systems’. We agree with the Law Commission that when it comes to exchanges the choice of law governing the use of the platform may also apply to the trades on the platform. However, problems may arise when the trades occur in short sequence across multiple platforms that include different choice of law clauses in the terms and conditions and the fraudsters are located in unidentified jurisdictions. This is a problem that occurs in other contexts in today’s financial world but it is likely to be exacerbated in the crypto space given the volume of transfers that can take place and the anonymity of some parties involved.

- 8.4. One area may merit further clarification. Given that in the absence of choice the applicable law is likely to be that of the habitual residence of the party whose contractual performance least resembles ‘payment’, and most resembles the thing that is paid for, we anticipate that there may be instances where this habitual residence is unclear. As we observed above, it is not uncommon in the crypto-space for businesses to refuse to divulge the information that would assist in ascertaining their habitual residence. Moreover, there are instances when the contracts with such businesses do not make the identity of the contracting parties clear, further complicating matters. In practice, such contracts often include choice of law provisions, however, the issue is more than a theoretical possibility. Notwithstanding this, we are of the view that Courts are likely to be able to overcome these difficulties on a case by a case basis, including by granting disclosure orders at a preliminary stage. In any event, as the crypto-space becomes more regulated, it is hoped that the difficulty of ascertaining the domicile of crypto-businesses (in particular cryptoexchanges) will diminish.

Consultation Question 9

9. This question concerns the for consumer contracts.

(1) Can the provisions of the Rome I Regulation for identifying the applicable law for consumer contracts be applied to contracts involving crypto-tokens without undue difficulty?

(2) If the provisions cannot be applied, or can only be applied with significant difficulty, what are the possible solutions?

(3) If the provisions can be applied easily or without undue difficulty, are there any areas that would benefit from further clarification?

(4) To what extent is the application of these provisions problematic in practice?

(5) If the issue is prevalent in practice, what would be the consequences if it were not resolved adequately as a matter of law?

(6) We seek views on whether the provisions of the Rome I Regulation for identifying the applicable law for consumer contracts can be applied to contracts involving crypto-tokens without undue difficulty.

9.1. We anticipate that the provisions of the Rome I Regulation for identifying the applicable law for consumer contracts can be applied to contracts involving crypto-tokens without undue difficulty. As with the definition of consumer in the CJJA 1982, we find it unlikely that the definition of “consumer” in Article 6(1) of the Rome I Regulation is going to cause significant difficulties in relation to individuals entering into contracts with crypto-businesses, including by way of buying crypto-tokens. The same goes for the test for whether the crypto-business is “pursuing” or “directing” its activities to the country where the consumer has his habitual place of residence.

9.2. We agree with the Law Commission’s view that Article 6(4) of the Rome I Regulation is likely to cause most difficulty in practice, in particular the exception in Article 6(4)(d) on rights and obligations which constitute a financial instrument. We also agree with the Law Commission’s view at para 8.85 that a restrictive approach in which consumers are protected should be adopted. The issues surrounding the exceptions in Articles 6(4)(d) and (e) of the Rome I Regulation are discussed in further detail in our response to question 10 below.

9.3. We consider that even applying a narrow interpretation there is some residual uncertainty.

However, this residual uncertainty stems from the fact that it is not clear which crypto-tokens are “financial instruments” or “transferable securities”. This is likely to be problematic for practitioners, as a lot of time and resources is likely to be spent on considering whether a crypto-token is a transferable security. Given the active steps taken by regulators and other bodies in relation to the classification of crypto-tokens it is possible that by the time the Law Commission reaches the stage of legislative recommendations some of this uncertainty may be resolved. However, as discussed in our answer to question 10 below, some authors of this response are of the view that it may be preferable to repeal the exceptions in in Articles 6(4)(d) and (e) altogether.

Question 10

10. This question concerns the exclusions in Articles 6(4)(d) and (e) of the Rome I Regulation

(1) Do the exclusions of financial instruments and transferable securities, as set out in Articles 6(4)(d) and (e) of the Rome I Regulation, apply to crypto tokens?

(2) What would be the positives and negatives of interpreting those provisions in an international way, bearing in mind guidance from the European Securities and Markets Authority?

(3) Should the courts simply apply the Financial Services and Markets Act 2000 (Regulated Activities) Order 2001 in line with the Financial Conduct Authority guidance?

(4) To what extent do these exclusions cause problems in practice (now or in the future)?

(5) If these exclusions are problematic in practice, what would be the consequences if they were not addressed as a matter of law?

(6) What kind of reform is needed?

10.1. We do not answer each sub-category of this question separately or in the same order. The answer below is intended to provide a global view of the issues that have arisen and will continue to arise regarding the exclusions in Articles 6(4)(d) and (e) of the Rome I Regulation (the “**Exclusions**”).

10.2. In our view it is possible for crypto-tokens to fulfil the definitions of “financial instrument” and “transferable security” within the meaning of Article 6(4)(d) and (e) of the Rome I Regulation. However, that will depend on the particular features of the particular crypto token.

10.3. In practice, we have found application of the Exclusions extremely difficult (including in the context of cryptoassets) due to the lack of clarity in the terms used and the policy reasons underpinning the Exclusions. This arises in relation to many types of crypto token; among others, problems have arisen in particular when applying the definitions to certain stablecoins and certain kinds of staking activity.

10.4. We understand the policy reasons underpinning the Exclusions to be those set out in paras 8.58-8.59. Whilst there is a certain logic to those policy reasons, it appears to some authors that the differing treatment of a financial product from one territory to the next is inevitable where financial regulation is not harmonised and the Exclusions do not remedy that. The application of a country's regulatory laws and their territorial application is a matter for the individual state such that an issuer of a product may well fall outside their home state regulatory perimeter whilst falling within a host state's regulatory perimeter where they provide access to the product to (for example) consumers resident in the host state. That is not a matter for the Rome I Regulation, but for financial regulation and legislation.

10.5. Some authors of this response therefore struggle to see the practical utility of the Exclusions in achieving the policy reasons which underlie them.

10.6. The same authors further struggle to see why a consumer should be deprived of protections that would otherwise attach to a consumer contract based on the regulatory framework of a foreign jurisdiction. It is easy to see how entities seeking to make such products available in the UK would base themselves in a jurisdiction without much by way of protection for investors or consumers whilst also benefiting from the Exclusions.

10.7. Some authors are of the view that it is also unclear whether the economic concerns about the potential effects on capital markets expressed by the UK and the Commission at the time of the proposal of the Rome I Regulation justify the Exclusions given that "many contracts between consumers and financial exchanges will not fall within the Exclusions (see para 8.84). Indeed in the case of contracts falling outside the Exclusions, it is considered appropriate that the factors of the nature of the parties to the transaction and the place of the parties' habitual residence do have an impact on the selection of the applicable law. It is not clear whether transferable securities and/or financial instruments are so different in their nature and economic impact that consumers should be stripped of protections they would otherwise have under the Rome I Regulation.

10.8. Indeed, the provision of the protections for consumers under the Rome I Regulation in the context of cryptoasset financial products would have significant benefits for consumers where the risks of investing in those products are particularly high.

10.9. Additionally, in general we frequently struggle to apply the concept of “transferable security” in practice. First, the cross-referral to (what is now) MiFID II/the RAO is unhelpful and creates unnecessary complexity. Secondly, the concept of ‘transferability’ is unclear in the context of cryptoassets (e.g. whether transferability on an exchange or within a single network is sufficient). Definition by reference to terms such as “capital markets” is not of assistance in the context of a completely different industry.

10.10. One possibility favoured by some authors would be to repeal the Exclusions entirely and leave it to regulatory law and legislation to determine whether a particular product ought to fall within the UK’s regulatory perimeter (which is what occurs anyway with or without an applicable law clause in, for example, an exchange’s terms of service). This would simplify the applicable law regime and would provide consumers with protections that the FCA considers to be of vital importance in the cryptoasset industry. This would result in further divergence from the approach in the EU; however, as the Law Commission has noted, there is already not a uniform approach between the UK and EU positions.

10.11. Subject to the more general comments above, as regards interpreting the Exclusions in an ‘international way’, if it were possible to interpret these provisions in an international way then it would obviously increase certainty and establish a level playing field for consumer protection across the EU (or more widely). However, the key issue with doing so is a practical one. At this stage in the development of the financial regulation of cryptoassets, there is no uniform international approach allowing these provisions to be interpreted in an international, and we do not envisage there being a uniform understanding of how such assets should be defined or regulated for some time, if it happens at all. Whilst it would be beneficial for there to be a harmonised international approach, it seems to us that individual states such as the UK will first need to develop their own clear and comprehensive legal and regulatory frameworks for these assets before being in a position to negotiate any international co-operation on the matter.

10.12. On the other hand, some authors are concerned about the impact that repealing Exclusions could have on financial instruments. It appears to these authors that there are no principled reasons to make exceptions to the Exceptions solely for cryptoassets. UK Rome I would need to be amended so that the Exception are repealed altogether. While

there is a lot of force in the concerns above in relation to consumer protection, these authors are concerned that the repeal of the Exclusions is likely to mean that the rights and obligations in relation to a transferable product will depend on the consumer or non-consumer status of the parties and would depend arbitrarily on the domicile of the consumer investors. This may prove unworkable in the case of cryptoasset transferable products traded on international exchanges from multiple jurisdictions. The same authors are of the views that the uncertainty that would be created is likely to outweigh the consumer protection benefits.

Consultation Question 11

11. We seek views and evidence on localising damage arising in tortious claims relating to crypto-tokens for the purposes of applicable law.

(1) To what extent is it likely that claims in tort, such as those pleaded in the crypto-token litigation for the purposes of service out of the jurisdiction, will proceed to trial before the courts of England and Wales? Is it likely that the question of applicable law will be in dispute between the parties?

(2) If it becomes necessary for the courts of England and Wales to determine the question of applicable law, how could the courts approach the question of localising tortious damage in the broader digital asset and electronic trade documents context? Please indicate whether your response should be considered in the context of the CJEU jurisprudence or in the context of a potential common law approach.

11.1. As a preliminary point, we are concerned that the Law Commission underestimates how widespread applicable law arguments are in commercial cases before the Courts, and how potent they can be. We are also not clear as to the basis on which the Law Commission considers there to be “*an especially strong presumption that courts of England and Wales will apply the law of England and Wales to both the procedural and substantive matters in a dispute*” (para 6.11).

11.2. Further, *Mooij* shows that personal (not just proprietary) remedies against persons unknown are possible (see paragraph 7.7 above), and *Law* shows that the English court will (in a fraud case) be willing to require the transfer of non-traceable assets controlled by the persons unknown defendants to safekeeping, pending determination of the claim for such personal remedies (see paragraph 5.6 above).

11.3. As for procedural matters, it is a well-established *rule*, and not merely a presumption, that these are governed by the *lex fori* (see generally *Dicey, Morris & Collins* Ch 4) – instead, disputes generally centre around what is a matter of substance and what is a matter of procedure. As for substantive matters, we consider that the Law Commission’s description of there being a “*presumption*”, at para 6.11-6.12, (i) appears not to take account of Lord Leggatt’s judgment in *Brownlie v FS Cairo (Nile*

Plaza) LLC,⁶⁴ (ii) appears not to appreciate Lord Leggatt’s distinction between the default rule and the presumption of similarity, and (iii) is exaggerated as a matter of practice.⁶⁵ Both parties may decide as a matter of convenience not to plead and prove foreign law, in which case the law of England and Wales applies by way of the default rule – it appears that this is the point that the Law Commission may have had in mind at para 6.12. Once the applicable law is disputed between the parties and the default rule is therefore displaced, one party may wish to rely on the presumption of similarity in order to avoid going to the full expense of pleading and proving the content of foreign law. In that case, the court is duty-bound to consider whether “*in the circumstances is it reasonable to expect that the applicable foreign law is likely to be materially similar to English law on the matter in issue*”: *Brownlie* [126]. It is only if the answer to that question is ‘yes’ that the presumption will apply. If a party fails to prove its claim under the applicable law, including because on balance the presumption of similarity is not appropriate, “*the ordinary consequence must follow that... the claim is dismissed*”: [117].

11.4. The existence of specific guidance at paras H.3.1-H.3.7 of the *Commercial Court Guide* (revised 11th ed, July 2023) on foreign law evidence shows that applicable law disputes are frequently dealt with by the courts.

11.5. It is worth observing that even countries with historically similar legal systems to England and Wales may be less amenable to the application of the presumption as different jurisdictions develop different legal approaches to digital assets and emerging technologies at different rates. Moreover, whilst some jurisdictions are leaving the role of legal development to the courts, others are addressing these issues via legislation – indeed, the Law Commission itself has advocated a hybrid approach to legal development via the courts and via specific legislation to confirm the existence of a “*third category*” of personal property rights in its *Digital assets: Final report* and *Digital assets as personal property: Short consultation on draft clauses*. Courts have generally demonstrated a far greater resistance to applying the presumption where a party wishes to argue in favour of the similarity of English

⁶⁴ [2022] AC 995.

⁶⁵ See also *Granville Technology Group Ltd (in liquidation) v LG Display Co Ltd* [2024] 1 WLR 100, on the nature and application of the evidential presumption.

statute law by comparison with English common law.⁶⁶ Parties to commercial disputes may well seize upon those differences as they develop to make the most of whatever advantages they can identify by doing so.

11.6. As to how the courts could approach the question of localising damage in the broader context of digital assets, we make several observations. This response should be considered both in the context of the CJEU jurisprudence and as our view as to the most likely approach in England and Wales. We do not think it likely that the common law will depart radically from Rome II principles, nor do we see good reason for it to do so.

11.7. First, we consider that the courts should approach the question of localising damage in the digital asset and ETD context by incremental development of existing Art. 4(1) principles and case law. We do not see value in any of the more drastic solutions contained in Chapter 6 of the *Call for Evidence* – ranging from the “*bare proper law*” approach suggested at para 6.162 to wholesale abandonment of multilateralism at para 6.180. It is right to acknowledge that the conventional approach under Art. 4(1) may sometimes lead to imperfect results. However, we consider it less imperfect than the alternatives for identifying a real and close connection to the dispute, while retaining sufficient predictability as to outcome. Further, the incremental approach is sufficiently flexible to respond to the undoubted further evolutions of digital assets in future. We would also have concerns about the sustainability of adopting such fundamentally different approaches just for digital assets (even if that were to include ETDs) – as the Law Commission implies in its consideration of alternative approaches, some of the imperfections arising under Art.4(1) arise just as much in ordinary disputes as they do to disputes involving digital assets (and ETDs). Adopting a fundamentally different approach in the context of digital assets (and ETDs) could put pressure on the existing principles applied to other disputes. It could be dangerous to the certainty and predictability of commercial litigation to adopt a distinct approach for digital assets (and ETDs) without considering the potential adverse knock-on effects for commercial litigation more generally. Pending a multilateralist approach being adopted by a significant number of jurisdictions, the law of England and Wales

⁶⁶ *Brownlie v FS Cairo (Nile Plaza) LLC* [2022] AC 995 at [145].

must as a matter of practical necessity provide a framework for the resolution of disputes involving digital assets.

11.8. Second, we agree that where tortious damage in the digital asset context manifests as a physical object being damaged, it should be straightforward to localise the damage at the place where the object was located when the damage was sustained: para 9.27. We do not think it impossible that a case could arise where direct damage is to a physical object associated with a crypto-token (e.g., a USB key holding a private key) rather than the crypto-token itself,⁶⁷ so do not consider that the only type of damage one could get in a crypto-token case is ‘damage by deprivation’ (paras 9.27-9.28). However, we agree that these have been the most common type of case so far, and that these may well continue to constitute the majority going forward.

11.9. Third, we do not all agree that the damage to the digital asset constitutes pure economic loss (see paragraph 3.5 above).

11.10. Fourth, insofar as a digital asset case engages the *Kronhofer/Kolassa/Löber* case law, it will require the application of admittedly complex CJEU case law where it is difficult to identify a single coherent principle. For the avoidance of doubt, we are not certain whether it is accurate to describe this case law as confined only to instances of PEL (note *Dicey, Morris & Collins* para 35-026 cites some of these cases, among others, in connection both with financial transactions giving rise to pure economic loss and with instances of “*dealing in an intangible asset*”). Nor would we necessarily summarise the effect of that line of cases as “*clearly hold[ing] that localising pure economic loss, particularly in the investment context, entails a multifactorial approach, taking into account all the facts of the case*”: para 9.18. We also note that, beyond the reasoning in those cases being complex even where they apply directly, an additional complexity arises from transposing their principles from the jurisdiction context in which they were developed, to the applicable law context where rather different considerations may be at play (e.g., engaging multiple possible enforcement jurisdictions is less of a concern than engaging multiple applicable laws). We consider that the basis for, and practical implications of, transposing the

⁶⁷ One example might be cases where the damage is done to a physical object linked to a crypto-token.

Kronhofer/Kolassa/Löber jurisdiction case law to the applicable law context may warrant further reflection from the Law Commission.

11.11. Fifth, we consider that the problem goes beyond cases of pure economic loss, to any instance where the direct damage occurs in a virtual space. For that reason, it may be more helpful to conceptualise the above case law as concerned with dealing with both pure economic loss and with intangible assets. Those cases are instructive insofar as they indicate the types of connecting factor that might be relevant, for example the rationalisation of *Kolassa* in Case C-12/15 *Universal Music Industries*⁶⁸ that purely financial damage occurring directly in the applicant's bank account may be relevant where the circumstances do not make that fortuitous (c.f., *Universal Music* may have had the choice of several bank accounts from which to pay); or references to place(s) of registration or listing on a stock exchange (see, e.g., Case C-709/19 *Vereniging van Effectenbezitters v BP Plc*⁶⁹). The analogy between the latter and the ledgers on which cryptoassets are held is apparent. We agree that truly decentralised ledgers will pose particular problems, whereas centralised or private applications of DLT technology are unlikely to be problematic: para 3.142.

11.12. Sixth, we do not consider that the law (or laws) of the servers (or other hardware) on which digital assets are held is necessarily very helpful. There may be exceptional cases where, for example, an intermediary advertises that its servers will be located in a particular jurisdiction (or will not be located in a particular jurisdiction) and in those contexts then server location may be important. However, in a different context, Case C-523/10 *Wintersteiger AG v Products 4U Sondermaschinenbau GmbH*⁷⁰ pointed out that a connecting factor based on server location is uncertain and unforeseeable. Whether a digital asset is held on a truly decentralised ledger such that the relevant data is “sharded” as described at para 3.68-3.69, or whether it is hosted on servers all located in one country, we do not consider that the place of the server should be typically be relevant to identifying the governing law for a digital asset or any associated ledger/DAO. Insofar as one may ask what the proper law of the ledger/DAO is to determine the proper law of the tort concerning the digital asset, the

⁶⁸ [2016] QB 967 at [36-39].

⁶⁹ [2021] ILPr 23.

⁷⁰ [2013] Bus LR 150 at [36].

law of the ledger/DAO should similarly not turn on the location(s) of the servers presently hosting those systems.

11.13. Seventh, the jurisdictional context has seen the development of a ‘mosaic approach’ to omniterritorial torts such as defamation (see e.g. Case C-68/93 *Shevill v Presse Alliance SA*⁷¹). It may be appropriate to consider a similar doctrine in the context of digital assets. However, it would involve a degree of fragmentation and application of multiple laws in the same case, possibly creating overlapping regulatory burdens in respect of the same issue. We expect that the unitary nature of digital assets, and the types of damage that can be associated with them, *means* that a mosaic approach is unlikely to be appropriate at least in the vast majority of cases. However, insofar as a mosaic approach were to emerge in cases of virtual damage, we consider that identification of the countries whose laws comprise the ‘mosaic’ should only be based on genuine connecting factors, and not arbitrary ones such as location of the server.

11.14. Overall, we do not have a definitive solution to the problems raised by the Law Commission, in particular how best to identify a connecting factor linking a territorial system of law to damage to a purely virtual asset. Indeed, we query whether a definitive solution would be helpful in this context, in particular if it risked unduly restricting the law’s flexibility to adapt to fast-moving technologies. However, we consider that the Courts should continue to consider the circumstances of each case with a view to incremental development of the existing case law, drawing analogy where possible with similar areas, e.g., treatment of other financial registers, and of digital assets in the jurisdiction context.

11.15. We are extremely cautious about the suggestion at para 9.20 to seek consistency between rules for localising pure economic loss between jurisdiction and applicable law for the sake of consistency. While consistency ought to be considered as one factor when Courts are developing the law incrementally, that should not we consider be determinative.

⁷¹ [1995] 2 AC 18.

Consultation Question 12

12. We seek views and evidence on recourse to the “escape clause” in Article 4(3) of the Rome II Regulation.

(1) In what circumstances in the digital assets and electronic trade documents contexts would it be appropriate for the courts of England and Wales to have recourse to the escape clause on the basis of a pre-existing contractual relationship?

(2) To what extent would the parties in a tort claim involving digital assets and electronic trade documents have a pre-existing contractual relationship? Would these represent the vast majority of cases?

(3) If the parties to a tort claim do not have a pre-existing contractual relationship, when else would it be appropriate for the courts of England and Wales to have recourse to the escape clause? What factors should the courts consider when identifying the country “manifestly more closely connected” to the tort?

12.1. As an overarching point, we consider that it is not desirable to have a system that is reliant on an ‘escape clause’ to achieve justice the particular case. This is for similar reasons to those we have already given for our rejection of the “*bare proper law*” approach, above. Predictability and coherence are better served by developing how the general rule is to apply to digital assets such that they are typically governed by the law with the closest and most real connection to the dispute even absent special factors. Accordingly, whether the parties have a pre-existing relationship or not, it would only be appropriate to have recourse to the escape clause as the exception rather than the rule.

12.2. We do not agree that tort claims in respect of digital assets where there is a pre-existing contractual relationship would “*represent the vast majority of cases*”. The crypto-fraud cases are a case in point where tort claims are also relied upon.

12.3. As to when it would be appropriate to have regard to the escape clause where parties do have a pre-existing contractual relationship, the Law Commission is implicitly asking the extent to which there should be a rule as follows: ‘where there is (1) a contract and (2) the law of the contract is Country A, (3) is the tort manifestly more closely connected with Country A such that its law should also govern the tort?’. We

note that a pre-existing contractual relationship will not always mean that the most appropriate outcome is for the law of the tort to be the same as the law of the contract, in particular where the country whose law governs the contract is not “*manifestly closer*” than the law otherwise applicable to the tort under Art 4(1).

12.4. While the question falls to be addressed on a case-by-case basis, we are sceptical that the tort will always have a “*manifestly closer connection*” with the same country whose law governs the contract between the user and the host of a relevant online platform, particularly where the latter may be just as arbitrary in an online space (if not more so) than the former. With regard to para 9.43, the law chosen in an online host’s user agreement will often be selected for the host’s own ends, and buried in a document (or web of related documents) that the user will never read. It could de facto allow platform hosts to choose the law to which a non-contractual obligation is subject, giving rise to the concern identified at [47] of Case C-191/15 *Verein für Konsumenteninformation v Amazon EU Sarl*.⁷² We therefore do not consider that it would necessarily provide greater legal certainty for holders of digital assets, nor that it would necessarily be desirable, to default to the law governing the user agreement with the platform hosting the asset. The Courts should have recourse to the escape clause in the context of a pre-existing contract only where a case-specific analysis indicates a “*manifestly closer connection*” with the country whose law governs the contract.

12.5. Where the parties have no pre-existing contractual relationship, we agree that it will be an exceptional case in which the courts apply the escape clause. The possible list of relevant circumstances is not closed. Beyond that, we do not consider that it would be either useful or informative to enumerate the types of circumstances in which a court may conclude that another country’s law has a “*manifestly closer connection*” to the tort.

⁷² [2017] QB 252.

Consultation Question 19

19. We seek views on the law applicable to property disputes in relation to digital assets and ETDs. Where possible, we ask that stakeholders contextualise their responses, for example, give details as to whether it relates to a pledge over an ETD or property entitlements in crypto-token litigation.

(1) To what extent would recourse to contractual principles obviate the need for us to consider the lex situs rule?

(2) Do permissioned networks and/or cases where there is clearly a contractual or hierarchical relationship between the parties represent the vast majority of DLT applications for digital assets and ETDs?

(3) Should we need to consider a new conflict of laws regime for property rights in digital assets and ETDs, what approach should we take to any new regime and what broader objectives of the conflict of laws should we keep in mind? Stakeholders may wish to refer back to Chapter 6 from paragraph 6.103.

(4) To what extent would recourse to a distinct rule based on the connecting factor of the “owner” or “transferor” for cases where parties have voluntarily dealt with one another obviate the need for us to consider further the application of the lex situs rule to cases where the parties to the dispute are strangers?

(5) In what circumstances could a rule based on the “owner” or “transferor” be satisfactorily used? Do creditors taking security over ETDs typically require, as a matter of contract, that the debtor warrants their title to grant the security interest?

(6) To what extent is it 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”?

(7) How should courts approach the question of applicable law in such disputes relating to decentralised digital assets held in permissionless DLT networks where the parties have not dealt with one another and there has been an “involuntary dispossession”?

19.1. We are agreed that where the issues between parties can be characterised as ‘contractual’ in a broad sense (i.e., obligations voluntarily assumed by a party) then recourse to contractual conflict of laws principles would be desirable and helpful.

19.1.1. This would likely be of greatest assistance to lawyers in the transactional sphere, as the parties they work with will (or at least can) enter into contracts to regulate their dealings and usually will include choice of law clauses in their contracts. Going further, and making all conflict of laws issues as between the ‘original parties’ subject to express choice of law, as advocated by the UNIDROIT principles, may be welcomed by transactional lawyers, given the certainty this would bring to those entering into contracts.

19.1.2. This may also be beneficial to those in the insolvency field where disputes arise in relation to cryptoassets held by or claimed by a ‘contractual’ creditor, although in some circumstances a party asserting rights in an insolvency may not be in a pre-existing contractual relationship (for example, where it is alleged the cryptoassets have been misappropriated by the insolvent entity or bankrupt individual).

19.2. Contractual principles would be of less assistance in cases involving fraud (the vast majority of cases which have come to the Courts so far), as the defendants are generally in no pre-existing relationship with the claimants prior to the wrongdoing. In such cases, it would be necessary to have recourse to a general conflict of laws rule to determine underlying proprietary issues.

19.3. However, the majority of crypto-asset cases have so far involved a claim based upon a constructive trust arising from misappropriation, deceit, intimidation, breach of confidence, misuse of private information and/or unlawful means conspiracy. The law applicable to any trust in this situation (e.g., over rights against the exchange or wallet-provider obtained as a result of the initial wrong) should be the law governing the tort/equitable wrong: Rome II Article 15(a), (c) and (d). The situations where it would be necessary to consider the law applicable to any property rights ‘in’ the cryptoassets would therefore be limited.

19.4. In that residual category however, we are concerned that an attempt to create a rule based upon ‘situs’ could have significant drawbacks (and see our comments in response to question 5).

19.4.1. Insofar as it is said that a crypto-asset is neither a thing in possession nor a thing in action, then the existing rules cannot cater for them. As the Law Commission

appears to accept, the situs rule in relation to tangible things derives from the ability of a sovereign power to control entitlement to things within its territorial jurisdiction. The situs rule in relation to intangible things assumes that such things are things in action, and therefore derives from the law which creates the right of action (be it the law of the contract, the law of incorporation etc.), with a residual category of locating the thing at the place where the debtor or company is located. There appears to be (at least) high level agreement between legal systems on these principles.

19.4.2. However, if cryptoassets do not have any physical existence in the natural world (and are therefore not ‘situated’ anywhere) and nor does any person have a right ‘to’ anything represented by the cryptoasset (i.e., it is not a tokenisation of a real-world asset or chose in action), then these rules of situs cannot work. The creation of a new situs rule for cryptoassets would be entirely fictional and involve a potentially arbitrary choice of location.

19.4.3. This is a particular concern in relation to a rule which chooses the law of the ‘owner’ or ‘transferor’ or ‘relevant participant’ (referred to at para 12.113). This is the opposite approach to that taken in relation to debts, where the location of the debtor is the relevant factor. A choice of law which favours the law of the claimant’s ‘home forum’ (referred to in European law as the ‘forum’). This may be problematic at an international level (see paragraph 5.6.1 above).

19.4.4. In such circumstances, other legal systems may not only reach a different view as to the legal fiction chosen but may consider the choice of forum actoris taken by English law to offend mandatory rules or otherwise be contrary to public policy. This could impact the ability of parties to enforce judgments obtained in England in foreign courts.

Submitted to Law Commission Call for Evidence on digital assets and ETDs in private international law
Submitted on 2024-04-26 12:23:27

About you

What is your name?

Name:
Marina Comninos

What is your email address?

Email:
[REDACTED]

What is your telephone number?

Telephone number:
[REDACTED]

Questions on international jurisdiction - specific issues (Chapter 5)

Question 1: In this question, we seek views and evidence on jurisdiction over consumer contracts.

Please share your views and evidence below::

Question 2: In this question, we seek views and evidence on jurisdiction founded on the basis that a contract was concluded in England and Wales.

Please share your views and evidence below::

Question 3: In this question, we seek views and evidence on jurisdiction founded on the basis that damage or detriment was suffered in England and Wales.

Please share your views and evidence below::

Question 4: In this question, we seek views and evidence on jurisdiction founded on the basis that an unlawful act was committed in England and Wales.

Please share your views and jurisdiction::

Question 5: In this question, we seek views and evidence on jurisdiction founded on the basis that the claim relates to objects within England and Wales.

Please share your views and evidence below::

Question 6: In this question, we seek views and evidence on the types of claims and causes of action relied upon in applications to serve proceedings relating to crypto-tokens out of the jurisdiction.

Please share your views and evidence below::

Questions on applicable law - negotiable instruments, bills of lading, and the exclusions from the Rome Regulations (Chapter 10)

Question 13: We seek evidence, particularly from market participants, on how market practice in respect of bills of lading has been affected, or how it is likely to be affected, by the introduction of the Electronic Trade Documents Act 2023.

Please share your views and evidence below::

- Legislative change to recognise eBLs as the equivalent of their paper counterparts should enable 2 things which will greatly accelerate adoption of eBLs: (1) legal certainty; and (2) interoperability
- However, the ETDA is enabling legislation: it allows market participants to change their current practices. Once that is enabled, significant change management is required (processes at load ports need to change and agents onboarded, agreements with counterparties and carriers need to be adjusted, financing terms need to be amended, etc.). As such, markets are not going to react overnight to such a legislative change.
- As a result, multilateral contractual frameworks will not disappear overnight, but the legislative change is critical for broader market adoption.
- We have seen renewed interest in eBLs from market participants who consider that the legislation will (i) facilitate the use of eBLs as collateral, (ii) enable

platform interoperability, and (iii) in time, remove the need for complex multilateral contractual frameworks. There is still some uncertainty around reliability and the need for broader international adoption of MLETR inspired legislation, but with targeted utilisation this will be overcome.

Question 14: We seek evidence on market sentiment relating to use of DLT platforms for electronic bills of lading.

Please share your views and evidence below::

(1) Is it likely that market participants will move towards a wholly decentralised DLT platform for bills of lading?

IDT Response: save for wholly permissionless decentralised systems, which are very unlikely to ever happen, all other options are open - central registries will continue to be part of the eBL ecosystem post ETDA, as will permissioned decentralised, and hybrid where part of the solution is on blockchain and part in a central registry. In the case of interoperable eBLs, they could move from a central registry system to a decentralised DLT platform and back to central.

(2) To what extent can we assume that market participants will be reluctant to join a DLT platform that does not at least offer a user agreement setting out the terms on which the DLT platform will operate, and the rights and obligations of all users of the platform?

IDT Response: in our view, access to eBL solutions, whether DLT or central registry or anything else that may come up over time, will always have bilateral terms and conditions of use, governing the relationship between the solution provider and the user. This is standard for all software solutions and will set out the obligations of the provider as to security, uptime, confidentiality, liability limits, etc. However, complex multilateral contracts which bind all users of the platform to each other and require broad industry consent will not, in our view, be required once eBL legislation becomes the norm for regulating eBL validity.

(3) Other than wholly decentralised DLT platforms, how else might DLT be used to issue and transact with electronic bills of lading (under the 2023 Act or otherwise)?

IDT Response: there are a number of different ways DLT can form part of a solution provider's technology stack - for example, the title/holdership log can be on DLT. Interoperability is another place where DLT can be useful: when eBLs are transferred from one platform to another, DLT could be used as an independent central ledger, which can serve as a golden record across platforms to identify the platform which hosts the original ETR at point in time.

Question 15: We seek evidence on the difficulties, if any, of incorporating the Hague-Visby Rules where an electronic bill of lading has been used.

Please share your views and evidence below::

(1) How often do disputes arise as to incorporation of the Hague-Visby Rules, specifically because an electronic bill of lading has been used, and how likely are they to in future?

IDT Response: in our experience, in the 14 years we have been providing an operational eBL solution, this has never been escalated to us as a concern. We have also never been advised of any dispute relating to this issue.

(2) Are there concerns in the market, both in the marine insurance and shipping sectors, regarding the incorporation of the Hague-Visby Rules in electronic bills of lading? Please provide detailed examples in your answer and, where possible, distinguish between electronic bills under the Electronic Trade Documents Act 2023 and electronic bills held within contractual "approved systems."

IDT Response: none have ever been expressed to us. All our eBL templates, both those that are subject to the terms of our multilateral contract and those that are governed by the ETDA/Singapore ETA, include an express Hague/HVR incorporation clause on the back of the bill - exactly as they do in paper.

Question 16: We seek evidence on market practice to help us identify where it could be said that an electronic bill of lading is "issued" for the purpose of the Hague-Visby Rules, as implemented in the UK by the Carriage of Goods Act 1971

Please share your views and evidence below::

(1) How, in practical terms, does a carrier wishing to issue an electronic or tokenised bill of lading do so within the respective electronic "approved" system or DLT system? What steps must a carrier take within the system?

IDT Response: a master will sign the eBL directly by logging into the solution and clicking 'Sign & Issue', or will appoint an agent to sign and issue on his behalf - other than the fact that the signature which is applied to the eBL is electronic rather than a manual 'wet' signature, the process is no different to that adopted in paper (the master either directly signs a paper BL on board the vessel before the vessel departs or instructs the agent to do so on his behalf).

There is an additional possibility facilitated through the use of digital solutions, which is for vessel management companies to sign on behalf of the vessel. This is already prevalent in paper bills of lading in the container industry, where the line arranges for all paper BLs to be signed/issued centrally and distributed. The process will be replicated for eBLs and can now also be done for bulk eBLs if the management company prefers to maintain control of the signing/issuing of eBLs.

(2) How, in practical terms, does a shipper "receive" an electronic or tokenised bill of lading within an "approved" system or DLT system? What steps must a shipper take within the system?

IDT Response: on issuance, the eBL appears in the shipper's inbox, along with the ability to exercise control over the eBL (i.e. by having the function to endorse, transfer, surrender, etc.). The eBL looks identical to paper, with a front and back, and a shipper can check that the eBL meets the requirements of the Documentary Instructions. If the eBL and related supporting documents are in order, the shipper can endorse (blank or to order) and transfer to its buyer/bank.

(3) Does the issue of an electronic or tokenised bill of lading between carrier and shipper involve the platform provider, or do the systems allow for electronic or tokenised bills to be sent directly from carrier to shipper?

IDT Response: no, the platform is not involved - it is a direct 'message' between the carrier and the shipper. Imagine the platform as the courier service, just a very fast one...

(4) What are the market standards or best practices relating to existing electronic or DLT systems on the “issue” of a bill of lading?
IDT Response: place of issue is identified in the bill by the agent, just like they do in paper - and has never to our knowledge been disputed.

Questions on applicable law - section 72 of the Bills of Exchange Act 1882 (Chapter 11)

Question 17: We seek views on the most appropriate connecting factor for determining where an electronic bill of exchange is “delivered to a first holder” for the purposes of section 72(1) of the Bills of Exchange Act 1882.

Please share your views and evidence below::

Question 18: We seek views on whether it would be desirable to have a single conflict of laws regime to cover all types of electronic trade documents that fall within the scope of the Electronic Trade Documents Act 2023.

Please share your views and evidence below::

While this area is outside the scope of our expertise, we would like to comment on the suggestion that the ‘reliable system’ may be ‘a’ or ‘the’ connecting factor: while it may be a connecting factor for an eBL dispute which relates to the reliability of the system, for the vast majority of disputes relating to shortage, cargo damage, freight, rights to possess the cargo, it will be completely irrelevant. In those circumstances, the parties in dispute will be brought to the jurisdiction of the registry or the registry’s servers, which has no connection whatsoever to the matters in dispute or the identity or location of the parties to the dispute. It does not appear that this will assist in identifying a system of law and a jurisdiction that is the most appropriate to hear and resolve the dispute, taking into account the transaction between the parties. Our solution to the PIL issue, at least at this nascent stage of use of eBLs which are governed by ETDA/ETA, is to commit to our users that we will ensure that any such eBLs issued on our platform will have a English or Singapore law governing law clause on the face of the bill.

Question on applicable law - property (Chapter 12)

Question 19: We seek views on the law applicable to property disputes in relation to digital assets and ETDs. Where possible, we ask that stakeholders contextualise their responses, for example, give details as to whether it relates to a pledge over an ETD or property entitlements in crypto-token litigation.

Please share your views and evidence below::

D2 Legal Technology Response

Law Commission Call for Evidence on “Digital assets and Electronic Trade Documents in private international law: which court, which law?”

Introduction

This paper sets out the views of D2 Legal Technology (“**D2LT**”) on the Law Commission’s Call for Evidence titled the “Digital assets and Electronic Trade Documents in private international law: which court, which law?” published on 22 February 2024 (the “**Consultation**”).

D2LT is a legal data and change consulting firm, sitting at the intersection of FinTech and LegalTech. With offices in London, Frankfurt, New York, Charlotte, Singapore, Hong Kong and Sydney, it provides inter alia, strategic advice and implementation services to c. twelve leading investment banks and various other financial firms on the digitisation of legal agreements and opinions. This has assisted its clients in the areas of resource management (such as capital, liquidity and collateral), regulatory reporting and compliance (such as qualified financial contract reporting (often colloquially known as “living wills reporting”), client assets and money compliance and ECB close-out netting reporting) and operational management.

D2LT’s work has included leading legal data and agreement digitalisation programmes for major trade associations in the capital markets industry, such as the International Swap and Derivatives Association (ISDA), International Capital Markets Association (ICMA) and the International Securities Lending Association (ISLA). This has included creating for these clients, an industry Clause Taxonomy and Library for their published master agreement documentation, which is regarded as an important stepping-stone and legal agreement data standard to facilitate the use of smart contracts in the OTC derivatives, repo and securities lending industries respectively. As part of its engagements at major investment banks to set up and provide expertise to LegalTech and Legal Innovation teams, it has been involved in a number of projects and consultations related to smart contracts and digital assets in recent years (including in relation to the operational infrastructure required). It has been instructed by regulators to advise on digital asset regulation, infrastructure and supervision, and has supported a number of digital asset vendors and service providers operating in the finance, crypto-token and blockchain ecosystems.

Its responses have been mainly provided by:

Akber Datoo – Founder and CEO of D2LT. Akber is a computer science graduate, having worked in the early part of his career as an IT developer at UBS. After leading a number of industry initiatives (e.g. FpML – a markup language for communicating the terms of transactions between the derivatives industry) and developing various trade platform and pricing applications, Akber grew frustrated with his in-house team and a growing gap between the legal function and the use of technology and systems in the management of financial instruments (that ultimately simply consist of contractual obligations). He re-

qualified as a solicitor (of England and Wales) and trained and practiced as a derivatives lawyer at Allen & Overy LLP. In 2011, he founded D2LT, utilising his dual-skill set as both technologist and lawyer. Akber is the chair of the Law Society's subcommittee of Smart Contracts and Digital Assets, as well as an appointed member of its Technology and Law Committee. As well as being a P.R.I.M.E. Finance Expert, he is a visiting professor at the University of Surrey and teaches undergraduate and master's students on topics such as legal data, distributed ledger technologies, smart contracts and artificial intelligence as part of the Law and Technology module. He has published a leading practitioner text published by Wiley, "Legal Data for Banking".

Claire Gerrand – Consultant at D2LT. Since graduating from the University of Oxford with a law degree, she has worked on a variety of projects at D2LT relating to legal technology and contract negotiation and has led training and consultation responses on digital asset regulation in foreign jurisdictions, utilising her background in international law and a special interest in the operation of legal technology within financial services.

Jeffrey Golden KC (Hon) – Senior Adviser to D2LT. Jeffrey is the founder and chair emeritus of the P.R.I.M.E. Finance Foundation in the Hague and one of its leading experts. He is currently joint head of chambers at 3 Hare Court, having retired from international law firm Allen & Overy LLP which he joined as a partner in 1994 and was a founding partner of its US Law practice. Jeffrey acted extensively for ISDA and principal author of its master agreements, also acting as an arbitrator and expert witness in several high-profile derivatives cases. He is the general editor of the Capital Markets Law Journal (Oxford University Press) and his most recent book (co-edited with Carolyn Lamm) "International Financial Disputes: Arbitration and Mediation" is also published by Oxford University Press.

Emma Wooldridge – Consultant at D2LT. Emma has experience in capital markets trading documentation across a number of client projects, such as development of legal agreement databases, negotiating trading documentation, document review exercises, and assisting with the linkage between trade confirmations and their related master trading agreements and collateral arrangements. She was involved in the team which drafted the Network Access Rules for the BSV Blockchain.

We welcomed the opportunity to respond to the Law Commission's Call for Evidence in 2021 and the Consultation Paper in 2022 on the topic of digital assets, and we commend the tremendous effort that has clearly gone into producing the related Final Report in 2023, which we believe is already serving to promote legal certainty in this industry and has greatly assisted market participants in observing the desire and efforts of the judicial system of England and Wales to support the digital assets industry. We are looking forward to receiving the Law Commission's work arising out of the call for evidence on Decentralised Autonomous Organisations and to continuing to engage with the Law Commission in this vital area, to support the growing digital agenda and to support the progress to date, and we welcome any further discussion on these matters.

Consultation Questions

Question 1. In this question, we seek views and evidence on jurisdiction over consumer contracts.

- (1) To what extent can the issue of jurisdiction over consumer contracts in the digital and decentralised contexts be accommodated by section 15B of the Civil Jurisdiction and Judgments Act 1982?
- (2) Does the fact that the business is a crypto-business, as opposed to any other business, change the analysis of whether a business has directed its services to consumers located in the UK?
- (3) Are there any changes or clarifications that are needed in respect of the issue of jurisdiction over consumer contracts?
- (4) To what extent does this issue cause problems in practice (or is likely to in future)?

We consider that the issue of jurisdiction over consumer contracts in digital and decentralized contexts can be accommodated by Section 15B of the Act, in the same manner as other contracts between consumers and overseas businesses. We expect that in the majority of cases, the availability of evidence of online advertising from crypto-businesses (such as exchanges or custodians) will be the conclusive factor in determining if a crypto-business has “directed activities” in the UK.

There are practical challenges in applying the “directed activities” analysis to crypto-businesses. Certain types of crypto-businesses (e.g. DeFi platforms) may not be able to control or be aware of the location of the consumers which they are contracting with. It would be helpful if guidance was provided concerning the non-exhaustive factors to be considered by the courts in determining this issue that are specific to crypto-businesses.

Question 2. In this question, we seek views and evidence on jurisdiction founded on the basis that a contract was concluded in England and Wales.

- (1) How should the courts apply gateway 6(a) to a smart contract? Should the relevant connecting factor be the participating computer, or the real-world actor?
- (2) If gateway 6(a) should use a connecting factor based on the real-world actor, how should their location be determined? Should it be by their habitual residence, their domicile, or at the place where they happen to be at the time the contract was formed?
- (3) Has the question of where a smart contract is made arisen in legal and commercial practice? If so, please provide details.
- (4) To what extent is it likely that the question of where a smart contract is made will become prevalent in practice?

The connecting factor for gateway 6(a) should be the real-world actor who is a party to the contract. Gateway 6(a) relies on the location of the receipt of the offer or the effecting of acceptance, and is not necessarily the actual location at any time of any party. It is unlikely that the question of jurisdiction of a smart contract being made will arise where the connecting factor is deemed to be the location of the real-world actor, as a smart contracts should not be treated differently in respect of the gateway from any other type of contract that is binding on a real-world actor, solely because of its digital mechanism of offer and acceptance. An emphasis on the importance of the computer’s location can be problematic

because the distributed nature of DLT means that nodes are located globally and therefore can be manipulated or difficult to predict.

We are not aware of caselaw concerning smart contracts on this point. Guidance notes from the European Commission on Directive 2011/83/EU (“**CRD**”) covering consumer contracts acknowledged that a “consensus definition of ‘smart contracts’ is yet to be reached” but clarified “the application of the CRD does not depend on the technology used by a trader. It is irrelevant if a consumer concludes a ‘normal’ distance contract over the internet or uses blockchain execution technology”¹. The factors applicable to other types of commercial contracts concluded at a distance should apply in respect of smart contracts, although it is possible that this will be challenged in due course.

The Law Commission noted that “it is relatively rare for those contracting through DLT to make a choice of law... contractual parties would be well advised to choose a law”. By their nature, the standard contractual terms of a smart contract are not typically negotiated by the parties to it. If an encoded choice-of-law election in a smart contract is automatically English law, then it may fall foul of Article 3(1) Rome I which requires evidence that the parties actually had the will to choose the applicable law. Notwithstanding this, we have seen a growing use of oracles and multisig functionality that addresses this (especially in the case of private blockchains, rather than public distributed ledgers). There has also been developments in the formal rules or terms and conditions of blockchain protocol ledgers which provide for a choice of arbitration². By signing up to a protocol or network of this type, parties can sign up to these rules and associated governing law without needing to know, at the time of adherence, the identity of the other parties, who are also bound by them³.

Question 3. In this question, we seek views and evidence on jurisdiction founded on the basis that damage or detriment was suffered in England and Wales.

- (1) Do you consider the approach of the courts of England and Wales so far in the crypto litigation when localising damage or detriment for the purposes of jurisdiction to be theoretically sound?
- (2) To what extent can it be said that the tortious damage pleaded in the crypto-token litigation are not cases of pure economic loss? How else could tortious damage in the crypto-token context be conceptualised?
- (3) If the crypto-token cases are cases of pure economic loss, to what extent would it be desirable that a consistent approach is taken in England and Wales to localising pure economic loss as between jurisdiction and applicable law?

¹ Commission, E., 29 December 2021. Commission notice – Guidance on the interpretation and application of Directive 2011/83/EU of the European Parliament and of the Council on consumer rights (Volume 64, 2021/C525/01). [Online] Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:C:2021:525:FULL>

² E.g. the Network Access Rules between the BSV Association and the nodes on BSV [<https://nar.bsvblockchain.org/>]

³ This has been fundamental to the rollout of various commercial association bodies e.g. ISDA Protocols. Dato, A. & Golden, J., June 2021. “Sailing into the rules of smart contracts...”. Butterworths Journal of International Banking and Financial Law, p. 387. Available at: https://www.3sharecourt.com/wp-content/uploads/2021/08/Articles.JIBFL_Satanita.June_2021.pdf

We consider the approach to localising damage or detriment has been relatively consistent in pointing to a “location” of a claimant’s tokens at the time of the tort (either conceptualised as on-their-person, under their control or at their home/business) and has been adaptable to new issues facing the courts, in the interest of protecting consumers and victims of fraud. The majority of cases (except *Lubin*) have dealt primarily with identifiable connecting factors in England only. Differences in the approach of these judgements are likely to become apparent as more complicated cases arise, where we suspect that the simplest test to apply will be the domicile or residence of the claimant who has sustained damage.

Question 5. In this question, we seek views and evidence on jurisdiction founded on the basis that the claim relates to objects within England and Wales.

- (1) To what extent is the approach so far of the courts of England and Wales in localising a crypto-token for the purposes of jurisdiction theoretically sound? What would be the relative merits and demerits of any alternatives?
- (2) What point in time is relevant for gateways 11 and 15(b)? Do these gateways require that a crypto-token is within England and Wales: at the time of proceedings, at the time of misappropriation, or some other time?
- (3) To what extent does the question of where a crypto-token is located for the purpose of jurisdiction raise issues in practice?

We consider that the approach thus far has been theoretically sound while being adaptable to the specific novel facts of the cases. The point in time for 11 and 15(b) should be the time of misappropriation. Determining the “location” of a specific crypto-token is inevitably difficult, for reasons noted above in relation to the “on-the-chain” location.

For the majority of cases, the location of a crypto-token should be determined by reference to the location of its owner, by either pointing to their residence or the place where the owner was when the damage was sustained. If a crypto-token is controlled by a custodian or exchange on behalf of its beneficial owner, the relevant location of the third party service provider should be used. However, there may be advantages in recognising limited circumstances where the crypto-token can be traced to the location of the relevant computer/server that is, for example, controlled or owned by a party to the contract, if the location of the computer/server was a consideration for a party when accepting the contract (e.g. certain crypto-token custody services use the security of their server location as a selling point⁴) or if the centralised nature of the token (e.g. central bank digital currencies) means that the record of ownership was always recorded on computers/severs within a specific jurisdiction. If English law gave greater deference to this factor (for those limited types of crypto-tokens where a location can be identified) where it reflects the party’s intentions, it could provide a commercial incentive to conduct crypto-custody or web-hosting businesses within the jurisdiction, and give the courts an additional factor to rely upon when determining jurisdiction, in line with traditional analysis of jurisdiction. In a fully decentralised network, on the other hand, the “location” of the crypto-token is not discernible and other connecting factors such as the place of the person who owns and/or controls (i.e. the person who in fact exercises control over e.g. by effecting a transfer) the token, is more useful.

⁴ E.g. Beeks Financial Cloud Group plc, Cryptocurrency Hosting Provider.
<https://beeksgroup.com/services/low-latency-network/data-centres/sgx-singapore-sgx/>

Question 7. In this question, we seek views on applicable law and decentralised finance (DeFi).

- (1) Do you agree that contractual disputes in the context of DeFi are not likely to come before the courts?
- (2) Do you agree that, as a result, these disputes will not be resolved with reference to private international law and the question of applicable law?
- (3) Would the law applicable to these kinds of disputes benefit from further clarification?

We agree that contractual disputes in the context of DeFi are less likely to come before the courts and be resolved with reference to private international law and the question of applicable law, in comparison to contractual disputes where there is an intermediary (e.g. centralised exchanges) or the equivalent financial market transaction/instrument types, for the reasons set out by the Law Commission.

In addition to these reasons, DeFi platforms are increasingly making use of dispute resolution rules requiring arbitration proceedings and referring to technical experts. For example, when designating an arbitrator in a dispute arising under the BSV Association Blockchain rules⁵, the parties are invited to appoint an arbitrator from the specialised panels formed by the P.R.I.M.E. Finance Panel of Experts to deal with particular categories of blockchain or digital assets-related cases. The BSV network has also developed software allowing miners to freeze tokens in order to return them to their rightful owner, if required (according to the view of the miners themselves) by a court order. The scope and ambition of these types of protocol rules are increasing, with the UKJT Digital Dispute Resolution Rules⁶ taking innovative steps to increase the speed of resolution, allow for optional anonymity and provide for the tribunal to have the power to “operate, modify, sign or cancel any digital asset relevant to the dispute”.

While arbitration can reduce the burden on the court’s time, it can disadvantage consumers and removes the publicity function of court proceedings⁷, thereby slowing the development of judicial precedent in relation to DeFi contractual disputes, which is already hampered by the tendency for disputes over DeFi transactions to arise where there was no clearly-identifiable contractual agreement. In the absence of clear precedent or statutory rules, contractual disputes will inevitably arise in due course.

However, new developments in the DeFi markets may increase the likelihood of disputes. First, the perception that the courts lack the necessary technical expertise may shift if the government takes steps to carry out the recommendations from the Law Commission to, among others, create a panel of industry-specific experts to support the judiciary and enact the ‘Property (Digital Assets etc) Bill’. Second, parties have previously been less likely to pursue litigation against ‘persons unknown’ because of the uncertainty of achieving any

⁵ The Network Access Rules between the BSV Association and the nodes on BSV [<https://nar.bsvblockchain.org/>].

⁶ UK Jurisdiction Taskforce, 2021. Digital Dispute Resolution Rules. [Online] Available at: https://27221500.fs1.hubspotusercontent-eu1.net/hubfs/27221500/UKJT%20work/Digital%20Dispute%20resolution%20rules.pdf?_hstc=251652889.8c845dcc6a0ab1054b7f909d9059ebf4.1716307562944.1716307562944.1716307562944.1&_hssc=251652889.2.1716546001530&_hsfp=260

⁷ Soleymani v Nifty Gateway LLC [2022] EWCA Civ 1297 (2022).

meaningful recovery against the costs of disclosure and freezing orders. As more DeFi platforms or protocols require acceptance of participation terms and conditions, and offer front-end platforms to interact with the protocol, it is more likely that claimants will have a named person or platform to seek recovery from. Third, despite these two existing barriers to contractual disputes, the courts have in recent years demonstrated a willingness to flexibly apply existing rules to achieve outcomes for claimants, by finding that the courts have jurisdiction over a dispute, and by granting injunctions, disclosure and ordering DeFi platforms “to take all necessary steps” (including exploiting a vulnerability in their own platforms⁸) to return crypto-tokens to claimants. It appears unlikely that an England and Wales court will find that it does not have jurisdiction over a particular dispute in the context of DeFi (unless there is no single connecting factor, acknowledging those tenuous cases are unlikely to appear before the courts), and DeFi companies that might have otherwise (in an equivalent traditional financial market) sought to exclude the jurisdiction of English courts, cannot rely on their overseas incorporation or lack of physical location.

Question 8. This question concerns the applicable law for non-consumer contracts.

- (1) Can the provisions of the Rome I Regulation for identifying the applicable law for non-consumer contracts be applied to contracts involving crypto-tokens without undue difficulty?
- (2) If the provisions cannot be applied, or can only be applied with significant difficulty, what are the possible solutions?
- (3) If the provisions can be applied easily or without undue difficulty, are there any areas that would benefit from further clarification?
- (4) To what extent is the application of these provisions problematic in practice?
- (5) If the issue is prevalent in practice, what would be the consequences if it were not resolved adequately as a matter of law?

Question 9. This question concerns the applicable law for consumer contracts.

- (1) Can the provisions of the Rome I Regulation for identifying the applicable law for consumer contracts be applied to contracts involving crypto-tokens without undue difficulty?
- (2) If the provisions cannot be applied, or can only be applied with significant difficulty, what are the possible solutions?
- (3) If the provisions can be applied easily or without undue difficulty, are there any areas that would benefit from further clarification?
- (4) To what extent is the application of these provisions problematic in practice?
- (5) If the issue is prevalent in practice, what would be the consequences if it were not resolved adequately as a matter of law?
- (6) We seek views on whether the provisions of the Rome I Regulation for identifying the applicable law for consumer contracts can be applied to contracts involving crypto-tokens without undue difficulty.

⁸ E.g. by ordering Oasis, a platform for decentralized finance, “to take all necessary steps that would result in the retrieval of certain assets involved with the wallet address associated with the Wormhole Exploit”. [<https://blog.oasis.app/statement-regarding-the-transactions-from-the-oasis-multisig-on-21st-feb-2023/>].

Question 10. This question concerns the exclusions in Articles 6(4)(d) and (e) of the Rome I Regulation.

- (1) Do the exclusions of financial instruments and transferable securities, as set out in Articles 6(4)(d) and (e) of the Rome I Regulation, apply to crypto-tokens?
- (2) What would be the positives and negatives of interpreting these provisions in an international way, bearing in mind guidance from the European Securities and Markets Authority?
- (3) Should the courts simply apply the Financial Services and Markets Act 2000 (Regulated Activities) Order 2001 in line with Financial Conduct Authority guidance?
- (4) To what extent do these exclusions cause problems in practice (now or in the future)?
- (5) If these exclusions are problematic in practice, what would be the consequences if they were not addressed as a matter of law?
- (6) What kind of reform is needed?

In the majority of cases, the provisions of the Rome I Regulation for identifying the applicable law for consumer contracts over crypto-tokens without significant difficulty. As noted by the Law Commission, where a consumer contracts with a trader who has directed activities to the UK, Article 6 of the Rome I Regulation offers important protections over the consumer contracts, however Articles 6(4)(d), 6(4)(e) and Article 4(1)(h) exclude from these protections contracts over the “rights and obligations” of financial instruments and transferable securities, including those concluded within a multilateral system. The definition of ‘specified investments’ under the RAO is broader than the definition of ‘financial instruments’ under MiFID II, therefore a crypto-token can be a ‘specified investment’ under the RAO, but not a ‘financial instrument’ under MiFID II. In respect of retail clients who have accepted the terms and conditions of crypto-asset exchanges or entered into contracts for crypto-tokens, the scope of this exclusion should be narrowly construed using the MiFID II definition and relating solely to the rights and obligations which constitute the instrument itself.

The FCA financial promotion regime for cryptoassets requires crypto-businesses to seek approval from an authorised person for their advertisements if they are “capable of having an effect in the United Kingdom”. However, the FCA regime is limited to those crypto-businesses that offer purport to offer an opportunity to “engage in investment activity”, which will not extend to crypto-assets such as non-fungible or FPO utility tokens.

Overall, it would be helpful to receive additional guidance on the distinctions between the types of crypto-assets that qualify as financial instruments, as well as advertising activities that trigger consumer protections, that would bring a contract or product offered by a crypto-token business under the rules of (1) section 15B of the Civil Jurisdiction and Judgments “directed activities” in respect of jurisdiction, (2) the Rome I Regulation “pursuing” or “directing” activity, or ‘manifesting an intention to establish commercial relations with UK consumers’, in respect of “financial instruments” (in respect of the RAO and/or MiFID II) and (3) promotions that are “capable of having an effect in the United Kingdom” in relation to “qualifying crypto-assets” under the FCA regime.

Submitted to Law Commission Call for Evidence on digital assets and ETDs in private international law
Submitted on 2024-05-08 16:38:36

About you

What is your name?

Name:
Sean Edwards

What is your email address?

Email:
[REDACTED]

What is your telephone number?

Telephone number:
[REDACTED]

Questions on applicable law - section 72 of the Bills of Exchange Act 1882 (Chapter 11)

Question 17: We seek views on the most appropriate connecting factor for determining where an electronic bill of exchange is "delivered to a first holder" for the purposes of section 72(1) of the Bills of Exchange Act 1882.

Please share your views and evidence below::

Whilst I have given my views on these questions, I wish to make it clear that I believe that most, if not all, of the issues raised and the problems to be solved would be resolved by a single conflicts regime as set out in my answer to Question 18.

1. Of the two options, the most suitable, or least problematic, is the reliable system. This is because divestment in a digital or electronic context must take place on an IT system or using an electronic platform which places the relevant persons into a separate electronic or digital environment. This is quite different to paper, delivery of which can take place in the "real world" and where the conscious act of divestment can happen simultaneously with delivery. The reliable system can also be viewed, interrogated and its rules, if any, read and understood by third parties thereby allowing certainty as to the applicable law and jurisdiction (in a rule-book, this should be explicitly set out). The demerit, or drawback, of relying on the reliable system is that it is not always clear where the system is located. Should the law require identification of the location of the reliable system in order to promote certainty, it can reasonably be anticipated that parties will cause this to happen and it does not seem a difficult issue to resolve. Finally, the laws validating the creation of electronic trade documents (MLETR and the ETDA), emphasise the importance of the reliable system and reliability (whether relying on the factors set out in the laws or not) must be demonstrated by reference to factors and criteria which have substance and which are anchored or supplied to an identifiable place of business eg cybersecurity services and validation.

2. No to the first question although it will be easier to find the connecting factor in a central registry system.

Yes to the second question.

3. Yes as the technology is generic. Note, however, that there may be commercial preferences for using central registry/rulebook systems for bills of lading and stand-alone non-rulebook systems for bills of exchange and promissory notes although this may just reflect current market usage.

4. In both cases, the problem is that of "shifting" applicable laws when dealing with the same parties who may change location and frequent lack of up-front visibility and certainty of the applicable law given this especially where dealings are with a group of companies who may utilise a financing facility through an arranger parent "agent" where the legal counterparty is the subsidiary.

5. This is very rare. Defences to payment are usually based on fraud.

The only additional defence that might arise in relation to an electronic bill of exchange.

6. No.

Question 18: We seek views on whether it would be desirable to have a single conflict of laws regime to cover all types of electronic trade documents that fall within the scope of the Electronic Trade Documents Act 2023.

Please share your views and evidence below::

1. An "extended application" of S.72 would require an amendment to S.72 which is my main area of concern. As to whether other digital trade records should also be subject to the same changes, through other legal means, the answer is yes as these other instruments e.g. warehouse receipts, are generally subject to the same laws and, commercially, are often used in conjunction.

2. It should cover both. In a negotiable instrument, it is quite difficult from a legal point of view (I refer to paragraph 10.20 of the Call for Evidence) and pointless from a commercial point of view, to try to separate out the two.

3. A single conflict of laws regime should apply, based on, or inspired by, the UNIDROIT Principles on Digital Assets and Private Law. This recognises the primacy of party autonomy and importance of the party choosing the "right" system of law for them based on its commercial suitability which includes choosing a jurisdiction which will give effect to trade document digitalisation laws which, while growing, are not universal. It will also deal with the fundamental issue that electronic trade documents, like most digital assets, are everywhere and nowhere at the same time and have no or a shifting physical location. The nature of electronic bills and notes makes inclusion of choice of law and jurisdiction language easy to achieve something which the association I chair, ITFA, has been recommending and which has been incorporated into instruments issued by a number of platforms and users. This, I have been told, is necessary in order to reassure users and investors that the relevant digitalisation law will be effective and the documents they will

control will be valid electronic documents.

This is also critical for the spread and adoption of electronic trade documents globally. Many trade documents are governed by English law (80% of certain bills of lading for example) and the change of law in the UK in the form of the Electronic Trade Documents Act has caused many to look to electronic trade documents governed by English law to ensure their validity as electronic documents. A number of suppliers and solution providers are marketing on this basis and it reasonable to expect that the new law would support their and their customers' expectations. It is a legitimate objective of the new law that it validate trade documents which parties have freely chosen to have governed by English law even where the parties are not located in England. The importance of English law as an international utility, in view of its sophistication, commerciality and quality of its judiciary is well known. In the current state of the law, there is a possibility that S.72 could overrule an express choice of law clause agreed for this purpose and apply the law of a foreign country without a trade document digitalisation law or that overcautious legal advisers could advise to this effect which will have a chilling effect on the global effort to digitalise trade.

Submitted to Law Commission Call for Evidence on digital assets and ETDs in private international law
Submitted on 2024-05-16 16:37:45

About you

What is your name?

Name:
Elisabet Dahlman Löfgren, Head of Legal, Enigio AB

What is your email address?

Email:
[REDACTED]

What is your telephone number?

Telephone number:
[REDACTED]

Questions on applicable law - negotiable instruments, bills of lading, and the exclusions from the Rome Regulations (Chapter 10)

Question 13: We seek evidence, particularly from market participants, on how market practice in respect of bills of lading has been affected, or how it is likely to be affected, by the introduction of the Electronic Trade Documents Act 2023.

Please share your views and evidence below::

Market participant

Here is a brief description of our system:

Enigio provides a document centric solution (i.e. i.e. not a platform) for creating and managing digital original documents, functionally replicating the properties of paper, but in a digital form, i.e. trace:original™. This means that a customer can maintain a completely digital process for original documents, with all the security, efficiency and convenience of digital documents. With the trace:original™ solution, it is possible to create a digital original master document (i.e. singularity) where the one in possession of the master document (the holder) has exclusive control of the continued management of the original. Only the holder can append content to the original while the current original will always be distinguishable from its digital copies or earlier versions. With the exclusive control being centered to the actual electronic document, in contrast with document and data on a centralized platform, the physical location of the electronic document is controlled and managed by the holder in due course.

The holder can add new content, while added content can neither be changed or deleted, for retention of the original audit trail. The holder may freely transfer ownership of the digital original and distribute full control of the digital original document to a new holder, being a person or a legal entity.

The system is a patented cryptographic assurance system with central governance of a distributed block chained ledger, independently validated and approved by its participants. This is a network and infrastructure where participants in the network and other stakeholders through a shared cryptographic ledger can share a common trust in the truth of what is an original, what is the current version of an original document and if the original document has been invalidated by the holder or not. Furthermore, the integrity and shared truth can be upheld in the system, while business data always remain private in the original document. No business data is stored in a central register or public ledger; but only in the document and may therefore always be kept secret and stored in a place where only assigned stakeholders have access. The cryptographic proof of a digital original document is, however, shared with all in a shared public ledger.

An original trace:original™ document needs appended promises in writing and in the form of electronic signatures to form legal agreements between parties and to secure the parties' intent.

Enigio's customers are banks and corporations equally distributed in Europe, North America, Africa, Asia, and the Middle East.

Effect on market practices

The BoL is a critical document/instrument in a trade transaction, and a key document for enabling a digital transformation of trade. The willingness and commitment from market participants to accelerate digital trade has been communicated by the carrier industry, i.e. DSCA and BIMCO members. In our experience, the market practice in relation to how to actually transact and process trade transactions involving bills of lading has not changed significantly as a result of the adoption of the Electronic Trade Documents Act (ETDA). Expectation and willingness for adopting changes to the current global trade process when going digital is limited, due to the complex and multi-party involvement in the trade chain, as well for the well cemented practices instills confidence and trust among participants. Adoption would most certainly increase with technology mirroring the current practices.

The request and need for digitalization are strong, and the ETDA is perceived strongly positive. However, there remains some uncertainty still on how ETDA is to be applied, and there is a general sense of caution with any potential legal risks involved.

The cautious characteristics of the trade industry, given its nature, shows that the ETDA and MLETR approach to only make minor amendments, not to discriminate an ETD solely because it's in electronic form, was the right approach. A similar positive effect on adoption was gained when implementing the functional equivalents with physical trade document. A more comprehensive and far-reaching change when implementing the legislation would most probably have led to a significantly longer and more difficult adoption.

The market is and has been positively affected, since there are a number of test cases which have been carried out based on this new legislation validating the benefit and usability of ETDA.

The following are examples of the use of the legislation:

1. Mercore (digital bill of exchange)

On 7 May 2024 Mercore, a UK global trade focused fintech group announced that it had completed a receivables purchase transaction backed by digital bills of exchange. The finance facility supported a Kenyan producer of organic pesticides growing its sales into Belgium and the wider European Union. The deal was Mercore's first digital negotiable instrument-backed facility.

2. Fr. Meyer' Sohn (eBL)

Freight forwarder F. Meyer's Sohn organized the transportation from Rotterdam and subsequent issue of the eBL with global trader Th Brunijs & Co AB adding trade documents including invoice, packing list, insurance policy and certificate of origin. The eBL was issued under English law. The documents were received digitally as trace:original documents by the importer as well as F. Meyer's Sohn in India who released the goods. Document transaction time was reduced from nine days to one day and the documentation was in place prior to the vessel's arrival in Mumbai.

These cases would not have been possible without the legislation being in force.

General reflections on the issue

The Call for Evidence is a very comprehensive description of the current legal situation. However, it is important to bear in mind that we are in the midst of a transformation and what we see now may not necessarily be exactly what we see in the future.

It would therefore seem unwise to target specifically the very oldest type of law to amend to better suit the new technology, especially when there is technology that caters to the current legal space. There is technology available, such as trace:original, where you can identify the location of an electronic asset in the same way as you could with a negotiable instrument in paper form.

The mere explanation of the legislation and the concepts indicate that it would seem much more viable to apply the rules to the technology, i.e. functional equivalent, then adjusting all the rules to legacy technological (i.e. closed platforms) not adopted by the market.

Parties involved in the shipping industry have relied on contractual frameworks as a solution to the law not (yet) recognizing electronic bills of lading as possessable. We therefore consider that these practices may be indicative of the private international law issues that may arise from the use of electronic trade documents that qualify under the ETDA. In our opinion, this does not say anything about the interpretation of the law, but only provide an indication of the practical necessity of a legal framework.

The conservatism and the adoption of eBL will more likely be similar to that of electronic signatures, being widely accepted and used under adopted legal frameworks. eBL is expected to be as widely used once we reach a tipping point.

There is a slight misconception about the distributed ledger technology. The perceived problem is not the distribution itself. That can be perceived as problematic because of a lack of a general understanding of how such a system functions, but the distributed technology is further secure due to being incorruptible. Distributed ledger technology does not equal a system that is not governed. Many of the examples in the Call for evidence, relating to Bitcoin etc. have the inherent problem that there is no governance at all. A system that uses distributed ledger technology to ensure reliability and singularity of an eBL, can still be governed and it is the integrity and reliability of the original issuer that should be scrutinized, not the distributed ledger technology itself. A legal framework that does not discriminate between paper and electronic form and thereby uphold operation under existing legal framework, as well as not favoring any particular type of technology, is primarily what is required for a wider use of eBL.

Closed platform under contract law arrangements have not gained traction, or proven sustainable.

Onboarding all platforms provided by major shipping companies or using platforms governed by their own regimes has proven to be non-viable. In goods transports to and from the countryside in multiple jurisdictions on both sea and road and require a system that can be used also at the end point under such conditions. In these situations, you need a document that can be read by the human eye, with the security provided by a digital solution, backed up by a distributed ledger to avoid any risk of tampering.

The use of eBL platforms accounts for less than 1.5% of the BL:s, and should not be used as a framework for this type of legislation.

It is also from a competition and anti-trust perspective important not to implement legislation that will favor the use of platforms, especially in a space already dominated by a handful of large corporations. A stable legal framework, in combination with a reliable system approach is much more effective and opens for transparency, competition and efficiency. The carrier industry is already concentrated to a few global players, and it would be unfortunate if legislation were to push also eBL in that direction.

Question 14: We seek evidence on market sentiment relating to use of DLT platforms for electronic bills of lading.

Please share your views and evidence below::

1. Firstly, it is important to differentiate between the different forms of technology. If it is decentralized it is usually not a platform.

From our perspective it seems highly unlikely that market participants will move towards ONE wholly decentralized DLT platform for bills of lading in the foreseeable future. There is not a single example of ONE platform used to create legally binding actions that can be used globally.

On a macro level and with a geopolitical impact on trade it's difficult to see how an alignment would be possible were market participants from various regions and countries would be able to join the same singular platform. On a micro level further complexity and challenges are added, preventing such scenario.

Should you opt for the use of a platform – meaning that it is normally not decentralized – you would in almost all cases want a user agreement. To issue an eBL you would need an agreement with the provider of that technology, but not necessarily if you are provided with an eBL produced in a reliable system or under a well-functioning legal framework. You do not have to have a SasS agreement to receive a paper BL and that has worked for centuries. It seems highly unlikely that global trade could be unanimously digitalized in one go. Instead – provide a solid framework for the use and acceptance of electronic documents and the market will quickly adapt, finding solutions that a single platform could never provide.

2. Market participants and technology providers will have to require user agreements stipulating the terms and conditions, responsibilities and liabilities in relation to providing the services. To extend such technology agreements to include rights and obligations of third parties rights and obligations in form of contract-law, has only been a substitute for the lack of support by common law. Market participants will be significantly more comfortable acting under a harmonised common law framework, and particular when entering into new way of operating digitally. Common law will further to trust, also increase the flexibility on technology to operate in a multi-party and industry supply chain in comparison to under contract law in a user agreement. Therefore, increase the usability and wider adoption of digitalisation by the industry.

In addition, the required development, clearly requested by the market participants, is to eliminate the role of the DLT and platform part for holding business data, but only provide a secure and verifiable record of transactions without third party use of business data. We see a firm resistance to share business data with any third-party platform, and subsequently post such data in the DLT. This has been and is still, a restrainer for adoption for commercial, data security and confidentiality perspective. Further, recent wind-downs and insolvency of DLT platform has triggered concern by market participants on the data and ETD/asset operation and preservation post- DLT platform cessation of business, due to dependencies on such platform. Therefore, the ETD/assets are to be separated from dependency of a DLT platform to ensure such business sustainability and contingency in the event of DLT platform cessation of business.

3. Firstly, it must again be made clear that there is no opposition between the decentralized and the governed. The main issue is that the initial issuing of the eBL is governed, the following transactions can be governed by law just as a paper BL.

A central depository with everyone's data available (such as a platform) is much more vulnerable from a data security point of view. If there is a security breach on a platform, the amount of damage may be immense given concentration of data. Using a decentralized approach – much like how paper is today – is more secure by its structure.

Enigio trace:original operates as a wholly decentralized DLT ETD solution, where the ETD/asset are operated and business data maintained independently in the actual ETD only and not on DLT platform. The DLT solely work as a ledger for “fingerprints” of the ETD to provide secure and verifiable records of transaction with full control of the data only by the holder of the ETD.

Question 15: We seek evidence on the difficulties, if any, of incorporating the Hague-Visby Rules where an electronic bill of lading has been used.

Please share your views and evidence below::

1. --

2. The current concerns we experienced relates to gain trust in the enforcement of eBL under ETDA in jurisdictions other than UK. The main concern is that the legislation governing the eBL and the choice of law made by the original issuer of the eBL for some reason may not be relied upon, when presenting the eBL in a jurisdiction that has not adopted the MLETR. This is a concern that is not as prevalent for paper BL.

For example, the novation of an eBL is dependent on the validity of the actual eBL as an BL. The novation chain is to be upheld by each court in jurisdiction of destination for the eBL.

Further there has been uncertainty around the qualification of a reliable system or method for the creation and management of electronic transferable documents or records. Our view is that such concern are now being adequately addressed by ICC DSI ´ efforts to roll-out a Reliable Assessment Framework to the industry. Such framework assessment will in the first step be on self-assessment basis, with the possibility to provide “evidence”, such as supporting 3rd party opinions.

The initiative will have to be adopted broadly geographically, to avoid a fragmented and deviating reliability assessment for technology system providing ETD which travel through multiple jurisdictions. A certification of reliability would be pre-matured in the current early phase of ETD. The first step alignment through self-assessment in accordance with a common framework is expected to provide transparent comparison of the various technologies which would benefit the industry and create a foundation for certification in a next step.

Most are relying on an approval by the IGP&I Club, which now covers most platforms, and also Enigio's trace:original document solution.

Question 16: We seek evidence on market practice to help us identify where it could be said that an electronic bill of lading is “issued” for the purpose of the Hague-Visby Rules, as implemented in the UK by the Carriage of Goods Act 1971

Please share your views and evidence below::

1.

We believe that it is important to keep in mind that all bills of lading are born digital. They are created in a word processing software system (such as Microsoft Word) and then saved as a PDF (such as Acrobat Adobe). The bill of lading could also be created in a specific software used for document templates, but the bill of lading is always created digitally before it is printed.

Enigio's solution trace:original taps into the existing process and enables the carrier to upload (manually or via APIs) the PDF or required data to a trace:original “virtual printer” to create an eBL, instead of sending it to a physical paper printer. This process functionally mirrors the paper process. The

signing and the issuing of the eBL happens momentarily in the system. The integrity of the documents is secured by hashing the documents, which are timestamped and published on the DLT. Each eBL (or other electronic trade document) is uniquely identified and will get a public and private cryptographic key to secure the control, possession and management of the eBL.

The steps taken are the following:

1. Create the eBL by drafting or uploading it, including adding of additional terms, adding attachments, adding signature field, add party, specifying the key owner
2. Sign and issue the eBL
3. Manage the eBL by updating, transferring or invalidating the eBL, each step validated by a signature and the use of your key

2.

The following applies to the Enigio trace:original system:

The shipper must receive an invitation to take possession over the eBL, which must be initiated by the holder of the eBL in due course. Such invitation can be sent via any channel (i.e. e-mail). By clicking on the enclosed link the shipper gets access to review the ETD and is thereafter asked if to take possession (i.e. accept transfer). Upon taking possession a new private key will be created, simultaneously with the old key being invalidated, and a new version of the document is created, all which are published to the DLT in new blocks. An audit trail on all activities is included in the last version of the document, i.e. includes the activity of transfer. The shipper now has exclusive control and possession of the eBL, evidenced by the latest version of the eBL and the cryptographic key. This can be validated against the DLT.

The shipper then stores the eBL and the key where they find appropriate, e.g. on a document management system, on their own computer, on a Yubi key, etc.

Due to the ETD centric solution, specific localization of the actual ETD is not a constrain and may follow the principle of paper.

3.

The following applies to the Enigio trace:original system:

Enigio is not involved in the issuing or management of the eBL and has no access to the information in the eBL. The information regarding the shipment is a) visually legible to the human eye by the person holding the eBL, same as with a PDF file and b) stored as data within the eBL, meaning that the PDF file itself actually contains the data.

Enigio is not involved in the actual issuing of any specific eBL. Enigios part is to provide the capability to create eBL or any other ETD, i.e. the initial issuer, by providing a Node from which the eBL can be created and to store the block chain evidencing its singularity and information on the occurrence of a transfer, amendment or invalidation (not information on any specifics of these occurrences). As a system approved by the IGP&I Club, the terms and conditions applicable to the original issuer states that all eBL:s must be governed by the laws of England & Wales or other governing law compliant with MLETR.

Any subsequent transfer is made using the public node, where the carrier can transfer the trace:original eBL to the freight forwarder, to the banks and so on. In case of such subsequent transfer, or further transfers, Enigio only acts as the provider of the public ledger (i.e. the block chain). Any amendment, transfer or invalidation of the eBL is registered on the blockchain, to be validated by anyone, but only the holder of the eBL in due course has access to the information on the eBL.

4.

As the current market standard is paper BL, we would advocate that the best practice for eBL is an eBL issued in a way that mirrors the paper BL in functionality. Thereby, making the transition from analog to digital as low as possible for all parties involved in the trade chain, and also being able to leveraging the ETD advantages. I.e. safe and secure, cost, speed, interoperability, etc.

Any platform is merely used to circumvent the fact that there previously was no legislation to cater to the issuance of electronic bills of lading.



Digital Assets: Governing Law and Jurisdiction

6 June 2024

Brian Gray

Chief Executive

Becky Jacombs

Senior Researcher

Working Group*

Conall Patton KC (Chair), One Essex Court

Antony Beaves, Bank of England (Observer)

Anne Bodley, Queen Mary University of London

Sam Brown, Clifford Chance LLP

Rory Conway, Linklaters LLP

Jonathan Gilmour, member of the International Digital Assets & Cryptocurrency Association

Natalie Lewis, Travers Smith LLP

Carolyn H. Jackson, Katten Muchin Rosenman UK LLP

Jason Rix, Allen Overy Shearman Sterling LLP

Sanjev Warnakula-suriya, Latham & Watkins LLP

**Note that Members act in a purely personal capacity. The names of the institutions that they ordinarily represent are given for information purposes only.*

Registered Charity Number: 1164902.

"FMLC" and "Financial Markets Law Committee" are terms used to describe a committee appointed by Financial Markets Law Committee, a limited company ("Company"). Registered office: 3rd Floor, North Wing,

Guildhall, London EC2P 2EJ. Registered in England and Wales with number: 8733443

Table of Contents

| | | |
|----|--|----|
| 1. | Introduction | 1 |
| 2. | Scope and Assumptions | 1 |
| 3. | DLT Systems: An Update | 3 |
| 4. | Characterisation of a claim as proprietary | 7 |
| 5. | Governing Law | 8 |
| 6. | Jurisdiction | 16 |
| 7. | Conclusion | 17 |

1. Introduction

- 1.1 The role of the Financial Markets Law Committee (the “**FMLC**” or the “**Committee**”) is to identify issues of legal uncertainty or misunderstanding, present and future, in the framework of the wholesale financial markets which might give rise to material risks and to consider how such issues should be addressed.
- 1.2 The FMLC published a paper in 2018 which examined governing law and related conflicts of law issues in the context of distributed ledger technology (“**DLT**”) systems (the “**2018 Report**”).¹ The paper outlined the possible connecting factors to be used when identifying the governing law for the proprietary effects of transactions conducted on a DLT system, and recommended elective *situs* as the starting point for any conflict of laws analysis. The paper also concluded that any solution would need to be promulgated by an international body to ensure international adherence.
- 1.3 This sector has seen significant development since 2018, not merely because of the growth in the use of DLT systems and digital assets, but legal developments such as the Law Commission’s work clarifying the proprietary nature of digital assets² (the “**Law Commission’s Report on Digital Assets**”) and its recent call for evidence, “*Digital assets and ETDs in private international law: which court, which law?*”³ (the “**Call for Evidence**”), UNIDROIT’s project on Digital Assets and Private Law⁴ and a variety of cases across the world where digital assets have been treated, at least arguably, as being capable of giving rise to property rights.⁵
- 1.4 Given the remaining uncertainties in the conflict of law rules which should be applied to DLT systems and digital assets, this paper aims to reconsider the issues in light of the developments in the sector and recommend how those conflicts of law rules should develop.

2. Scope and Assumptions

- 2.1 This paper assumes that digital assets are capable of giving rise to property rights, consistent with the conclusion reached in the Law Commission’s Report on Digital

¹ Distributed Ledger Technology and Governing Law: Issues of Legal Uncertainty, 2018, found here: <https://fmlc.org/publications/report-finance-and-technology-27-march-2018/>

² <https://lawcom.gov.uk/project/digital-assets/>

³ <https://lawcom.gov.uk/project/digital-assets-and-etds-in-private-international-law-which-court-which-law/>

⁴ <https://www.unidroit.org/work-in-progress/digital-assets-and-private-law/>

⁵ The decision of highest authority in England and Wales is currently the Court of Appeal’s decision, at the jurisdictional stage, in *Tulip Trading v Bitcoin Association for BSV* [2023] EWCA Civ 83. Additionally, there have been a number of first instance decisions supporting the position that digital assets are capable of being objects of personal property rights, albeit mostly decided in connection with interim relief: *Piroozzadeh v Persons Unknown* [2023] EWHC 1024 (Ch); *Osbourne v Persons Unknown Category A* [2023] EWHC 340 (KB); *Osbourne v Persons Unknown Category A* [2023] EWHC 39 (KB); *D’Aloia v Persons Unknown* [2022] EWHC 1723 (Ch); *Amir Suleymani v Nifty Gateway LLC* [2022] EWHC 773 (Comm); *Nicholls v Little* [2022] EWHC 2344 (QB); *HDR Global Trading Ltd v Shulev* [2022] EWHC 1685 (Comm); *Tulip Trading Ltd v Van Der Laan* [2022] EWHC 667 (Ch); *Osbourne v Persons Unknown* [2022] EWHC 1021 (Comm); *Danisz v Persons Unknown and Huobi Global Ltd* [2022] EWHC 280 (QB); *LMN v Bitflyer Holdings Inc* [2022] EWHC 2954 (Comm); *Jones v Persons Unknown* [2022] EWHC 2543 (Comm); *R v Wright (Nigel)* [2022] EWCA Crim 882; *DPP v Briedis* [2021] EWHC 3155 (Admin); *Wang v Darby* [2021] EWHC 3054 (Comm); *Fetch.ai Ltd v Persons Unknown* [2021] EWHC 2254 (Comm); *Litecoin Foundation Ltd v Inshallah Ltd* [2021] EWHC 1998 (Ch); *Reyes v Persons Unknown* [2021] EWHC 1938 (Comm); *Marian Toma, David True v Ciaran Murray* [2020] EWHC 2295 (Ch); *Ion Sciences vs Persons Unknown* (unreported, 21 December 2020, Commercial Court); *AA vs Persons Unknown* [2019] EWHC 3556 (Comm), [2020] 4 WLR 35; *Liam David Robertson v Persons Unknown* (unreported, 15 July 2019); *Vorotyntseva v Money-4 Ltd* [2018] EWHC 2596 (Ch).

Assets. It should be noted that not all DLT systems will have the characteristics necessary to create a thing of property. This paper does not consider whether any particular DLT system is likely to give rise to property rights; it proceeds on the assumption that there will be instances where property rights are at issue.

- 2.2 Disputes concerning digital assets may give rise to a variety of different causes of action, each raising their own questions of jurisdiction and governing law. The Call for Evidence ranges over a broad field, including issues of contract (including consumer contracts), tort, electronic trade documents and electronic bills of lading. However, consistent with the focus of the 2018 Report, this paper will focus on the proprietary effects of DLT transactions in financial instruments or assets, recognising the particular need in the financial markets for certainty as to how proprietary issues of transfer, priority and security perfection will be governed within a financial services context. Many disputes involving DLT transactions within the financial markets may not need to consider proprietary issues, such disputes being capable of being resolved by the application of contract law alone. We have not considered questions of governing law and jurisdiction for contractual disputes involving DLT transactions in this paper as these do not give rise to the same uncertainties as disputes involving proprietary issues. We agree with the Law Commission that there are likely to be no particular problems in deciding the applicable law for non-consumer contracts involving digital assets,⁶ particularly in financial markets contracts where express choice of law provisions are usually present.
- 2.3 Whereas the 2018 Report was solely concerned with the identification of the governing law, this paper will also consider the circumstances in which the courts of England and Wales should have jurisdiction to determine disputes concerning proprietary rights to a digital asset.
- 2.4 Although the increasing prevalence of digital assets is likely to be a matter of intense focus for regulators, this paper is exclusively concerned with questions of governing law and jurisdiction in the context of private law disputes.
- 2.5 This paper addresses the position from the perspective of the law in England and Wales. The Call for Evidence points out that the Law Commission for England and Wales can make law reform recommendations only for England and Wales, and not for Scotland or Northern Ireland.⁷ The Law Commission has nevertheless invited stakeholders in Scotland and Northern Ireland to provide information about the ways in which these issues are being dealt with by their judiciary, and any particular challenges under the laws of those jurisdictions. For certainty in the financial markets, it is important that a consistent approach to the issues canvassed in this paper be adopted across the financial markets of the United Kingdom.
- 2.6 The proposals in the paper are unlikely to conflict with Scottish law. The key difference under Scottish law is the property analysis. Digital assets are capable of giving rise to property rights but a “third way”, as set out in the Law Commission’s Report on Digital Assets, is not needed under Scottish law as digital assets can be incorporeal moveable property. It should be noted the trusts do exist and will tend to be analysed as proprietary interests where the Recognition of Trusts Act 1987 does not require otherwise. Additionally, equitable interests do not exist under Scottish law and purported equitable interests would be analysed in Scotland as proprietary interests. However, once it is established the digital assets in question give rise to property rights under Scottish law, the questions of governing law and jurisdiction are substantially the same.⁸

⁶ Call for Evidence, para 7.83.

⁷ Call for Evidence, paras 1.30-1.32.

⁸ The FMLC is grateful to Dr Hamish Patrick (Shepherd and Wedderburn LLP) for his assistance with this section.

3. DLT Systems: An Update

- 3.1 The 2018 Report described DLT systems as records of electronic transactions which are maintained by a shared or “distributed” network of participants (known as “nodes”), thereby forming a distributed validation system, that make extensive use of cryptography i.e. computer-based encryption techniques such as public/private keys and hash functions which are used to store assets and validate transactions on a distributed ledger.⁹ This remains a valid description today.
- 3.2 The 2018 Report also suggested that three broad distinctions exist which provide a helpful base for legal analysis:
- a) Permissionless and permissioned systems: “permissionless” systems are open to the public, whereas in “permissioned” systems only authorised participants are able to create records and verify changes to the ledger.
 - b) Record and title ledgers: the distinction here is that “record ledgers” evidence or record title transfers carried out through underlying transaction documentation, whereas “title ledgers” transfer title directly on the ledger.
 - c) Off-platform asset tokens and on-platform asset tokens: “off-platform” asset tokens, also known as “linked” tokens, represent or are pegged to underlying “real world” assets, whether tangible or intangible, whereas “on-platform” asset tokens are assets created within, and whose value is entirely derived from the sphere of the DLT system, with no underlying asset referenced.
- 3.3 These distinctions remain valid and important to the legal analysis today. In particular, as regards (a) (permissioned/permissionless systems)¹⁰, the 2018 Report referred to the possibility that the greatest future advances within the DLT sphere would be delivered via permissionless systems. Although there is little publicly available data to gauge the relative prevalence of digital assets in permissionless as opposed to permissioned systems, it is likely, given that Bitcoin and Ethereum are both permissionless systems, that permissionless systems today account for the majority of digital assets by current market value. The continuing growth in the importance of permissionless systems is reflected by a recent joint submission by various trade bodies to the Basel Committee on Banking Supervision arguing against certain restrictions on the ability of banks to hold permissionless blockchain assets.¹¹
- 3.4 As regards (b) (record/title ledgers), the 2018 Report proposed that where the asset has an existence which is wholly independent of the system, such that the system serves purely as a means of recording the transaction and neither title nor the asset is constituted thereby, the proprietary effects of the transaction should

⁹ See ESMA, The Distributed Ledger Technology Applied to Securities Markets (7 February 2017) n.2 at p.4, available at: <https://www.esma.europa.eu/press-news/esma-news/esma-assesses-dlt%E2%80%99s-potential-and-interactions-eu-rules>.

¹⁰ It is important to note that permissions can exist in different layers. The network itself could be permissionless in the sense that anyone can download the protocol and connect to it, but applications can be built on the DLT which are permissioned. There is a trend towards DLTs having multiple layers, increasing the ability to have different levels of “permission” and therefore combining the benefits of permissioned (control, security) and permissionless (scale, resilience) approaches.

¹¹ Consultation response dated 28 March 2024 by the Global Financial Markets Association, the Futures Industry Association, the Institute of International Finance, the International Swaps and Derivatives Association and the Financial Services Forum, available at [joint-associations-cryptoassets-working-group-bcbs-cryptoasset-standard-amendments.pdf \(gfma.org\)](https://www.gfma.org/joint-associations-cryptoassets-working-group-bcbs-cryptoasset-standard-amendments.pdf).

be determined according to the conflict of laws rules which would ordinarily apply outside the system.¹² That remains our view.

- 3.5 We understand that the current implementations of digital assets in the financial markets largely involve financial instruments, or settlement assets used for payments, that are merely recorded or evidenced on a distributed ledger within a permissioned system that is administered by a central operator, without giving rise to a distinct token asset that is capable of being the object of property rights. Such uses are generally capable of being accommodated, with a sufficient degree of certainty, under existing rules of private international law.
- 3.6 For example, in relation to a system designated under the Financial Markets and Insolvency (Settlement Finality) Regulations 1999 (the "**SFRs**"),¹³ it is possible to structure arrangements so as to fall within the conflict of laws provisions of the SFRs. These provide, for example, that the English courts will apply the governing law of the system to determine questions relating to the rights and obligations arising from or in connection with a person's participation in the system in the insolvency proceedings of that person. Similarly, depending on the structure, conflict of laws rules under the UK Financial Collateral Arrangement (No. 2) Regulations ("**FCARs**") or Rome I (Onshored)¹⁴ ("**Rome I**") may apply to determine certain matters within the scope of those instruments concerning the recorded assets. While there may be a case for expanding or clarifying the scope of these existing statutory frameworks to accommodate structures that are not adequately catered for, we do not propose cutting across existing statutory frameworks with any new intervention. This would risk undermining legal certainty within the financial markets. Accordingly, digital assets of the nature described in the first sentence of this paragraph are outside the scope of this paper.
- 3.7 Rather, this paper is instead focused on digital assets that comprise a token asset that constitutes an object of property distinct from any attached right or interest, to the extent not otherwise falling within the statutory frameworks described above. Such digital assets may be transferable within either a permissioned or permissionless system. We acknowledge that such digital assets have not been used widely in the regulated financial markets to date given obstacles under applicable financial regulation. However, their use, particularly as settlement assets, could increase given, for example, the upcoming regulatory frameworks for fiat-backed stablecoins as proposed by the Bank of England and the FCA.
- 3.8 As regards (c) (off-platform/on-platform tokens), it remains the case that a distinction must be drawn between a token that is "linked" to real-world assets and a "native" token whose value is entirely derived from the DLT system. In the case of tokens that represent a real-world asset, the initial question whether a proprietary interest in that asset can be represented in the form of a digital token must be a matter for the law which governs questions of title to the real-world asset. If this is permitted, there is an argument for saying that, following such a determination, questions concerning title to the token should be governed by the framework that we propose below in relation to native tokens. This would ensure that, where a DLT system encompasses both native and linked tokens, the same rules for determining governing law can apply to dealings in tokens of either kind. However, there are counter-arguments that proprietary questions in relation to a linked token should be governed by the same law as applies to the real-world asset. If one law applies to determine proprietary disputes over the real-world asset, and a different law applies to determine title to the linked token, there may be a risk of a mismatch in outcomes. A deeper examination of this question would be required,

¹² 2018 Report, para 7.8.

¹³ SI 1999/2979, implementing Directive 98/26/EC.

¹⁴ Regulation (EC) No 593/2008, as onshored into UK domestic law.

particularly the initial question of whether it is possible for a proprietary interest in a real-world asset to be represented in the form of a digital token. Such questions are outside of the scope of this paper which focuses on native tokens.

- 3.9 We would add that the 2018 Report mentioned the possible existence of “fully decentralised networks”, where there is no central validation system and no central point of control. It remains a controversial question whether such a network genuinely exists, but this is not critical to the issues discussed in this paper.
- 3.10 The use cases of DLT in the financial markets have developed since the 2018 Report was written, including (i) tokenised fund units for distribution; (ii) tokenised money market fund units in particular for collateral to satisfy margin calls; (iii) tokenised carbon credits; (iv) tokenised trade finance assets and loan exposures for risk distribution as a securitisation or repackaging method; (v) testing for DLT for trade reporting and (vi) native digital bonds (which are now being issued with firms looking at how to use them in secondary markets). There are other tokenisation use cases and examples beyond the ideas that were discussed at the time of the 2018 Report, such as digital commercial paper and certificates of deposit, gold and collateral management, as well as tokenised deposits for FX settlement and sale and repurchase (repos).
- 3.11 These use cases and market trends raise a number of issues relevant to the question of governing law in respect of property disputes:
- i) As stated in paragraph 3.5, in many of the current use cases, the token is designed to not be property and therefore the question does not arise. For example, many tokenisation platforms for traditional securities are structured deliberately so the technology is part of the custody structure rather than creating a digital token in its own right. If native digital securities become prevalent in the future, questions of property rights and governing law in respect of such assets will need to be addressed.
 - ii) Transactions in digital assets are increasingly seeing the use of professional intermediaries. Depending on the intermediary and the holding structure, the assets can be held in segregated cold wallets or general client wallets. The use of these intermediaries means the law that governs proprietary aspects of digital assets is likely to be less important than the law governing the contractual terms agreed between clients and intermediaries.
- 3.12 The 2018 Report stressed the desirability of a solution to the question of governing law being promulgated by a body such as the Hague Convention, UNIDROIT or International Swaps and Derivatives Association (“**ISDA**”), in order to ensure adherence on an international basis. Since then, there have been a number of developments in this regard.
- 3.13 Since 2018, ISDA (along with a number of partners) has published two papers considering the private international law aspects of smart derivative contracts using DLT. In relation to a number of jurisdictions, the papers conclude that courts would not generally disapply an express choice of a national law in a contractual agreement related to a DLT-based transaction.¹⁵ However, the publications do note “*there may be additional conflict-of-laws issues arising from a potential lack of legal*

¹⁵ (1) Private International Law Aspects of Smart Derivatives Contracts Utilizing Distributed Ledger Technology, ISDA, Clifford Chance, R3 and the Singapore Academy of Law, January 2020. Available at: <https://www.sal.org.sg/sites/default/files/SAL-LawReform-Pdf/2020-08/2020-Private-International-Law-Aspects-of-Smart-Derivatives-Contracts-Utilizing-DLT.pdf>, and (2) Private International Law Aspects of Smart Derivatives Contracts Utilizing Distributed Ledger Technology: New York Law, ISDA, Clifford Chance and R3, October 2020. Available at: <https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2020/10/Private-International-Law-Aspects-of-Smart-Contracts-Utilizing-Distributed-Ledger-Technology-New-York-Law.pdf> (the “**ISDA New York Law Paper**”)

certainty around the situs of tokens that are used".¹⁶ It is recommended that parties "agree that all on-ledger transactions or collateral arrangements taking place on a DLT platform are subject to a uniform choice of law"¹⁷; such law could then be used to determine the *situs* of any tokens native to that DLT system. The paper recognises that adopting such an approach would require national governments, judiciaries, regulators and international standard-setting bodies to work on adapting or developing global legal standards.

- 3.14 More recently the UK Jurisdiction Task Force published a statement on Digital Assets and English Insolvency Law¹⁸ which noted the continued uncertainty on the question of *lex situs* in relation to digital assets.
- 3.15 The United States has taken steps to address the question of governing law for digital assets in recent amendments to the Uniform Commercial Code ("**UCC**").¹⁹ In 2022, Article 12 was introduced to create a legal regime for electronic intangible assets. It sets out legal rules governing the transfer (both outright and for security) of interests in these assets and certain rights (primarily property rights) of transacting parties and other persons that might be affected by the transactions. Section 12-107 of the UCC sets out how the governing law of these transactions is to be determined, the general rule being the location of the relevant digital assets' jurisdiction. The digital assets' jurisdiction is then determined by a "waterfall" of rules containing a series of provisions which rely on some type of express provision in the asset or system as to location or governing law. The end of the waterfall states that without any express provision, the jurisdiction is the District of Columbia. The official comments on the UCC amendments note that it might be thought that the logical choice for the bottom of the waterfall would be the location of the debtor; however, that location may not be readily ascertainable because the transferor may not be known or be easily discoverable by the purchaser. As at the date of this paper, these amendments have been enacted by only 19 US states. In particular, New York has not enacted Article 12 and the amendments were referred to the judiciary at the beginning of 2024.
- 3.16 In May 2023, the UNIDROIT Governing Council adopted a set of UNIDROIT Principles on Digital Assets and Private Law. Principle 5(1) lays down a "waterfall" of rules to determine the governing law for proprietary issues in respect of a digital asset. The top of the waterfall looks to the domestic law of the state expressly specified in the digital asset or, if none is specified in the asset, the system. Failing an express provision, in relation to a digital asset of which there is an issuer, the domestic law of the state where the issuer has its statutory seat. The end of the waterfall treats the law of the forum state as the applicable law. The full text of Principle 5 is set out in Annex 1 to this paper.
- 3.17 These developments reveal growing international support for the view that the governing law should be that chosen in the digital asset or DLT system, where such a choice has been made. However, there is no real developing consensus on how governing law should be determined in the absence of a chosen law.

¹⁶ At p 21, ISDA New York Law Paper.

¹⁷ At p 21, ISDA New York Law Paper.

¹⁸ Available at: <https://lawtechuk.io/reports/ukjt-legal-statement-on-digital-assets-and-english-insolvency-law/>

¹⁹ Uniform Commercial Code Amendments (2022). Available at: <https://www.uniformlaws.org/committees/community-home/librarydocuments?communitykey=1457c422-ddb7-40b0-8c76-39a1991651ac&LibraryFolderKey=&DefaultView=&5a583082-7c67-452b-9777-e4bdf7e1c729=eyJsaWJyYXJ5ZW50cnkiOiI0MjRjNDIiZC1jNGRmLTQyMGEtYWJjOS0yNjgxZGZkNWVhYmYifQ%3D%3D>

4. Characterisation of a claim as proprietary

- 4.1 The question of the proper characterisation of a claim is the essential starting point for determining its governing law. It is well established, for example, that the governing law may well differ depending on whether a claim is properly characterised as lying in contract or in tort.
- 4.2 The paradigm case of a claim that is properly characterised as proprietary in nature is where the claimant seeks a declaration upholding its title or seeking orders for delivery to it of the relevant asset. A hallmark of a proprietary claim is that the claimant's title to the asset, if upheld, stands good against the rest of the world.
- 4.3 Such claims can frequently be expected to arise in relation to digital assets. For example, A may assert that its interest in a digital asset has been misappropriated by B. That claim may be asserted in proceedings against B or, perhaps more likely, against a third party such as a custodian, the operator of an exchange or the issuer of the digital asset.
- 4.4 In relation to digital assets created within a permissionless system, it is particularly plausible that the proper characterisation of such a claim will be proprietary in nature. In the case of permissioned systems, on the other hand, there may be greater room for argument that the law of contract is sufficient to address disputed questions as to a party's entitlement to digital assets within the system: a permissioned system could be conceived as giving rise to a multilateral contract between its participants so that a dispute about who holds the relevant interest becomes a dispute as to the contractual rights of participants *inter se*. However, proprietary issues could arise in relation to permissioned systems where a system participant purports to transfer / confer rights in a digital asset to a non-participant outside of the system, as that person may not be considered to be a party to the multilateral contract referred to above. Thus, it would be a question for the law of property whether valid security has been granted over the digital asset in favour of a non-participant or whether a non-participant purchaser has acquired equitable or other title to a digital asset, free from any proprietary, equitable or other similar interest of another person.
- 4.5 Characterising a claim as proprietary in nature presents important benefits for claimants in terms of the armoury of remedies that may be available. At the interim stage, a proprietary injunction may be granted to prevent dealings in the digital assets pending trial. Following trial, a proprietary claim may entitle the claimant to orders for the delivery of property or to trace into assets held by third parties. The vindication of a proprietary rather than personal claim may make all the difference in the event that the holder or custodian of the asset becomes insolvent.
- 4.6 Even where the relief sought is purely monetary, issues may arise which turn on the existence or otherwise of proprietary rights. For example, in order to advance a claim for damages in tort, the claimant may need to establish, as a threshold question, whether it held title to the asset alleged to have been misappropriated, lost or damaged.
- 4.7 Against this background, it is clear that the selection of the law which determines whether the claimant has a well-founded property interest may be of decisive importance to the outcome. The system of law will also decide such questions as whether a proprietary claim is defeated by a transfer to a bona fide purchaser without notice of the prior claim, and it may have important implications for what final remedies are available.
- 4.8 The forum in which a dispute about ownership can be determined may likewise prove decisive to the outcome. This is not least because the conflict of laws rules of the forum will dictate the selection of the governing law for proprietary issues. The 2018 Report recommended that any solution to the governing law of digital

assets should be promulgated by an international body. If a common rule as to governing law were adopted in many jurisdictions, this would reduce the significance of the forum for the governing law issue; but it remains to be seen whether this will occur. In any event, the forum may still have important implications for the availability of remedies (such as declaratory and injunctive relief), as well as for the enforceability elsewhere of the resulting judgment. In addition, the available forum will affect more practical questions, such as the availability in the forum of skilled lawyers, experts and judges with an up-to-date understanding of digital assets.

5. Governing Law

The 2018 Report

- 5.1 The 2018 Report identified the real potential for uncertainty in relation to the application of traditional property rules of private international law to digital assets. When dealing with tangible goods, a question as to rights or entitlement should generally be governed by the law of the place in which the property or claim to property is situated (*lex situs*). A key difficulty with this in the digital context is that the decentralised nature of DLT means that the ledger may not be located in a single country and may even have simultaneous and equally valid connections to a large number of jurisdictions across the world (a phenomenon sometimes referred to as “omni-territoriality”). A subsidiary but related point is that it may in practice be difficult or even impossible to ascertain which those jurisdictions are.
- 5.2 The 2018 Report considered a number of possible connecting factors as a basis for selecting the governing law applicable to the proprietary effects of transactions conducted on DLT systems:
 - a. *Lex Situs*
 - b. Elective *Situs* / Modified Elective *Situs*
 - c. Deemed Election
 - d. Chosen law of the transaction/transfer/assignment
 - e. Place of the Relevant Administrator/Operating Authority/Private Encryption Master key-holder (PROPA/PREMA)
 - f. Location of the Issuer Master Account
 - g. Location of the Participant/Transferor/User Private Encryption Key
 - h. Law of the assigned claim
 - i. *Lex Codicis* (the primary residence of the original coder)
- 5.3 The 2018 Report recommended that elective *situs* should be the starting point for any analysis of a conflicts of law approach to virtual tokens. As explained above, the focus of this paper concerns the impact of subsequent developments on the recommendation that elective *situs* remains the correct starting point for “on-platform”, “native” or “endogenous” tokens (these expressions are synonymous), i.e. those whose value is entirely derived from the DLT rather than from any “real world” asset.

What is meant by elective *situs*?

- 5.4 The label “elective *situs*” is capable of causing confusion. The reference to *situs* may suggest that the concept is concerned with a physical location. The addition of the word “elective” could be understood as suggesting a choice as to where a DLT system (and the digital assets recorded in it) are deemed to be located. If “elective

situs” were understood as a legally-recognised ability on the part of participants to deem a DLT system (and relevant digital assets) to be located in a particular place, that would have important implications, in particular, for the rules on forum/jurisdiction, many of which are concerned with identifying the place where a thing is located or where an event took place. However, it would, we believe, be novel for parties to be able, by mere agreement, to deem a thing to be located in a particular place and thus require the law to give effect to a legal fiction as to its location.

- 5.5 Properly understood, despite the reference to *situs*, the concept of an elective *situs* is not concerned with location at all. It refers to the system of law chosen by the network participants for the DLT system to govern proprietary issues affecting the digital assets recorded in the system. As noted in the 2018 Report,²⁰ the label “elective *situs*” is used to preserve an analogy with the *lex situs* conflicts rule. In substance, however, it means a chosen governing law.

Permissioned DLT systems

- 5.6 As noted earlier, in permissioned DLT systems, only authorised participants are able to create records and verify changes to the ledger. Participants may perform only specific actions for which authority has been granted to them, and they are usually required to identify themselves. The financial markets are the most likely context in which permissioned DLT systems will arise, including in the context of innovation by incumbent and new FMIs. Further, the regulated context of the financial markets means that, as at today’s date, permissioned systems predominate over permissionless systems.
- 5.7 An FMI may create on-platform or “native” tokens recorded in a permissioned DLT system, which are designed to have a particular economic value or utility in themselves. For example, an FMI may create its own native tokens taking the form of “stablecoins”, cryptocurrencies or other digital settlement assets which are not linked tokens, which are used to settle payment or other obligations owed between its participants. In this way, the transfer of the stablecoin or other token from one participant to another participant may be treated as the performance of (and as discharging) a contractual obligation owed by that participant to the other participant in accordance with the contract between the parties (or their principals).
- 5.8 The proper law of the relevant contractual obligation may well have been expressly chosen, and it is to be expected that a court hearing a dispute about contractual performance would typically apply that law (as the English courts would, on well-established principles). As described in paragraph 4.4, it is possible that the majority of transactions involving participants of permissioned DLT systems can be resolved as a matter of contract law (on the basis of the multipartite contract between the participants) and not necessarily encounter the uncertainties considered in this paper in relation to property disputes or the *ex ante* steps that must be taken to “perfect” or otherwise give third party effects to rights or interests in or in relation to a native token under a transaction relating to the token.
- 5.9 Nonetheless, issues of a proprietary nature relating to transactions in the native tokens may arise which may affect outcomes as noted in paragraphs 4.4, 4.5 and 4.6. These proprietary issues could in principle be governed by a law other than the proper law of the contract between the participants in the DLT system.
- 5.10 We remain of the view that, in such a case, the English courts should apply an elective *situs* rule to determine the property law issue. Such a rule would support DLT-based innovation in the financial markets and facilitate the use of digital assets as collateral by FMIs, their participants and/or others in the financial markets, by

²⁰ Para 6.5.

enhancing legal certainty. This is consistent with the approach to existing systemically important FMI systems, including payment systems and securities settlement systems operated by central securities depositories, which are "designated" (for systemic reasons) under the SFRs. As foreshadowed earlier, under regulation 24 of the SFRs, upon the opening of insolvency proceedings against a participant in a designated system, any question relating to the rights and obligations arising from, or in connection with, that participation is required to be determined in accordance with the law chosen by the participants to govern the system. Any such determination in accordance with the selected governing law (including one which gives effect to the contractual or other "default arrangements" of the system) will, in accordance with regulation 24, be effective against and binding upon the insolvency office-holder of the participant, any creditor of the insolvent participant and any other third party claiming an interest in or in relation to (a) any rights of the participant arising from, or in connection with, its participation, or (b) any other assets of the participant subject to the obligations of the participant arising from, or in connection with, such participation.²¹

- 5.11 When FMIs design the rules, procedures and other standardised arrangements for a permissioned DLT system, they should consider what law may be applicable to contractual, non-contractual and proprietary rights, obligations and liabilities arising from the system. Being able to select a single law to govern, universally and exclusively, the relationships between participants *inter se*, the relationships between participants and the FMI, and the proprietary effects of a participant's holding of digital assets, participants can assess the risks and potential liabilities associated with their participation with greater certainty. They will be able to do so by reference to a single, ascertainable governing law, which is familiar to the participants, and which is regarded by them as having consistent and predictable effects. Similar benefits apply for those who take the digital assets recorded in the system as collateral.
- 5.12 The proposition that property disputes should be governed by the chosen law of the system is not uncontroversial. There is a respectable counter-argument that, while a choice of law should carry the day in contract law for the simple reason that the contracting parties have agreed to be bound by it, it is wrong in principle to extend the reach of the chosen law to third parties who have made no such agreement. Nevertheless, we consider that a failure to give effect to a chosen law of the system in the context of proprietary disputes risks impeding the safe, efficient and effective operation of permissioned DLT systems by FMIs, and the liquidity of the digital assets issued, held and transferred by means of those systems. This is for a number of reasons.
- 5.13 First, there will be material concerns for participants in permissioned DLT systems (and non-participant collateral-takers) of the unexpected application of a different law to govern their title to a digital asset in the system, particularly in the context of taking digital assets as collateral.
- 5.14 If the law applied to resolve proprietary issues differs from the law expressly designated as such in that system, neither the FMI nor its participants will be able, readily and with certainty, to determine whether issues or transfers of digital assets, or other proprietary transactions effected through the permissioned DLT system, will be valid and effective so as to be binding upon, and good against, third parties. The FMI, its participants and non-participants as collateral-takers would also be unable readily to determine the perfection or priority requirements applicable to any collateral arrangement over digital assets recorded in the permissioned DLT system. This, in turn, is likely to impede the effective and efficient operation of the

²¹ See paras 4.4 – 4.5 and 6.4 of the 2018 Report for further commentary on the position for intermediated securities and the so-called PRIMA principle.

permissioned DLT system by the FMI and undermine confidence in the system by preventing the FMI, the participants and collateral-takers from assessing, with a sufficient degree of certainty, the risks and potential liabilities they may face through their participation or (as non-participants) taking a collateral or other interest in or in relation to digital assets recorded in the system.

- 5.15 Secondly, it may be difficult for an operator of a permissioned DLT system to obtain legal opinions or analyses concerning the proprietary effects of transactions in digital assets by means of that system.
- 5.16 By applying the law expressly designated as governing participation in the DLT system, the operator (and, if relevant, the participants) will be able to obtain well-reasoned independent legal opinions and analyses from expert counsel in the jurisdiction of the expressly-designated law of the system, which support the legality, effectiveness and enforceability of the arrangements for the issue and transfer of digital assets in property law, as well as any collateral arrangements over such digital assets. This necessary process would be impeded by any need to consider multiple potentially applicable laws, dependent on features of the particular parties to the transaction and/or of the transaction itself.
- 5.17 It is important to bear in mind that, if the application of a different governing law resulted in the invalidation of a single transfer of a digital asset (for example, because that law declined to recognise the transfer mechanism of the DLT system as valid and effective to transfer title to the digital asset), this could call into question the integrity and finality of all subsequent transfers of the relevant digital asset through the system (even if each subsequent transfer were valid and effective according to the law that governed them). This would be the case if, upon a proper analysis of the transfer mechanism, the title to the asset of each subsequent transferee is considered to derive from the title of the transferee under the initial (invalid or ineffective) transfer.
- 5.18 This concern is particularly acute for FMIs operating DLT systems who are in-scope for the purposes of the CPMI-IOSCO Principles for Financial Market Infrastructures (the “**PFMIs**”), whose supervisory authorities are likely to expect the FMI to be able to obtain such legal opinions and analyses. Principle 1, Key Consideration 3 of the PFMIs requires an FMI to be able to articulate the legal basis for its activities to relevant authorities, participants and (where relevant) participants’ customers in a clear and understandable way. An important method of achieving this, as set out in paragraph 3.1.3 of the PFMIs, is for the FMI “*to obtain well-reasoned and independent legal opinions or analyses*”. In addition, without these opinions or analyses, it is difficult to see how an FMI operating a DLT system would be able to assure itself that it has a well-founded, clear and enforceable legal basis for each material aspect of its activities in accordance with Principle 1.
- 5.19 Thirdly, as a practical matter, orders of a court or jurisdiction, which apply a law other than the one expressly adopted by participants in a permissioned DLT system, may be of little or no practical effect. This is for the following reasons.
- 5.20 The application of an elective *situs* test would give effect to the law that has been accepted for that purpose by participants in that system. As rightly recognised by the UNIDROIT Principles, a person who transfers, acquires or deals in digital assets within a particular DLT system must be taken to accept the applicable law designated by the DLT system. Further, as the operational process for any update to the ledger (so as to effect a transfer of legal title by a state change on the ledger) is an intrinsic part of the transferable digital asset itself, the law chosen by the participants to govern that transfer process “attaches” to the asset and travels with it so as to bind any person (whether a participant or non-participant) taking an interest in the asset. Participants in the system and those claiming any such interests in those digital assets can therefore be expected to comply with orders of the courts that involve the application of that law.

- 5.21 In this regard, it is worth considering the position of validating node operators ("VNOs"). VNOs are responsible for discharging functions operating as part of the consensus mechanism used to validate transactions in certain DLT systems. These VNOs will have an overriding economic self-interest to operate this mechanism (which serves as the means by which transfers are effected through the system) exclusively in accordance with the law which they have accepted as governing their functions in connection with the system. A failure to do so would undermine the predictable and safe operation of the relevant DLT system which, in turn, is likely adversely to affect the value of the cryptoassets recorded in that system.
- 5.22 A court order purporting to apply a different law may, therefore, be met (indeed, is likely to be met) by non-compliance on the part of the VNOs. In that event, it must be recognised that there would be real practical difficulties (to say the least) in giving effect to the court order, assuming that the majority of the VNOs are not located in a single sovereign jurisdiction and are not, therefore, subject to the *in personam* enforcement jurisdiction of the court in question. Given the need for consensus on the part of a sufficient number of VNOs, there would appear to be no practical means to compel compliance with the court order in such circumstances.
- 5.23 Even if, for example, a court were able to direct the software developers of a DLT system to write new code to record a party on the distributed ledger in accordance with the proprietary rules of a different legal system (for example, the law of the location of the software developers or of the transferor), there would still be no means to compel the VNOs participating in the consensus mechanism to validate, accept and effect an update to the ledger in respect of any transaction subsequently input to the system by the new "owner".
- 5.24 An order of a court is, therefore, most likely to be effective, and to command the requisite consensus, where it is made in accordance with the proprietary rules of the legal system that the participants in the system have accepted.

Digital assets on permissionless DLT systems

- 5.25 The need for clarity and certainty as to the legal system that will determine the existence or otherwise of property rights (including the relevant rules determining perfection, priority, innocent acquirer or other proprietary issues) is no less important in the case of a permissionless DLT system.
- 5.26 However, it is in principle less likely that such a system will contain a choice of governing law. A permissionless system is unlikely to have a single operator able to establish multilateral rules, standards and other arrangements and is more likely to have a decentralised governance structure. By its very nature, it is possible (subject to the point made below) that the participants in such a system may be less likely to favour the inclusion of a chosen governing law and, even if the position were otherwise, it may be a more complex question to determine whether the participants could be said to have evinced an intention to select a single governing law. In principle, it might be possible for a choice of governing law to be included within a new permissionless DLT system at the time of its initial creation or for new code to be written for an existing permissionless DLT system that includes in each update to the blockchain a new "constitution" specifying a governing law to determine proprietary issues affecting relevant digital assets recorded in the system. However, we are not aware of any widely-used permissionless DLT system to date which includes a choice of governing law.
- 5.27 That said, there is no reason to exclude the possibility of future permissionless systems adopting a chosen governing law. If that were to occur, it would be appropriate for the English courts to give effect to that chosen law.
- 5.28 This would enable permissionless systems to achieve similar objectives as canvassed above in terms of clarity, certainty, the availability of legal opinions and

analyses and court orders which are likely to be accepted by the participants because they are the product of the law which the DLT system has specified.

- 5.29 Indeed, we agree with the approach of UNIDROIT that giving effect to a chosen governing law provides “an incentive for those who create new digital assets or govern existing systems for digital assets to specify the applicable law” in the digital asset or the relevant system.²²
- 5.30 It is however necessary, in the case of a permissionless DLT system, to cater for the situation (currently widespread) where no governing law has been designated.
- 5.31 Although a number of decisions of the English courts since the 2018 Report have touched on this issue, they have generally done so in the context of jurisdiction challenges where it has not been necessary for a final conclusion to be reached on the governing law for property law issues affecting the relevant digital assets. The provisional and tentative views expressed by the courts to date indicate, in our view, that the question of governing law continues to raise real problems of legal uncertainty. We do not consider that the basic principles of English private international law provide a sufficiently clear or satisfactory basis for deriving a conflict of laws rule that would govern the incidence of property rights in respect of digital assets. This is not the fault of the English principles but is a function of the fact that, as UNIDROIT rightly pointed out, the usual connecting factors for choice-of-law rules, such as the location of persons, offices, activity or assets, usually have no useful role to play and indeed will often be “incoherent and futile”, simply because digital assets are intangibles without any physical situs.
- 5.32 In our view, therefore, the problem of legal uncertainty in connection with the governing law for proprietary issues affecting a digital asset in a permissionless DLT system (or in a permissioned DLT system which lacks a chosen governing law) can best be solved by the creation of a new governing law rule enacted through legislation.

A new statutory rule

- 5.33 From the point of view of the financial markets, the overriding consideration is that a new statutory governing law rule should be clear and capable of being administered consistently and reliably in practice. The precise content of the rule is secondary to this overriding consideration.
- 5.34 The rule should apply to permissioned and permissionless systems alike. This is consistent with principles of technological neutrality and avoids the risk that the application of the rule is hidebound by categorical distinctions (permissioned/permissionless) which may in future reduce in importance or disappear altogether.
- 5.35 For the reasons given above, we consider that the starting point for the rule should be that effect will be given to a chosen law specified in the system or (if different) the digital asset itself (the latter taking priority on the basis that the more specific rule takes priority over the more general). We do not consider that this should be subject to any override or escape clause by reference to other possible connecting factors. Any override provision would undermine the legal certainty which the primary rule is intended to bring about. It cannot, of course, be excluded that a chosen law may be liable to be overridden by compelling considerations of the public policy of the forum.
- 5.36 Thereafter, we consider there is much to be said for the structure adopted by UNIDROIT in setting out a “waterfall” of rules, to cater for the very real risk that,

²² UNIDROIT Principles, para 5.4.

in view of the variety of DLT systems that may come before the courts, one or other sub-rules may prove difficult or impossible to apply in a given case.

- 5.37 We would suggest that the second stage in the waterfall, in the absence of a chosen law, should be that, if there is an operator or other central administrator of the DLT system in which the digital asset is recorded, the law of the country or territory in which that operator or administrator has its registered office or other statutory seat, provided that the registered office or statutory seat is readily ascertainable.
- 5.38 This involves a departure from UNIDROIT's Principles, whose second stage refers to the "issuer" of the digital asset rather than the operator of the system. UNIDROIT defines the "issuer" as the legal person who put the digital asset in the stream of commerce for value and identifies itself as such in a way that is readily ascertainable by the public. Our rationale for preferring the location of the operator or administrator is that, where such an entity exists (which is most likely to be in a permissioned system), the operator or administrator is likely to reserve the power to amend or correct the ledger through use of a "master node" or "master key". If a decision regarding proprietary rights is made in accordance with the law of the country in which the operator or administrator is located (in the absence of a chosen law), this is likely to promote the prospect of the operator or administrator complying with any order requiring an amendment or correction of the ledger.
- 5.39 Our proposed third stage is the law of the country or territory in which the issuer of the digital asset has its registered office or other statutory seat. This reflects UNIDROIT Principle 5(1)(c).
- 5.40 We recognise that the second and third stage are most likely to be applicable to a permissioned rather than a permissionless system, because, as described in paragraph 5.26, permissionless systems are significantly less likely, in principle, to have an identifiable central administrator or issuer due to their more decentralised governance structure when compared to permissioned systems. It is therefore important that the waterfall provide for further fallback sub-rules.
- 5.41 We consider that the fourth stage should be the law of the country which was the location of the person last known to have controlled the relevant private key or (if that person cannot be ascertained) where the last known transferor of the relevant digital asset was located.
- 5.42 Three points about this sub-rule require further explanation. First, the sub-rule refers to the location of a person. Location in this context could mean (a) domicile, (b) habitual residence or (c) actual location at the time of the transfer. These are, self-evidently, different concepts and there is room for reasonable disagreement as to which concept is best suited. For example, domicile may be the most readily ascertainable, at least in the case of legal persons, but may have only a remote connection to the subject matter of the dispute. A test of habitual residence may be said to involve evaluative judgments and be less certain. The actual location of a person at a given point in time is a straightforward question of fact, but the downside is that it may be transient and therefore arbitrary, and ascertaining the factual position is far from straightforward. It may be that a "mini-waterfall" is required which establishes a primary test (possibly habitual residence), with the actual location becoming relevant only if the answer to the primary test cannot readily be ascertained.
- 5.43 Secondly, the sub-rule refers first to the person who controls the relevant private key and, as a fallback, to the transferor of the digital asset. The concept of the controller of the relevant private key could be said to raise a legal issue as to what is meant by control. It would obviously be undesirable if a sub-rule, intended to identify the governing law, had embedded within it an anterior legal question as to what is meant by control. In our view, however, the concept of control here must be regarded as an essentially factual one. Alternatively, insofar as it raises legal

questions, the English court would be expected to apply English law concepts of control, as part of the law of the forum.

- 5.44 It might be objected to this sub-rule that the controller of the key or the transferor in question may be someone who is alleged to be illegitimately in control of the key or an illegitimate transferor. However, we consider that it would be unnecessarily complex for the identification of the governing law to depend on questions of "legitimacy" that may themselves be hotly disputed and require further anterior questions of fact and law to be resolved before the governing law can be ascertained.
- 5.45 Thirdly, the sub-rule refers to the "last known" person. This recognises the fact that the identity of the relevant controller or transferor may not be ascertainable, from which it necessarily follows that their location will be unascertainable as well. The sub-rule caters for this by enabling reliance to be placed on the location of the last known controller or transferor.
- 5.46 This sub-rule should be seen as a last resort, because it is likely to be less easily ascertained in practice. For example, where an agent acts on behalf of a principal who has factual control of the asset, the location of the principal may not be evident or apparent to a third party dealing with the agent, particularly as they may not even know they are dealing with an agent. Furthermore, a sub-rule of this kind is liable to lead to different laws governing the proprietary effects of different transactions within the same DLT system, which is inherently undesirable from the point of view of certainty and practicality.
- 5.47 Nevertheless, a rule of last resort is unavoidable given the serious prospect that certain DLT systems may lack any chosen law and lack an operator or issuer whose identity and location is publicly ascertainable. A legislative governing law rule would fall far short of its purpose if it failed to cater for that scenario.
- 5.48 We raise, if only to dismiss, the possibility that the fourth stage should instead take account of the law of the jurisdiction in which the person bringing the relevant claim (who will often be the purported transferee) is located; or that there should be a fifth stage to this effect. We consider that the location of the claimant, without more, has an insufficient connection with the subject matter of the claim to justify treating it as determinative of the governing law. Furthermore, there may be an element of moral hazard in defaulting to the law of the claimant's home country, in that this would incentivise the claimant to argue that it is impossible to ascertain the governing law by reference to any of the earlier stages of the waterfall.
- 5.49 The effect of the proposed statutory rule would be to allow an elective *situs* test to determine the governing law for proprietary issues relating to digital assets recorded in both permissioned and permissionless DLT systems, where this is expressly chosen and specified in the digital asset itself or the DLT system. In the absence of any such election, another test would apply. The proposed rule therefore recognises the benefits of – and gives priority to – elective *situs* where the participants, exercising party autonomy, have made an election, while still providing for situations where elective *situs* is not available.
- 5.50 Such a rule thus offers the legal certainty that is crucial to the safe and efficient operation of systemically important DLT systems (such as those that are likely to be employed by FMIs), while still accommodating current and prospective permissionless DLT systems which lack an expressly designated governing law.
- 5.51 As already noted, the rule, in affording primacy to a chosen law, may also serve to encourage developers and operators of, and participants in, permissionless DLT systems to specify the law governing such DLT systems, on the basis that the enhanced legal certainty of such an approach promotes the protection of the economic interests of investors and may in turn enhance the liquidity and thus the value of their digital assets.

6. Jurisdiction

- 6.1 This section expands on our recommendations in the 2018 Report by considering the impact of our recommendation of a new statutory governing law rule on the rules on forum/jurisdiction in relation to proprietary claims in respect of digital assets.
- 6.2 The question of governing law is distinct from that of jurisdiction. That said, in the context of claims about conventional forms of property (and associated proprietary rights), the rules for determining governing law and jurisdiction both tend to focus upon the territorial location of the assets in question. We consider it beneficial for any development in the rules for determining governing law in respect of digital assets to be similarly aligned to those for determining jurisdiction, not least because (generally speaking) local courts may be best placed to apply local law.
- 6.3 The Call for Evidence has provided a detailed and helpful analysis of jurisdiction in the context of digital assets. To avoid duplication, and consistent with the scope of the rest of this paper, our analysis is therefore limited to the gateways most applicable to the application of jurisdictional rules in the context of disputes involving proprietary issues arising from transactions in digital assets, namely gateway 11 (property) and gateway 15(b) (constructive or resulting trustees).

The current gateways

- 6.4 The Call for Evidence provides an overview for each of gateway 11 (property)²³ and gateway 15(b) (constructive or resulting trustees)²⁴ which we do not seek to repeat in this paper.
- 6.5 Both gateways permit the courts of England and Wales to take jurisdiction in respect of claims relating to property / assets which are located within England and Wales.
- 6.6 As noted in paragraph 5.1 above, the decentralised nature of DLT systems presents challenges in determining the location of the property / asset, as the ledger may not be located in a single country and may have simultaneous and equally valid connections to a large number of jurisdictions.²⁵
- 6.7 As the Call for Evidence²⁶ points out, the application of the current gateways to claims concerning digital assets has arguably resulted in the application of the relevant gateways in ways that are potentially distorted, sometimes in circumstances where it is not clear whether the causes of action to which the gateways were applied would actually arise on the facts pleaded. In particular, the current case law regarding determination of location of on-platform digital assets for the purpose of determining jurisdiction is inconsistent.²⁷ Given the novel features of digital assets, and the circumstances in which those claims are generally brought (as noted in the Call for Evidence), that is not perhaps surprising.
- 6.8 The result is that, notwithstanding the best efforts of the courts, the application of the gateways to digital assets remains uncertain.

²³ Call for Evidence, paras 4.59-4.62.

²⁴ Call for Evidence, paras 4.63-4.67.

²⁵ See also Call for Evidence, paras 5.83-5.98.

²⁶ Call for Evidence, paras 4.100-4.112.

²⁷ Call for Evidence, paras 5.86-5.95.

A new jurisdictional gateway

- 6.9 As with governing law, the financial markets would benefit from legal certainty as to the determination of jurisdiction for proprietary disputes concerning digital assets. In order to avoid the issues arising in the current case law, we recommend that a new gateway should apply to such disputes which does not look to the location of the asset / property.
- 6.10 Instead, we propose that a new gateway is introduced which applies to claims which relate wholly or principally to digital assets on permissioned and permissionless DLT systems.
- 6.11 We propose the new gateway should apply where (i) there the digital asset or (failing that) the DLT system contains an express election in favour of the jurisdiction on the courts of England and Wales or (ii) in the absence of an express election, the governing law of the claim would, pursuant to the “waterfall” in the proposed statutory governing law rule described in section 5 above, be the law of England and Wales. This approach would be consistent with the approach taken by existing gateways allowing for the courts of England and Wales to accept jurisdiction over claims governed by the law of England and Wales, such as for claims concerning contracts (gateway 6(c)), torts (gateway 9(c)), express trusts (gateway 12), constructive or resulting trustees (gateway 15(c)), fiduciary duties (gateway 15B(c)) and restitution (gateway 16(c)).
- 6.12 Such a gateway would take as its starting point the relevant parties’ election as to jurisdiction, or failing that, applicable law and, to the extent there is no such election, would take advantage of the greater certainty engendered by the proposed new statutory governing law rule.

7. Conclusion

- 7.1 The problem of legal uncertainty in identifying the governing law of proprietary claims in respect of digital assets can best be resolved by statutory intervention. Our proposed statutory rule would give primacy to the system of law specified in a digital asset or in the DLT system. Absent a choice of law, the rule would establish a waterfall that would enable the governing law to be identified with sufficient certainty in most cases.
- 7.2 We also propose a new jurisdictional gateway whereby the courts of England and Wales would have jurisdiction to determine proprietary disputes in relation to digital assets where (i) the digital asset or DLT system contains an express election in favour of the jurisdiction on the courts of England and Wales or (ii) in the absence of an express election, the governing law of the claim would, pursuant to the proposed statutory rule, be the law of England and Wales.

Appendix 1

Extract from the UNIDROIT Principles on Digital Assets and Private Law²⁸

Principle 5

(1) Subject to paragraph (2), proprietary issues in respect of a digital asset are governed by:

- (a) the domestic law of the State expressly specified in the digital asset, and those Principles (if any) expressly specified in the digital asset; or, failing that,
- (b) the domestic law of the State expressly specified in the system on which the digital asset is recorded, and those Principles (if any) expressly specified in the system on which the digital asset is recorded; or, failing that,
- (c) in relation to a digital asset of which there is an issuer, including digital assets of the same description of which there is an issuer, the domestic law of the State where the issuer has its statutory seat, provided that its statutory seat is readily ascertainable by the public; or
- (d) if none of the above sub-paragraphs applies:

OPTION A:

- (i) those aspects or provisions of the law of the forum State as specified by that State;
- (ii) to the extent not addressed by sub-paragraph (d)(i), those Principles as specified by the forum State;
- (iii) to the extent not addressed by sub-paragraphs (d)(i) or (d)(ii), the law applicable by virtue of the rules of private international law of the forum State.

OPTION B:

- (i) those Principles as specified by the forum State;
- (ii) to the extent not addressed by sub-paragraph (d)(i), the law applicable by virtue of the rules of private international law of the forum State.

(2) In the interpretation and application of paragraph (1), regard is to be had to the following:

- (a) proprietary issues in respect of digital assets, and in particular their acquisition and disposition, are always a matter of law;
- (b) in determining whether the applicable law is specified in a digital asset, or in a system on which the digital asset is recorded, consideration should be given to records attached to, or associated with, the digital asset, or the system, if such records are readily available for review by persons dealing with the relevant digital asset;
- (c) by transferring, acquiring, or otherwise dealing with a digital asset a person consents to the law applicable under paragraph (1)(a), (1)(b) or (1)(c);

²⁸ The full principles are available at: <https://www.unidroit.org/wp-content/uploads/2023/04/C.D.-102-6-Principles-on-Digital-Assets-and-Private-Law.pdf>

- (d) the law applicable under paragraph (1) applies to all digital assets of the same description;
 - (e) if, after a digital asset is first issued or created, the applicable law changes by operation of paragraph (1)(a), (1)(b) or (1)(c), proprietary rights in the digital asset that have been established before that change are not affected by it;
 - (f) the 'issuer' referred to in paragraph (1)(c) means a legal person:
 - (i) who put the digital asset, or digital assets of the same description, in the stream of commerce for value; and
 - (ii) who, in a way that is readily ascertainable by the public,
 - (A) identifies itself as a named person;
 - (B) identifies its statutory seat; and
 - (C) identifies itself as the person who put the digital asset, or digital assets of the same description, into the stream of commerce for value.
- (3) The law applicable to the issues addressed in Principles 10 to 13, including whether an agreement is a custody agreement, is the domestic law of the State expressly specified in that agreement as the law that governs the agreement, or if the agreement expressly provides that another law is applicable to all such issues, that other law.
- (4) Paragraphs (1) and (2) are subject to paragraph (3).
- (5) Other law applies to determine:
- (a) the law applicable to the third-party effectiveness of a security right in a digital asset made effective against third parties by a method other than control;
 - (b) the law applicable to determine the priority between conflicting security rights made effective against third parties by a method other than control.
- (6) Notwithstanding the opening of an insolvency-related proceeding and subject to paragraph (7), the law applicable in accordance with this Principle governs all proprietary issues in respect of digital assets with regard to any event that has occurred before the opening of that insolvency-related proceeding.
- (7) Paragraph (6) does not affect the application of any substantive or procedural rule of law applicable by virtue of an insolvency-related proceeding, such as any rule relating to:
- (a) the ranking of categories of claims;
 - (b) the avoidance of a transaction as a preference or a transfer in fraud of creditors;
 - (c) the enforcement of rights to an asset that is under the control or supervision of the insolvency representative.

FMLC Members

Lord Thomas of Cwmgiedd (Chair)

Kate Gibbons (Deputy-Chair)

Andrew Bagley, Goldman Sachs International

Sir William Blair, Queen Mary, University of London

Claude Brown, Reed Smith LLP

Raymond Cox KC, Fountain Court Chambers

Simon Firth, Linklaters LLP

Jonathan Grant, Bank of England

Carolyn H. Jackson, Katten Muchin Rosenman U.K. LLP

Peter King, HM Treasury

Sir Robin Knowles CBE

Ida Levine, Impact Investing Institute

Karen Levinge, Financial Conduct Authority

Jon May, Marshall Wace LLP

Chris Newby, AIG

Conall Patton KC, One Essex Court

Jan Putnis, Slaughter and May

Barnabas Reynolds, Allen Overy Shearman Sterling LLP

Claire Schrader, Lloyd's of London

James Smethurst, Freshfields Bruckhaus Deringer LLP

Tom Smith KC, 3-4 South Square

Sanjev Warna-kula-suriya, Latham & Watkins LLP

Brian Gray (Chief Executive)

Registered Charity Number: 1164902.

"FMLC" and "Financial Markets Law Committee" are terms used to describe a committee appointed by Financial Markets Law Committee, a limited company ("Company"). Registered office: 3rd Floor, North Wing, Guildhall, London EC2P 2EJ. Registered in England and Wales with number: 8733443

Submitted to Law Commission Call for Evidence on digital assets and ETDs in private international law
Submitted on 2024-05-16 23:53:21

About you

What is your name?

Name:
Dr Lorna Gillies

What is your email address?

[REDACTED]
[REDACTED]

What is your telephone number?

[REDACTED]
[REDACTED]

Questions on international jurisdiction - specific issues (Chapter 5)

Question 1: In this question, we seek views and evidence on jurisdiction over consumer contracts.

Please share your views and evidence below::

1. Jurisdiction may be accommodated depending on:

(i) whether such contracts fall within the definition of a consumer contract under the Civil Jurisdiction and Judgments Act 1982 Act. Recent cases such as Dooley (2022 EWCA Civ 1569) and Soleymani v Nifty (2022 EWCA Civ 1297) indicate that the English court continues to consider CJEU cases on the scope and purpose of the consumer jurisdiction rule;

(ii) if the consumer is able to establish the identity of the business and its location to establish whether it is situated in a different part of the UK, has a branch in a part of the UK or is situated outside the UK (see response to Q2, below).

Furthermore, s.15B(7) 1982 Act may be significant if a consumer dispute arises from the operations of a UK-based branch of a non-UK domiciled business.

2. Yes with two caveats:

(i) provided the definition of a crypto-business falls within the scope of a consumer contract in the 1982 Act, which will be fact dependent,

(ii) if such a business is selling/acquiring crypto-currencies, such a business would require to be domiciled in part of the UK (s.42 1982 Act) and subject to rules of establishment either under UK AML and/or EU MiCA or other non-EU AML regulation(s) as applicable to the facts in dispute, and

(iii) as above for Q1, s.15B(7) 1982 Act may have a role to play where a dispute arises from the operations of a crypto-business's branch based in the UK.

3. The directing activities concept may benefit from further clarity as to its application to decentralised technologies, to support courts in interpreting this fact based concept.

4. Whilst I am not in practice, I envisage two issues (i) determining the establishment of crypto-business and (ii) suitability of the directing activities concept to decentralised technologies.

Question 2: In this question, we seek views and evidence on jurisdiction founded on the basis that a contract was concluded in England and Wales.

Please share your views and evidence below::

1. The court may take account of the recommendations of the Law Commission's report on Smart Contracts (2021). It focusses on the conduct of the parties when entering into a smart contract. The smart contract may be still be binding irrespective of whether the parties are identifiable or not. As a minimum, the connecting factor should be the place where the contract was made or acceptance of offer received by the real world actor. This would fall in line with CPR PD6B. The 'participating computer' should not be used as a connecting factor for jurisdiction of itself, or as a deemed branch or agent. An analogy can be drawn with the concept of the special jurisdiction of 'branch, agency or other establishment' in Art 7(5) Regulation EU 1215/2012 (previously Article 5(5) Regulation EC 44/2001). When the 2001 Regulation was being drafted, I argued at the time that the location of a web server should not be regarded as a branch, agency or other establishment for the purposes Art 5(5).

2. Following the response to Q1 above, to fall in line with CPR PD6B the connecting factor for jurisdiction should either the place where the contract is made or accepted, per above.

3. Whilst I am not a practitioner, I would suspect not as parties are likely to agree a jurisdiction and/or arbitration of their smart contract. However, this may cause problems for consumers in the context of arbitration agreements (Soleymani, above).

4. Whilst I am not a practitioner, it is anticipated that the question of where a smart contract is made is a question of material validity. Such questions are

determined by the putative applicable law of the contract (Article 10, Rome I Regulation EC 593/2008). Smart contracts will increasingly contain an applicable law clause. If the matter is brought before the English courts, the applicable law will be determined by Article 3 or 4, or Article 6 for consumer contracts (Rome I). If the applicable law is English law, then as above the connecting factor is proposed to be the place where the contract was made or acceptance of offer received by the real world actor.

Question 3: In this question, we seek views and evidence on jurisdiction founded on the basis that damage or detriment was suffered in England and Wales.

Please share your views and evidence below::

1. In so far that the question is concerned with damage arising from a crypto-asset as a intangible property, I agree with Professor Dickinson's view applied in *Ion Science Ltd v Persons Unknown* (2020, unreported), *Osbourne v Persons Unknown* [2023] EWHC 33, Dicey and Morris, 16th ed, para 23.50 and *Tulip Trading v Bitcoin Association for BSV* [2023] EWCA Civ 83 that the *lex situs* of damage or detriment is the place where the owner of the crypto asset is 'resident'. Residence is a connecting factor used to determine domicile of individuals for the purposes of the Civil Jurisdiction and Judgments Act 1982 ss.41(2)-(4). The approach of the Court of Appeal in *Tulip Trading* will be relevant in determining the extent of a fiduciary duty owed by software developers to owners of crypto-assets.

2. Pure economic loss requires intention which may be challenging to definitively establish in cases where the defendant is unknown. It may be useful to contrast with *NZ* e.g. *Singh v Patel & Elite Business Service NZ Ltd* [2020] NZHC 2242 and [2021] NZCA 242 considered by Jessica Lai in 2022 (6) JBL, 529-546 at 534 citing the Appeal Court in *Singh* and Professor Green's paper in 2008 71(1) MLR.

If pure economic loss cannot be applied, then per *AA v Persons Unknown* [2019] EWHC 3556, one option may be adaptation of the common law tort of conversion. The benefit of conversion as a remedy would be strict liability and a pragmatic recognition of the status of crypto assets. However, at present common law conversion requires possession of the intangible asset. If adopted, it would go beyond the Supreme Court's approach to intangible assets in *OBG v Allen* [2007] UKHL 21.

Another option may be to consider the role of the bailee and the concept of bailment in the Torts (Interference with Goods) Act 1977 as part of the emerging fiduciary duty of software developers in *Tulip* above. For example, in *Tulip* at para 48, the Court of Appeal referred to *Bristol and West v Mothew* 1998 Ch 1 per Millett LJ (at 18C) that a fiduciary owes obligations to another "because he is subject to" those obligations. The concept of 'incremental development' of the concept of fiduciary duty was also recognised in *Tulip*, at para 71.

A further option may be to apply constructive trust as an equitable remedy, in favour of the victim of fraud, following *Jones v Persons Unknown* [2022] EWHC 2543 (Comm) and as a jurisdictional gateway under CPR PD6B. Whilst these options may be beyond direct questions of jurisdiction and applicable law, they may be relevant to parties when deciding if the English courts and English law is selected as their agreed choice of forum and law.

3. Pure economic loss issues may impact jurisdiction and applicable law, both of which are concerned with claims for direct damage. This approach is to ensure consistency and predictability in determining 'litigation and transactional risk' (Fentiman, OUP, 2015) in cross-border cases and appears to work across different types of claims. Any change would need to be fully justified, logically consistent between jurisdiction and applicable law and attractive as a choice of forum and applicable law.

Jurisdiction is based on direct damage, not financial implications arising from the original harm; *C-364/93 Marinari v Lloyds Bank Plc* [1996] QB 217.

Applicable law for contractual obligations under EC Regulation 593/2008 (Rome I) applicable in the UK via SI 2019/834 is determined on the basis of either party choice of applicable law (Art 3) or the applicable law in the absence of choice (Art.4), unless the claim concerns a consumer contract and Art 6 may apply.

Applicable law for non-contractual obligations is also limited to claims for direct damage through Regulation EC 864/2007 (Rome II) applicable in the UK via SI 2019/834; *Bourlakov v Bourlakov* [2022] EWHC 1269 (Ch) at para 228, referring to *C-220/88 Dumez France SA v Hessische Landesbank* [1990] ECR I-49 at para 20 and *London Helicopters Ltd v Heliportugal LDA-INAC* [2006] 1 CLC 297 at p.305H; *C-350/14 Lazar v Allianz SpA* [2016] 1 WLR 835, para 25.

Question 4: In this question, we seek views and evidence on jurisdiction founded on the basis that an unlawful act was committed in England and Wales.

Please share your views and jurisdiction::

1. I think the three-step approach to establishing jurisdiction is theoretically sound and ensures consistent and predictability of result; *Tulip Trading*, above at para 4.

2. Whilst I am not a practitioner, regardless of the number of cases there should be consideration of the effect of unlawful acts on the claimant's ability to request permission to serve out of the jurisdiction and to ensure the choice of English law equips parties with sufficient protection from such acts.

Question 5: In this question, we seek views and evidence on jurisdiction founded on the basis that the claim relates to objects within England and Wales.

Please share your views and evidence below::

1. I refer to my answer to Q4(1) above.

2. The relevant point in time is the date of the application for request to serve proceedings out of the jurisdiction; CPR PD6B para 3.1. This point was considered by Mr Justice Lavender in *Osbourne v Persons Unknown* [2023] EWHC 39 (KB), at paras 30-38 and discussion at para 36 in particular. For Gateway 15(b), being a claim for assets contained in the jurisdiction, the asset must have been in the jurisdiction at the time before the justiciable act occurred; *Fetch.ai v Persons Unknown* [2021] EWHC 2254 (Comm) per HHJ Pelling KC at para 35. Transferring the assets had the effect of placing them in

constructive trust and the defendants as constructive trustees.

In *Osbourne*, Mr Justice Lavender made two points that should be considered further (i) the relevant point in time under para 3.1 of PD6B is the date of the application for permission to serve out of the jurisdiction, and (ii) the application to serve out may depend on whether the crypto asset was still in England or had been transferred outside the jurisdiction. At para 37, Mr Lavender referred to two cases which confirm that the Gateways are based on property situated within the jurisdiction (*Chellaram v Chellaram* [2002] EWHC 632) and are discretionary (*Pakistan v Zardari* [2006] EWHC 2411) with discretion operating to ensure exorbitant jurisdiction is not established in cases concerned with "easily moved assets"; *Pakistan v Zardari*, at para 159. Therefore, there should be guidance as to what would justify discretion in cases such as *Osbourne* where assets were moved out of England before the application to serve out was made to the court.

3. Whilst I am not a practitioner, as above the place where the crypto-token is located will be relevant for the purposes of requesting the court's permission application to serve out of the jurisdiction.

Question 6: In this question, we seek views and evidence on the types of claims and causes of action relied upon in applications to serve proceedings relating to crypto-tokens out of the jurisdiction.

Please share your views and evidence below::

1. Whilst the court in *Piroozzadeh* did not determine the question of serious issue to be tried, I refer to *AK Investment CJSC v Kyrgyz Mobil Tel Limited and Others* at para 71 which confirmed earlier authority that the 'serious issue to be tried' is one of three requirements for service out of a defendant. For a serious issue to be tried, there must be a "substantial question of fact or law, or both. The current practice in England is that this is the same test as for summary judgment, namely whether there is a real (as opposed to a fanciful) prospect of success." In my view, this is to ensure that the claimant is able to bring an application for service out for a matter that is not frivolous, vexatious or oppressive to the foreign defendant or the court.

2,3,4 - no view offered, as the questions suggest a practitioner response would assist.

Questions on applicable law - non-consumer contracts (Chapter 7)

Question 7: In this question, we seek views on applicable law and decentralised finance (DeFi).

Please share your views and evidence below::

1. I suspect contractual disputes concerning DeFi transactions, as well as other cases, will come before the courts before long. On DeFi, a 2022 paper by Nydia Remolina outlines the benefits and challenges, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4243544. Another paper from 2023, by Ellen Naudts from the European Central Bank identifies the benefits and risks of DAO (Decentralised Autonomous Organisations); available at <https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op331~a03e416045.en.pdf?ca341296edabc184a32dc15e30d3020b>. The benefits and challenges to both DeFi and DAOs require national and international coordination, hence the role for international private law.

2. Given the nature of such transactions, there might - or might not - be choice of court and choice of law agreements, as well as arbitration agreements, embedded in smart contracts used to execute transactions and/or in contracts between the parties to DeFi such as peers/users and app providers. So I think it would be worthwhile to consider the role, purpose and protective function of private international law and applicable law, particularly for weaker parties to such transactions. I refer to the Hague Conference's "Developments with respect to PIL Implications of the Digital Economy," Preliminary Document Rev No 4 of January 2022, para 19 at p.5, available at <https://assets.hcch.net/docs/b06c28c5-d183-4d81-a663-f7bdb8f32dac.pdf>.

3. Yes, and I think the relationship between the various UK regulators should form part of the discussion to ensure any party, including weaker parties, to such transactions are considered. I refer by analogy to the issues of data protection and competition regulation in *C-252/81 Meta v Bundeskartellamt* 04.07.2023.

Question 8: This question concerns the applicable law for non-consumer contracts.

Please share your views and evidence below::

1. I would say yes, provided that the contract involving crypto-tokens is expressed with reasonable certainty or in accordance with another option in Article 3 of Rome I. The choice must be that of a country/territorial legal system. Alternatively, if there is no choice of law selected then I envisage that the seller's habitual residence will apply (Art 4(1)). If the seller's habitual residence cannot be determined then Art 4(2) will apply the law of the characteristic performer's habitual residence. If that party is not identifiable, then the applicable law is the law manifestly more closely connected (Art 4(3)), failing which the law of the country most closely connected to the transaction (Art 4(4)).

2. I think my answer to Q1 above shows that there is wide scope for application of Rome I based on party choice or to determine the applicable law in the absence of choice.

3. The Question title refers to non-consumer contracts. I would suggest review of Article 6 as well.

4. I would be interested to read responses from practitioners to this question.

5. There would be the risk of legal uncertainty as to the scope of the applicable law and the practical effect on the parties rights, obligations, remedies and damages (Article 12), the validity of the contract (Articles 10 and 11) and of the role of the forum's mandatory rules and public policy (Articles 9 and 21 respectively).

Questions on applicable law - non-consumer contracts (Chapter 8)

Question 9: This question concerns the applicable law for consumer contracts.

Please share your views and evidence below::

1. Article 6 might apply provided (i) the Article 6 (1) criteria can be applied to such contracts and (ii) that such contracts are not classified as concerned with financial instruments so as to be excluded by Article 6(4)(d).
2. Article 6(4) may need to be revised if such contracts fall within the scope of the exclusion in Article 6(4)(d).
- 3, 4 and 5 - appear to be questions that are practitioner focussed.
6. I think in summary Article 6 could be problematic if either (a) the defendant business cannot be identified (b) the directing activities test cannot be sufficiently established e.g. *Khalifeh v Blom Bank* [2021] EWHC 3399 (QB) and *C-282/08/ C-144/09 Pammer and Alpenhof* 07.10.2010, and (c) or such contracts are classified as financial instruments and excluded by Article 6(4)(d).

Question 10: This question concerns the exclusions in Articles 6(4)(d) and (e) of the Rome I Regulation.

Please share your views and evidence below::

1. This would principally depend on the classification given to crypto-tokens by the lex fori. If the classification is one of property, then Article 6 might apply. If the classification is one of financial instrument, then Article 6(4)(d) might apply. A helpful summary on Cryptocurrencies and PIL Issues is provided by Francesca Villata, available at <https://brill.com/edcollchap-oa/book/9789004514850/BP000020.xml?language=en>, 07.11.2023.
2. It would be beneficial to have regard to the interpretation of Rome I Regulation from the CJEU where applicable.
- 3-6 - I would be interested to hear views from practitioners.

Questions on applicable law - torts and delicts (Chapter 9)

Question 11: We seek views and evidence on localising damage arising in tortious claims relating to crypto-tokens for the purposes of applicable law.

Please share your views and evidence below::

1. I think it is very likely that there will be claims in tort arising from crypto-token litigation and questions of applicable law will arise in the context of tortious claims. Whether such cases proceed to trial depends on the dispute in question and the certainty of English law as the applicable law.
2. If we are to take account of CJEU jurisprudence in the context of the Rome I Regulation and crypto-tokens, then I suggest consistency and apply CJEU jurisprudence for the Rome II Regulation as well, or at the very least be seen to have regard to it.

Question 12: We seek views and evidence on recourse to the “escape clause” in Article 4(3) of the Rome II Regulation.

Please share your views and evidence below::

For 1-3, the collective response is that Article 4(3) is of an exceptional nature. By way of example, *Fortress Value Recovery Fund I LLC v Blue Skye Special Opportunities Fund LP* [2013] 2 BCLC 351 per Flaux J at para 47 said Article 4(3) applies on an exceptional basis, and at para 74 “may involve focusing on the country in which “ the ‘puppet masters’ pulling the strings” ; *Avonwick Holdings v Azitio Holdings* [2020] EWHC 1844 (Comm) per Picken J observed at para 156 that the exception applies only where “the alleged wrongdoing “was planned, orchestrated and implemented,” Both cases were applied in *Commercial Bank PJSC v Shetty* [2022] EWHC 529 (Comm) at para 77. *W Nagel (A Firm) v Chaim Pluczenik, Pluczenik Diamond Company NV, Varda Shine* [2022] EWHC 1714 (Comm) at paragraph 93 also confirmed the exceptional nature of Article 4(3). Two fairly recent cases have applied Article 4(3): *O’Loan v Motor Insurers’ Bureau* [2021] 8 WLUK 313 applied Article 4(3) focussing on the centre of gravity of the tort. In *Silverman v Ryanair DAC* [2021] EWHC 2955 (QB) , Article 4(3) applied due to a choice of law in the particular contract.

Questions on applicable law - negotiable instruments, bills of lading, and the exclusions from the Rome Regulations (Chapter 10)

Question 13: We seek evidence, particularly from market participants, on how market practice in respect of bills of lading has been affected, or how it is likely to be affected, by the introduction of the Electronic Trade Documents Act 2023.

Please share your views and evidence below::

Question 14: We seek evidence on market sentiment relating to use of DLT platforms for electronic bills of lading.

Please share your views and evidence below::

Question 15: We seek evidence on the difficulties, if any, of incorporating the Hague-Visby Rules where an electronic bill of lading has been used.

Please share your views and evidence below::

Question 16: We seek evidence on market practice to help us identify where it could be said that an electronic bill of lading is “issued” for the purpose of the Hague-Visby Rules, as implemented in the UK by the Carriage of Goods Act 1971

Please share your views and evidence below::

Questions on applicable law - section 72 of the Bills of Exchange Act 1882 (Chapter 11)

Question 17: We seek views on the most appropriate connecting factor for determining where an electronic bill of exchange is “delivered to a first holder” for the purposes of section 72(1) of the Bills of Exchange Act 1882.

Please share your views and evidence below::

Question 18: We seek views on whether it would be desirable to have a single conflict of laws regime to cover all types of electronic trade documents that fall within the scope of the Electronic Trade Documents Act 2023.

Please share your views and evidence below::

Question on applicable law - property (Chapter 12)

Question 19: We seek views on the law applicable to property disputes in relation to digital assets and ETDs. Where possible, we ask that stakeholders contextualise their responses, for example, give details as to whether it relates to a pledge over an ETD or property entitlements in crypto-token litigation.

Please share your views and evidence below::

In response to Q3 above, I would suggest that there ought to be further consideration as to the conflict of laws and ETDs in the light of para 12.35-36 of the Call for Evidence which neatly summarises the purpose and socio-legal function of the *lex situs*.

Response Submitted by Dr Uglješa Grušić, Associate Professor, Faculty of Laws, University College London

Law Commission of England and Wales

Call for Evidence on Digital Assets and Electronic Trade Documents in Private International Law: Which Court, Which Law?

1. I am an Associate Professor in the Faculty of Laws at University College London. At UCL, I convene the LLB Conflict of Laws module and the Notarial Practice Course Private International Law module. Additionally, I teach on the LLM International Commercial Litigation module. I am a co-author of the 15th edition of *Cheshire North and Fawcett's Private International Law* (OUP 2017) and the author of two monographs in the field of private international law: *Torts in UK Foreign Relations* (OUP 2023) and *The European Private International Law of Employment* (CUP 2015). I have also authored or co-authored articles and contributions to edited collections in the field of private international law.¹
2. I am responding to Questions 1-5, 7-12 and 17-19 in the Call for Evidence. My response is divided into three parts. The first part focuses on jurisdiction. The second part addresses choice of law. The third part discusses several issues that digital assets raise within the third key component of private international law, recognition and enforcement of foreign judgments, which were not addressed by the Law Commission in its Call for Evidence.

1. Jurisdiction

3. This part of my response is divided into two sections. The first section addresses jurisdiction in general, focusing on Chapter 4 of the Call for Evidence. The second section deals with specific issues within the law of jurisdiction, focusing on Chapter 5 of the Call for Evidence.

1.1. Jurisdiction in General

4. The Law Commission's current thinking on jurisdiction, outlined in Chapter 4 of the Call for Evidence, revolves around three key ideas. First, that there is a tension between the territorial premise of the English² law of jurisdiction and the transnational or global nature of digital assets. However, this tension is less pronounced compared to the field of choice of law, as jurisdictional rules do not need

¹ My detailed profile and a list of my selected publications are available at <https://profiles.ucl.ac.uk/56546>.

² In this response, all references to "English law" should be read as references to "the law of England and Wales" and all references to "English courts" should be read as references to "the courts of England and Wales".

to single out one connecting factor that points only to one jurisdiction.³ Second, that the rules of jurisdiction in public international law regulate adjudicatory jurisdiction and that the exercise of adjudicatory jurisdiction should be consistent with public international law.⁴ Third, that English jurisdictional rules ought to be based on “justifiable”, “legitimate”, “appropriate” or “proper” jurisdictional grounds⁵ to facilitate the recognition and enforcement of English judgments abroad.⁶ There is a close connection between the second and third ideas, as English judgments are more easily recognised and enforced abroad if the English courts’ exercise of jurisdiction is consistent with public international law.

5. While I agree with the first key idea, the second and third key ideas raise some concerns.

1.1.1. Consistency with Public International Law

6. There is no consensus on whether and, if so, how public international law regulates adjudicatory jurisdiction. For instance, the drafters of the influential *Restatement of the Law (Fourth): The Foreign Relations Law of the United States* take the controversial position that “modern customary international law generally does not impose limits on jurisdiction to adjudicate”.⁷ According to the drafters, the only limit on adjudicative jurisdiction under public international law relates to jurisdictional immunities.⁸ Even if this position is incorrect (which is likely), there is not much in public international law that can tell us how to design jurisdictional rules in relation to digital assets. As Ryngaert, a leading authority on public international law jurisdiction, explains:

“The scholarly field is quite divided on the issue whether public international law limits adjudicative jurisdiction... In my view, the better position regarding the relationship between public international law and adjudicative jurisdiction in civil matters is that the latter is at least potentially governed by public international law... This does not mean that, currently, public international law imposes hard limits on adjudicative jurisdiction. In fact, where a domestic court’s assumption of adjudicative jurisdiction is followed by a choice-of-law analysis that may lead to the application of foreign law, so far there has been relatively little evidence that foreign states have taken fundamental issue with particular types of adjudicative jurisdiction... Still, it remains difficult to make definitive statements regarding the motives driving states’ inaction.”⁹

³ Law Commission, ‘Digital Assets and ETDs in Private International Law: Which Court, Which Law? Call for Evidence’ (2024), paras 4.84-4.112.

⁴ Ibid, paras 1.44, 4.12, 4.17, 4.40, 4.95, 4.96, 4.98, 4.99 and 6.134.

⁵ Ibid, paras 4.10, 4.18, 4.25 and 4.26.

⁶ Ibid, paras 4.26-4.28.

⁷ Restatement (Fourth), § 422, Reporters’ Note 1.

⁸ Ibid, § 422, Reporters’ Note 1, 230.

⁹ C. Ryngaert, ‘The Restatement and the Law of Jurisdiction: A Commentary’ (2022) 32 EJIL 1455, 1465-1468 (footnotes omitted).

7. Similarly, English case law does not support the notion that public international law can inform the design or interpretation of jurisdictional rules. There is no indication of this in the Supreme Court judgments in the *Brownlie* case,¹⁰ the leading recent authorities on the English law of jurisdiction.
8. Despite its rhetoric, even the Law Commission's Call for Evidence does not support the notion that public international law can inform the design or interpretation of jurisdictional rules in English law. While Chapter 4 states that public international law regulates adjudicatory jurisdiction and that the exercise of adjudicatory jurisdiction should be consistent with public international law, Chapter 5, which focuses on specific jurisdictional gateways, conspicuously avoids any reference to public international law.
9. In contrast, the design of the gateways is motivated by practical, rather than theoretical, considerations. These practical considerations are so dominant that the Law Commission's Call for Evidence notes that "There is no inherent logic underpinning the gateways as a coherent whole".¹¹ Whether this assertion is correct is debatable. As Mr Justice Foxton has written extra-judicially, despite the fact that "At first sight, the current set of gateways represents a rather rag-bag collection, added to in a piecemeal fashion over time", there are rationales that underpin them.¹² Moreover, Mr Justice Foxton has noted that the gateways concerned with the efficient trial of disputes balance the conflicting considerations of "the territorial nature of jurisdiction under international law, and the desirability of ensuring all necessary parties are before the court".¹³ This sentiment that theoretical considerations are sometimes sacrificed for practical considerations is echoed in Mr Justice Foxton's statements that the gateways provide "*to a significant extent* internationally recognised nexus between a claim and this jurisdiction"¹⁴ and "that the considerations which underpin them, enjoy *a degree of* international support".¹⁵
10. At most, public international law tells us that English courts cannot exercise jurisdiction over all claims and that there must be some justification for their exercise of jurisdiction. However, this requirement is so broad that it cannot effectively serve as a guiding idea for designing jurisdictional rules in a field as complex as digital assets. Therefore, I recommend that the Law Commission not regard the core problem in the field of jurisdiction "essentially as one of public international law".¹⁶

¹⁰ *FS Cairo (Nile Plaza) LLC v Lady Brownlie* [2021] UKSC 45; *Four Seasons Holdings Inc v Brownlie* [2017] UKSC 80.

¹¹ Law Commission (n 3), para 4.107.

¹² D. Foxton, 'The Jurisdictional Gateways – Some (Very) Modest Proposals' [2022] LMCLQ 73.

¹³ *Ibid*, 79.

¹⁴ *Ibid*, 82 (emphasis added).

¹⁵ *Ibid*, 82-83 (emphasis added).

¹⁶ Law Commission (n 3), para 6.134.

1.1.2. Linking Jurisdiction with Recognition and Enforcement of Foreign Judgments

11. There are at least two problems with trying to base jurisdictional rules on “justifiable”, “legitimate”, “appropriate” or “proper” jurisdictional grounds to facilitate the recognition and enforcement of English judgments abroad.
12. The first problem is that there are not many jurisdictional grounds that are internationally accepted. During its membership in the European Union (EU), the United Kingdom (UK) was bound by the Brussels I *bis* Regulation¹⁷ and its predecessors. Jurisdictional rules in these legal instruments were based on jurisdictional grounds accepted within the EU. The jurisdictional grounds that enjoy true international acceptance form the bases of the “jurisdictional filters” in the 2019 Hague Judgments Convention,¹⁸ which the UK Government is preparing to ratify in the very near future.¹⁹ However, most existing jurisdictional rules in English law are based on broader jurisdictional grounds.
13. The second problem is that framing a discussion of existing jurisdictional rules in English law in terms of “justifiable”, “legitimate”, “appropriate” or “proper” jurisdictional bases may not improve the prospects of recognition and enforcement of English judgments abroad. For instance, a system of recognition and enforcement of foreign judgments based on English law would never recognise or enforce an English judgment against a person who did not submit to the jurisdiction of English courts or was not present within the territorial jurisdiction of English courts at the moment of commencement of proceedings, regardless of how reasonable the exercise of that jurisdiction was.
14. Therefore, I recommend that the Law Commission separate its discussion of jurisdiction from recognition and enforcement of foreign judgments.
15. A more productive approach would be to analyse existing jurisdictional rules in English law in light of the goals these rules aim to achieve. Three goals appear particularly relevant. First, protecting British consumers. Second, protecting British victims of fraud and theft. Third, promoting England as a leading centre for litigating disputes relating to digital assets. While existing rules support the first two goals, achieving the third goal requires a review of the English law of jurisdiction to identify gaps and

¹⁷ 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 (recast) [2012] OJ 351/1.

¹⁸ Convention of 2 July 2019 on the Recognition and Enforcement of Foreign Judgments in Civil or Commercial Matters, entered into force on 1 September 2023, Art 5.

¹⁹ On 15 and 16 January 2024, the UK Government made ministerial statements to the House of Commons and the House of Lords announcing the signing of the convention. On 25 March 2024, it laid the convention before Parliament, which is, pursuant to the Constitutional Reform and Governance Act 2010, a necessary step before ratification can occur. The period for Parliament to object to the ratification of the convention expires on 16 May. The Government also prepared a draft statutory instrument and the Civil Procedure Rule Committee amended the Civil Procedure Rules to facilitate the implementation of the convention into UK law. It is not expected that Parliament will object to the ratification of the convention. For references, see U. Grušić, ‘UK Government Prepares to Ratify the 2019 Hague Judgments Convention’ (EAPIL Blog, 9 May 2024).

ambiguities in the gateways, considering the practical considerations and rationales that underpin them. While the Law Commission’s ongoing review of the English law of jurisdiction pursues this approach, its analysis would be conceptually more coherent if it were not distracted by public international law and recognition and enforcement concerns. However, this does not negate the need for the Law Commission to address recognition and enforcement of foreign judgments. As discussed in part 3 below, digital assets raise several issues within the field of recognition and enforcement of foreign judgments that the Law Commission should address.

1.2. International Jurisdiction: Specific Issues

16. This section deals with specific issues within the law of jurisdiction, focusing on Questions 1 to 5 asked in Chapter 5 of the Call for Evidence.

Question 1

17. I agree with the Law Commission’s preliminary view that the vast majority of consumer contracts in digital and decentralised contexts do not pose any significant new difficulties compared to other cross-border consumer contracts.²⁰ Key issues concerning the jurisdictional rules over consumer contracts in sections 15A, 15B, 15D and 15E of the Civil Jurisdiction and Judgments Act 1982 are the interpretation of concepts of “consumer”, “consumer contract” and “pursuing” and “directing” commercial or professional activities to the UK. These concepts have been clarified in the jurisprudence of the Court of Justice of the European Union (CJEU) and domestic courts, including UK courts, on section 4 of chapter II of Brussels I *bis*, as well as some other provisions of EU law.²¹ The relative ease with which these concepts have been applied to various factual circumstances in different contexts suggests that section 15B of the 1982 Act can accommodate the issue of jurisdiction over consumer contracts in digital and decentralised contexts, that the fact that a business is a crypto-business, as opposed to any other business, does not change the analysis of whether the business has directed its services to consumers located in the UK and that there

²⁰ Law Commission (n 3), para 5.9.

²¹ See the recent judgment of the UK Supreme Court in *Lifestyle Equities CV v Amazon UK Services Ltd* [2024] UKSC 8, where the court dealt with the concept of targeting of a commercial activity carried on through a website for the purposes of Regulation (EU) 2017/1001 of the European Parliament and of the Council of 14 June 2017 on the European Union trade mark [2017] OJ L154/1. To deal with this issue, the court referred to the case law of the CJEU on the interpretation of this concept for the purposes of the Brussels I Regulation (Joined Cases C-585/08 and C-144/09 *Pammer v Reederei Karl Schlüter GmbH & Co KG; Hotel Alpenhof GesmbH v Heller* ECLI:EU:C:2010:740) and EU trade mark (Case C-324/09 *L’Oréal SA v eBay International AG* ECLI:EU:C:2011:474), copyright (Case C-5/11 *Criminal proceedings against Donner* ECLI:EU:C:2012:370) and database protection (Case C-173/11 *Football Dataco Ltd v Sportradar GmbH* ECLI:EU:C:2012:642) law.

are no changes or clarifications that are needed in respect of the issue of jurisdiction over consumer contracts.²²

18. However, it is worth noting that, unlike the equivalent rules of Brussels I *bis*, the jurisdictional rules over consumer contracts in the 1982 Act are subject to the application of the *forum non conveniens* doctrine.²³ This can lead to practical problems that do not arise under the equivalent rules of Brussels I *bis*.²⁴ Another potentially problematic area not discussed in the Law Commission's Call for Evidence is the derogatory effect of arbitration clauses in consumer contracts.²⁵

Question 2

19. The application of gateway 6(a) to smart legal contracts is fact-sensitive. If there are natural language negotiations, gateway 6(a) applies without many problems.²⁶ However, solely smart code contracts present difficulties.
20. The location of a participating computer or computers should not be used as the relevant connecting factor. As noted by some consultees to the Law Commission's consultation on smart legal contracts, the nodes across which a smart legal contract is deployed are likely to be located in different countries, may not have a stable location or their location may be difficult to identify and arbitrary; moreover, the location of a node or nodes running a coded element of a smart legal contract, the location of the user who deployed it and the location of the user interacting with it can all be in different countries.²⁷
21. The location of a real-world actor should be used as the relevant connecting factor. English law rules for determining the place of contract formation, which are used to establish whether a contract was made in England for the purposes of gateway 6(a), prioritise the location of the offeror at the time of communication of the acceptance of the offer if the parties use instantaneous means of communication.²⁸ However, the offeror's location at the place where they happen to be at the time the contract was formed can be arbitrary in the context of solely smart code contracts. Thus, for the purposes of gateway 6(a), the choice should lie between the offeror's domicile and habitual residence at the time of communication of acceptance. Common law domicile is an inappropriate connecting factor because the domicile of origin, which applies when there is no domicile of choice or dependency, depends on whether the

²² See *Ang v Reliantco Investments Ltd* [2019] EWHC 879 (Comm) (a person speculating on Bitcoin futures for a purpose outside her trade or profession was a consumer).

²³ Civil Jurisdiction and Judgments Act 1982, s 49.

²⁴ Case C-281/02 *Owusu v Jackson, trading as "Villa Holidays Bal-Inn Villas"* [2005] ECR I-1383.

²⁵ *Soleymani v Nifty Gateway LLC* [2022] EWCA Civ 1297.

²⁶ Including on the basis of the rule that a contract can be made in two or more places at once for the purposes of gateway 6(a): *Conductive Inkjet Technology Ltd v Uni-Pixel Displays Inc* [2013] EWHC 2968 (Ch).

²⁷ Law Commission, 'Smart Legal Contracts: Advice to Government' (2021) Law Com No 401, paras 7.28 and 7.29.

²⁸ L. Collins and J. Harris (gen eds), *Dicey, Morris and Collins on the Conflict of Laws* (Sweet & Maxwell, 16th edn, 2022), para 11-150.

person in question was a legitimate child and on the domicile of their parents,²⁹ which are eminently inappropriate rules to be used in the context of smart legal contracts. Instead, domicile, as defined in sections 41 and 42 of the Civil Jurisdiction and Judgments Act 1982, is an appropriate connecting factor. Both domicile in this sense and habitual residence have advantages and disadvantages. Domicile, as defined in sections 41 and 42 of the 1982 Act, is already used as a connecting factor in the Civil Procedure Rules Practice Direction 6B,³⁰ whereas habitual residence is not. However, if, as argued in paragraph 74 below, the habitual residence of the controller of a digital asset prevails as the connecting factor for determining the location of the digital asset, it may make sense to also use it in the context of gateway 6(a). A problem with solely smart code contracts is that acceptance of the offer may never be communicated to the offeror. In such cases, English law rules for determining the place of contract formation can only operate on the assumption that there is a waiver of the requirement that acceptance must actually be communicated. In such cases, the offeror's domicile/habitual residence at the time of contract formation can be used instead as the relevant connecting factor.

22. Gateway 6(a) has not generated much case law, indicating that it is not widely used. This suggests that the question of where a smart contract is made is unlikely to become prevalent in practice.

Question 3

23. The tortious damage pleaded in the crypto-token litigation is pure economic loss. I believe there is no other way to conceptualise such damage.

24. In *Brownlie II*, Lord Lloyd-Jones noted that the broad interpretation of gateway 9(a) adopted in this case does not necessarily apply to cases involving pure economic loss:

“there is an important difference in this regard between physical damage and ‘the financial consequences of a tort which itself is wholly economic in nature’. The nature of pure economic loss creates a need for constraints on the legal consequences of remote effects and can give rise to complex and difficult issues as to where the damage was suffered, calling for a careful analysis of transactions. As a result, the more remote economic repercussions of the causative event will not found jurisdiction...”

I would certainly not disagree with the proposition, supported by the economic loss cases, that to hold that the mere fact of any economic loss, however remote, felt by a claimant where he or she lives or, if a corporation, where it has its business seat would be an unsatisfactory basis for the exercise of jurisdiction...”³¹

²⁹ Ibid, para 6R-025.

³⁰ CPR PD 6B, 3.1(1).

³¹ (n 10), [75]-[76].

Lord Lloyd-Jones further noted that this approach of distinguishing between pure economic loss cases and physical damage cases “is not inconsistent with the cases on economic loss considered above”.³² However, it does not necessarily follow that the approach to localising damage or detriment for jurisdictional purposes should be the same as the approach for choice of law purposes. After all, Lord Lloyd-Jones also noted that the economic loss cases he considered should be approached with caution because “they 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”.³³ This line of authority fails to recognise that the differences between the two systems are significant and have increased as the systems have diverged.³⁴ Finally, it is worth noting that Lord Collins, sitting as a non-permanent judge of the Hong Kong Court of Appeal in *Fong v Ascentic Ltd*, adopted a broad interpretation of the Hong Kong equivalent of gateway 9(a) to cover “financial damage”.³⁵ This means that the relatively broad interpretation of gateways 9(a) and 21(a) adopted in the crypto-token litigation is not theoretically unsound.

25. In most cases involving digital assets falling within gateways 9(a) and 21(a), suffering pure economic loss in England alone was not sufficient. Except for *AA v Persons Unknown*,³⁶ the location of the digital assets in these cases, represented by the domiciles/habitual residences of the controllers/owners of the digital assets, was in England.³⁷ Even *AA* can be justified on the basis of the principle that “If the claimant becomes legally liable to pay over money within the jurisdiction, it seems that he does sustain damage, in the sense of economic loss, within the jurisdiction”.³⁸ For these reasons, these cases can be regarded as having a sufficient jurisdictional connection with England and as being in line with the dicta from *Brownlie II* regarding the treatment of pure economic loss cases under gateway 9(a).

26. Moreover, the relatively broad interpretation of gateways 9(a) and 21(a) adopted in the crypto-token litigation serves to protect British victims of fraud and theft. This is a

³² *Ibid*, [76]. His Lordship considered *Societe Commerciale de Reassurance v Eras (International) Ltd (The Eras Eil Actions)* [1992] 1 Lloyd’s Rep 570; *Bastone & Firminger Ltd v Nasima Enterprises (Nigeria) Ltd* [1996] CLC 1902; *ABCI (Formerly Arab Business Consortium International Finance & Investment Co) v Banque Franco-Tunisienne* [2003] EWCA Civ 205; *Eurasia Sports Ltd v Tsai* [2018] EWCA Civ 1742.

³³ (n 10), [74].

³⁴ *Ibid*.

³⁵ [2022] HKCFA 12, [107]: “the natural and ordinary meaning of the word ‘damage’ is just that, and the rule does not distinguish between the damage which completes a cause of action and that which does not, nor does it distinguish between direct or indirect damage, or between physical or financial damage.”

³⁶ [2019] EWHC 3556 (Comm).

³⁷ *Ion Science Ltd v Persons Unknown*, EWHC, 21 December 2020, [13] and [21]; *Reyes v Persons Unknown* [2021] EWHC 1938 (Comm), [21]-[22]; *Fetch.ai Ltd v Persons Unknown Category A* [2021] EWHC 2254 (Comm), [14]; *Osbourne v Persons Unknown* [2022] EWHC 1021 (Comm), [15]-[16]; *Tulip Trading Ltd v Bitcoin Association for BSV* [2022] EWHC 667 (Ch), [140]-[148], [159]-[164]; *D’Aloia v Persons Unknown* [2022] EWHC 1723 (Ch), [10]; *Jones v Persons Unknown* [2022] EWHC 2543 (Comm), [30]; *LMN v Bitflyer Holdings Inc* [2022] EWHC 2954 (Comm), [20].

³⁸ A. Briggs, *Private International Law in English Courts* (OUP, 2nd edn, 2023), 242.

legitimate goal for jurisdictional rules to pursue in a legal system where potential excesses of jurisdiction can be controlled by the *forum non conveniens* doctrine.

27. In contrast, choice of law rules generally aim to achieve the application of one applicable law most closely connected to the legal relationship in question. Since the goals of jurisdictional and choice of law rules differ, there is no reason to adopt a consistent approach to localising pure economic loss as between jurisdiction and choice of law.

Question 4

28. This question revolves around the location of “an unlawful act”.³⁹ However, I believe this label is not entirely accurate. According to the Law Commission’s Call for Evidence, the location of “an unlawful act” is used as a connecting factor in gateways 9(b), 15(a), 16(a), 16(b) and 21(b).⁴⁰ However, the causative acts and events under these gateways are not always unlawful. For instance, the gateway for claims in restitution is based on acts committed within the jurisdiction (gateway 16(a)) and the enrichment obtained within the jurisdiction (gateway 16(b)). A claim in restitution can arise even without an “unlawful act”, such as in cases where a person mistakenly pays another person. Furthermore, the enrichment of one person results from an act that causes a corresponding impoverishment of another person and is, therefore, more akin to damage or detriment, which are the focus of Question 3, rather than causative acts and events, which are the focus of Question 4. Therefore, in my opinion, it would be better to frame Question 4 around the location of a causative act or event and to discuss gateway 16(b) separately.
29. Otherwise, I agree with the Law Commission’s assessment that it is as difficult to locate where a causative act or event occurs as it is to determine the location of the consequences of that act or event and that the reasoning of *Ashton Investments Ltd v OJSC Russian Aluminium (RUSAL)*⁴¹ cannot be applied to distributed servers or decentralised ledgers.⁴² However, I do not believe that the relatively broad interpretation of gateways 9(b), 15(a) and 16(a) adopted in the crypto-token litigation is theoretically unsound. In *Ion Science*⁴³ and *Jones*,⁴⁴ the claimants were domiciled in England and it seems that fraudulent representations were made in England and computers were remotely accessed in England. Therefore, substantial and efficacious acts were committed in England, even if other substantial and efficacious acts were committed elsewhere.⁴⁵

³⁹ Law Commission (n 3), para 5.76.

⁴⁰ Ibid, para 5.58.

⁴¹ [2006] EWHC 2545 (Comm).

⁴² Law Commission (n 3), paras 5.59-5.62.

⁴³ (n 37), [14].

⁴⁴ (n 37), [8].

⁴⁵ *Metall und Rohstoff AG v Donaldson Lufkin & Jenrette Inc* [1990] 1 QB 391, 437.

Question 5

30. I will address four separate questions raised by Question 5. The first is whether the courts' approach to localising crypto-tokens by reference to the location of real-world actors is theoretically sound. For the reasons given in the context of Question 2,⁴⁶ using the location of a computer or computers participating in a distributed ledger as the relevant connecting factor is not advisable. Instead, the location of real-world actors should be used. It is natural to consider the location of the "owner" of a crypto-token in this context.
31. The second question is whether the courts' approach to localising crypto-tokens by reference to the location of their "owners" is theoretically sound. Ownership is a legal issue and the question of jurisdiction may arise to determine whether English courts have the power to hear and decide who owns a crypto-token.⁴⁷ In this sense, identifying the owner of a crypto-token for jurisdictional purposes may be putting the cart before the horse. Furthermore, the Law Commission's final report on digital assets dealt with the concept of control and its legal consequences.⁴⁸ It described the factual concept of control that best captures the ability to exclude or to permit access to a third category thing and put it to the uses of which it is capable. It concluded that both the factual concept of control and its legal consequences work differently for, and are highly complex in relation to, third category things, particularly digital objects. This is important for private international law because it indicates that the location of the person exercising factual control over a crypto-token should be used as an indicator of its location. This was also the view of Butcher J in *Tulip Trading*, the only judgment to seriously address the location of crypto-tokens for jurisdictional purposes.⁴⁹ The Law Commission also recommended in its final report on digital assets that the Government create or nominate a panel of industry-specific technical experts, legal practitioners, academics and judges to provide non-binding guidance on the factual and legal issues relating to control involving third category things. A better understanding of factual control would help to identify persons exercising factual control over crypto-tokens in different circumstances.
32. The third question concerns the use of domicile and habitual residence of the person exercising factual control over a crypto-token as connecting factors. I have already expressed concerns about the use of the common law concept of domicile.⁵⁰ However, domicile, as defined in sections 41 and 42 of the Civil Jurisdiction and Judgments Act 1982, and habitual residence are appropriate connecting factors. Both domicile in this

⁴⁶ At para 20 above.

⁴⁷ As occurred, for example, in *Tulip Trading Ltd v Bitcoin Association for BSV* [2023] EWCA Civ 83.

⁴⁸ Law Commission, 'Digital Assets: Final Report' (2023) Law Com No 412, Ch 5.

⁴⁹ (n 37), [148]: "If necessary to my decision I would conclude that TTL has the better of the arguments on this point. I should add that in reaching that conclusion I have also taken into account the discussion in the Taskforce Statement, and in particular the suggestion at para 99 that *the location of control of a digital asset*, including by the storage of a private key, may be relevant to determining whether the proprietary aspects of dealings in digital assets are governed by English law." (emphasis added)

⁵⁰ At para 21 above.

sense and habitual residence have advantages and disadvantages. An advantage of habitual residence is that, unlike domicile, as defined in sections 41 and 42 of the 1982 Act, it can be used as a correcting factor for both jurisdictional and choice of law purposes.

33. Finally, the fourth question concerns the relevant time for establishing the location of crypto-tokens: whether it is when the cause of action arose, when the application for service out was made or some other time. I do not agree with the suggestion in *D'Aloia*⁵¹ that the relevant time for the purposes of gateway (11) is when the cause of action arose. Instead, the relevant time should be when the application for service out was made.⁵² This interpretation should also apply to gateway 15(b), especially considering that gateway 15(a) refers to past acts and events. Interpreting 15(b) as referring to the moment when the cause of action arose would lead to considerable, if not complete, overlap between these two gateways.

1.3. Conclusion on Jurisdiction

34. The fields of jurisdiction and choice of law are different, which has at least three consequences.
35. First, there is no need to adopt an identical interpretation of similarly or identically worded connecting factors used in these two fields, such as the place of tort used in gateway 9(a) and Article 4(1) of the Rome II Regulation.⁵³
36. Second, choice of law rules generally aim to achieve the application of one applicable law most closely connected to the legal relationship in question, while the gateways define the circumstances justifying the exercise of jurisdiction by English courts based on the connection between the parties and/or the claim and the forum. Consequently, choice of law rules must be designed in a way that leads to the application of only one law. However, jurisdictional rules can be designated in a way that enables English courts to exercise jurisdiction even if one or more foreign courts could also legitimately do so in the same case. This means, for example, that we may be able to accept that the domicile/habitual residence of a person exercising factual control over a crypto-token in England is a sufficient jurisdictional connection with this jurisdiction, even if other persons domiciled/habitually resident elsewhere also exercise factual control over the crypto-token. In contrast, choice of law rules require a more focused approach.
37. Third, while there must always be an applicable law to a claim, jurisdiction of English courts over a claim is not always necessary. For instance, some consultees to the Law Commission's consultation on smart legal contracts identified gaps in gateway 9(a) and suggested that the difficulties in identifying a smart legal contract's place of

⁵¹ (n 37), [22].

⁵² *Osbourne v Persons Unknown* [2023] EWHC 39 (KB), [35]-[37].

⁵³ 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) [2007] OJ L199/40.

formation could warrant a further broadening of this gateway.⁵⁴ However, this should be resisted. It is not necessarily problematic if a complex situation involving a digital asset does not fit within this gateway. With numerous and broad gateways available, different aspects of a situation may fall within other gateways, allowing all claims concerning the situation to be brought in England under gateway 4A. But if a situation does not fall within any gateway, it could be regarded as lacking sufficient jurisdictional connection to England and a broadening of gateway 9(a) is not needed.

38. A related point is that the law of jurisdiction is the most flexible part of English private international law, capable of being changed relatively quickly and easily by the Civil Procedure Rules Committee, which typically amends the gateways once a practical need has been identified through case law. Therefore, it is justified for the Law Commission to adopt a conservative approach by focusing on clarifying any ambiguities in the existing gateways and recommending new gateways only if absolutely necessary.

39. Finally, I believe that the Law Commission should look into the availability of *Bankers Trust* and *Norwich Pharmacal* orders in crypto-token litigation. Claimants have sought these orders in cases involving digital assets. However, most courts have refused to grant *Norwich Pharmacal* orders pursuant to *AB Bank Ltd v Abu Dhabi Commercial Bank PJSC*,⁵⁵ while allowing *Bankers Trust* orders on the same facts. Trower J indicated in *D'Aloia*⁵⁶ that there may be a conflict in the case law on this matter. Given the practical importance of these orders, the Law Commission should examine this potential conflict.

2. Choice of Law

40. This part of my response is divided into two sections. The first section focuses on the questions asked in Chapters 7-12 of the Call for Evidence. The second section mentions some fields of choice of law that have not been discussed in the Call for Evidence but are relevant for crypto-token litigation and should be addressed by the Law Commission. Throughout this part of my response, references to Rome I are to the assimilated Rome I Regulation⁵⁷ and references to Rome II are to the assimilated Rome II Regulation,⁵⁸ unless otherwise indicated.

41. A general comment that I would like to raise relates to the last paragraph of Chapter 6 of the Call for Evidence, where the Law Commission notes that “where the Rome

⁵⁴ Law Commission (n 27), para 7.34, referring to a suggestion by Allen & Overy.

⁵⁵ [2016] EWHC 2082.

⁵⁶ (n 37), [35]-[36].

⁵⁷ 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) [2008] OJ L177/6; Law Applicable to Contractual Obligations and Non-Contractual Obligations (Amendment etc.) (EU Exit) Regulations 2019 (SI 2019/83).

⁵⁸ (n 53); Law Applicable to Contractual Obligations and Non-Contractual Obligations (Amendment etc.) (EU Exit) Regulations 2019 (SI 2019/83)

Regulations apply, we are not in a position to propose different rules”.⁵⁹ I disagree with this statement. The Rome Regulations now apply not as directly effective EU law, but as assimilated EU law, which can be amended by Government in accordance with the Retained EU Law (Revocation and Reform) Act 2023. Indeed, in the rest of the Call for Evidence, the Law Commission seems to accept that the assimilated Rome Regulations can be amended. For example, paragraph 7.5 in Chapter 7 asks whether “reform [of the assimilated Rome I is] needed”.

2.1. Choice of Law: Specific Issues

Question 7

42. I cannot answer the question of whether contractual disputes in the context of DeFi are unlikely to come before the courts. However, if such disputes do come before the courts, the question of applicable law may arise. DeFi transactions involve at least three relationships: User 1 – User 2; User 1 – DeFi Platform Provider; User 2 – DeFi Platform Provider. The structure of DeFi transactions resembles that of transactions on a crypto exchange, which also entail at least three relationships: User 1 – User 2; User 1 – Crypto Exchange; User 2 – Crypto Exchange. In this sense, the Law Commission’s analysis of contractual choice of law issues arising in the context of trades taking place on a crypto exchange and not involving fiat currency is relevant in the context of DeFi.

Question 8

43. I agree with the Law Commission’s tentative view that there are no particular problems in determining the applicable law for non-consumer contracts involving crypto-tokens.⁶⁰ In other words, the provisions of Rome I for identifying the applicable law for non-consumer contracts can be applied to contracts involving crypto-tokens easily or without undue difficulty. Nonetheless, I believe there are two issues that would benefit from further clarification.

44. First, whether a hashed reference in an individual trade to the “constitution” of a permissionless blockchain or another document, such as a membership agreement, that aims to determine the applicable law for the trades on the blockchain can constitute an express choice of law. This is a matter of consent and material validity of consent, which, according to Articles 3(5) and 10 of Rome I, is governed by the putative applicable law. The Law Commission should at least assess whether English contract law supports the choice of English law through a hashed reference in an individual trade to the “constitution” of a permissionless blockchain or another

⁵⁹ Law Commission (n 3), para 6.190.

⁶⁰ Ibid, para 7.83.

document that aims to achieve the application of English law to the trades on the blockchain.

45. Second, whether the existence of the “constitution” of a permissionless blockchain or another document that aims to determine the applicable law for the trades on the blockchain can constitute an implied choice of law based on the circumstances of the case. According to the Green Paper on Rome I, an implied choice may exist where a contract is “part of a series of operations, the law having been chosen only for the basic contract underlying the general operation”.⁶¹ The editors of *Dicey, Morris and Collins* also mention the following scenarios: “where a charterparty is governed by English law (either expressly or by implication) the court may infer that it was intended that the bills of lading be governed by the same law. Similarly, where a contract is governed by a given law, it may be inferred that the parties to a guarantee of obligations under it intended that the guarantee should be governed by the same law, especially if the guarantor and the party whose performance is guaranteed are connected.”⁶² These examples may lend support to the possibility of an implied choice of law based on the circumstances of the case described in the beginning of this paragraph.

Question 9

46. My response to Question 9 aligns with my response to Question 1. I believe that the provisions of Rome I for identifying the applicable law for consumer contracts can generally be applied to contracts involving crypto-tokens easily or without undue difficulty. This opinion finds support in the relative ease with which the concepts of “consumer”, “consumer contract” and “pursuing” and “directing” commercial or professional activities to the UK have been applied to various factual circumstances in the context of Article 6 of Rome I and section 4 of chapter II of Brussels I *bis*, as well as in the context of some other provisions of EU law. Nonetheless, I believe there are three areas that would benefit from further clarification: the exclusions in sub-paragraphs (a), (d) and (e) of paragraph 4 of Article 6.
47. The exclusions in sub-paragraphs (d) and (e) of paragraph 4 of Article 6 are the focus of Question 9. While the Law Commission mentions in its Call for Evidence that “Another potentially relevant exemption is contained in Rome I Regulation (EC) No 593/2008, Official Journal L177 of 04.07.2008, art 6(4)(a)”,⁶³ it does not discuss this exclusion. The editors of *Dicey, Morris and Collins* state that “This exclusivity requirement has been interpreted narrowly by the European Court, as being applicable only if the consumer has no possibility of receiving the services in his or her

⁶¹ European Commission, ‘Green Paper on the Conversion of the Rome Convention of 1980 on the Law Applicable to Contractual Obligations into a Community Instrument and its Modernisation’ (COM/2002/0654 final), para 3.2.4.1.

⁶² *Dicey, Morris and Collins* (n 28), para 32-090 (footnotes omitted).

⁶³ Law Commission (n 3), fn 583.

home country and must travel in order to receive them.”⁶⁴ This suggests that this exclusion is unlikely to create problems in the context of crypto-token litigation. However, McParland expresses a view that points in the opposite direction:

“In financial services of the kind that might produce litigation, it is possible to see scope for uncertainty. Professor Proctor has suggested in the context of a typical banking transaction in which a foreign client instructs a London bank to execute a transaction and provide custodian services and advice, that:

the fact that the consumer receives and acts upon advice within his home State does not prejudice the conclusion that the services are provided exclusively outside that State. It is difficult to provide a professional or business service without communicating with the client at some point of the process!”⁶⁵

This uncertainty indicates that the Law Commission should explore the exclusion in Article 6(4)(a).

Question 10

48. It remains uncertain whether the discrepancy between sub-paragraphs (d) and (e) of paragraph 4 of Article 6 regarding the definition of “financial instruments” is an oversight or a deliberate policy choice. There is no indication in the Explanatory Memorandum⁶⁶ and the Impact Assessment⁶⁷ accompanying the Law Applicable to Contractual Obligations and Non-Contractual Obligations (Amendment etc.) (EU Exit) Regulations 2019 to suggest that the discrepancy was a deliberate policy choice. The fact that the 2019 Regulations replaced the reference to the Directive on package travel, package holidays and package tours in Article 6(4)(b), as well as the reference to the Directive on the protection of consumers in respect of certain aspects of timeshare, long-term holiday product, resale and exchange contracts in Article 6(4)(c), with the directives that replaced them,⁶⁸ but not the reference to MiFID I Directive in

⁶⁴ *Dicey, Morris and Collins* (n 28), para 33-171, referring to Case C-272/18 *Verein für Konsumenteninformation v TVP Treuhand- und Verwaltungsgesellschaft für Publikumsfonds mbH & Co KG* ECLI:EU:C:2019:827, [50]-[52].

⁶⁵ M. McParland, *The Rome I Regulation on the Law Applicable to Contractual Obligations* (OUP 2015), para 12.203, referring to C. Proctor, *The Law and Practice of International Banking* (OUP 2010), para 41.37, fn 32. See also, McParland, para 12.204.

⁶⁶ Available at https://www.legislation.gov.uk/ukxi/2019/834/pdfs/ukxiem_20190834_en.pdf.

⁶⁷ Available at https://www.legislation.gov.uk/ukia/2019/119/pdfs/ukia_20190119_en.pdf.

⁶⁸ Article 6(4)(b) of Rome I excludes “a contract of carriage other than a contract relating to package travel within the meaning of Council Directive 90/314/EEC of 13 June 1990 on package travel, package holidays and package tours” from Article 6. Article 6(4)(b) of the assimilated Rome I excludes “a contract of carriage other than a contract relating to package travel within the meaning of Directive (EU) 2015/2302 of the European Parliament and of the Council of 25 November 2015 on package travel and linked travel arrangements”.

Article 6(4)(c) of Rome I excludes “a contract relating to a right in rem in immovable property or a tenancy of immovable property other than a contract relating to the right to use immovable properties on a timeshare basis within the meaning of Directive 94/47/EC”. Article 6(4)(c) of the assimilated Rome I excludes “a contract relating to a right in rem in immovable property or a tenancy of immovable property other than a contract relating to the right to use immovable properties on a timeshare basis within the meaning of Directive 2008/122/EC”.

Recital 30,⁶⁹ suggests that the discrepancy is likely an oversight. Therefore, the courts should apply the Financial Services and Markets Act 2000 (Regulated Activities) Order 2001 to determine the scope of both exclusions.

Question 11

49. The question of applicable law can arise at two stages of court proceedings: at the jurisdictional stage and at the trial stage. This is because the question of applicable law can be relevant not only at trial but also in the jurisdictional context and, in particular, (1) as a factor under the *forum (non) conveniens* analysis,⁷⁰ (2) for the purposes of satisfying the tort claim governed by English law gateway,⁷¹ and (3) for the purposes of demonstrating that the claim has a reasonable prospect of success under the applicable law.⁷² If the question of applicable law arises in any of these situations, an English court has to localise the relevant damage. Therefore, I do not agree with the Law Commission's observation that "Whilst the cases show that the issue of localising tortious damage in the crypto-token context is a prevalent question so far in the context of jurisdiction, this theoretical issue is only relevant to one of three limbs of the test for service out of the jurisdiction."⁷³
50. Furthermore, I do not agree with the Law Commission's observation that "We are not aware of any case before the courts of England and Wales that has raised the question of either (i) where damage sustained by reason of being deprived of a crypto-token occurs, or (ii) where damage to a crypto-token is sustained specifically for the purpose of identifying the applicable law."⁷⁴ In fact, the question of applicable law has so far been raised, in the context of crypto-token litigation, in three cases: *Ion Science*,⁷⁵ *Fetch.ai*⁷⁶ and *LMN v Bitflyer Holdings Inc.*⁷⁷
51. In *Ion Science*, to determine whether a claim in deceit had a reasonable prospect of success, the court found that there was at least a serious issue to be tried that English law applied pursuant to Article 4(1) of Rome II on the basis that "England was the place where the damage occurred, either on the simple basis that the bank account which funded the Coinbase account was an English account or that the asset was taken from the claimants' control in England and Wales, because Mr Jones granted remote access

⁶⁹ The so-called MiFID I Directive, that is Directive 2004/39/EC of the European Parliament and of the Council of 21 April 2004 on markets in financial instruments [2004] OJ L145/1, which is referred to in Recital 18 of Rome I, has been replaced by the so-called MiFID II Directive, that is Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (recast) [2014] OJ L173/349.

⁷⁰ *VTB Capital plc v Nutritek International Corp* [2013] UKSC 5, [219].

⁷¹ CPR PD 6B, 3.1(9)(c).

⁷² See, in the context of crypto-token litigation, *Ion Science* (n 37), [13].

⁷³ Law Commission (n 3), para 9.36.

⁷⁴ *Ibid*, para 9.33.

⁷⁵ (n 37).

⁷⁶ (n 37).

⁷⁷ (n 37).

to his computer which was in England and Wales or alternatively because the relevant bitcoin were located in England and Wales prior to the transfer”.⁷⁸

52. *Fetch.ai* contains an unsatisfactory discussion of the applicable law under Rome II. The court seems to have accepted counsel’s suggestion to look at Rome II “for the purposes of demonstrating that the causes of action with which I am concerned come within its scope as justiciable in accordance with English law”.⁷⁹ The court also confused questions of jurisdiction and choice of law.⁸⁰ Be that as it may, the court found that the breach of confidence claim fell within the scope of Article 4(1) and that English law applied because the crypto-tokens in question were located in England, as their owners were located there, that is operated and held their digital assets there. Strangely, the court applied the rules for determining the presence of companies in the English law of jurisdiction, as set out in *Adams v Cape Industries plc*,⁸¹ to establish the location of a company owning a crypto-token. While English courts no longer apply Rome II as directly effective EU law, but as assimilated EU law, the interpretation of a provision of Rome II by reference to a common law jurisdictional authority cannot be justified, especially if such interpretation is adopted by a first instance court.
53. In *Bitflyer*, the court determined the *lex situs* of crypto-tokens on the basis of the claimant’s place of residence and business. Article 4(1) of Rome II was held to point to English law, the *lex situs*, because “either the cryptocurrency can be regarded as ‘damaged’ in England and Wales because it is in England that it was taken from C’s control... or because C as an English company has suffered loss and damage in England.”⁸²
54. In these three cases, the question of applicable law was raised for jurisdictional purposes. However, it is not unlikely that claims in tort, such as those pleaded in the crypto-token litigation for the purposes of service out, will proceed to trial before English courts.
55. I agree with the Law Commission that English courts should rely on the jurisprudence of the CJEU on pure economic loss to interpret Article 4(1) of the assimilated Rome II,⁸³ which they have not been doing so far in the context of crypto-token litigation. However, for the reasons advanced in paragraphs 24-27 above, I do not agree with the Law Commission that “responses given to Question 3 would be taken as equally relevant to the issue of applicable law that we consider here in Chapter 9”⁸⁴ because there is a significant difference between localising damage for jurisdictional and choice of law purposes.

⁷⁸ *Ion Science* (n 37), [13].

⁷⁹ *Fetch.ai* (n 37), [11]. See also [16].

⁸⁰ *ibid*, [13]-[15].

⁸¹ [1990] Ch 433.

⁸² *Bitflyer* (n 37), [21].

⁸³ Law Commission (n 3), para 9.24.

⁸⁴ *Ibid*, para 9.35.

56. Nevertheless, the approach of English courts to localising damage by reference to the domicile/habitual residence of the controller/owner of the digital asset and the location of the digital asset does not appear to be out of line with the CJEU jurisprudence on pure economic loss under Article 7(2) of Brussels I *bis* and its predecessors.
57. In *Marinari*⁸⁵ and *Kronhofer*,⁸⁶ neither the place where the damage occurred nor the place of the event giving rise to it was in the country of the claimant's domicile. In *Kolassa*,⁸⁷ the courts of the claimant's domicile had jurisdiction because the damage occurred directly in the claimant's bank account held with a bank established within the area of jurisdiction of those courts. In *Universal Music*,⁸⁸ the courts of the claimant's domicile lacked jurisdiction when the defendants' negligence resulted in an obligation for the claimant to pay a sum of money arising in another Member State and the claimant discharged this obligation by debiting its bank account held with a bank established within the area of jurisdiction of those courts. An important factor was that the claimant could have chosen to debit a bank account in another Member State. *Löber*⁸⁹ concerned similar facts to *Kolassa*. The CJEU held that the courts of the claimant's domicile had jurisdiction not only because the damage occurred directly in the claimant's bank accounts held with a bank established within the area of jurisdiction of those courts but also due to other circumstances, such as the acquisition of the investment in the secondary market in the claimant's Member State of domicile, the notification of the prospectus relating to the investment to the relevant regulator in that Member State and the claimant's entry into a contract for the investment in that Member State. However, in *Effectenbezitters*,⁹⁰ the direct occurrence of pure economic loss in an investment account situated in the claimant's Member State of domicile, used for the purchase of securities listed on the stock exchange of another state, was irrelevant because the issuer of those securities was not subject to statutory reporting obligations in that Member State.
58. With the exception of *AA v Persons Unknown*,⁹¹ the claimants' losses in the English crypto-token litigation related to digital assets located in England, which distinguishes these cases from *Marinari*, *Kronhofer* and *Universal Music*. These digital assets were not listed on a stock exchange, nor were they subject to statutory reporting obligations, which distinguishes these cases from *Löber* and *Effectenbezitters*. That leaves *Kolassa*, which lends support to the approach of English courts.

⁸⁵ Case C-364/93 *Marinari v Lloyd's Bank plc* [1995] ECR I-2719.

⁸⁶ Case C-168/02 *Kronhofer v Maier* [2004] ECR I-6009.

⁸⁷ Case C-375/13 *Kolassa v Barclays Bank plc* ECLI:EU:C:2015:37.

⁸⁸ Case C-12/15 *Universal Music International Holding BV v Schilling* ECLI:EU:C:2016:449.

⁸⁹ Case C-304/17 *Löber v Barclays Bank plc* ECLI:EU:C:2018:701.

⁹⁰ in Case C-709/19 *Vereniging van Effectenbezitters v BP plc* ECLI:EU:C:2021:377.

⁹¹ (n 37).

Question 12

59. A court applying the escape clause in Article 4(3) of Rome II can take all the circumstances of the case into account. If the parties are bound by a pre-existing contractual relationship and there is a related tort claim, the escape clause is likely to apply. The circumstances in the digital assets context in which it would be most appropriate for English courts to have recourse to the escape clause on the basis of a pre-existing contractual relationship are where there is a non-consumer contract between a user of a crypto exchange and the exchange and a party to this relationship brings a tort claim against the other. However, such cases are unlikely to represent the vast majority of cases.
60. If the parties are not bound by a pre-existing contractual relationship, but both are bound by a contractual relationship to a third party, such as a crypto exchange, and there is a tort claim related to trading on the exchange, this factor can be taken into account under the escape clause.
61. The application of the escape clause is highly fact-specific. Other relevant factors include: the location of a digital asset where the application of Article 4(1) or Article 4(2) points to the law of a country in which the digital asset is not located; the habitual residences and domiciles of the parties, their agents and/or intermediaries; the location of the gatekeeper/controller of a private or permissioned ledger; the place where any real-world asset to which a digital asset relates is located; the place where any real-world performance to which a digital asset relates takes place; and the location of a private key.

Question 17

62. A starting point of the Law Commission's analysis is that "the creation of equivalence between paper and electronic trade documents as a matter of substantive law does not necessarily mean there is, or need be, equivalence between them for the purposes of private international law".⁹² While it may be correct that there should be no equivalence for the purposes of private international law, the text of the Electronic Trade Documents Act 2023⁹³ leaves little room for doubt that section 72 of the Bills of Exchange Act 1882 applies to electronic bills of exchange, cheques and promissory notes.
63. I agree with the Law Commission that the technological requirements of section 2 of the 2023 Act, namely that a "reliable system" must be used to fulfil certain functions in relation to a document, are relevant for determining where an electronic bill of exchange is issued and that the reliable system seems to be a strong candidate for the

⁹² Law Commission (n 3), para 11.21. Similarly, para 11.28.

⁹³ Electronic Trade Documents Act 2023, s 3(2) ("An electronic trade document has the same effect as an equivalent paper trade document.") and (3) ("Anything done in relation to an electronic trade document has the same effect (if any) in relation to the document as it would have in relation to an equivalent paper trade document."). Section 3 is generally entitled "Possession, indorsement and effect of electronic trade documents".

connecting factor used to localise the place where an electronic bill of exchange is issued.⁹⁴

64. I also agree that we need to know more about market practice to assess whether the use of distributed ledger technology (DLT) necessarily precludes localisation by reference to the reliable system.⁹⁵ If the evidence shows, as is likely, that market participants favour centralised over wholly decentralised DLT reliable systems, the reliable system would be an appropriate connecting factor in the vast majority of, if not all, cases.

65. However, section 72 of the 1882 Act poses an issue that has not been considered by the Law Commission. The Call for Evidence mentions that reliable “system providers often occupy a central position in the factual and commercial matrix in which modern bills...are used, imposing rules on their participants via a user agreement and specifying a governing law... such central position is often sufficient in private international law to justify recourse to the central registry or platform provider as the connecting factor.”⁹⁶ It is not clear from the Call for Evidence what the Law Commission considers the relevant connecting factor to be. There are at least two possibilities in the described situation: (1) the applicable law specified in the user agreement, and (2) the habitual residence of the reliable system. There may be a discrepancy between these two connecting factors. A reliable system from country A might include a clause in the user agreement specifying that the law governing the contractual obligations arising under the bill of exchange in question is the law of country B. However, as the editors of *Dicey, Morris and Collins* explain:

“There is nothing in the Bills of Exchange Act 1882 which expressly prevents the parties from choosing the law to govern an instrument, but there is nothing which permits it either. However, though it may be rare or non-existent in practice for a bill or note to contain a choice of law, such a choice is not, in principle, unacceptable (at least for issues to which s.72 does not apply) if it appears on the face of the instrument. Providing anyone becoming a party to the instrument can see from the instrument itself what are going to be that party’s rights and obligations (and these can be ascertained by reference to the law chosen on the face of it) there is no compelling reason why such a choice should not now be accepted, but such a proposition is controversial.”⁹⁷

If party autonomy is not allowed in this context, choice of law clauses in user agreements are not effective. The Law Commission should consider the issue of party autonomy under the 1882 Act.

66. If the reliable system uses wholly decentralised DLT and it is not appropriate to use the reliable system as the connecting factor, it appears to be more appropriate to refer

⁹⁴ Law Commission (n 3), para 11.46.

⁹⁵ *Ibid*, paras 11.47-11.49.

⁹⁶ *Ibid*, para 11.30.

⁹⁷ *Dicey, Morris and Collins* (n 28), para 33-359.

to the habitual residence of the transferor than the transferee for the reasons given by Professor Dickinson.⁹⁸

Question 18

67. Given the problems of applying section 72 of the Bills of Exchange Act 1882 to electronic trade documents and the fact that the choice of law rule contained therein is outdated, I believe that it would be preferable to replace section 72 with a new choice of law rule. There are at least two options for the scope of a new rule: (1) it applies only to electronic bills of exchange, cheques, and promissory notes, which would otherwise fall within section 72, and (2) it applies to all electronic trade documents under the Electronic Trade Documents Act 2023. I do not believe that a new rule should apply to all electronic trade documents under the 2023 Act. The Act currently covers some trade documents that fall within the scope of Rome I, such as contracts evidenced by marine insurance policies and cargo insurance certificates.⁹⁹ There is no evidence that Article 7 of Rome I cannot be applied to insurance contracts where marine insurance policies or cargo insurance certificates are issued in electronic form or can only be applied to such contracts with undue difficulty.
68. Another question is whether a new rule should cover (1) contractual obligations only, or (2) both contractual and proprietary obligations arising within the reliable system. The answer to this question depends on the answer to Question 19, namely whether a new choice of law regime should be considered for property rights in digital assets and electronic trade documents. If a new choice of law regime is considered, a new choice of law rule replacing section 72 of the 1882 Act should cover contractual obligations only. Otherwise, a new choice of law rule replacing section 72 could cover contractual and non-contractual obligations arising within the reliable system.
69. Yet another question is how a choice of law rule replacing section 72 of the 1882 Act should be designed. At least for contractual obligations, the rule should uphold party autonomy. The rule could be modelled on sub-paragraphs (a) and (b) of paragraph 1 of Principle 5 of the UNIDROIT Principles on Digital Assets and Private Law. In the absence of party autonomy, the most appropriate connecting factor is the habitual residence of the reliable system. Habitual residence should be defined as the place where the reliable system has its central administration, in line with the definition of this connecting factor in the Rome Regulations.¹⁰⁰ The rule could also include an escape clause and a catch-all clause modelled on paragraphs 3 and 4 of Article 4 of Rome I. In other words, the rule could provide that:

⁹⁸ Law Commission (n 3), para 11.43, referring to A. Dickinson, 'Electronic Trade Documents and the Conflict of Laws in the United Kingdom' [2024] *Lloyd's Maritime and Commercial Law Quarterly* 55, 66.

⁹⁹ Electronic Trade Documents Act 2023, ss 1(2)(g) and 2.

¹⁰⁰ Rome I, Art 19; Rome II, Art 23(1).

1. Contractual issues in respect of an electronic trade document are governed by

(a) the domestic law of the country expressly specified in the document; or, failing that,

(b) the domestic law of the country expressly specified in the reliable system.

2. To the extent that the law applicable has not been chosen in accordance with paragraph 1, contractual issues in respect of an electronic trade document are governed by the domestic law of the country where the reliable system has its habitual residence.

Habitual residence, for the purposes of this provision, has the same meaning as Article 19 of the Rome I Regulation.

3. Where it is clear from all the circumstances of the case that the electronic trade document is manifestly more closely connected with a country other than that indicated in paragraph 2, the law of that other country governs.

4. Where the law applicable cannot be determined pursuant to paragraph 2, contractual issues in respect of an electronic trade document are governed by the law of the country with which the document is most closely connected.

Question 19

70. Generally speaking, there are two methods of acquiring title in a property object: original and derivative acquisition of title. Derivative acquisition of movables (excluding transfers requiring registration and transfers by operation of the law, such as a transfer to an heir) can be based on (1) a valid contract between the transferor and the transferee (in causal consensual systems), (2) a valid contract between the transferor and the transferee, coupled with a transfer or providing of possession (in causal tradition systems), and (3) a transfer, even if not based on a valid legal ground (in abstract tradition systems).¹⁰¹ Applied by analogy to digital assets, this classification suggests that in some legal systems, a transfer of control over a digital asset may be insufficient to transfer title. The Law Commission confirmed this in its Final Paper on Digital Assets, stating that under English law, a mere transfer of control “is not sufficient in itself to transfer superior legal title to a crypto-token for two reasons. First, in general, a transferor can confer no better title to a transferee than they have (the ‘*nemo dat principle*’). Second, the transaction between the transferor and the transferee must be legally valid in terms of the common law and equitable rules governing derivative transfers of title.”¹⁰² This underscores the need to

¹⁰¹ This classification is derived from L. van Vliet, ‘Transfer of Movable Property’ in J.M. Smits, *Elgar Encyclopaedia of Comparative Law* (Edward Elgar 2023), 508.

¹⁰² Law Commission (n 48), para 6.52.

distinguish between contractual and proprietary aspects of transfers of title. Furthermore, this classification shows that transfers of title cannot be approached on a purely contractual basis. Recourse to contractual principles cannot obviate the need for the Law Commission to consider choice of law for property issues, traditionally based on the *lex situs* approach.

71. Characterisation is key. Sometimes, the relevant issue is characterised as contractual. In these cases, choice of law in property does not arise and choice of law rules in contract determine the applicable law. Therefore, I agree with the Law Commission that recourse to party autonomy is justified “in cases where a contractual characterisation is valid. We think this would be most justified where, for example, access to the digital asset is premised on some degree of permission or consent to a user agreement, or the asset is issued for value.”¹⁰³ Recourse to party autonomy on the basis of contractual characterisation is also justified in some cases where a digital asset is held on a crypto exchange and there is a dispute between a user and the exchange or a dispute between two or more exchange users.¹⁰⁴ In Chapter 7 of the Call for Evidence, the Law Commission adopts a tentative view that there are no particular problems in determining the applicable law for non-consumer contracts involving crypto-tokens.¹⁰⁵ In other words, the provisions of Rome I for identifying the applicable law for non-consumer contracts can be applied to contracts involving crypto-tokens easily or without undue difficulty. If this is correct, there is no need to formulate a new choice of law rule based on the choice of law rule for multilateral systems that facilitate the third-party trading of financial instruments in Article 4(1)(h) of Rome I¹⁰⁶ because Articles 3 and 4 of Rome I can lead to the application of the law chosen by the issuer or system governor or the law of the issuer or system governor.
72. For cases that fall beyond the reach of contractual characterisation, the *lex situs* rule currently applies to determine the law applicable to property issues. Two questions arise in this respect. The first is whether the *lex situs* rule is suitable for determining the applicable law to property issues relating to digital assets. The second question is, if the *lex situs* rule is unsuitable, how a new rule should be formulated.
73. I do not believe that the *lex situs* rule, on its own, can systematically lead to the application of the law of the issuer of a digital asset or a crypto exchange, which are the two connecting factors favoured by the Law Commission.¹⁰⁷ Furthermore, English private international law currently does not allow party autonomy in the field of choice of law in property.
74. However, there are good reasons to use the location of the issuer or system governor of a digital asset, the location of a crypto exchange or the location of a reliable/approved system as connecting factors, as well as to allow party autonomy in

¹⁰³ Law Commission (n 3), para 12.56. Similarly, para 12.60.

¹⁰⁴ Ibid, paras 12.64-12.70.

¹⁰⁵ See the response to Question 8 above.

¹⁰⁶ As suggested in Law Commission (n 3), para 12.60.

¹⁰⁷ Ibid, paras 12.62 and 12.67.

the field of choice of law in property in relation to digital assets and electronic trade documents. A new choice of law rule could be modelled on sub-paragraphs (a)-(c) of paragraph 1 of Principle 5 of the UNIDROIT Principles on Digital Assets and Private Law. Where the applicable law cannot be determined on this basis, recourse to the *lex situs* rule is needed. The ideas on which the *lex situs* rule is based, such as legal certainty and foreseeability, security of transactions and state control over a digital asset, seem to point, as the editors of *Dicey, Morris and Collins* explain, to the law of the habitual residence of the controller of the digital asset.¹⁰⁸ As explained in paragraph 31 above, localising a digital asset by reference to the habitual residence of its controller (that is the transferor or grantor of a security interest) is theoretically more sound than relying on that of its “owner”.

2.2. Choice of Law: Missing Pieces of the Jigsaw

75. The Law Commission’s analysis should be informed by practical experience. The analysis of the crypto-token litigation shows that claimants have relied on several gateways to bring their claims so far. Among the most popular ones are the gateways for claims in constructive or resulting trust and for claims in restitution in paragraphs 3.1(15) and (16) of Civil Procedure Rules Practice Direction 6B. If a claim is brought under one or more of these gateways, an English court may have to determine the applicable law to the claim. However, the Law Commission does not discuss choice of law for trust claims, breach of equitable duties and restitution claims in its Call for Evidence.
76. Choice of law for trust claims and breach of equitable duties is a notoriously difficult subject. Lavender and Healy-Pratt JJ cited with approval in *Osbourne v Persons Unknown Category A* the following observation of the editors of *Dicey, Morris and Collins* “There seems to be no clear English or Commonwealth authority on the choice of law rules relating to constructive and resulting trusts”.¹⁰⁹ Fortunately, choice of law for unjust enrichment claims does not come with the same level of difficulty. The relevant choice of law rule is contained in Article 10 of Rome II. A particular difficulty with this rule in the context of crypto-token litigation is the application of Article 10(3), which points to the law of the country “in which the unjust enrichment took place”. Ascertaining where the unjust enrichment took place in restitution claims relating to digital assets is likely to give rise to similar problems as ascertaining the place of damage in tort claims and the location of property in property claims relating to digital assets. Since these fields of choice of law are relevant for crypto-token litigation, they should be addressed by the Law Commission.

¹⁰⁸ *Dicey, Morris and Collins* (n 28), para 23-050.

¹⁰⁹ [2023] EWHC 39 (KB), [43]; [2023] EWHC 340 (KB), [40], referring to *Dicey, Morris and Collins* (note 28), para 29-081.

3. Foreign Judgments

77. The Law Commission does not address recognition and enforcement of foreign judgments in its Call for Evidence. Nevertheless, there are two issues that the Law Commission could discuss.
78. The first is indirect jurisdiction. English courts can recognise and enforce foreign *in personam* judgments if the defendant in the foreign proceedings submitted to the jurisdiction of the foreign court or was present in the territorial jurisdiction of the foreign court at the moment of commencement of proceedings. English courts can give effect to foreign *in rem* judgments if the property, which was the subject-matter of the proceedings, was situated in the country of origin at the moment of commencement of proceedings. These indirect jurisdiction requirements are likely to preclude the recognition and enforcement of most foreign judgments given in litigation concerning digital assets.
79. The second is the requirement that only foreign money judgments can be enforced in England. As noted in the Law Commission's Final Report on Digital Assets, some foreign courts give judgments denominated in crypto-tokens. For instance, the United States District Court in *Titus Williams v Kasim Mahmood* (2022, Case Number 6:21-cv-03074-RK), granted to the defendant "conversion damages in the amount of 33.7398 bitcoin".¹¹⁰ Since this judgment is not a money judgment, it cannot be enforced in England. Nevertheless, there is a way around. As Briggs explains:

"If the foreign court has ordered a defendant to do something specific such as deliver up goods, or to refrain from doing something specific by ordering an injunction against contacting former clients or using a former employer's tangible or intellectual property, it is obvious that proceedings cannot be brought to collect a money debt, because the foreign judgment will have given rise to none.

Any English proceedings which the claimant will bring will therefore have to look back to and be founded on the original cause of action. However, so long as she is able to establish the jurisdiction of the court over the defendant in respect of the claim, she will be able to plead that a foreign judgment which satisfies the requirements for its recognition has already made the issues of substance on which liability depends *res judicata*. That being so, all that really remains to be done is for the English court to identify and grant the remedy which, as a matter of English procedural law, is the appropriate response to the substantive liability which has been established. This remedial response may not be identical with the order made by the foreign court, but it often will be; and the resulting English order may then be enforced, for example by contempt proceedings if it is not complied with."¹¹¹

¹¹⁰ Law Commission (n 48), fn 1291.

¹¹¹ Briggs (n 38), 360.

This means that English courts can give effect even to foreign judgments denominated in crypto-tokens in some circumstances.

80. Finally, it is worth noting that the UK Government is preparing to ratify the 2019 Hague Convention in the very near future.¹¹² The convention contains broader indirect jurisdictional rules and a broad definition of “judgment”, covering non-money judgments.¹¹³

I would be pleased to speak further about my response and am available to assist at

[REDACTED]

[REDACTED] 15 May 2024

*** * * ENDS * * ***

¹¹² See n 19 above.

¹¹³ 2019 Hague Convention, Arts 3(1)(b) and 5.

From: Denis Jude Haughton

Sent: 26 February 2024 10:44

To: LAWCOM Enquiries <enquiries@lawcommission.gov.uk>

Subject: Crypto Project [notes] Crypto Project [notes]

Hi, you can include these brief notes with your project submission

[REDACTED]

I have been observing the bitcoin phenomena since 2015 when with a bit of internet searching came to the conclusion that Bitcoin was a "pyramid scheme"

I tweeted about it and noticed that China and Brazil had already become suspicions of the mechanism anyway

I have thought of many ways to solve the bitcoin fiasco and come to a simple conclusion

1. cease all bitcoin trades with the dissolution of the Company and the issuing by the (i think) German registered company of eur1 per token number
2. have on a website that any holders of tokens/numbers who have received the nominal (true) value of the tokens of eur1 and wish to engage to get their "exchange value" back must go to a solicitor where that appointed solicitor can get some information about the previous holder (who received their clients money) bank account number and maybe jurisdiction etc
3. upon receiving this information a court case is formed and a letter sent to an address attached to the bank account number provided

There will of course need to be established joint agreements between different jurisdictions which I think your project is trying to establish

Hope this is of assistance

Denis Jude Haughton

Submitted to Law Commission Call for Evidence on digital assets and ETDs in private international law
Submitted on 2024-03-20 00:07:16

About you

What is your name?

Name:
Associate Professor Benjamin Hayward, Monash University

What is your email address?

Email:
[REDACTED]

What is your telephone number?

Telephone number:
[REDACTED]

Questions on applicable law - non-consumer contracts (Chapter 7)

Question 7: In this question, we seek views on applicable law and decentralised finance (DeFi).

Please share your views and evidence below::

Question 8: This question concerns the applicable law for non-consumer contracts.

Please share your views and evidence below::

Question 8: Call for Evidence [7.84]

(1) Can the provisions of the Rome I Regulation for identifying the applicable law for non-consumer contracts be applied to contracts involving crypto-tokens without undue difficulty?

I agree with the Law Commission's view, expressed in its Call for Evidence ('CFE'), that the provisions of the Rome I Regulation for identifying the applicable law in non-consumer contract cases can be applied to crypto-token contracts without undue difficulty. To the Law Commission's existing analysis, I add the following observations.

First, although the Law Commission did not specifically raise issues of characterisation in this context, it is an important background consideration (being 'a challenging and complex process': CFE [6.17]). Though courts will, in any given case, need to ask 'what kind of legal issue is in dispute between the parties?' (CFE [2.24]), characterisation issues do not raise practical difficulties for the application of Arts. 3–4 Rome I Regulation as they are ultimately matters for the parties' pleadings. Those pleadings, in so far as they characterise the relevant claim or claims, will either be correct or incorrect. This is a separate issue to the Rome I Regulation's application in and of itself.

Secondly, on the Law Commission's view that crypto-token contracts will (absent party choice of law) likely have their applicable law identified via Art. 4(1)(a) Rome I Regulation (goods), Art. 4(1)(b) Rome I Regulation (services), or Art. 4(2) Rome I Regulation (characteristic performance) – noting that these rules will likely converge in their results (CFE [7.43]–[7.46], [7.63]–[7.71]) – additional clarification is desirable. Even if these rules do converge in result, a situation of uncertainty as to which rule applies in any given case is analytically unsound. Noting the relevance of '[j]udicial experience in applying applicable law rules' to the Law Commission's present work (CFE [6.188]), it is not uncommon for the courts of England and Wales to grapple with difficult private international law questions. In *Raiffeisen Zentralbank Österreich AG v An Feng Steel Co Ltd* [2001] EWCA Civ 68, [2], for example, Mance LJ noted that the dispute involved 'an examination question on the applicable law'. It is preferable for this uncertainty to be confronted and resolved, particularly given the Commercial Court's reputation as a leader in international dispute resolution.

I agree with the Law Commission's views concerning characteristic performance (CFE [7.53]–[7.56], [7.67]–[7.71]). In particular, I note that the Giuliano and Lagarde Report (Report on the Convention on the Law Applicable to Contractual Obligations by Mario Giuliano and Paul Lagarde [1980] OJ C 282/1, 19–23 [1]–[9]) is an appropriate interpretative tool given the absence of an equivalent official Rome I Regulation commentary (Benjamin Hayward, *Conflict of Laws and Arbitral Discretion: The Closest Connection Test*, Oxford University Press, 2017, 225–6 [6.04]). The comments I make here will therefore focus on Art. 4 Rome I Regulation's goods and services rules. So far as their application is concerned, whilst 'empirical features' of crypto-tokens often rightly inform their conceptualisation (CFE [6.34]), the present problem is ultimately one of statutory interpretation.

In order to inform the Law Commission's understanding of Arts. 4(1)(a)–(b) Rome I Regulation's autonomous goods and services concepts, the Law Commission has identified persuasive EU law materials addressing the definition of goods and services in different but somewhat related contexts (CFE [7.47]–[7.52], [7.63]). To these materials can be added an analogy with the United Nations Convention on Contracts for the International Sale of Goods' conception of goods. Though the United Kingdom is not a CISG Contracting State, what is most important here is the fact that – at least for international sales law purposes – the CISG represents an agreement reached between now 97 Contracting States, and in this sense it constitutes a source of supranational law (CFE [2.11]). It is also noteworthy that, despite the United Kingdom's abstention from accession, it did participate in the 1980 Vienna

Diplomatic Conference at which the CISG's text was settled. Though, to the best of my knowledge, the matter has not yet arisen for judicial determination, it is strongly arguable that crypto-tokens are goods for the CISG's purposes (Benjamin Hayward, 'To Boldly Go, Part II: Data as the CISG's Next (But Probably Not Final) Frontier' (2021) 44(4) University of New South Wales Law Journal 1482, 1514–20). Although, like the Rome I Regulation, the CISG has its own autonomous meaning (Art. 7(1) CISG), its position vis-à-vis goods and crypto-tokens adds to the persuasive force of the EU law materials that have already been identified by the Law Commission.

For these reasons, it is in my view correct to treat crypto-tokens as goods for the purposes of Art. 4(1)(a) Rome I Regulation. It follows that contracts for services relating to crypto-tokens would constitute services contracts for the purposes of Art. 4(1)(b) Rome I Regulation. Where a crypto-token-related contract cannot be identified as being for the sale of goods or the provision of services, the characteristic performance rule in Art. 4(2) Rome I Regulation would then apply. This clarification will ensure that the analytic basis of applying the Rome I Regulation to crypto-token contracts is clear, even if it might be the case that outcomes under each of these provisions would not ultimately differ.

Finally, and noting with due sensitivity the fact that the Law Commission has recently undertaken extensive work in the arbitration field, attention can also be directed at the Rome I Regulation's capacity to identify the law governing non-consumer crypto-token contracts in arbitration. Although arbitration is not the Law Commission's primary focus here, it is also not excluded from this Call for Evidence's terms of reference (CFE Appx 1). The Rome I Regulation has the potential to apply in arbitration, notwithstanding Art. 1(2)(e) Rome I Regulation's exclusion of 'arbitration agreements', as that exclusion applies to arbitration agreements as separable contracts and not to the substantive matrix contracts within which arbitration clauses may appear (Benjamin Hayward, *Conflict of Laws and Arbitral Discretion: The Closest Connection Test*, Oxford University Press, 2017, 56 [2.14]).

Arts. 3–4 Rome I Regulation should, in principle, have the same operation in arbitration as in litigation, with one minor qualification based upon the absence of merits review in arbitration outside of the Arbitration Act 1996 (UK) s 69. This nuance means that (unlike in the litigation context) erroneous applications of the Rome I Regulation may stand without correction in arbitration. Otherwise, Arts. 3–4 Rome I Regulation will operate effectively in arbitration, just as in litigation, to the extent that they actually apply.

That extent is informed by the proposition that the Rome I Regulation applies compulsorily in England and Wales litigation, but does not apply compulsorily in arbitrations seated in England and Wales (seat here having its arbitration law, not its private international law, meaning: cf CFE xviii–xix). Pursuant to the Arbitration Act 1996 (UK) s 46(3), to the extent that there is no party choice of law in an arbitration (see generally Benjamin Hayward, 'Paying Attention to Choice of Law in International Commercial Arbitration – or – Why the Conflict of Laws Always Matters' in Michael Douglas et al (eds), *Commercial Issues in Private International Law: A Common Law Perspective*, Hart Publishing, 2019, 151), 'the tribunal shall apply the law determined by the conflict of laws rules which it considers applicable'. This rule confers discretion upon arbitrators to choose the conflict of laws rules that they apply. Those rules can be, but do not have to be, the Rome I Regulation (Benjamin Hayward, *Conflict of Laws and Arbitral Discretion: The Closest Connection Test*, Oxford University Press, 2017, 55 [2.14]). To the extent that minority opinion suggests that the Rome I Regulation is binding upon arbitrators (Burcu Yüksel, 'The Relevance of the Rome I Regulation to International Commercial Arbitration in the European Union' (2011) 7(1) *Journal of Private International Law* 149, 163–73), that view is premised upon the superiority of EU law and the direct application of EU regulations within EU Member States: both being considerations that are no longer relevant in the United Kingdom's context (see, eg, European Union (Withdrawal) Act 2018 (UK) s 5(A1)).

Given the non-mandatory status of the Arbitration Act 1996 (UK) s 46(3) (Arbitration Act 1996 (UK) s 4(2), sch 1), applicable law provisions in arbitration rules (which nearly always contain such provisions: Benjamin Hayward, *Conflict of Laws and Arbitral Discretion: The Closest Connection Test*, Oxford University Press, 2017, 54 [2.10]) will apply in preference to that provision (Arbitration Act 1996 (UK) s 4(3)). The Rome I Regulation's capacity to apply in arbitration pursuant to such arbitration rule applicable law provisions is outside of this Call for Evidence's scope given that arbitration rules 'are contractual in nature' (Benjamin Hayward, *Conflict of Laws and Arbitral Discretion: The Closest Connection Test*, Oxford University Press, 2017, 57 [2.19]) and are thus not the law of England and Wales.

(2) If the provisions cannot be applied, or can only be applied with significant difficulty, what are the possible solutions?

Building upon my response to Question 8(1), further – and slightly more difficult – issues also require exploration in order to fully demonstrate how Arts. 3–4 Rome I Regulation can apply to crypto-token contracts. Though – at least in theory (see CFE [6.190]) – the Rome I Regulation as assimilated European Union law can now be adjusted by the United Kingdom (CFE [2.47]), it is my view that no such adjustment is necessary.

The first and most important difficulty to address here concerns Lehmann's conception of omniterritoriality (CFE [3.94]), where crypto-token contracts 'cannot be linked to a specific country because they have simultaneous and equally valid connections to jurisdictions all over the world' (Matthias Lehmann, 'Extraterritoriality in Financial Law' in Austen Parrish and Cedric Ryngaert (eds), *Research Handbook on Extraterritoriality in International Law*, Edward Elgar Publishing, 2023, 427). Despite omniterritoriality being identified as a problem in the tech context, it is really just a specific manifestation of the evenly balanced connecting factors problem that has been recognised in the case law and in the literature for quite some time (see, eg, *Coast Lines Ltd v Hudig & Veder Chartering NV* [1972] 2 QB 34, 44; Benjamin Hayward, *Conflict of Laws and Arbitral Discretion: The Closest Connection Test*, Oxford University Press, 2017, 230 [6.15]; Australian Law Reform Commission, *Choice of Law*, Report No 58, 1992, 94 [8.38]). In my view, two existing solutions to the evenly balanced connecting factors problem can be applied within the Rome I Regulation's framework in the crypto-token contract context in order to overcome omniterritoriality.

Before looking to those solutions, it can be noted that omniterritoriality emerges as a genuine problem in the Rome I Regulation context first and foremost because Art. 4 Rome I Regulation is conceptually grounded in the closest connection test (Benjamin Hayward, *Conflict of Laws and Arbitral Discretion: The Closest Connection Test*, Oxford University Press, 2017, 250–1 [6.74]). Whilst Art. 4 Rome I Regulation's internal structure means that some omniterritoriality problems will be solved before they arise via the application of Arts. 4(1)(a)–(b), (2) Rome I Regulation, there remain some crypto-token contracts (including those analogous to barter: CFE [7.72]–[7.74]) where Art. 4(4) Rome I Regulation's closest connection test will be engaged. It is here that omniterritoriality problems may arise. Where that occurs, in my view, Art. 4(4) Rome I Regulation's closest connection test is sufficiently flexible so as to allow the omniterritoriality problem to be overcome.

The first solution involves judges, as a last resort, applying a tiebreaker test. This methodology is seen in the common law, where – in *Coast Lines Ltd v Hudig & Veder Chartering NV* [1972] 2 QB 34, 44 – Lord Denning MR held that where a charterparty is evenly connected to two jurisdictions, 'as a last

resort, you take the law of the flag'. The Rome I Regulation's autonomous interpretation requirement means that the common law cannot apply per se in the present context. Still, Art. 4(4) Rome I Regulation's closest connection test is sufficiently flexible to accommodate this type of reasoning. As to what the appropriate tiebreaker might be, judges might take into account the parties' legitimate expectations (CFE [6.167]–[6.169]) and perhaps also substantive justice considerations (CFE [6.170]–[6.172]), noting that the closest connection test 'effectively seeks to ascertain the law that reasonable persons in the parties' positions would have identified' (Benjamin Hayward, *Conflict of Laws and Arbitral Discretion: The Closest Connection Test*, Oxford University Press, 2017, 212 [5.55]).

The second solution arises only where omniterritoriality presents with respect to a crypto-token contract that is closely related to another contract having a more easily identifiable applicable law. In those circumstances, that closely related contract's applicable law becomes a relevant consideration in applying Art. 4(4) Rome I Regulation's closest connection test (CFE [7.76]–[7.77]). This proposition is reflected in the Rome I Regulation's own text, via its Recital [21], but is also reflected in judicial practice under Arts. 4(1), (5) Rome Convention (see, eg, *PT Pan Indonesia Bank Ltd TBK v Marconi Communications International Ltd* [2005] EWCA Civ 422, [55]; *The Bank of Baroda v The Vysya Bank Ltd* [1994] 2 Lloyd's Rep 87, 93). Where a crypto-token's connecting factors are otherwise evenly balanced because of the omniterritoriality problem, Art. 4(4) Rome I Regulation's flexibility permits judges to apply the closely connected contract's governing law, in a manner akin to a tiebreaker. Again, whilst Rome Convention jurisprudence is not automatically applicable under the Rome I Regulation given the latter instrument's autonomous interpretation requirement, the width of Art. 4(4) Rome I Regulation's closest connection test discretion permits this method of reasoning (Lord Lawrence Collins and Jonathan Harris (eds), *Dicey, Morris and Collins on the Conflict of Laws*, Sweet & Maxwell, 16th ed, 2022, 1831–2 [32-090]).

As is apparent from my explanation of these solutions, the key to both is the width of Art. 4(4) Rome I Regulation's closest connection test discretion. That discretion's width can be confirmed with reference to arbitration sources – arbitration being a context where the closest connection test is often applied (Benjamin Hayward, *Conflict of Laws and Arbitral Discretion: The Closest Connection Test*, Oxford University Press, 2017, 188–9 [5.03]) – and also a context in which arbitrators in general enjoy significant discretion in identifying the governing law (Benjamin Hayward, *Conflict of Laws and Arbitral Discretion: The Closest Connection Test*, Oxford University Press, 2017, 98 [3.03]). In arbitration, the closest connection test is recognised as conferring discretion with respect to arbitrators' identification of the relevant connecting factors and also with respect to their weighting of those factors (Benjamin Hayward, *Conflict of Laws and Arbitral Discretion: The Closest Connection Test*, Oxford University Press, 2017, 229 [6.14]). And since discretion implies the need for the exercise of judgment, it has even been said that 'it is difficult to argue' that an arbitrator's exercise of an applicable law discretion is 'wrong' (Franz Schwarz and Christian Konrad, *The Vienna Rules: A Commentary on International Arbitration in Austria*, Kluwer, 2009, 621 [24-046]). Though arbitration differs from litigation in that, outside of the Arbitration Act 1996 (UK) s 69, there is no review on the merits in arbitration, it remains the case that Art. 4(4) Rome I Regulation embodies sufficient flexibility so as to accommodate the two omniterritoriality solutions that I identify here. Notably, too, both solutions draw upon existing '[j]udicial experience in applying applicable law rules' (CFE [6.188]).

Secondly, and incidentally, reference can be made to the Law Commission's comments concerning incentivising party choice of law, arising in the property law context and with reference to the UNIDROIT Principles on Digital Assets and Private Law (CFE [6.177]–[6.179]). For the avoidance of any doubt, where judges are required to identify the governing law for a non-consumer crypto-token contract, applicable law rules should not take the form of penalty defaults that parties are expected to avoid via their own choices of law (Benjamin Hayward, *Conflict of Law and Arbitral Discretion: The Closest Connection Test*, Oxford University Press, 2017, 155–6 [4.28]). There are many reasons why parties to commercial contracts may not choose a governing law in the ordinary course of events (ICC Case No 7375/1996 (1996) 11(12) *Mealey's International Arbitration Report* A-1, A-35 [275]), crypto-token transactions present their own particular choice of law practices (CFE [7.33]), and many of the reasons why parties may not choose a governing law do not involve any legitimate attribution of party blame (Benjamin Hayward, *Conflict of Laws and Arbitral Discretion: The Closest Connection Test*, Oxford University Press, 2017, 114–18 [3.49]–[3.56], 156 [4.28]). It is thus important to confirm – as my responses to Questions 8(1) and 8(2) have sought to do – that Art. 4 Rome I Regulation can effectively identify the governing law for crypto-token contracts, even if there are often good reasons for parties to choose their own governing law (CFE [7.33]).

(3) If the provisions can be applied easily or without undue difficulty, are there any areas that would benefit from further clarification?

The matters that I have addressed with respect to Questions 8(1) and 8(2) all represent issues that would benefit from further clarification, which I have attempted to provide.

(4) To what extent is the application of these provisions problematic in practice?

The comments provided here with respect to Questions 8(1) and 8(2) are offered from an academic (rather than a practitioner or an industry expert) perspective. Whilst I therefore cannot comment on their prevalence or likely prevalence in practice, they remain important legal matters warranting attention.

(5) If the issue is prevalent in practice, what would be the consequences if it were not resolved adequately as a matter of law?

Assuming prevalence for present purposes, a failure to properly appreciate and clarify the matters that I have addressed in my responses to Questions 8(1) and 8(2) would embed uncertainty into the law. Such uncertainty would be inconsistent with the way in which England and Wales promotes its commercial law to the rest of the world, and may in turn adversely affect the economic activity that choices of English law (and choices of the England and Wales legal forum) support (see Stefan Vogenauer, 'Regulatory Competition Through Choice of Contract Law and Choice of Forum in Europe: Theory and Evidence' (2013) 21(1) *European Review of Private Law* 13, 31, 34).

Law Commission's Call for Evidence:
Digital assets and ETDs in private international law: which court, which law?

Response on behalf of Herbert Smith Freehills LLP

This is a response on behalf of Herbert Smith Freehills LLP to the Law Commission's Call for Evidence on digital assets and ETDs in private international law. We have not sought to comment on every question in the Call for Evidence.

As a preliminary point, we note that there are various suggestions in the Call for Evidence that it may be more difficult to enforce an English judgment abroad if the English court has not taken jurisdiction on a "clear and internationally recognised basis" (see eg paras 4.105 and 5.98) – the apparent implication being that an English judgment is likely to be enforceable abroad if the English court has taken jurisdiction on such a basis.

But this should not be taken too far. As the Call for Evidence recognises (at para 2.51), unless the foreign country is party to either the Hague Choice of Court Convention 2005 or the Hague Judgments Convention 2019¹, it will apply its own rules to the question of whether or not it should enforce a foreign (including an English) judgment.

An English judgment will only be enforceable under the Hague Conventions if (under Hague 2005) it is given pursuant to an exclusive English jurisdiction clause or (under Hague 2019) it meets at least one of a number of eligibility criteria, of which the only ones likely to apply to disputes relating to digital assets / ETDs are (in broad summary):

- Defendant's habitual residence, principal place of business, or branch / agency / establishment in state of origin
- Defendant agreed or submitted to jurisdiction of court of origin
- Judgment rules on a contractual obligation that took place, or should have taken place, in state of origin ("unless the activities of the defendant in relation to the transaction clearly did not constitute a purposeful and substantial connection to that State")

(The only eligibility criterion under Hague 2019 relating to tort claims is unlikely to apply as it is limited to claims arising from death, physical injury and damage to or loss of tangible property.)

Where the Hague Conventions don't apply, and it comes down to the rules of the foreign court, there is no reason to be confident that most of the grounds on which the English courts are currently prepared to take jurisdiction (ie under the various common law / CPR gateways) would be sufficient to allow enforcement of an English judgment. In the reverse circumstances, most of those grounds would not in fact be sufficient to allow an English court to enforce a foreign judgment. Under common law rules, an English court will enforce a foreign judgment **only** if the foreign court had jurisdiction on the basis of the defendant's presence in the foreign state when the proceedings were brought, or its agreement or submission to the jurisdiction of the courts of that state. So, for example, it would not be sufficient (in and of itself) if the relevant contract was concluded in the foreign state, or an unlawful act was committed or damage suffered there, even though the English court is itself perfectly happy to exercise jurisdiction on such grounds (subject to considerations of *forum conveniens*).

So while the questions raised by the Call for Evidence about whether or how the various jurisdictional gateways should be applied to claims relating to digital assets are perfectly legitimate ones, in terms of when the English courts should properly be prepared to exercise jurisdiction over such claims, the answers to those questions will not necessarily influence whether an English judgment given in such a claim will be enforced by a foreign court.

¹ The UK is not yet party to Hague 2019 but it has signed it and intends to ratify as soon as possible, so it should come into effect for the UK around the middle of 2025 and apply to proceedings commenced after that date.

Question 2

- (1) Where a contract has been concluded by a machine or the operation of smart contract code, we can see that it may be difficult to apply the connecting factor (which essentially depends on the location of the offeree or offeror at the time of the offer or acceptance respectively) to the participating computer. However, we do not see any justification for applying that connecting factor to the "real-world actor", whether on the basis of their habitual residence or domicile or on the basis of where they happen to be at the time of the offer or acceptance.

The rationale for the gateway based on contract formation, as we understand it, is that where parties choose to conclude a contract in a foreign jurisdiction (including by communicating the offer or acceptance to a person in that jurisdiction) they voluntarily create a link between their contract and that place – though even that basic proposition may be difficult to justify in these days of mobile communication, where parties may be anywhere in the world when they receive a call (or text message, email, etc) communicating a contractual offer or acceptance, without the sender of that offer or acceptance knowing where the recipient is.

In circumstances where the parties do not themselves receive the offer or acceptance, but the contract is instead concluded by a machine, a rule based on where the parties happen to be at the time of the offer or acceptance would seem entirely random.

A rule based on where the parties are domiciled (or habitually resident) at the time of the offer or acceptance would also seem difficult to justify. In any event, there is already a gateway that applies where the defendant is domiciled in England and Wales (and domicile for those purposes is a broad concept that essentially encompasses habitual residence). Extending the "contract formation" gateway to the domicile or habitual residence of both offeror and offeree would mean that the court could exercise jurisdiction in practically all cases where the claimant is domiciled or habitually resident here. That would seem contrary to principle.

- (2) Not applicable.
- (3) We have not seen the question of where a smart contract is made arise in practice in our cases to date.
- (4) We expect that in most cases where a smart contract is (at least arguably) made in England and Wales, it is likely that there will be other connecting factors with the jurisdiction that mean another gateway will apply. Where there are no such factors, it may be doubtful whether the court would find England and Wales to be the appropriate forum in any event.

Question 3

- (1) No, we agree with the view expressed in the Call for Evidence that the case law to date is inconsistent.
- (2) Clerk & Lindsell on Torts defines pure economic loss as "an economic loss to the claimant which does not result from any physical damage to or interference with his person or tangible property". If that definition is adopted and digital assets are concluded not to be "tangible property" in this context, it seems unlikely that tortious damage pleaded in the crypto-token litigation context would be anything other than pure economic loss. The Law Commission may wish to consider, however, whether / how this rule would apply in relation to its proposed third category of property.
- (3) This question raises issues that go far beyond disputes relating to crypto tokens. In the *Brownlie* case, in the context of a personal injury claim, the Supreme Court held that the tort gateway was satisfied by indirect damage, and there was no reason to limit the gateway to direct damage as required by the EU jurisdiction rules (ie under the recast Brussels Regulation and its predecessors) and no reason that damage for the purposes of jurisdiction should be interpreted consistently with damage for the purposes of the applicable law rules under Rome II, which distinguish between direct and indirect damage (though that distinction is by no means straightforward to apply in cases of pure economic loss, as the cases referred to at para 9.17 of the Call for Evidence illustrate).

The court held that “damage” for the purposes of the gateway simply referred to actionable harm, direct or indirect, caused by the wrongful act alleged. The court was satisfied that this wider reading of “damage” would not mean claimants based in England could always sue in the English courts, since the “forum non conveniens” rules mean the English courts can decline to exercise jurisdiction where there is a more appropriate forum for the dispute.

The Supreme Court noted, however, that there is an important difference between a case involving physical damage, as in that case, and the case of a tort which is wholly economic in nature. It recognised that the latter situation can give rise to complex and difficult issues as to where the damage was suffered, calling for a careful analysis – and that the mere fact of some economic loss, however remote, felt by a claimant where they were based would be an unsatisfactory basis for the exercise of jurisdiction – but it did not give further guidance as to how the courts should approach such a case.

Against that background, our view is that there may be a case for reviewing whether the tort gateway should apply to damage that is merely indirect, at least in cases of pure economic loss if not more generally – ie to restrict or potentially reverse the effect of *Brownlie*. However, the impact of this question goes far beyond disputes relating to digital assets. Any consideration of this question should therefore have in mind the entire range of tortious disputes that might be affected, rather than simply those relating to digital assets.

Question 4

- (1) It is difficult to say whether the courts' approach so far is theoretically sound, as there appear to be very few crypto cases (if any) in which the court has considered in any detail the gateways based on where the unlawful act was committed.

The general rule, at least in the context of the tort gateway relating to an act committed within the jurisdiction, is that there must be “substantial and efficacious acts” committed within the jurisdiction, even if other acts constituting the tort have taken place elsewhere.

In the context of a misrepresentation claim, it is legitimate to look at where the misrepresentation is received and acted upon (see eg *The Albaforth* [1984] 2 Lloyd's Rep 91). So to the extent that the courts have found this gateway to be satisfied even where those perpetrating a fraud may have been abroad at the time they made representations to individuals in England, this approach is not necessarily inconsistent with principle.

However, we do not consider that it would be legitimate to decide that an unlawful act was committed in England simply because the claimant was domiciled in England. If that is the basis for the court's decision in *Jones v Persons Unknown* (as suggested at para 5.72(1) of the Call for Evidence), we do not consider that approach to be theoretically sound, though we would note that the court's decision on the point is very brief and not entirely clear.

- (2) If a broad approach continues to be taken to the question of when damage is sustained within the jurisdiction, claimants are unlikely to have to rely on this gateway very often, at least in claims relating to tort. How often it matters will also depend on the approach the courts take to other relevant gateways, including the gateways relating to property or assets within the jurisdiction.

See also our comment in response to Question 11, below, that any recommendations for reform should be considered against the broader context of potential cases, rather than just fraud claims against “persons unknown” which have tended to be most prevalent to date in terms of the claims coming before the court.

Question 5

- (1) It seems fair to say that, to date, the English courts' approach to localising a crypto-token for the purposes of jurisdiction has had a shaky theoretical underpinning. As noted in the Call for Evidence, most of the cases that have considered this question have concluded that a crypto-token is located where its owner is domiciled, based on an academic article by Professor Andrew Dickinson in the context of applicable law rules, but as pointed out in the *Tulip Trading*

case Professor Dickinson's article actually supports an approach based on residence or place of business (not domicile) of the participant in the relevant DLT system (not necessarily the owner).

Given the conceptual difficulty in identifying any particular location for a crypto-asset, it would seem sensible to lay down a rule that should apply in all such cases. Between domicile and residence / place of business, in cases where there is a difference, we consider that the latter would represent a closer connection with the jurisdiction in question and so would be preferable.

As for whether it should be the owner of the cryptoasset or (where different) the participant in the DLT system whose residence / place of business is relevant, we consider that it should be the latter.

- (2) Based on the wording of the gateways, the better argument would seem to be that the assets must be within the jurisdiction at the time of the application for service out. In light of the conflicting case law, however, it would be helpful to have greater clarity on this point.
- (3) The question of where a crypto-token is located for the purpose of jurisdiction is important in many cases.

Question 6

- (1) The question of whether there is a serious issue to be tried that an exchange has received crypto-assets as constructive trustee will depend on the facts and circumstances of each case, including whether the claimant has a real prospect of establishing that the exchange received the claimant's assets and that it was on notice of the claimant's interest in them.
- (2) To date exchanges have tended to defend such claims on the basis that: (i) they did not receive the claimant's assets; or (ii) if they received them, they did so as a bona fide purchaser for value without notice and therefore free of the claimant's interest, alternatively that they disposed of them in the ordinary course of business before they had notice of the claimant's interest. See for example the defences filed by the various exchanges in the case of *D'Aloia v Persons Unknown*, which are publicly available.
- (3) We are not sure what this question has in mind. As noted above, the question of whether there is a serious issue to be tried in such claims is highly fact-dependent, but that is not surprising. We do not think it gives rise to problems as a matter of principle.
- (4) If this question is asking whether there is a need to consider a departure from the test of "serious issue to be tried", either in this context or more generally, then our answer is "no". The test is long-established and seems to us to be perfectly serviceable both in the context of digital assets and more generally.

If however the question is asking whether there is a need for judges deciding applications for permission to serve out in this context to consider more carefully whether the claimant has in fact established that there is a "serious issue to be tried", then our answer is "yes". In our experience, there is very little scrutiny of the claimant's evidence in support of such applications, including whether the expert evidence relied on as to the exchange's receipt of the relevant assets has been prepared by someone with appropriate expertise and whether the expert has applied an appropriate methodology.

Question 11

- (1) We accept that most of the tort claims in this area to date have been against "persons unknown" who have committed a crypto fraud. There may in due course, however, be more traditional tort claims relating to crypto-assets, eg alleging negligence. Any recommendations for reform should therefore be considered against the broader context of potential cases, rather than just fraud claims against "persons unknown".
- (2) Although there may not be English case law on where tortious damage has been suffered for the purposes of Rome II and/or the Brussels regime in the context of crypto assets, there is

case law applying the CJEU jurisprudence in the context of other forms of pure economic loss, such as an investment in shares in *Kwok Ho Wan v UBS AG* [2023] EWCA Civ 222 (a transitional case applying the Lugano Convention, where the requirement for direct damage mirrors that of the recast Brussels Regulation).

In that case the claimants sued UBS (domiciled in Switzerland) claiming that UBS's alleged negligent misstatements and advice in Hong Kong had led them to make an investment in shares that was almost completely lost when UBS in London had exercised its right under a security agreement to sell the shares. Both the High Court and Court of Appeal held that the damage was suffered in London because that was where it was manifested, ie where the shares had been held and sold. The Court of Appeal emphasised that the question of where damage is manifested is fact-dependent, and it is therefore dangerous to seek to define the test for where damage occurs in a wide range of financial loss cases.

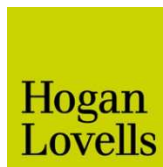
It may be that, at least in some cases, it is particularly challenging to decide where pure economic loss is "manifested" in the context of crypto assets, even compared to other cases relating to financial loss. But it is not clear to us that there is a better solution than leaving this question for the courts to decide on the facts of a particular case.

Question 19

We consider that how the lex situs of a digital asset is determined should be consistent with how a digital asset is localised for the purposes of jurisdiction. See our response to Question 5 above.

Herbert Smith Freehills LLP

16 May 2024



HOGAN LOVELLS INTERNATIONAL LLP

DIGITAL ASSETS AND ETDs IN PRIVATE INTERNATIONAL LAW: WHICH COURT, WHICH LAW?

RESPONSE TO CALL FOR EVIDENCE

Hogan Lovells International LLP
Atlantic House
Holborn Viaduct
London
EC1A 2FG

TABLE OF CONTENTS

| | | |
|-----------|--|----------|
| 1. | INTRODUCTION AND SCOPE | 1 |
| 2. | OVERARCHING PRINCIPLES | 1 |
| 3. | MISAPPROPRIATED DIGITAL ASSETS | 4 |
| 3. | TAKING SECURITY OVER DIGITAL ASSETS | 6 |
| 4. | SMART CONTRACTS | 8 |

1. INTRODUCTION AND SCOPE

- 1.1 In this document, we respond to the Law Commission's call for evidence: Digital assets and ETDs in private international law: which court, which law? (the "**Call for Evidence**"). The views expressed in this document are our own. However, we have, in considering our views, discussed the Call for Evidence with a number of our clients. Our views are therefore informed by these discussions.
- 1.2 The Call for Evidence relates to a variety of issues of private international law ("**PIL**") that arise from the digital, online and decentralised contexts in which modern digital assets and electronic trade documents are used. The Call for Evidence focuses on two key questions of PIL:
- (a) In which country's courts should parties litigate a dispute ("**jurisdiction**")?
 - (b) Which country's law should be applied to resolve the dispute ("**applicable law**")?
- 1.3 The Call for Evidence seeks input from stakeholders on questions listed in Chapter 13 of the Call for Evidence (the "**Questions**") in order to help the Law Commission identify and understand the main challenges and priorities in these PIL areas so that it can focus its future work appropriately. We do not seek to answer each Question; instead we have focused on areas we believe may benefit the most from clarification and/or matters we consider must be prioritised when considering next steps in providing such clarification.
- 1.4 This response considers challenges and clarification required in relation to PIL issues arising in the following contexts:
- (a) Overarching principles to bear in mind in determining PIL principles in digital assets.
 - (b) Disputes relating to misappropriated digital assets and particularly proprietary claims to misappropriated digital assets.
 - (c) Taking security over digital assets, providing certainty to those taking security and those in the transactional chain.
 - (d) Expressing a choice of law and smart contracts.
- 1.5 As the points set out at 1.4(a) – (d) above can be considered to fall into a number of the Questions raised in the Call for Evidence, for ease, we have identified in each section below Questions most relevant to the comments made.

2. OVERARCHING PRINCIPLES

- 2.1 As we have considered the Call for Evidence, a number of repeating themes have arisen that constitute useful overarching principles with which to approach the Questions.

Minimal intervention

- 2.2 While uncertainties exist and current laws are not entirely fit for purpose, we do not believe a full set of new PIL principles are required. Market participants have approached digital asset product design and use cases based on current laws and assumptions as to how those laws (and not a new set of laws) would or should apply as regards jurisdiction and governing law issues. A large degree of international agreement (including through treaties), cooperation and co-ordinated recognition is built into existing PIL principles and

whilst jurisdictional and governing law-based disputes still do clearly arise, it is helpful for maintaining confidence in developing digital assets markets that existing principles continue to apply to the extent possible. This is particularly the case in respect of assets that are simply recorded on DLT systems, where we would encourage the applicable principles should mirror those of the underlying asset itself. So although we have identified points for clarification and certain gaps that need to be filled, this should be done as far as possible using a minimal intervention approach, rather than developing a new legal approach to dealing with digital assets.

International cooperation

- 2.3 PIL requires cooperation and comity between courts in different jurisdictions. As mentioned above, this is evident in existing PIL principles. The development of new laws (or even provision of clarifications) for England and Wales without broader international agreement may not provide complete certainty to market participants. Any single jurisdictional approach will not prevent competition between litigants to be the first to bring a dispute to their preferred jurisdiction meaning that PIL uncertainties may continue. To avoid this, it may be necessary to review the approach in other jurisdictions and to compare that with any new principles and clarifications identified as a result of this Call for Evidence and to seek international agreement if appropriate. For this reason, again we prefer an approach that retains current laws so far as possible.

PIL and international regulation

- 2.4 As market participants continue to adapt to, and work to ensure compliance with, evolving and growing international regulations in the digital assets space, it would be preferable to limit competition between applicable law and regulatory powers. It would also be helpful for regulatory certainty that the way in which questions of “situs” are dealt with in respect of digital assets does not operate to bring market participants within unexpected regulatory perimeters. As such, so far as possible, we support an approach that seeks to match the scope of jurisdiction of national regulators with applicable laws governing digital assets.

3. MISAPPROPRIATED DIGITAL ASSETS

[Potentially relevant Questions include: Questions 3(1), 4(1), 4(2), 5(1) and (3).]

- 3.1 As the Call for Evidence identifies, English Courts have been required to deal with a number of claims that relate to allegations about the misappropriation of digital assets. These disputes have often arisen following cyber-attacks but can also flow from frauds or online scams.
- 3.2 Typically, an individual whose digital assets have been misappropriated can fairly easily trace them to an exchange or wallet. Claimants have sought recovery of the assets from (i) the alleged wrongdoers; or (ii) a third party such as an exchange or the issuer of a digital asset. The cases so far have largely been interim applications including interim proprietary injunctions and freezing orders as well as applications seeking disclosure of information from exchanges in relation to account holders.
- 3.3 We summarise the approaches taken by English courts in relation to jurisdiction and applicable law briefly below.

Jurisdiction

- 3.4 Greater clarity is needed on how English courts should determine whether they have jurisdiction to determine claims relating to misappropriated digital assets.

- 3.5 To date, claimants have framed their claims in different ways and relied upon different jurisdictional gateways (tort, property, constructive trust, restitution and breach of confidence) to bring their interim claims before the English courts. While the common theme of recent cases is that English courts have been relatively sympathetic to claimants based in England and Wales, the caselaw is inconsistent. For example, the connecting factor for the court to take jurisdiction in *Ion Science*¹ was held to be the place where the claimant was first deprived of access to the misappropriated crypto-tokens. In *Tulip Trading*², it was found to be the place where the claimant would experience the deprivation of access to the misappropriated crypto-token. In contrast, in *Lubin Betancourt Reyes*³, it was found to be the place of the claimant's habitual residence and/or where the claimant conducts business. In *Jones*⁴ it was the place of the Claimant's domicile.
- 3.6 The varying approaches offer uncertainty and could lead to inconsistent findings. For example, applying the current case law, where an English claimant was situated in Spain when their crypto-tokens were misappropriated, applying the different cases, an English court could conclude that jurisdiction belongs to:
- (a) English courts on the basis of the claimant's habitual residence; or
 - (b) Spanish courts on the basis of where the claimant was first deprived of access to the digital assets.

Applicable law

- 3.7 Again, English courts have not taken a consistent approach to determining the law applicable to disputes about misappropriated digital assets. In summary.
- (a) In *Ion Science*⁵, the claimants alleged that false representations had been made in relation to an initial coin offering, meaning that a claimant gave control of his computer to fraudsters for the purpose of transferring funds. It was held that applicable law would be the law of the location of a cryptocurrency, being the place where the person or company who owns it is domiciled.
 - (b) In *Tulip Trading*⁶, at first instance, the parties were in dispute as to whether the bitcoin should be regarded as being located in the Seychelles, as the place of the first claimant's domicile, or in England, as the place of residence. It was held that the law applicable to the dispute was the law of the location of control of a digital asset, including the storage of a private key.
 - (c) In *D'Aloia v Persons Unknown*⁷, an individual alleged he had been misled into using a trusted website by wrongdoers who had misrepresented their connection to the website and induced the claimant to transfer crypto-tokens into a digital wallet. Citing *Ion Science*⁸, it was held that there was a good arguable case that damage would be sustained in England because it was where the cryptocurrency was held

¹ *Ion Science v Persons Unknown* (21 December 2020) EWHC (Comm) (unreported).

² *Tulip Trading Ltd & others v Bitcoin Association for BSV & others* [2023] EWCA Civ 83 at [164].

³ *Lubin Betancourt Reyes v Persons Unknown* [2021] EWHC 1938 (Comm).

⁴ *Jones v Persons Unknown* [2022] EWHC 2543 at [30].

⁵ *Ion Science v Persons Unknown* (21 December 2020) EWHC (Comm) (unreported).

⁶ *Tulip Trading Ltd & others v Bitcoin Association for BSV & others* [2022] EWHC 667 (Ch) at [142] at [148].

⁷ *D'Aloia v Persons Unknown* [2022] EWHC 1723 (Ch).

⁸ *Ion Science v Persons Unknown* (21 December 2020) EWHC (Comm) (unreported).

immediately before the misrepresentations and the deceit. This therefore led courts to conclude that the applicable law should be the law of England & Wales.

Exchanges as potential constructive trustee

- 3.8 Another element of cases relating to misappropriated digital assets that we have seen in the current case law is that these disputes often rely on co-operation from the exchange. While exchanges are sometimes prepared to provide information about an account holder or to freeze a potentially fraudulent account, and even to give control of an account to a claimant (following a court order), they are unlikely to agree that they are constructive trustees or that they have assumed a duty through holding the misappropriated asset that is no longer in their control. We do not express a view on this position, save to note it is likely to be an important area of dispute where PIL issues may well arise if not addressed.

Clarification required

- 3.9 As is clear from the above, litigants and English courts have so far taken varying approaches to frame disputes and determine questions of jurisdiction and applicable law. In cases so far, we have seen limited, if any, challenge from Defendants or other related parties. We are concerned that, if and when Claimants eventually proceed beyond an interim application and seek permanent recovery of the digital assets, or a final award of damages resulting in the misappropriation, PIL issues will be more stringently tested. We consider this is more than a theoretical risk and matters will inevitably be tested. It is therefore our view that it is an area that would benefit from clarification and certainty. As use and ownership of digital assets increases, and in order to enhance the markets and use cases, we believe that trust and confidence in an owner's proprietary rights is a priority. Clarification of PIL issues outlined above will enhance and compliment the Law Commission's proposed introduction of a third kind of property (Law Commission's Final Report on Digital Assets⁹). Given the context and use of digital assets, it may be appropriate to seek to give priority to parties' choice of jurisdiction and applicable law over other principles where possible.

4. TAKING SECURITY OVER DIGITAL ASSETS

[Potentially relevant questions include: Questions 19(1) and 19(3).]

- 4.1 Another issue which is impacting market participants is how to take effective security over digital assets, in particular with regard to straightforward enforcement with predictable jurisdictional parameters. In practice, the ability to grant effective security and have certainty around enforcement is vital to the functioning of modern day commercial transactions. It is common for security to be granted over tangible moveable objects (such as machinery) but even this traditional use of security can raise PIL issues because it is possible for the assets in question to move across territorial borders and property laws may differ from country to country. It is also common for security to be granted over choses in action, for example pursuant to assignments by way of security, where the governing law of the security generally follows the governing law of the underlying contract. However, PIL issues can also arise here due to governing law uncertainties which may effectively pass-through from an underlying contract. PIL issues are amplified in relation to security over digital assets because of the interaction between effective security and proprietary

⁹ Law Commission's Final Report on Digital Assets which can be accessed here: <https://s3-eu-west-2.amazonaws.com/cloud-platform-e218f50a4812967ba1215eaecede923f/uploads/sites/30/2023/06/Final-digital-assets-report-FOR-WEBSITE-2.pdf>

rights in respect of digital assets, which itself would benefit from clarification, as set out in paragraph 3.9 above.

- 4.2 Security can be relevant for digital assets transactions in a number of ways (and many that we or our clients are unlikely to fully understand yet, given the evolution of decentralised finance models). As it stands, to some degree due to technology features around private keys (particularly the concept of establishing exclusive control) and to some degree due to situs and other PIL uncertainties (particularly as to, for example, what governing law is going to be effective as regards decentralised cryptoasset collateral), tri-partite control agreements using a custodian (essentially who can hold, and transfer effective control of, private keys between transactional parties), and which agreement has a clear chosen governing law, is often put forward as a solution to lack of certainty regarding proprietary rights based security in respect of cryptoassets collateral.
- 4.3 However, tri-partite control arrangements may also not always be effective, for example if there are asset recovery complications due to undisclosed sub-custody arrangements, fraud, theft and technology failures. In these types of circumstances, lenders may well want certainty of effective proprietary-based security that they can enforce over the borrower's property rights in the underlying cryptoassets themselves (security which, when enforced, establishes appropriate priority of title in favour of the lender in respect of those cryptoassets over potential competing title claims of third parties in respect of those assets), and not just rely on contractual claims against the borrower and potentially the custodian in light of the failed control arrangement.
- 4.4 It is also conceivable that security might be granted to two parties over the same digital assets. The hierarchy of that security may be challenging to determine for digital assets; for example if knowledge of private keys might be shared by more than one party, each of whom might take competing jurisdiction and applicable law positions in their own favour. In the absence of clear contractual terms, such issues such may be difficult to reconcile for digital assets and may turn on challenging questions, such as the situs of digital assets.
- 4.5 In addition, an intermediary custodian may not always be appropriate for a structure. Cryptocurrency assets can be self-custodied by a borrower or held at an exchange where it is not appropriate for the exchange to be involved in the borrower's financing arrangements. If security can only be confidently obtained over those assets by the intervention of a third party, that seems potentially limiting by comparison to traditional collateral which does not require an intermediary to confidently apply security structures including assignments by way of security and charges, for example.
- 4.6 Questions over appropriate form and governing law of security to establish effective proprietary rights on enforcement over digital assets may be somewhat mitigated in a situation where a digital asset had a governing law applied to it on issuance, such as may be the case with a native digital bond, where the associated bond terms and conditions may include relevant provisions, where it was created on a private platform and the platform terms included relevant provisions, where it is a digital asset that is "linked" to a real world asset (such as a tokenised, non-native, security that refers to a traditional underlying), where the terms applicable to the underlying may be adopted as being the same for the linked digital asset (particularly in this latter case, we expect that if this is considered pragmatic and appropriate, clarity could be given concerning this intended treatment for a linked digital asset).
- 4.7 We expect that greater certainty on these security-based issues would enable institutions and financiers to scale their financing activities that use digital assets as collateral, and that in turn will generate more appetite for creation and investment in digital assets across the

financial markets. English law has a particularly flexible form of security commonly used to support lending transactions in the form of the floating charge, typically forming part of the security package within an English law governed “all assets debenture”. For businesses which have a substantial proportion of their assets in the form of cryptocurrency and digital assets (including looking forward to the future when this may be increasingly the case), having these accepted by lenders as part of the “acceptable collateral” within a standard all assets debenture security approach, would clearly be valuable in terms of replicating existing secured financing transactions in the traditional markets.

5. SMART CONTRACTS

[Potentially relevant Questions include: Question 2(3) and 2(4)]

- 5.1 Save for certain limited exceptions (eg in relation to consumer contracts), English courts will protect contractual parties’ right to choose the jurisdiction and applicable law of disputes relating to a contract. The same principle of contractual freedom should be protected in the digital assets space. Our experience of working with smart contracts demonstrates that there is some uncertainty in the market as to how to record a choice of law in smart contracts and whether that choice will be supported if tested.
- 5.2 In the absence of an express choice of law, there are difficulties in determining which court should take jurisdiction and which law should apply to a smart contract in particular. However, we would anticipate that most users would make a choice if it was clearly supported.
- 5.3 Options for recording a choice of jurisdiction and governing law include:
 - (a) Inserting wording describing a choice in a free text box;
 - (b) Including the choice in a linked website; and
 - (c) Including the choice in the website that leads to the smart contract.
- 5.4 While industry convention may be sufficient to identify the most appropriate method, guidance from legislature that supports the principle and provides clarity would be valuable. This is especially so when dealing with consumers and individuals.

Hogan Lovells International LLP

16 May 2024

Submitted to Law Commission Call for Evidence on digital assets and ETDs in private international law
Submitted on 2024-05-13 16:55:57

About you

What is your name?

Name:
Dr Sara Hourani

What is your email address?

Email:
[REDACTED]

What is your telephone number?

Telephone number:
[REDACTED]

Questions on international jurisdiction - specific issues (Chapter 5)

Question 1: In this question, we seek views and evidence on jurisdiction over consumer contracts.

Please share your views and evidence below::

(1) To what extent can the issue of jurisdiction over consumer contracts in the digital and decentralised contexts be accommodated by section 15B of the Civil Jurisdiction and Judgments Act 1982?

It can be stated that if a consumer enters into a transaction with a trader (such as a crypto exchange platform) in the UK as a result of having found or accessed the trader's platform in this jurisdiction, then this would fall under the scope of section 15B of the Civil Jurisdiction and Judgments Act 1982. Many crypto exchange platforms operating in the UK indicate in their terms and conditions that the relevant applicable law to the transactions concluded with them and competent courts to deal with disputes arising from these transactions are those of England and Wales.

This can of course be debated as there is no clear position or meaning provided by English law on what the 'pursuit' or 'direction' of trading activities in the UK through the internet would constitute.

(2) Does the fact that the business is a crypto-business, as opposed to any other business, change the analysis of whether a business has directed its services to consumers located in the UK?

No- the contract between the consumer and the cryptocurrency exchange trader is not decentralised in nature as the practice in the majority of cases has so far been to use clickwrap agreements concluded over the internet.

(3) Are there any changes or clarifications that are needed in respect of the issue of jurisdiction over consumer contracts?

Yes- there is a need for clarification on the position or meaning on what the pursuit or direction of trading activities in the UK through the internet would be under English law.

(4) To what extent does this issue cause problems in practice (or is likely to in future)?

This further clarification would be important if for example the contract between the trader and the consumer would be in the form of a smart contract that is solely based in code and that runs on a blockchain network, as this could cast uncertainty on different aspects of the transaction such as the place where the contract was concluded.

Question 2: In this question, we seek views and evidence on jurisdiction founded on the basis that a contract was concluded in England and Wales.

Please share your views and evidence below::

-How should the courts apply gateway 6(a) to a smart contract? Should the relevant connecting factor be the participating computer, or the real-world actor?

Real world actor- especially in the case of a consumer transaction as this position adds more legal certainty. The adoption of the participating computer position in light of the first part of gateway 6(a)(ii) might add confusion as to whether acceptance has been made as it might have just solely been made by computer nodes. Placing focus on the interaction between computer nodes at this moment in time would thereby create uncertainty regarding whether acceptance has been communicated.

-If gateway 6(a) should use a connecting factor based on the real-world actor, how should their location be determined? Should it be by their habitual residence, their domicile, or at the place where they happen to be at the time the contract was formed?

If the position of the connecting factor of the real-world actor is adopted, then it would be logical to determine their location based on the place where they happened to be at the time the contract was formed.

For consumer protection purposes, it might make more sense to choose the habitual residence and their domicile approach, but this could clash with the location where the real-world actor concluded the smart contract.

However, if the real-life actor's bank account or main financial activities are held in England and Wales, it could be possible to determine their location according to their domicile or habitual residence. Choosing this position might also allow the claimant to benefit from more rights to raise a claim in case of breach as shown by English case law involving cryptocurrencies so far.

-To what extent is it likely that the question of where a smart contract is made will become prevalent in practice?

It depends on how widespread the practice of smart contracts becomes. It seems likely that it may become more prevalent in the future considering the current developments.

Question 3: In this question, we seek views and evidence on jurisdiction founded on the basis that damage or detriment was suffered in England and Wales.

Please share your views and evidence below::

-Do you consider the approach of the courts of England and Wales so far in the crypto litigation when localising damage or detriment for the purposes of jurisdiction to be theoretically sound?

The case law so far has focused on the idea of protecting the consumer.

The trend in the case law can be seen to be compliant with the idea of using the real-life actor as the connecting actor in the conclusion of the contract discussed under question 2 of this call for evidence.

Question 4: In this question, we seek views and evidence on jurisdiction founded on the basis that an unlawful act was committed in England and Wales.

Please share your views and jurisdiction::

-To what extent is the approach of the courts of England and Wales so far in the crypto litigation when localising where an unlawful act was committed for the purposes of jurisdiction theoretically sound?

In line with my answers to the previous questions, I would interpret 'the place where the unlawful act was committed' in the context of decentralised transactions as the domicile/usual residence of the real-life owner who controls the private key to the cryptoasset or where their computer which has access to the crypto-wallet was located at the time of the incident.

The courts of England and Wales have tried to grant as much access to justice rights as possible to the claimants in the case law so far and seem to have complied with 'the place where the unlawful act was committed' element. However, the Jones and Ion Science decisions could lead to divergence in the interpretation and application of the law in future cases as the cases have chosen diverging factors to determine the location of the unlawful event.

Question 5: In this question, we seek views and evidence on jurisdiction founded on the basis that the claim relates to objects within England and Wales.

Please share your views and evidence below::

- To what extent is the approach so far of the courts of England and Wales in localising a crypto-token for the purposes of jurisdiction theoretically sound? What would be the relative merits and demerits of any alternatives?

I think that the approach taken by the courts of England and Wales has been theoretically sound. In my understanding, other jurisdictions such as Singapore have adopted a similar position in their case law (see for example *Cheong Jun Yoong v Three Arrows Capital* [2024] SGHC 21).

There is need for clarification of course on how gateway 11 should be applied in the context of cryptoassets.

- What point in time is relevant for gateways 11 and 15(b)? Do these gateways require that a crypto-token is within England and Wales: at the time of proceedings, at the time of misappropriation, or some other time?

At the time of proceedings.

Question 6: In this question, we seek views and evidence on the types of claims and causes of action relied upon in applications to serve proceedings relating to crypto-tokens out of the jurisdiction.

Please share your views and evidence below::

- To what extent can it be said that there is a serious issue to be tried where claimants allege that exchanges are constructive trustees in the circumstances pleaded in *Piroozzadeh v Persons Unknown* and comparable cases?

Case law from other jurisdictions such as Singapore has considered that the defendant withholding the cryptoassets would be considered to be a trust (*Cheong Jun Yoong v Three Arrows Capital* [2024] SGHC 21). Of course, cases where exchange platforms are claimed to be constructive trustees in situations where one of their customers have misappropriated the claimant's cryptoassets are different from the former, which raises the difficulty of this answer.

It can be suggested that since exchange platforms have access to the data of the customers withholding the claimant's cryptoassets, then they may somehow be seen as guardians of their customer's property. It is however difficult to qualify the situation as the exchanges being considered to be constructive trustees due to the reasons mentioned in the call for evidence. What is clear though is that since the exchanges have access to the customer's data, an injunction can be made against them to give that data to the court.

- Are these cases indicative of a need to consider more carefully the "serious issue to be tried" limb of the three-stage test for service out of the jurisdiction?

Yes.

By Email

17th May 2024

Response to the Law Commission's call for evidence in respect of 'Digital Assets and ETDs in private international law: which court, which law?'

The International Swaps and Derivatives Association, Inc. ("ISDA") very much welcomes the opportunity to respond to the Law Commission's call for evidence in respect of 'Digital Assets and ETDs in private international law: which court, which law?' (the "Call for Evidence").

Digital asset markets continue to develop with increasing pace and complexity. This brings risks and opportunities. ISDA is playing a vital role in promoting standardization and digitization to help ensure that derivatives markets referencing digital assets are safe and efficient.

It is in our view integral to the proper functioning of digital asset markets that market participants understand the laws that may apply, and the courts which may assert jurisdiction, in the context of their transactions. That clarity is central to achieving legal certainty for digital asset derivatives markets.

We, therefore, strongly support the Law Commission's stated objective to test which digital asset use cases can be satisfactorily accommodated within existing private international law rules in England and Wales.

Importantly, in many instances in digital asset derivatives markets, those existing rules already deliver sufficient certainty for the market. As noted in the Call for Evidence, the challenge to existing private international law rules is most acute in relation to direct (rather than intermediated) participation in decentralized networks, and in relation to direct dealings in digital assets. Often in the digital asset derivatives markets, however, dealings are intermediated, and transactions are governed by contractual frameworks, such as under the ISDA Master Agreement, with clear governing law and submission to jurisdiction provisions. Furthermore, structural solutions can be adopted, for example in relation to arrangements relating to tokenized collateral, in order to achieve clarity as to treatment from a private international law perspective under existing frameworks.

ISDA has undertaken a number of initiatives in the context of digital assets and smart contracts, including as to their private international law treatment, as well as other novel legal and regulatory issues in relation to such assets and contracts. ISDA's work in this area may help inform some of the issues the Law Commission is considering.

We have, in this response to the Call for Evidence, only addressed those questions of most relevance to derivatives market participants that transact in digital assets or use smart contract technology. We have also sought to provide some context to our views (including by referring to the work we have undertaken in relation to digital assets and smart contracts), before addressing some of the specific questions posed in the Call for Evidence.

We would welcome further discussion on any of these matters.

1 ISDA's work in relation to digital assets and smart contracts

1.1 Digital assets

ISDA believes that participants in the digital asset derivatives markets should have clarity as to the contractual arrangements that apply to their transactions, including as to governing law and applicable jurisdiction. The ISDA Master Agreement establishes a globally consistent contractual framework for derivatives contracts, with clear and tested governing law and submission to jurisdiction provisions. ISDA has extended its standardized contractual framework to the nascent digital asset derivatives markets with a number of initiatives, culminating in the publication of our Digital Asset Derivatives Definitions, which establish an unambiguous, standardized contractual framework for digital asset derivatives under the umbrella of the ISDA Master Agreement (including its provisions as to choice of law and submission to jurisdiction).

More specifically, ISDA's work in this context includes the following.

- **Contractual Standards for Digital Asset Derivatives:** In December 2021, ISDA published a whitepaper¹ (the “**Contractual Standards Whitepaper**”) highlighting the need for contractual standards in respect of privately negotiated digital asset derivatives in order to support the development of a safe and efficient market. Among other things, the Contractual Standards Whitepaper identified various features particular to digital asset markets that might warrant specific consideration in derivatives documentation, including to ensure that all relevant risks are identified and appropriately allocated.
- **Digital Asset Derivative Definitions:** Building on the work of the Contractual Standards Whitepaper, ISDA published a set of contractual standards to document non-deliverable digital asset forwards and options in respect of bitcoin and ether (the “**Digital Asset Derivative Definitions**”) in January 2023. These standards were developed with a broad working group of market participants and have been widely welcomed across the industry. They have been designed in a modular format to facilitate incremental development.
- **Netting and Collateral Enforceability and Custody Whitepapers:** Alongside the Digital Asset Derivatives Definitions, ISDA published two further whitepapers. The first explored the application of close-out netting to digital asset derivatives and the enforceability of collateral arrangements that involve transfers or exchanges of digital assets² (the “**Netting and Collateral Enforceability Whitepaper**”). The second focused on the different ways in which digital assets may be held, how those holdings might be treated in an insolvency scenario, and the relevant documentation and due diligence issues that would need to be addressed to achieve the intended level of customer asset protection³ (the “**Custody Whitepaper**”).
- **Tokenized Collateral Model Provisions:** Following the Digital Asset Derivative Definitions, ISDA published model provisions (the “**Tokenized Collateral Model Provisions**”) in respect of tokenized collateral for use in the ISDA 2016 Credit Support Annexes for Variation Margin (the “**2016 VM CSA**”). These provisions are intended for

¹ Available at <https://www.isda.org/a/QVtgE/Contractual-Standards-for-Digital-Asset-Derivatives.pdf>

² Available at <https://www.isda.org/a/mlxgE/Navigating-Bankruptcy-in-Digital-Asset-Markets-Netting-and-Collateral-Enforceability.pdf>

³ Available at <https://www.isda.org/a/CrLgE/Navigating-Bankruptcy-in-Digital-Asset-Markets-Digital-Asset-Intermediaries-and-Customer-Asset-Protection.pdf>

use by parties transferring tokenized securities or ‘stablecoins’ that utilize distributed ledger technology (“DLT”) under the 2016 VM CSA⁴.

1.2 Smart derivatives contracts

ISDA has, in collaboration with various partners, undertaken a range of important initiatives with respect to smart contracts with a view to identifying some of the key legal issues presented by the deployment of DLT and smart contracts in derivatives market. These have included:

- **Private International Law Aspects of Smart Derivatives Contracts Utilizing DLT⁵:** In this series of papers⁶, ISDA sought to identify specific private international law issues that may arise when trading derivatives in a DLT environment and proposed recommendations on how these issues may be clarified or resolved. These issues were considered, and recommendations were given, in the context of two different types of derivatives transactions (collateralized and uncollateralized interest rate swap transactions) implemented on Corda, an open-source blockchain and smart contract platform developed by R3.

The key findings from this paper are:

- **English courts would give effect to an express choice of law in respect of DLT transactions.** We concluded that, in respect of the most straightforward implementations of uncollateralized and collateralized DLT transactions, it is not likely that either implementation would result in an English court disapplying an express choice of law, whether in the ISDA Master Agreement or any agreement between the parties and a platform provider.
- **Existing private international law principles can be applied to tokenized assets⁷:** If tokenized assets are used as a medium of value, or to effect

⁴ Available at: [https://www.isda.org/book/tokenized-collateral-model-provisions-for-vm-csa/#:~:text=Variation%20Margin%20\(VM\)-,Tokenized%20collateral%20model%20provisions%20for%20inclusion%20in%20ISDA%202016%20Credit,ledger%20technology%20\(Tokenized%20Collateral\)%20as.](https://www.isda.org/book/tokenized-collateral-model-provisions-for-vm-csa/#:~:text=Variation%20Margin%20(VM)-,Tokenized%20collateral%20model%20provisions%20for%20inclusion%20in%20ISDA%202016%20Credit,ledger%20technology%20(Tokenized%20Collateral)%20as.)

⁵ Private International Law Aspects of Smart Derivatives Contracts Utilizing DLT in England and Singapore, available at: <https://www.isda.org/a/4RJTE/Private-International-Law-Aspects-of-Smart-Derivatives-Contracts-Utilizing-DLT.pdf>. This paper was supplemented by papers in respect of a number of other jurisdictions (namely, France, Ireland, Japan and New York): a comparative summary of the private international law aspects of smart derivatives contracts utilizing distributed ledger technology is available at <https://www.isda.org/a/zCrTE/Private-International-Law-Aspects-of-Smart-Derivatives-Contracts-utilizing-Distributed-Ledger-Technology-Jurisdiction-Comparison.pdf,%20and%20associated%20whitepapers,%20available%20at%20www.isda.org/2019/10/16/isda-smart-contracts/>. All papers can be found are available at <https://www.isda.org/2019/10/16/isda-smart-contracts/>.

⁶ We refer to the paper issued in respect of the laws of England and Wales and Singapore as the “**Private International Law (Smart Derivatives Contracts) Paper.**”

⁷ We use the term tokenized assets in this response to refer primarily to tokens that constitute Digital Twins as contrasted with Digital Native assets (as defined in the Commodity Futures Trading Commission’s Global Markets Advisory Committee’s taxonomy entitled ‘Digital Assets Classification Approach and Taxonomy’ (the “**GMAC’s Taxonomy**”) available at https://www.cftc.gov/media/10321/CFTC_GMAC_DAM_Classification_Approach_and_Taxonomy_for_Digital_Assets_030624/download). A Digital Twin is defined in the GMAC’s Taxonomy as “an electronic controllable record representing an asset that has been immobilized on another system or record, and reconciled with that original system of record to ensure ownership is reflected precisely.” Examples of Digital Twins include Tokenized Alternative Assets, Tokenized Deposits, Tokenized Derivatives and Tokenized Securities (each as defined in the GMAC’s Taxonomy).

We also consider that this analysis will apply to tokenized assets that constitute Deposit Tokens (which evidence a deposit claim) and Financial Digital Assets (which include Security Tokens and Derivative Tokens, and respectively satisfy the definition of security and/or financial instrument or derivative instrument under local law), each as defined in the GMAC’s Taxonomy. It may also apply to other Digital Native assets that confer rights against a person or entity, such as the issuer of the token.

payments or exchanges of collateral arising under derivatives transactions, it is likely that existing private international law principles can be applied to determine the location of the underlying assets (which will, in turn, inform the location of the tokens and therefore the applicable governing law).

- **Proposal for elective situs in relation to tokens that constitute cryptoassets⁸:** Where an entirely disintermediated form of securities holding systems or trading platforms is established through the development of a permissionless DLT system, such that it is not possible to identify individual platform participants, it may not be possible to establish precisely where participants or assets are located. It would therefore provide greater clarity for all parties to agree that their transactions should be subject to a common 'law of the platform', 'law of the system', or elective situs – that is, a uniform choice of law that the parties agree will govern all on-ledger transactions. Where national authorities and regulators are concerned that allowing parties an unfettered choice of a governing law of the platform is undesirable, the choice of law could be restricted to the laws of countries where parties such as the issuer of assets, the system administrator and market participants are subject to sufficient legal and regulatory oversight. The functionality of DLT platforms such as Corda⁹ could assist with the practical enforcement of judgment. However, the feasibility of this proposal in the context of public, permissionless ledgers remains a significant challenge. This proposal will therefore require national governments, judiciaries, regulators and international standards-setting bodies to work on adapting or developing global legal standards.
- **ISDA Legal Guidelines for Smart Derivatives Contracts¹⁰:** ISDA has published a series of guidelines for smart derivatives contracts which were intended to explain the core principles of the ISDA documentation and raise awareness of important legal terms that should be maintained when a technology solution is applied to derivatives trading. These guidelines also established the concept of a smart derivatives contract being a derivatives contract where some terms are capable of being automatically performed (either by expressing those provisions using some formal representation that enables their automation or by referring to the operation of a smart contract code that is external to the contract).
- **ISDA Smart Contract Whitepapers:** ISDA's Legal Guidelines for Smart Derivatives Contracts were preceded by a number of whitepapers that sought to identify and address

⁸ We use the term 'cryptoasset' as defined in the GMAC's Taxonomy (which are assets with the following features: "*are not pegged to the value of a reference asset, do not represent ownership or other legal claim against a company or other type of issuer, nor guaranteed by a regulated financial institution, their value is driven by market dynamics and/or supply and demand mechanics.*")

Unless otherwise stated in this response, references to digital assets should be taken to include tokenized assets and cryptoassets.

⁹ Unlike permissionless blockchains where anyone can participate anonymously, Corda requires that all participants are identified and authorized prior to joining the network. This architecture ensures that all parties are known to each other, thereby facilitating a secure and regulatory-compliant environment for conducting transactions.

¹⁰ These guidelines included (among others) ISDA Legal Guidelines for Smart Derivatives Contracts: Introduction (January 2019), available at: <https://www.isda.org/a/MhgME/Legal-Guidelines-for-SmartDerivatives-Contracts-Introduction.pdf>; ISDA Legal Guidelines for Smart Derivatives Contracts: The ISDA Master Agreement (February 2019), available at: <https://www.isda.org/a/23iME/Legal-Guidelines-for-Smart-Derivatives-Contracts-ISDA-Master-Agreement.pdf>; ISDA Legal Guidelines for Smart Derivatives Contracts (September 2019) and available at: <https://www.isda.org/2019/09/12/legal-guidelines-for-smart-derivatives-contracts-collateral/>.

some of the key legal issues arising from the use of DLT and smart contracts in derivatives markets. These included:

- **The Future of Derivatives Processing and Market Infrastructure**¹¹ (September 2016)
- **Smart Contracts and Distributed Ledger – A Legal Perspective**¹² (August 2017).
- **Smart Derivatives Contracts: From Concept to Construction**¹³ (October 2018).

2 General considerations

In many instances in digital asset derivatives markets, existing private international law rules will achieve the degree of legal certainty the market expects and requires.

Contractual matters

Derivatives transactions are governed by contractual frameworks. To the extent documented under an ISDA Master Agreement, clear choice of law and submission to jurisdiction provisions will apply. Even where that is not the case, existing private international law rules are apt to deal with the arrangements between parties to a derivatives contract in the way they would in other contexts.

Collateral

The most likely scenario in relation to digital asset derivatives markets which may give rise to incremental issues of private international law relates to collateral arrangements. Even so, in many instances, existing private international law rules will be capable of being applied with sufficient certainty. This is particularly the case as in many instances, collateral arrangements will involve the presence of an intermediary responsible for control of the relevant collateral on behalf of one, or both, parties. We agree with the conclusion in the Call for Evidence that intermediated arrangements are significantly less likely to present the types of novel challenge that arise in the context of direct participation in fully decentralized systems.

We also note that, furthermore:

- tokenized cash or securities can be created within permissioned systems with an operator, or which may otherwise have been structured intentionally to facilitate the deemed location of the assets recorded within the system in a particular jurisdiction for conflicts of laws purposes. For example, tokenized securities may be structured so as to amount to book entry securities collateral under the Financial Collateral Arrangements (No 2) Regulations 2003¹⁴ (the “**FCARs**”), or equivalent legislation, such that certain matters are governed by the law of the country of the ‘place of the relevant intermediary account’ (the so-called PRIMA principle), which may be the jurisdiction of the system operator or of a participant in the relevant system. However, certain digital assets would

¹¹ Available at: <https://www.isda.org/a/UEKDE/infrastructure-white-paper.pdf>.

¹² Available at: <https://www.isda.org/a/6EKDE/smart-contracts-and-distributed-ledger-a-legal-perspective.pdf>.

¹³ Available at: Available at: <https://www.isda.org/a/cHvEE/Smart-Derivatives-Contracts-From-Concept-to-Construction-Oct-2018.pdf>.

¹⁴ SI 2003/3226, implementing Directive 2002/47/EC.

not fall within the definition of 'financial collateral' for the purposes of the FCARs¹⁵. Similarly, systems on which tokenized securities are issued may also be structured, in England and Wales, to fall within conflicts of laws provisions under the Financial Markets and Insolvency (Settlement Finality) Regulations 1999¹⁶ (the "SFRs"), which include similar provisions – but again, this would only apply to transfers of digital assets that constitute financial instruments (or that are equivalent to "money") (i.e., involving securities transfer orders or payment transfer orders) and further only to transactions occurring within designated systems;

- as a result of the adoption of the PRIMA principle in the FCARs, SFRs, related European Directives, some international treaties, and in other legal systems, PRIMA is often regarded as of potentially broader application and as a starting point for the governing law in analogous situations, as a matter of general private international law; and
- to the extent that tokenized collateral embeds rights (such as a debt claim against an entity), those rights will often be capable of being accommodated within existing private international law rules.

In general, therefore, in the context of digital asset derivatives markets, existing private international law rules will be capable of accommodating many arrangements without material incremental uncertainty. This gives legal certainty to derivatives market participants already transacting in digital assets and using smart contracts on this basis.

3 Response to select issues

3.1 Question 2: Jurisdiction over non-consumer contracts

The Law Commission has, in its Call for Evidence, invited feedback on the application of gateway 6(a) (which concerns contracts that are made within the jurisdiction or concluded by the acceptance of an offer, which offer was received within the jurisdiction) to digital assets. The gateway, however, that is of more relevance to digital assets derivatives is that set out in paragraph 6(c), which refers to contracts governed by the laws of England and Wales. The ISDA Master Agreement contains an explicit choice of governing law by the contracting parties, as do many other derivative transactions. If the parties to a digital asset derivative transaction have elected for the laws of England and Wales to govern that transaction, gateway 6(c) will in general be satisfied. The application of gateway 6(a) would therefore not in this context be the primary gateway falling to be considered.

In any event, these matters are perfectly capable of being addressed through existing conflicts of laws rules.

The ISDA Master Agreement similarly contains provisions whereby the parties agree to submit any claims arising out of their derivative transactions to the jurisdiction of courts in certain territories. When the parties to a dispute have contractually agreed that the English courts have jurisdiction over the matter, the English courts will generally give effect to this agreement. Alternatively, the parties may have contractually agreed that a foreign court has

¹⁵ Only arrangements over "financial collateral" can benefit from protection under the FCARs. Financial collateral is defined as "cash, financial instruments or credit claims". "Cash" is any "money in any currency, credited to an account, or a similar claim for repayment of money and includes money market deposits and sums due or payable to, or received between the parties in connection with the operation of a financial collateral arrangement or a close-out netting provision." "Credit claims" mean pecuniary claims which arise out of an agreement whereby a credit institution grants credit in the form of a loan. "Financial instruments" are limited, primarily, to shares and bonds and instruments related thereto.

¹⁶ SI 1999/2979, implementing Directive 98/26/EC.

jurisdiction over disputes. In this scenario, an English court may stay any claims brought in England in breach of this agreement or will refuse permission for process to be served out of the jurisdiction for the purpose of any English proceedings, unless the claimant can prove that there are strong reasons for the English proceedings to continue. Again, there are, therefore, unlikely to be material novel issues raised in respect of the courts' jurisdiction to hear claims that concern digital asset derivatives transactions.

3.2 Question 5: Jurisdiction over proprietary claims

If a claim relates to digital assets, we agree that it may be difficult to attribute a single location to those assets for the purposes of establishing jurisdiction in respect of proprietary claims.

This is not an issue, however, that frequently arises in practice in the derivatives markets. This is because where derivatives do reference digital assets, they generally give rise to claims that are primarily contractual in nature (given that the derivative constitutes or is transacted in under a contractual framework), in which case the choice of law and jurisdiction under the contract will apply to govern disputes (in accordance with existing jurisdictional principles). Proprietary claims may arise in the context of collateral arrangements or in the case of contested title (e.g. following an appropriation of assets). However, in the derivatives markets to the extent applicable, disputes over collateral will generally involve some form of intermediation (such as a custodian holding the relevant collateral). For the reasons given above and in the Call for Evidence, intermediated arrangements present fewer challenges to existing jurisdictional rules than direct participation in fully decentralized systems. In any case, although increasing, tokenized collateral is not yet widely used in the derivative markets meaning these issues do not yet often fall to be considered.

In any case, as noted above, the ISDA Master Agreement (and many other derivatives contracts) include an express submission to jurisdiction provision. In many instances, this again limits the need in the derivatives market to consider where a digital asset is situated and at which point in time this is relevant for the purposes of gateway 11 (as set out in paragraph 3.1 of Practice Direction 6B).

3.3 Question 8: Applicable law for non-consumer contracts

We agree with the initial conclusion set out in the Call for Evidence that material incremental issues are unlikely to arise when deciding the applicable law for non-consumer contracts involving digital assets, in particular where an express choice of law is made. This conclusion is also important to give legal certainty as to choice of law for derivatives market participants that are currently transacting in digital assets and employing smart contract technology.

The ISDA Master Agreement, as noted above, embeds an explicit choice of law by the contracting parties. Many other derivative transactions also contain an express choice of law. We concluded in our Private International Law (Smart Derivatives Contracts) Paper that there appears to us to be no reason under private international law rules (specifically those that arise under the Rome I Regulation¹⁷) why a court in England and Wales would reject the express choice of law made by derivatives market participants in the absence of any countervailing mandatory legal rule or public policy reason.

3.4 Question 19: Applicable law for property disputes in relation to digital assets

¹⁷ Regulation on the Law Applicable to Contractual Obligations (Reg (EC) No 593/ 2003 (in the UK, as it forms part of assimilated law pursuant to the European Union (Withdrawal) Act 2008 as amended).

We refer to our response to question 8 in which we consider that the majority of disputes that arise in relation to digital asset and smart contracts derivatives will take the form of contractual, as opposed to proprietary, claims. The complexities in ascertaining applicable law for property disputes in relation to digital assets therefore do not typically arise in the respect of digital assets and smart contracts derivatives.

There are, however, some scenarios (albeit less likely to arise) in which derivatives market participants transacting in digital assets or employing smart contracts may bring proprietary claims in respect of those digital assets.

Tokenized assets

Tokenized securities may be provided as collateral in respect of derivative transactions. If those digital securities are tokenized assets (i.e., digital securities that represent Digital Twins or digital securities that are Digital Natives but constitute Tokenized Securities¹⁸) a dispute over the entitlement of a party to those digital assets would (in our view and as we contemplate in our Private International Law (Smart Derivatives Contracts) Paper) be decided by the situs of the securities. This could be, depending on the particular situation, the *lex incorporationis* (including the law of some place other than the *lex incorporationis* if the latter allows the securities to be dealt with there) or, where the securities are held in a centralized deposit system, the law of the country where the register, account or centralized deposit system is situated. Current principles of private international law are, in each case, capable of accommodating (and ascertaining the law applicable to) such a dispute.

Cryptoassets

The question of applicable law becomes more complex if the digital assets collateralizing the derivative transaction involve cryptoassets¹⁹. It may not, in this case, be possible to determine the *lex incorporationis* applicable to cryptoassets, especially where the cryptoasset is not also held in a centralized deposit system nor in an account with an intermediary.

We do not consider that this is an issue that frequently arises in practice with respect to derivatives transactions referring to digital assets and/or deploying smart contract technology. This is because where derivatives do reference digital assets, they give rise to claims that are primarily contractual in nature (given that the derivative constitutes or is transacted in under a contractual framework), in which case the choice of law and jurisdiction under the contract will apply to govern disputes (in accordance with existing conflicts of laws principles). Proprietary claims may arise in the context of collateral arrangements and in cases of contested title (e.g. following an appropriation of assets). Although increasing, tokenized collateral is not, however, yet widely used in the derivatives markets meaning that these issues do not yet often fall to be considered. In the case of an appropriation of assets in the control of the seller prior to delivery, the seller would still be obliged to fulfil its contractual obligations to the buyer and must therefore source new assets; any dispute as to title would fall outside the scope of the derivative contract. We have, in our Private International Law (Smart Derivatives Contracts) Paper, however, proposed that one solution to these complexities is for the situs of the token to be the 'law of the platform' or the 'law of the system' that the parties have agreed will govern all on-ledger transactions on the relevant DLT system. This would mirror the approach taken under the SFRs where on the opening of

¹⁸ These terms having the meanings given to them in the GMAC's Taxonomy. Please see footnote 7 of this response for further detail as to the meaning of these terms.

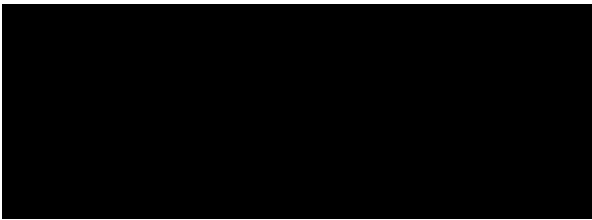
¹⁹ We refer to the meaning of 'cryptoassets' given in the GMAC's Taxonomy. Please see footnote 8 of this response for further detail as to the meaning of 'cryptoasset'.

insolvency proceedings against a participant in a designated system, any question relating to the rights and obligations arising from, or in connection with, that participation is required to be determined in accordance with the law chosen by the participants to govern the system. A similar approach that prioritizes party autonomy has also been proposed by UNIDROIT in its 'Principles on Digital Assets and Private Law.'²⁰ However, there would be significant challenges faced in implementing this solution in the context of permissionless ledgers, particularly given that it may be impractical or, in some instances, impossible to ensure parties engaging with these permissionless ledgers agree a single governing law (raising questions as to how a single governing law could be chosen and enforced). This solution, therefore, is likely to be most relevant in the context of permissioned systems.

We consider, in any case, that this is unlikely to be an issue that frequently arises in practice in the context of digital asset derivatives and derivatives employing smart contract technology. Where the possibility of such issues arises, these issues can also generally be addressed by appropriate structuring (for instance, conflicts of laws questions arising in respect of security interests granted over digital assets may be cured by transferring those digital assets to be a third-party custodian who enters into contractual agreements with both the collateral taker and collateral provider).

We are grateful for the opportunity to respond to the Law Commission's Call for Evidence and we would welcome any further discussion on this topic.

Yours sincerely,



Scott O'Malia
Chief Executive Officer
International Swaps and Derivatives Association

²⁰ Available at: <https://www.unidroit.org/work-in-progress/digital-assets-and-private-law/>.



Kennedys response: Law Commission Call for Evidence on digital assets and ETDs in private international law

May 2024

About Kennedys

Kennedys is a global law firm with expertise in dispute resolution and advisory services. Founded in 1899, we have a rich history of delivering straightforward advice, even when the issues are complex.

With over 2400 people and 71 offices around the world, we are a fresh-thinking firm willing to bring new ideas to the table beyond the traditional realm of legal services.

Marine team

Our global team of market leading marine specialists have experience of marine insurance, charter parties and bills of lading, admiralty, ship building and offshore construction, logistics and trade, fine art and specie, trade credit and political risk.

Corporate affairs team

Kennedys have a dedicated Corporate Affairs team responsible for generating insights on emerging industry risks and trends, as well as the impact of legal and political shifts on the international business environment. Industry and government engagement helps us and our clients stay informed and align our activities and business objectives with current and emerging industry activities.

Kennedys IQ

Kennedys IQ is an award-winning part of the global Kennedys Group. At Kennedys IQ, we blend our leadership’s vision with our technologists’ expertise and the Group’s legal excellence in order to help the insurance sector to use lawyers less.

Contacts



Chris Chatfield

Partner

[Redacted contact information]



Marco Pedretti

Associate (Foreign Qualified Lawyer - Australia)

[Redacted contact information]



Joanna Manthorpe

Senior Corporate Affairs Lawyer

[Redacted contact information]



Joe Cunningham

Product Manager

[Redacted contact information]

Response

Questions on applicable law - negotiable instruments, bills of lading, and the exclusions from the Rome Regulations (Chapter 10)

Q13: We seek evidence, particularly from market participants, on how market practice in respect of bills of lading has been affected, or how it is likely to be affected, by the introduction of the Electronic Trade Documents Act 2023.

Please share your views and evidence below:

Kennedys has previously welcomed moves towards establishing a regime for electronic trade documents. A very substantial proportion of contracts for the carriage of goods by sea are subject to English law jurisdiction and English dispute resolution processes. Accordingly, reforms to English law concerning carriage of goods by sea, notably the Electronic Trade Documents Act 2023 (the Act), will have a significant global impact and will undoubtedly have a considerable impact on global trade. Moreover, if English law is to remain a leading choice for global trade markets (with the consequent revenue generated by insurance and legal services) it is essential that it remains at the forefront of technology.

Kennedys has previously commented that until application of the law was clarified through litigation, the Act was likely to result in uncertainty for market participants. Our view remains that resolving this uncertainty, and creating a reliable and secure system for electronic bills of lading, will be essential prerequisites to foster participation by the global market.

Carriage of goods by sea has functioned in much the same way for centuries and electronic bills of lading are the next natural step for the market in the 21st century. However noting previous, largely unsuccessful, attempts to introduce electronic bills of lading, it is clear the transition from established practices to modern ones will require careful thought.

If the current issues regarding electronic bills of lading (which are largely practical issues concerning their security, efficiency and suitability to modern trading practices) can be resolved, the Act has the potential to markedly change market practice around the world.

Q14: We seek evidence on market sentiment relating to use of DLT platforms for electronic bills of lading.

1) Is it likely that market participants will move towards a wholly decentralised DLT platform for bills of lading?

2) To what extent can we assume that market participants will be reluctant to join a DLT platform that does not at least offer a user agreement setting out the terms on which the DLT platform will operate, and the rights and obligations of all users of the platform?

3) Other than wholly decentralised DLT platforms, how else might DLT be used to issue and transact with electronic bills of lading (under the 2023 Act or otherwise)?

Please share your views and evidence below:

To achieve the policy objective of transitioning current paper bills of lading to electronic bills of lading, DLT platforms will need to perform both in practice and in law.

At the outset we note that to a large extent the answers to the questions being asked in this consultation will turn on exactly how the DLT platform is set up. There are myriad ways in which a DLT platform for the issuing of electronic trade documents could be established and accordingly we suspect that further market consultation will be required once there is greater clarity on the technological infrastructure surrounding electronic bills of lading.

In order to perform in practice, DLT platforms will need to gain the confidence of their users. To do so they will need to ensure that the systems in place supporting electronic bills of lading are reliable and secure. Market participants may be reluctant to adopt practices which present increased security risks when compared to paper-based systems. Market participants will also be reluctant to adopt practices that do not suit modern day logistic arrangements.

A relevant decision to these issues will be whether DLT platforms are permissioned or permissionless. A permissioned DLT system requires a certain level of control or maintenance from an authorised administrator. Access to the platform is not open to the public but rather is controlled by the administrator and can be considered “partly decentralised”. A permissionless system on the other hand is open to the public and transactions are largely anonymous.

We anticipate that it is unlikely that a completely decentralised or permissionless system will receive market support. As these would be publicly accessible and transparent, market participants would lose the confidentiality which is offered by the current paper system of bills of lading. Further, market participants are unlikely to support a system where market participants can remain largely anonymous which might expose them to fraudulent transactions, unreliable counterparties or even expose them to sanctions liabilities.

However, careful thought will be required to ensure that permissioned DLT platforms are consistent with current market practice whereby bills are passed from a carrier to a shipper and consignee, and also from a holder to a transferee, without the approval of a carrier. With increasingly long logistics chains (carriers, cargo owners, forwarders, clearance agents, local transporters and various providers of ancillary services), transferability of electronic bills of lading, without requiring the approval of the carrier, is essential.

We note that universal adoption of electronic bills of lading will be not be possible until all of the parties to the supply chain have sufficient access to the technology required to access the relevant DLT platforms. We anticipate that certain parties to supply chains, for example local hauliers, may struggle with the technological investment and upskilling required to participate in DLT platforms. Accordingly we anticipate that there will be some practical difficulties with electronic bills of lading, especially if it is not possible to convert that electronic bill of lading into a conventional hard copy bill of lading.

A user agreement which sets out the terms on which the DLT platform will operate will be essential. Carriers assume considerable responsibility and potential liability when dealing with negotiable bills and they will wish to ensure that any users of a DLT platform are doing so responsibly and securely. Given the consequences of a failure in the system, such agreements will need to clearly set out responsibilities and liabilities.

Insurance will also play an essential role in the process and insurers will require clear contractual obligations to be set out in such a user agreement. Insurers will expect to be able to understand where liability sits and whether there are any limits or restrictions in such liability. They will also wish to assess the reliability of the system (and thus assess their risk). Without the backing of both cargo and liability insurers, it is unlikely that parties would wish to participate in the system.

Furthermore, a user agreement will be essential to the acceptance of that platform by market participants. From a legal perspective, a user agreement will be essential to determining whether a DLT platform is a “reliable system” within the meaning of section 2 of the Act. Market participants will likely want to regularly review the operating terms of a DLT platform to ensure that the system remains reliable.

As technology improves and as cyber crime advances, the reliability of a system may change, both from a legal perspective under the Act but, but also from a commercial perspective. Market participants and underwriters will also want to review and consider their legal rights in relation to the DLT platform should there be a technical issue which impacts their ability to use the DLT platform.

Q15: We seek evidence on the difficulties, if any, of incorporating the Hague-Visby Rules where an electronic bill of lading has been used.

1) How often do disputes arise as to incorporation of the Hague-Visby Rules, specifically because an electronic bill of lading has been used, and how likely are they to in future?

2) Are there concerns in the market, both in the marine insurance and shipping sectors, regarding the incorporation of the Hague-Visby Rules in electronic bills of lading? Please provide detailed examples in your answer and, where possible, distinguish between electronic bills under the Electronic Trade Documents Act 2023 and electronic bills held within contractual “approved systems.”

Please share your views and evidence below:

In theory, at least, the applicability of the Hague-Visby Rules (HVR) should not be affected by whether a bill is issued electronically or on paper. The HVR apply to a qualifying contract of carriage (which depends on the issue of a bill of lading in certain circumstances). The 2023 Act seeks to give

the same effect to electronic bills as paper bills. Consequently, the form of the bill (whether on paper or electronic) should not matter.

It is not clear to us the extent to which disputes arise in practice regarding the incorporation of the HVR simply because an electronic bill of lading has been issued. We note that already in practice many bills of lading are issued “electronically” in the sense that they are generated by software using company servers and are not issued in hard copy at the load port. This suggests that issues regarding the incorporation of the HVR into bills of lading issued via DLT platforms may not arise in practice.

We do not think that the issue of whether the HVR have been incorporated into a bill of lading will require different consideration simply because a bill of lading has been issued via a DLT platform. In this respect, we note that pursuant to Art X of the HVR, HVR apply where:

- The bills of lading issued in a contracting state;
- The carriage is from a port in a contracting state;
- The contract contained in or evidenced by the bill of lading provides that the rules of this Convention or legislation of any State giving effect to them are to govern the contract.

Accordingly, regardless of where the bill of lading is issued, the parties will be unable to avoid the application of the HVR in circumstances where the carriage is from a port in a contracting state. If HVR do not automatically apply because the carriage is from a port which is not in a contracting state, then in practice the parties have two other ways in which they can bring the contract of carriage under the application of HVR: by having the bill issued in a contracting state or by incorporating them contractually.

Issuing bills electronically may give rise to questions as to where a bill has been issued. However, that is not something which has been introduced by the 2023 Act or by the use of a DLT. The information used for paper bills tends to be entered into a central electronic system with the bill printed off at a local office. The parties then opt for a place of issue in the relevant box within the bill. This does not seem to have given rise to particular issues in practice.

For these reasons, we do not think that market participants will have concerns regarding the application of the HVR to bills of lading which have been issued via a DLT platform.

Q16: We seek evidence on market practice to help us identify where it could be said that an electronic bill of lading is “issued” for the purpose of the Hague-Visby Rules, as implemented in the UK by the Carriage of Goods Act 1971

1) How, in practical terms, does a carrier wishing to issue an electronic or tokenised bill of lading do so within the respective electronic “approved” system or DLT system? What steps must a carrier take within the system?

2) How, in practical terms, does a shipper “receive” an electronic or tokenised bill of lading within an “approved” system or DLT system? What steps must a shipper take within the system?

3) Does the issue of an electronic or tokenised bill of lading between carrier and shipper involve the platform provider, or do the systems allow for electronic or tokenised bills to be sent directly from carrier to shipper?

4) What are the market standards or best practices relating to existing electronic or DLT systems on the “issue” of a bill of lading?

Please share your views and evidence below:

We note that there is no rule which prescribes the location where a bill of lading must be issued. The HVR provide that, after receiving the goods the carrier or the master or agent of the carrier shall, on demand of the shipper, issue to the shipper a bill of lading. In practice therefore these factors might facilitate the issue of bills of lading more easily or efficiently at particular places, however the parties are in theory able to agree for the bill of lading to be issued in any place.

Further, as we noted above, in practice many bills of lading are issued “electronically” in the sense that they are generated by software using company servers and are not issued in hard copy at the load port. We do not think that the fact that a bill of lading may now be issued using a DLT platform, as opposed to existing technology, will pose any significant legal or practical difficulties for the parties.

In practice, we understand that carriers would issue electronic bills of lading via DLT platforms in the following way:

- After receiving the cargo to be shipped by from the shipper, the carrier would review the information provided by the shipper (as they do already).
- The carrier will record the same data in the electronic bill of lading as they already do in a paper bill of lading, namely the cargo description, the vessel, port of loading, port of discharge, the names of the shipper and consignee, etc..
- The carrier would then sign the bill of lading electronically.
- The carrier would then issue a transaction on a blockchain using its key which would be accessible by the shipper using its own key.
- The shipper would then be able to confirm that the message had not been altered and could safely decrypt the message which would give it possession of the tokenised bill of lading.
- If the bill of lading is endorsed, this would also be facilitated by the platform provider in the same way, enabling the transfer of title on the DLT platform.

- The entity with possession of the tokenised bill of lading would allow (or send an invitation to) the subsequent endorsee to register to the platform, thereby allowing access. This would allow the endorsee to validate the transaction and accept the transfer of title.
- The ultimate consignee with possession of the tokenised bill of lading would then be able to surrender the electronic bill of lading and demand release of the cargo.
- Once transfer of title has been accepted by the endorsee, the platform, by virtue of the blockchain mechanism itself, would recognise that the person who previously had possession of the bill of lading no longer had possession of or access to the tokenised bill of lading. This would prevent them from transferring the tokenised bill of lading to multiple transferees or surrendering it on their own behalf and demanding release of the cargo.
- In practical terms, an example is illustrated on the cargox.io platform, this includes the endorser being able to view the audit log of a *previously sent* negotiable bill of lading, and downloading content with a watermark. The immutability of ownership records is performed by the cryptographic linking of blocks and the consensus mechanisms of the chain itself but how that is presented to an individual entity in the chain is likely to be software developer/platform specific in the absence of any legislative requirement.
- All steps are undertaken on the DLT platform, providing an auditable and transparent chain of events.
- We understand that the validation of the transaction(s) containing the ‘tokenised bill of lading’ would be undertaken by the DLT that underpins the blockchain. Administration would be facilitated by various platforms, an example being <https://cargox.io/electronic-bill-of-lading>.

However, one of the main purposes of a bill of lading is that it entitles the holder to demand delivery of the goods. In the case of electronic bills of lading, where there is no “original” paper bill of lading, careful thought will need to be given to how delivery and collection of the cargo at the discharge port is not susceptible to fraudulent activity or theft.

We note that in modern practice it is rare for the consignee to actually attend the discharge port with a bill of lading in hand and demand delivery of the cargo themselves. Rather, they normally will have already handed over the bill of lading to the carrier in exchange for a delivery release note and will often appoint a local agent to attend the port and collect the cargo on the consignee’s behalf. In order to collect the cargo, the local agent will normally need to comply with some form of security procedure (such as entering the container number and a pin code which is assigned to a particular consignment or container), which will allow that person to collect the container.

In practice, we see the highest level of fraud take place at this stage of the chain of carriage and carriers may become liable for misdeliveries (see for example the decision in *East West Corporation v Dampskibsselskabet AF 1912 A/S* [2002] EWHC 83).

It is very important that electronic bills of lading ensure that they replicate the process of handing over an “original” bill of lading, such that only the party with the right to demand delivery of the cargo at the discharge port (and not an earlier party in the logistics chain who has since transferred that right) can in fact collect the cargo. This will be integral to whether the DLT platform is considered to be a “reliable system”, and whether the electronic bills of lading come within the meaning of an “electronic trade document” under the Act. We also note that pursuant to section 1(2)

of the Act, information in electronic form can only constitute an “electronic trade document” if a reliable system is used to:

(a) identify the document so that it can be distinguished from any copies,

...

(c) secure that it is not possible for more than one person to exercise control of the document at any one time,


...

(e) secure that a transfer of the document has effect to deprive any person who was able to exercise control of the document immediately before the transfer of the ability to do so (unless the person is able to exercise control by virtue of being a transferee).

Accordingly, if a DLT platform is unable to replicate the process of handing over an “original” bill of lading, it would seem that any electronic bills of lading issued under that platform would not in fact constitute electronic trade documents within the meaning of the Act.

Kennedys

 kennedyslaw.com

 [Kennedys](#)

 [KennedysLaw](#)

 [KennedysLaw](#)

Kennedys is a trading name of Kennedys Law LLP. Kennedys Law LLP is a limited liability partnership registered in England and Wales (with registered number OC353214).

kennedyslaw.com



Linklaters LLP
One Silk Street
London EC2Y 8HQ
Telephone (+44) 20 7456 2000
Facsimile (+44) 20 7456 2222
DX Box Number 10 CDE

By Email

16 May 2024

Response to the Law Commission's call for evidence in respect of 'Digital Assets and ETDS in private international law: which court, which law?' (the "Call for Evidence")

We welcome the opportunity to contribute to the Law Commission's work on the application of private international law to digital assets and electronic trade documents ("**ETDS**").

We agree with the Law Commission that emerging technologies can raise novel questions of private international law. It is critical to the proper functioning of financial markets that participants are able to structure their arrangements to achieve sufficient clarity as to the laws that may apply, and the courts that may assert jurisdiction.

We are, therefore, very supportive of this project that aims to stress test the existing private international law rules in England and Wales, and the extent to which they can accommodate challenges created by emerging technologies including digital assets and ETDS.

We have already contributed to various industry responses highlighting, in particular, that, in many financial market transactions involving digital assets, the existing rules of private international law will achieve the degree of clarity and certainty the market requires with respect to the determination of applicable law. For example, arrangements can be structured so as to fall within the conflicts of law rules under existing statutory frameworks such as the Settlement Finality Regulations,¹ the Financial Collateral Arrangement Regulations,² or Rome I³. While there may be merit in clarifying or expanding the scope of these rules (for example, to cater for arrangements where there is no "account" or "register"), it is important that any new intervention does not cut across existing statutory frameworks which could create unnecessary confusion and risk undermining legal certainty and principles of technological neutrality.

The purpose of this response is to highlight some relevant considerations as to how the principle of territoriality should be applied to identify applicable law in property disputes where the relevant proprietary right or interest is evidenced by mere data recorded in a system. In particular, we would challenge the suggestion in paragraph 3.93 of the Call for Evidence that the location of a cloud storage service provider is necessarily an appropriate determining connecting factor; rather, this *may* be the case, depending on the context, whereas in other contexts, there may be other more appropriate prevailing factors. For example, where a dispute or other issue arises concerning data maintained in the cloud *as mere data* (as in the case of case law mentioned in the Call for Evidence), the location of the cloud service provider may be the most appropriate determining factor; by contrast, where the relevant issue relates instead to that data *as constitutive elements* of separate legal rights (such as rights to registered securities recorded to an

¹ Financial Markets and Insolvency (Settlement Finality) Regulations 1999 (SI 1999/2979, implementing Directive 98/26/EC)

² Financial Collateral Arrangement (No. 2) Regulations

³ Regulation (EC) No 593/2008, as onshored into domestic law

electronic register maintained in the cloud), the location of the cloud service provider will very unlikely be the most appropriate determining factor.

We agree that the traditional common law rules for the determination of the law applicable to property disputes generally identify the applicable law by reference to the *lex situs* of the relevant property. We also agree that such rules are easier to apply to tangible objects than intangible objects,⁴ particularly in the context of wholly decentralised arrangements.

The Law Commission considers how applicable law may be determined with respect to intangible objects that are: (i) wholly decentralised digital assets legally recognised as distinct “things” independent of any legal rights that they might otherwise represent;⁵ (ii) *choses in action* (i.e. intangible property not in a person’s possession but enforceable by legal process) such as debts, shares and patents;⁶ and (iii) pure data or information such as digital files that are not intangible assets in their own right or otherwise representative of legal rights, but nevertheless are required to be connected to a single legal territory for the purposes of a dispute.⁷

However, we do not believe the Call for Evidence considers in sufficient detail how the common law would localise *choses in action* that are represented or evidenced by pure data or information, including in a decentralised context. We are thinking specifically about intangible property such as uncertificated registered securities, i.e. registered instruments where ownership of the security is recorded on a digital register maintained by or on behalf of the issuer and where rights under it are transferred upon application to the registrar and a recording in the register, and similar arrangements (for example, where a record of claims is maintained by a third party recordkeeper).

In the case of registered securities, the location of the register is generally understood as being determinative of the *situs* of the securities. Generally speaking, if the registered securities may be transferred only by registration on a particular register, they will be regarded as situate at the place where the register is kept.⁸ If they are transferable on more than one register, they will be situate at the place of the register on which they would be dealt with in the ordinary course of affairs by the registered owner for the time being.⁹ This was relatively straightforward in the days when the register was a physical account

⁴ We use the term ‘intangible object’ broadly to encompass both intangible property and mere data or information (such as digital files or records) which does not constitute an intangible asset in its own right.

⁵ The Call for Evidence acknowledges that applying the *lex situs* rule to wholly decentralised digital assets (or ‘crypto-tokens’) is one of the most difficult problems raised by DLT as such assets are the paradigm example of “omniterritorial” phenomena, existing “nowhere and everywhere at the same time”.

⁶ The Call for Evidence notes at 3.5.2 that it is common practice to ascribe an artificial *situs* to *choses in action* in order to bring them within the scope of rules of law expressed in terms of *situs*. It notes that it is sometimes said that “the (artificial) situs of a patent is considered the place where the relevant register is kept” or “the (artificial) situs of a debt is the place where the debtor is domiciled.”

⁷ Citing *Ashton Investments v OJSC Russian Aluminium* [2006] EWHC 2545 (Comm), [2006] 2 CLC 739 and *United States v Microsoft Corp* 584 US ____ (2018), the Call for Evidence suggests that, in such circumstances, it would be possible for private international law to focus, not on the data itself, but instead on the data provider. A hybrid personal-territorial connecting factor, such as the domicile of the third-party provider responsible for maintaining the relevant data centres may be used as an “artificial” *situs*.

⁸ *Att-Gen v Higgins* (1857) 2 H. & N. 339; *New York Breweries Co v Att-Gen* [1899] A.C. 62; *Commissioners of Inland Revenue v Maple & Co Ltd* [1908] A.C. 22; *Brassard v Smith* [1925] A.C. 371 (PC); *Baelz v Public Trustee* [1926] Ch. 863; *London and South American Investment Trust v British Tobacco Co (Australia)* [1927] 1 Ch. 107; *Erie Beach Company Ltd v Att-Gen for Ontario* [1930] A.C. 161 (PC). In *Macmillan Inc v Bishopsgate Investment Trust Plc (No.3)* [1996] 1 W.L.R. 387 (CA) the Court of Appeal was divided on this question: Auld L.J. favoured the place where the register is kept (at p.411); Aldous L.J. seemed to regard the place of the register to be irrelevant (at pp.418–425); Staughton L.J. left the matter open (at p.405).

⁹ *Re Clark* [1904] 1 Ch. 294, 298; *Re Aschrott* [1927] 1 Ch. 313; *R. v Williams* [1942] A.C. 541 (PC); *Treasurer of Ontario v Aberdeen* [1947] A.C. 24 (PC); *Standard Chartered Bank Ltd v IRC* [1978] 1 W.L.R. 1160.

book or similar physical object in which entries were recorded by hand. As registers have evolved into electronic form, a legitimate question arises as to where the digital register itself is located.

In answering this question, we believe it is necessary to distinguish between the location of the register and the location of any relevant servers on which the data representing the register is maintained or the location of any cloud service provider (in the event that an electronic securities register is maintained in the cloud). Yeowart and Parsons suggest that the question of the location of a dematerialised securities register is akin to the question of the location of an intermediated securities account.¹⁰ In this context, they have argued that:

“An account is, however, itself intangible. It is a relationship between an account-holder and the person maintaining the account. Accordingly, in order to determine the ‘country in which the relevant account is maintained’ one needs to consider the physical associations of that account and then decide whether they clearly point to a single country. If they point to more than one country, then it is necessary to decide which physical association should be privileged over others. Possible physical associations of an account relationship include: the place of the relevant intermediary’s corporate seat (that is, in relation to a company incorporated in England, its ‘registered office’ under the Companies Act 2006); the place of the office through which the relevant intermediary is acting for purposes of maintaining the account; the place where a customer may visit to discuss the customer’s account with a representative of the intermediary; the place where the intermediary maintains a call centre for those who wish to speak with a representative of the intermediary by telephone; the place where the intermediary maintains the relevant server on which account information is stored; and the office that issues account statements to customers. These locations could all correspond, but they may not. If not, which should be privileged? It may not be difficult to sort this into a hierarchy, but will that lead to a certain result in terms of identifying the ‘location’ of an account? Perhaps so in a specific case, but this approach does not appear to yield a rule that provides *ex ante* certainty for all or even the majority of cases involving the use of intermediated securities as collateral.”

We agree with Yeowart and Parsons that there is a strong analogy between the location of an intermediated securities account and the location of the digital securities register. By their logic, in order to localise the register, it is necessary to take account of all the “physical associations” of the relevant system, including the entity responsible for operating the register, the governing law of any applicable rulebook, and the location of personnel with the ability operationally to rectify or amend entries in the register or otherwise exercise administrative control and exceptions management related to the operation of the system. Whilst Yeowart and Parsons consider the “location of the server on which account information is stored” to be a relevant factor, there is no suggestion that this should be privileged or disproportionately weighted. Indeed, other commentators such as Marie Ooi suggest that it should not be referenced at all.¹¹ Ooi notes that, in the context of registered securities, there is no legal consequence to the situation of the “central computer unit” as it is not kept under the authority of the law of the jurisdiction in which it is located.¹²

This analysis also needs to be considered in light of the fact that, increasingly, some of the physical associations outlined above are less straightforwardly associated with a single location or with a location that is associated with the principal infrastructure or service provider. For example, data storage may be outsourced to (potentially multiple) offshore providers, and the location of cloud-based servicers may be unknown or change without notice or control.

More broadly, in applying the *lex situs* rule to *choses in action*, the courts have sought to keep the idea of control in mind and have laid down the general principle that *choses in action* are regarded as situate where

¹⁰ Yeowart, G. & Parsons, R., *The Law of Financial Collateral*, (Cheltenham: Edward Elgar Publishing, 2016), pg. 13.

¹¹ Ooi, M., *Shares and Other Securities in the Conflicts of Laws*, (Oxford: Oxford University Press, 2003).

¹² *Ibid.*, pg. 106.

they are properly recoverable or can be enforced.¹³ On the basis that, in accordance with the terms of a registered security, its holder is to be identified by reference to a register, or record that taken in its own right amounts to mere data or information but with regard to which title to the securities is determined, it stands to reason that the deemed location of the securities should be the location of the administration, oversight and upkeep of the register – that is to say, the jurisdiction from which the records in the register are capable of being controlled in the ordinary course of the performance of the functions of the registrar, rather than the location where the data representing the register happens to be stored, or any cloud storage service provider happens to be located. In each case, the analogue to possession of the physical register is the ability to exercise control over the records.

All of this indicates that the office or "seat" of the organisation providing services against which enforcement action would normally be taken in its place of business is a more robust (and permanent) basis for determining true *situs*. For similar reasons, it would not be appropriate to consider the location of an outsourced service provider to the principal service provider as the *situs*, as there may be more than one such outsourced service provider in different jurisdictions and each such outsourced service provider will be subject to control by the principal provider of the organisation providing the register or record keeping services.

This analysis can also be applied by analogy to other arrangements under which mere data is used to evidence *choses in action*, beyond registered securities. Similar considerations may also apply in a decentralised context, particularly in circumstances where the record is ultimately maintained and controlled by a central operator. This is a common feature of deployments of distributed ledger technologies in the context of regulated financial market arrangements.

We think the consultation process would benefit from a more fulsome consideration of this issue.

We would be happy to expand on any elements of this response if that would be helpful.

Yours sincerely,

Linklaters LLP¹⁴

¹³ See Dicey, A. V., Morris, J. H. C., & Collins, *Dicey, Morris, and Collins on the conflict of laws*. 15th ed (London: Sweet & Maxwell, 2006), 22-025. See also *New York Life Insurance Co v Public Trustee* [1924] 2 Ch. 101, 109 (CA); *Alloway v Phillips* [1980] 1 W.L.R. 888, 893–894, 897 (CA).

¹⁴ With contributions from: Michael Voisin, Richard Hay, Sophia Le Vesconte and Henry Wells.

Call for evidence on digital assets and ETDs in private international law

Norton Rose Fulbright response

2.

While this question is of considerable theoretical importance, we have not seen it arise in practice. In general, we have not been involved in disputes where finding a relevant gateway has been an issue. For cases involving digital assets, we have found the effective control mechanism for limiting the jurisdiction of the English Courts to be the discretionary test of ‘appropriate forum’ rather than the mandatory application of the gateways.

3.

We have two points in response to this question:

First: loss to digital assets will often not be pure economic loss. The analysis in the Call for Evidence on this point has been superseded by the recent Supreme Court decision in *Armstead v Royal and Sun Alliance* [2024] UKSC 6 (overruling the Court of Appeal on this point). In *Armstead*, the Supreme Court held that the claimant’s contractual liability to pay a sum of money to a third party was not pure economic loss where it was consequent on the defendant having damaged the claimant’s property. The Supreme Court defined pure economic loss as “*economic loss that is not consequent on damage to, or loss of, the claimant’s property (or on personal injury to the claimant)*” (para. 20, per Lord Leggatt and Lord Burrows). The loss in *Armstead* would have been pure economic loss from the viewpoint of the third party – that is, if the contractual liability had been that of the third party to pay the claimant, then the third party’s loss would have been pure economic loss. But, as the loss was a consequence of damage to the claimant’s property, it was not pure economic loss from the claimant’s perspective.

Applying this principle, many scenarios involving digital assets may not involve pure economic loss. Where a digital asset is damaged or lost, the resulting loss will not be pure economic loss. There is some uncertainty as to how these concepts will be applied to digital assets, which will need development by the Courts. By contrast, for instance, where a negligent misrepresentation leads to a change in the price of a digital asset or the purchase or sale of a digital asset at an incorrect price, this will generally be pure economic loss.

Second: we do not consider harmonisation between jurisdiction and applicable law to be necessary for pure economic loss, or generally. They are two different questions subject to different policy issues and there is a risk of inaccuracy if they are conflated. ‘Applicable law’ seeks to determine the single system of law which should apply to a specific issue at a specific time, usually in relation to an event occurring at that moment. ‘Jurisdiction’ seeks to determine a range of possible jurisdictions that may be suitable for hearing the dispute, with suitability judged both in relation to the time proceedings are initiated and the time the relevant dispute arose or the relevant event took place.

Rules for jurisdiction may apply a number of different, mutually inconsistent rationales that permit a variety of different fora. In English private international law, order is maintained through the use of the concept of ‘appropriate forum’, which allows the English Court to determine on the facts of a particular case whether the possible forum indicated by a jurisdictional rule should actually be permitted to proceed with the dispute. Several rationales are evident in the current rules for

jurisdiction. These include: practical ability of the Court to enforce any resulting judgment against a party to the dispute; ability of the Court to enforce any judgment affecting disputed property; consistency with international norms so as to enhance the possibility that any judgment is enforceable abroad; expertise of the English Courts in dealing with questions of English contract and tort law.

Accordingly, fashioning a single legal rule to suit a particular jurisdictional basis rather than the relevant applicable law may not be appropriate. For pure economic loss, for instance, applicable law requires localisation to a single place whereas jurisdiction may lead to a range of different locations.

5.

We consider that the *lex situs* rule should be considered primarily in relation to applicable law rather than jurisdiction. The rule that is there developed could be applied to jurisdiction as one of the many possible gateways. Accordingly, we defer our discussion of *lex situs* to question 19 below.

There is, however, one aspect of *lex situs* that raises an issue peculiar to jurisdiction. This is the temporal aspect. Applicable law is determined in the context of a particular event, generally a transfer of the asset. A transfer requires a transferor and a transferee and this gives some assurance that a *lex situs* based on the asset's location at the time of the transfer is discoverable. But, for jurisdiction, *lex situs* may be determined at the time of the proceedings. This moment has nothing to do with any action in relation to the asset. *Lex situs* at this arbitrary time may be harder to discover. Accordingly, we suggest a gloss to the *lex situs* rule when it is used for jurisdiction: to allow the *lex situs* of the digital asset either at the time of issue of proceedings or, if that cannot be determined, at the time of the most recent event in respect of that asset.

6.

We note that, in *Piroozzadeh, Trower J* accepted the uncontested evidence of the defendant crypto exchange that clients of the exchange retained no property in digital assets deposited with them. Rather, the arrangement was similar to a banking deposit. The underlying assets were swept into a general account owned by the exchange and the client was allocated a credit balance in an account with the exchange. This balance was simply a contractual right against the exchange – again, just as with a deposit held by a bank.

If this is the case, then an exchange would not ordinarily be a constructive trustee in misappropriated digital asset cases. This issue would benefit from a thorough ventilation before the Courts and may also have regulatory implications. As a complex and novel issue, it has not been fully resolved by preliminary, mainly *ex parte*, jurisdiction applications, but we do not consider this to be a failing of the test for service out of the jurisdiction.

7.

We do not agree with this statement. We are aware of several DeFi disputes, including contractual and non-contractual claims, that might have led to Court proceedings had they not settled at an earlier stage. Accordingly, we consider that fact-situations involving DeFi should be considered as part of clarifying private international law in this area.

11.

We consider that tort claims involving digital assets are likely to proceed to trial before the English courts and that applicable law may be an issue in those claims. For instance, we envisage disputes

analogous to debt securities negligent misrepresentation claims involving prospectuses and other marketing materials could apply to issuances of digital assets or promulgation of DeFi platforms.

The relevant test for applicable law – the place where the damage occurs – has been problematical for the CJEU to apply. In cases involving jurisdiction from *Kolassa v Barclays* (C-375/13) onwards, the Court has struggled to articulate a cohesive principle that does not default in practice to the domicile of the claimant, contrary to the aims of European jurisprudence on jurisdiction. The CJEU has also consistently made clear (including recently in *BMA Braunschweigische Maschinenbauanstalt AG v Stichting Belangbehartiging Crediteuren BMA* (C-498-20)) that localisation of damage should apply to applicable law in the same way as to jurisdiction. Accordingly, we do not derive significant assistance from the CJEU caselaw.

If the *lex situs* of the digital asset is used, as we suggest below (see answer to 19), the question of localisation of damage may actually be less problematic for digital assets while still achieving a result that in practice is similar to the CJEU case law. For assets in the existing capital markets, the problem is that the complex holding structures via depositaries do not correspond to participants' interaction via accounts with intermediaries. This leads to a tension between legal doctrine, which points towards a single place of damage, and claimant's expectations, which may be directed to the place of their securities account or where securities were sold. CJEU case law may be seen as attempting to reconcile these positions. This problem does not arise for digital assets held directly by market participants assuming that the place where the damage occurs is the *lex situs* of the asset (although intermediation by exchanges may reintroduce similar problems).

19.

(1)

Many uses of distributed ledger technology involve permissioned blockchains. These platforms may generally only be accessed by users following a predetermined process that includes entering into a legal agreement. For these platforms, the consensus mechanism may be the confirmation of a single person or small group of people. Some of these platforms are simply centralised databases that happen to employ blockchain technology and may be analysed in purely contractual terms, with no new property being created. Other permissioned platforms may satisfy the criteria to create digital assets. Where no new property is created, we agree that contractual principles will be sufficient to determine disputes relating to the platform. We consider below the situation where, despite their permissioned nature, the criteria for the creation of new property are met.

Alternatively, the platform may be a governed blockchain: a permissionless blockchain where the underlying protocol requires every transaction to be signed with a hashed reference to an agreement governing use of the platform. Here, the relevant contractual framework may contain a choice of law that is intended to apply to proprietary as well as contractual questions. This is similar to the permissioned case and the extent to which this should be effective is also considered below.

(2)

In our experience, they do not. **Bitcoin, Ethereum and similar non-permissioned digital assets are a key component of the digital ecosystem. The decentralisation of these sorts of digital assets is a fundamental part of their utility. Accordingly, we regard the non-permissioned digital asset as the central case and permissioned blockchains as peripheral cases that may share only some of the characteristics of digital assets.** In particular, many permissioned platforms will be assimilated to purely contractual arrangements and not involve question of digital asset property at all.

(3)

We consider that a conflicts of law rule to determine the applicable law for property questions relating to digital assets is necessary, and that the paradigm digital asset is based on a permissionless blockchain. Our view is that lex situs is the appropriate connecting factor.

Conceptual basis for conflicts of law rule

We view it as vital for there to be a distinct legal concept that intermediates between the factual circumstances of the digital asset and proprietary rights and liabilities in respect of that asset. This is because property rights, although they exist in and are created by virtue of a legal system, are unique in that they relate to objects. For tangible assets, these objects exist in the real world and have attributes – such as colour, size and location – that subsist independently of any legal system. For the legal system to apply legal rights of property in a consistent and sensible way to tangible objects, these real world properties must be respected: for instance, if the asset disappears, the legal system must recognise that it no longer exists and nobody owns it. This is not a negotiation. If there is a mismatch between reality and the legal system, reality wins. It is incumbent on a legal system simply to recognise and apply physical facts, and changes to them, when determining property rights.

Legal systems achieve this aim and avoid mismatches with reality through the use of separate concepts that intermediate between the legal right and the physical facts. For tangible assets, one such concept is possession (here we mean mainly physical possession). Possession provides a legal analogue that takes account of the relevant facts applicable to a tangible asset so that rights in relation to that asset are consistent with reality.

The lex situs rule arises naturally in relation to tangible assets. To determine the applicable legal system for a proprietary right in respect of a tangible asset, one seeks not only to use the nature and extent of those legal rights but also to connect those legal rights to the physical facts relating to that asset, so that any reality mismatch is avoided. Among these physical facts, the principal one is location. Lex situs is an intermediary concept applying facts about the real world location of a tangible asset to determine a legal rule.

Note that this reasoning does not apply to choses in action. Lex situs is applied to choses in action by extension of the rule for choses in possession, but there is no danger of inconsistency with the real world whatever rule is chosen. If the legal system decrees that a debt exists, it exists. If it determines that a debt does not exist, it does not exist. The legal system may choose to create or alter choses in action dependent on actions or circumstances in the real world, but in the case of any mismatch, it is the legal system that determines the correct answer – nothing in the real world logically requires any different conclusion. This leads to artificiality in applying lex situs to certain choses in action.

Crucially, this artificiality is not applicable to digital assets. A key distinction in property is between assets that exist by virtue of a legal system and assets that exist independently of any legal system. Digital assets, unlike choses in action, fall into the former category. If a court decrees that a bitcoin does not exist, that does not cause it to disappear. Digital assets exist by virtue of facts in the real world, independently of legal systems. And so, as with tangible assets, they require concepts to intermediate between the real world and legal rights in relation to those assets. We note that control is the principal concept currently being employed (except for electronic trade documents where possession is applied directly due to recent legal reforms initiated by the Law Commission).

Avoiding mismatches with reality is relevant for digital assets just as it is for tangible assets and so *lex situs* is appropriate as an intermediary concept. Whereas the application of *lex situs* to choses in action is convenient but artificial, for digital assets it reflects a principled need to maintain consistency between the real world and legal rights.

Objectives of conflicts of law rule

Certainty and enforceability are the two broad objectives of the conflicts of law that should be borne in mind. Resistance to abuse is also crucial and may be seen as one aspect of certainty. Relating this to *lex situs*, the argument runs that the courts where an asset is located will be best able to enforce any judgment in respect of it and the location of an asset, being unique in time and space, provides a means of linking it to a legal system that is independent and certain. For immovables, this argument is unimpeachable: clearly, the jurisdiction where the land or similar asset is located is uniquely able to enforce judgments in respect of it and any person dealing with the asset would naturally assume that this is also the law applicable to it.

Similar arguments apply to some existing intangible assets, although these are classed as movables for private international law purposes. For many intangible assets, there is a clear choice of *lex situs* that is effectively fixed: the place of incorporation of a company or the location of its share register does not generally change location. Certainty is thereby established according to easily discoverable criteria that also correspond to the location where enforcement is most convenient.

Tangible assets have a definite location but raise a new problem, due to the temporal aspect: their location can change. This creates an additional tension between certainty and enforcement. These values may be directly in conflict with each other. For enforcement, one considers the time when the dispute arises; for certainty, one considers the time when the relevant event involving the asset took place. A consistent, multilateralist approach to private international law requires certainty to be preeminent over enforcement as embodied in Dicey, Morris & Collins's Rules 141 and 142, which states that proprietary rights in respect of a transfer are governed by the *lex situs* at the time of the transfer. Rule 141 applies the *lex situs* at a given moment and Rule 142 forbids that application from being displaced retrospectively. Although they appear to overlap, Rule 141 creates a certain and predictable rule and Rule 142 guards it against abuse (by dealing with *conflict mobile*: where *lex situs*, the connecting factor, subsequently changes location). These are two desiderata of a connecting factor: certainty in application and resistance to manipulation.

Certainty requires a connecting factor that operates at the time of the relevant event. As property rights necessarily affect third parties this factor must be discoverable. To avoid abuse, it must also be an effective control mechanism – not something that can be arbitrarily manipulated by the parties to the original transaction. This suggests using some fact related to the physical manifestation of the asset. Where there is no physical manifestation, as with contractual rights, a rule can still be manufactured that maximises certainty by reference to the legal system creating the right, although it may be somewhat artificial. For digital assets, *lex situs* is the appropriate connecting factor.

In addition, the importance of enforceability in relation to tangible assets is largely illusory. In almost all situations, claims will be satisfied by payment of a sum of money rather than any physical movement of the relevant asset. The default remedy for a claim in conversion is payment of the value of the asset, not return of the asset. Even proprietary claims involving digital assets have generally sought remedies such as knowing receipt, which is a personal claim available where the defendant does not still possess the asset.

The recent Supreme Court decision in *Byers v Saudi National Bank* [2023] UKSC 51 illustrates the policy choices behind *lex situs*. Shares registered in Saudi Arabia were transferred in breach of an English law trust to the defendant, a Saudi bank. The defendant was aware of the trust and so was not, in English terms, a bona fide purchaser of the legal estate for value without notice. Saudi law did not recognise the trust and treated the transactions as an effective legal transfer of the shares. The Supreme Court held that a knowing receipt claim against the defendant failed because the claimant had no continuing proprietary interest in the shares after the transfer, its legal effect being governed by Saudi law, as it had determined in a previous judgment (*Akers v Samba* [2017] UKSC 6). Enforcement was not the problem: the English law governed claim was being brought in the English courts in respect of an English law trust. But certainty and discoverability required Saudi law to apply to the proprietary issues.

Imagine a different rule applied to the converse to the *Byers v Saudi National Bank* situation: transfer of an English registered share in breach of trust to a recipient who is not a bona fide purchaser. If proprietary consequences followed the governing law of the transfer agreement, the parties could simply arrange for this to be Saudi law: English trust law would be instantly and comprehensively undermined. Proprietary consequences following the location of the transferor or the asset (if it is a tangible movable rather than a registered share) can only be manipulated by moving things – assets or people – in the real world. And, of these, the location of the asset is the circumstance most closely associated with that asset and likely to be the most discoverable and predictable. An even worse solution would be a rule that refers to the time that the dispute arises rather than the time of the relevant event – this would enable abuse by participants even after the fact, turning an invalid transfer into a valid transfer in defiance of legal common sense. Considering the practicalities of hypothetical alternatives leads back to *lex situs*.

Omniterritoriality

Our view is that the objection to *lex situs* based on the ‘omniterritoriality’ of blockchain is misplaced.

We consider a permissionless blockchain where transactions are recorded in a distributed ledger verified by a consensus mechanism. The ledger is a database containing a record of the current state of the system, via a complete list of transactions or a set of account balances or some equivalent data. There is no privileged single version of this ledger and nor is there any entity that can confirm its veracity. Rather, the consensus mechanism enables anyone to obtain a copy of the ledger and to verify that it is accurate.

Anybody wishing to add a new transaction does not do so by amending the ledger directly – they need not have a copy of the ledger at all. Rather, they will interact with the consensus mechanism, generally by sending a message in some electronic format to the system operating that mechanism. One universal feature of these platforms is the use of cryptographic means to link a person with an account or an asset – knowledge of the relevant private key is the only means to effect a transfer of that asset.

New transactions can be added but old transactions cannot be removed. That sometimes leads to the assertion that rectification and rescission are not available for distributed ledgers. This is wrong. Rectification of contracts on the physical world does not require the participants to go back in time and reverse the original transfers of value – instead, future transfers are made to align the world with the rectified contract. Similarly, rectification and rescission of distributed ledger arrangements are accomplished by adding suitable new transactions (see Sanitt, Remedies for smart legal

contracts: Rectification and rescission reconsidered in Baris Soyer (Ed), *Damages, Recoveries and Remedies in Shipping Law* (London, 2024)).

This error is an example of a wider misconception about distributed ledgers. The ledger is not a means of making changes in the way that an electronic database is both a record and a means of making changes to its contents. A distributed ledger is a fixed view of the world that is available to any person downloading software that is compatible with it. ~~Those who possess a copy of the distributed ledger are not thereby participants in the system,~~ in the sense that they can actively influence it, but are only observers. Even an individual involved in updating the ledger via the consensus mechanism – in Bitcoin, a miner – does not have the ability to influence the system. They are performing a purely mechanical task that allows the system as a whole to operate in return for some personal reward.

Participants in the distributed ledger must, in respect of any particular transaction, be divided into observers and actors. The actors are those who involved in the particular transaction: undertaking actions to bring it about (other than as part of running the system as a whole to bring about all transactions) or whose individual accounts or balances are changed by that transaction. ~~Observers are all other participants in the system.~~

Observers may be located throughout the entire world, but it does not follow that digital assets thereby exist everywhere in the world at once: the idea of ‘omniterritoriality’. A physical object might be observable from anywhere in the world – perhaps if an image of it is broadcast on television or it is particularly large or if distant observers use telescopes to see it – but it does not thereby exist everywhere in the world. A physical object exists in just one place, which is where people can actually interact with it and move it to another place. Similarly, the *lex situs* of a digital asset should be based not on all participants in the system, **but only those who interact with it, those who are actors in the relevant transaction.** The distributed ledger, miners and software developers being located everywhere does not affect the calculation of *lex situs* – **only those who are actors in the relevant transaction need to be considered.**

Lex situs as connecting factor

A digital asset on a permissionless blockchain requires a connecting factor **that prioritises certainty and discoverability** and is based on some physical manifestation of the asset. The connecting factor operates at the time of the relevant event, when there is a very limited group of actors (usually just two) in respect of that event (as opposed to the wider universe of participants, who may observe the event). It must also be resistant to abuse.

The attributes of the digital asset exist in the virtual world maintained by the blockchain consensus. Of these attributes, the two that interface with the real world and may provide data for a physical location are the public key – that is, the account associated with an asset – and the particular usage of the private key at the moment of a transfer. Apart from when it is used to transfer an asset, the private key does not directly interact with the digital asset and is not part of the blockchain consensus. Accordingly, we view criticism of the applicability of property rights to digital assets based on the non-rivalrous nature of private keys (as mere information) as misplaced.

Accordingly, the use of *lex situs* as a connecting factor that intermediates between the virtual world of digital assets and the geography of the real world should focus on ownership of the public key and, only at the moment of transfer, use of the private key. Generally, this will entail the residence (or possibly domicile) of the owner of the digital asset at the moment of the relevant event, which is relatively stable and resistant to abuse. It has the requisite degree of certainty and discoverability.

Conceptually, it provides the closest possible analogy to the location of a physical asset: the owner of a digital asset is generally the person with the private key who is physically able to exercise control over the asset. Practically, it is the fact about the digital asset most likely to be ascertainable, as the private key must be used by the owner at the moment of the relevant event. Where there is more than one person with access to the private key, the relevant location is that of the person who actually does use it – just as the person in possession of tangible property is the one who actually takes hold of it, even if several other people might have been able to do so.

Even where a digital asset has a disputed history, the ownership of the asset at the time of a particular event is unlikely to be disputed, if one accepts a peculiar feature of one current legal understanding of the nature of digital assets. This feature is that transfers of digital assets take place through the extinction of one asset and its replacement by an identical copy in another place. Accordingly, proprietary claims against a digital asset will proceed by tracing that asset through the platform, rather than following it. So, if a digital asset is stolen and transferred into a different account and then the corresponding digital asset is transferred again, the owner of the asset at the time of the second transfer will be the person with control over the private key for the second account and not the victim of the thief. The victim will have various remedies, including proprietary remedies based on tracing the digital asset into its replacement in the second account, but that does not affect the ownership of the replacement asset at the time of the second transfer. If this analysis is adopted, many concerns about resolving ownership of digital assets for *lex situs* purposes are misplaced.

One genuine difficulty in applying this *lex situs* rule is reconciling off-chain transactions involving a digital asset. For instance, consider the situation where the owner of a digital asset enters into a written contract of sale with a third party and then a relevant event, such as a transfer of the digital asset, occurs at a time after the transfer of title specified in the contract. The legal effect of this chain of events is currently unclear – this is a weakness not of conflicts of law and *lex situs* but of the law generally relating to digital assets. It may well be that legal title to the digital asset is not transferred to the buyer until a corresponding entry is made in the digital ledger. Until this situation is clarified, the application of *lex situs* to it cannot be finalised.

Overall, principle leads us to use an intermediary concept that is linked to the physical manifestation of a digital asset and practicality requires that this concept is certain and discoverable. This concept is *lex situs* and it is defined as the residence of the owner at the time of the relevant event – if the event is a transfer, the residence of the transferor.

Permissioned and governed blockchains

The two options here for a choice of law are the *lex situs*, as for permissionless blockchains (that is, ignoring any express choice of law for proprietary questions), or the choice of law expressed in the platform. Unlike permissionless blockchains, the argument here is finely balanced. If the situation is seen as analogous to creation of a registered asset, then the chosen law would be apposite, so there is conceptual support for this position. Certainty and discoverability also point to the chosen law.

The major obstacle to this option is the possibility of abuse. Proprietary choice of law is often seen as distinct to contractual in that it is a mandatory choice, determined by rules of conflicts of law and not the parties. One key policy behind this distinction is to prevent abuse. Proprietary rules affect third parties who are not involved in any choice and may be disadvantaged by it. They apply exactly when the interests of the parties to a transaction may be distinct from the interests of the third party.

Governed and permissioned blockchains have some support against this argument because any party involved in the platform will have to agree to the relevant law. Any third party will have expressly opted for the chosen law, and so should be taken to have agreed to the consequences, as they are a participant in the platform. Unfortunately, not all third parties fall into this category. The third parties affected by a voluntary selection of proprietary governing law are not only those who come after the relevant transaction – transferees, takers of security – but also those who come before – such as trust beneficiaries. While third parties who are involved afterwards might be expected to find out about the implications of the proprietary governing law before they engage with the asset, those involved before have no such opportunity.

The fundamental problem is that party choice of proprietary governing law in relation to digital assets is too easy: there is no control mechanism, such as requiring the parties to be in a certain jurisdiction or to move the relevant asset to that jurisdiction, that can adequately protect third parties.

The problem is not just that a party choice rule is susceptible to abuse, but that there are no anti-avoidance rules that protect against such abuse. This is not surprising as the legal rule implementing party choice which would require such anti-avoidance limitations does not yet exist. Compare the rule permitting voluntary choice of applicable law for contracts. Although contract law does not affect third parties in the same way as property law and so there is less scope for abuse, voluntary choice is still limited by anti-avoidance rules that apply provisions of the law of another country in specified circumstances. An effective choice of proprietary law would contain similar, probably more extensive, limitations. Delivery of this entire package as a single unit is likely to be beyond the incremental approach of the common law – it could only be done by statute.

Our, somewhat hesitant, conclusion is that a voluntary proprietary rule for permissioned blockchains – that is, a voluntary *lex situs* – would be feasible, but only if it was created by a statute that included all the anti-abuse provisions necessary to protect third parties. The hesitation arises from the fact that once limitations and exceptions are admitted to the rule, it becomes less appealing. Instead of a simple, universally applicable rule, there would be a qualified rule subject to exceptions. Whether this would create more problems than it solved would depend on the details of its statutory implementation.

(4)

Property rights are generally enforceable against the whole world and so apply where third parties are affected by the transfer or another event involving an asset. Rules that apply only between parties to a voluntary arrangement do not obviate the necessity to formulate property rights.

As noted above, extension of voluntary choice to third parties creates the possibility of abuse.

(5)

Our suggested *lex situs* connecting factor is defined by reference to the owner of a digital asset at the time of the relevant event.

(6)

We envisage that it is very likely Courts will be required to deal with this situation.

(7)

We recommend the application of *lex situs* as the appropriate connecting factor as set out above.

‘Digital assets and ETDs in private international law: which court, which law?’

Call for Evidence- UK Law Commission

Submitter: Associate Professor Sagi Peari (University of Western Australia Law School, Australia)

Publications upon which this submission is based:

Books:

1. Sagi Peari, *The Foundation of Choice of Law: Choice & Equality* (NY: Oxford University Press, 2018) [Peari, 2018];
2. Benjamin Geva & Sagi Peari, *International Negotiable Instruments* (Oxford: Oxford University Press, 2020) [Geva & Peari, 2020].

Articles:

1. Sagi Peari, ‘Savigny Theory of Choice-of-Law as a Principle of Voluntary Submission’ (2014) 64 (1) *University of Toronto Law Journal* 106 -151;
2. Sagi Peari, ‘Conflict of Laws Rules Applicable to Negotiable Instruments’ (2022) 38 (3) *Banking and Finance Law Review* 155-178;
3. Sagi Peari, ‘Negotiable Instruments Law: Two Layers of Harmful Discrepancy’ (2023) in Gulati et al eds, *Elgar Companion on the United Nations Commission on international Trade Law* (Elgar, 2023) 462- 479.

1. Laudable Approach

- (a) **Qualification of the Existing Rules, not Elimination**: I commend the Commission for embracing an approach which takes seriously the existing rules of private international law,¹ aiming to accommodate the challenges of technology within their scope. The traditional private international law doctrines, concepts and principles have been designed through centuries of case adjudication, legislative deliberation, and the intricacies of particular cases. There is no reason to hastily discard the wisdom of decades and centuries in light of the challenges that new technologies, electronic payments and digital currencies posit for the legal systems. Rather, one may need to uncover the underlying rationale of the traditional rules and then qualify those rules in a digital reality. The notions of justice, reasonable expectations of the parties, certainty and Rule of Law all favour this approach to the challenges of technology;²
- (b) **Westphalian Order**: I also commend the Commission for rightly recognising that cross-border interactions and the complex web of financial dealings still takes place within the Westphalian paradigm³ which comprises of sovereign states which are situated in equal relation to each other and are governed by positive law. This observation is critical for the careful exercise of tracking the underlying rationale of the existing rule of private international law which, given the Westphalian paradigm, must respect the equality between states, the formal structure of the rules of private international law and limiting the substantive assessment of foreign rules to a minimum⁴;
- (c) **Taking the actual practice as the point of departure for the inquiry**⁵- naturally, practice informs theory and *vice versa*. For centuries, private international law rules have been designed, qualified and reformed in light of actual cases, the challenges related to the increased mobility of goods and people, technological inventions (such as phones/facsimile and a broad distribution of newspapers) and the sophistication of financial instruments and commercial dealings. An approach which focuses on contemporary challenges such as the storage of digital files and deprivation of cryptocurrencies fully aligns with the classical development of private international law.

¹ *Summary of the Call for Evidence* at 7-8, 11-12 [Summary].

² Peari (2018), chapter 6 (E), Geva & Peari (2020), chapter 8.

³ *Summary* at 11.

⁴ Peari (2018), chapter 4.

⁵ *Summary* at 7-8.

(d) **My replies with respect to particular inquiries:** the above laudable positions expressed by the Commission in the *Call for Evidence* with respect to the above (a) (b) & (c) points, lead us to agree with the majority (albeit not all) of the suggestions made by the Commission.

Specifically:

- In the context of **digital files** stored online, I support assigning a central legal role to the location of the data-storage provider. In the context of the question of applicable law, such a location should serve as a presumption (see 2 (b) below);⁶
- In the context of the required ‘gateways’ for acquisition of ‘**international jurisdiction**’, I support the suggested connecting factor of the place of damage.⁷ The exercise of tracking the underlying rationales of the traditional rules indeed suggests that some connecting factors (such as the physical location of the asset) must lose their traditional strength in a digital reality. Since I do not accept the principles of sovereignty/territoriality of the exclusive principle of the discipline [see 2 (a) below], there is no reason to insist on the physical location of the asset;
- In the context of the law **applicable to contracts**, I support the existing three-fold hierarchal structure of: (1) party autonomy, (2) presumptions, and (3) the flexible ‘manifestly more connected’.⁸ One may argue that this unified structure fundamentally epitomises the underlying rationales of the discipline.⁹ There is no reason to undermine this structure in light of the challenges of digitalisation.
- In the context of the **exclusion of financial products** by Rome I Regulation, I support the suggested liberal reading of the Regulation. In similar to the unjustified exclusion of negotiable instruments (as Professor Benjamin Geva and I have argued¹⁰), the inclusion of financial instruments must be accompanied by a careful analysis of their doctrinal bases and subsequent qualification to become a part of the Regulation;
- In the context of the financial damage sustained because of a **claimant’s deprivation of their cryptocurrencies**,¹¹ I support the suggested focus on the financial consequences of that deprivation, at least as a point of departure for the legal analysis [see 2 (a) below]. Such an approach would be consistent, according to my view, with the nature of financial assets and the exercise of mapping the focal points of the parties’ interaction.

2. Matters of Concern

(a) **The axiom about states’ sovereignty and territoriality-** with respect, one could challenge what appears to be the underlying axiom of the *Call for Evidence* according to which private international law rules must be based on the single notion of states’ sovereignty and territoriality.¹² In fact, it could be argued that the foundational father of private international law- Friedrich Carl von Savigny, rejected this strictly sovereign/territorial approach, at least with respect to the first two questions of private international law: jurisdiction and choice-of-law.¹³ In line with this reading of Savigny, contemporary scholars have argued that private international law has already integrated and must further integrate within its foundational principles such notions as¹⁴:

- Certainty and predictability;

⁶ Summary at 6.

⁷ Summary at 9-10.

⁸ Summary at 12-13

⁹ Peari (2018), chapter 3.

¹⁰ For a discussion of this point, see Geva & Peari (2020), Introduction.

¹¹ Summary at 13-14.

¹² Eg Summary at 5 (“...they [contemporary technologies] challenge the territorial basis upon which the modern systems of private international law are premised”).

¹³ Sagi Peari, ‘Savigny Theory of Choice-of-Law as a Principle of Voluntary Submission’ (2014) 64 (1) *University of Toronto Law Journal* 106 -151.

¹⁴ Peari (2018); Geva & Peari (2018).

- Party autonomy;
- Approximation towards party autonomy;
- Individual justice and fairness;
- Reasonable expectations and risk allocations of the parties;
- The internal structures and underlying rationales of the distinctive private and commercial law categories and structures (contracts, torts, property, negotiable instruments etc')

This point is quite critical for the laudable exercise of mapping and tracking the underlying rationales of the traditional doctrines of private international law. If one says that the underlying rationale is not about territoriality/sovereignty (as the Commission seems to assume), the challenge of technology becomes a manageable task for the traditional legal doctrine to cope with. Here are some examples:

- **Presumptions**- while I support attributing central significance to such connecting factors as the geographical location of the data-storage provider [see 1 (d) above], in the context of the applicable law question this connecting factor must only serve as a presumption, or a point of departure for the legal analysis. Freed from the stringency of the territoriality/sovereignty principle, the digital reality directs towards a flexible assessment of the parties' interaction;
- **DLT**- similarly, the apparent weakness of the traditional geographical location of the 'thing' in the digital context, does not present an analytical difficulty for an approach that does not take the 'sovereignty'/'territoriality' axiom for granted. Rather, the digital context would require re-focusing the analysis on other factors and reconsidering the presumptions;
- The alleged **difficulty of the conflict of laws** (i.e. applicable law) **analysis**- while it could be argued that digitalisation disappointingly leads the conflict of laws analysis to 'point to several legal systems, each in equal direction',¹⁵ this observation is based on the 'territoriality'/sovereignty' axiom. Once we free ourselves from this axiom, the challenge of digitalisation becomes no more difficult than the challenges private international law faced at the times of the invention of phone and introduction of a wide distribution of newspapers;
- The application of the '**manifestly more connected**' principle- it is impossible to contemplate on the operation of this principle without taking into the consideration the related two principles: (1) party autonomy and (2) the focal points- the presumptions. Furthermore, taken together, the three principles (party autonomy, presumptions and 'manifestly more connected) must be contextualised within the particular private and commercial law categories. This is a basic exercise of the conflict of laws process which requires careful consideration and attention to the circumstances of a particular dispute.¹⁶
- **Bills of lading**¹⁷- bills of lading do have features of negotiable instruments. This feature needs to be taken into consideration while contemplating on the design on the nature and content of conflict of laws rules applicable to bills of lading. Professor Benjamin Geva and I discuss these issues in Chapter 7 of the *International Negotiable Instruments* monograph;¹⁸
- **Property**¹⁹- equally, freeing ourselves from the sovereignty/territoriality axiom, would enable us to reconsider the role of the traditionally powerful connecting factor of *lex situs*. While this connecting factor must continue to dominate the field of immovable property/land, the underlying rationales of the discipline may suggest that *lex situs* should play only a marginal role in the context of digital assets and financial transactions.

¹⁵ Summary at 11.

¹⁶ See Peari (2018) chapter 6; Geva & Peari (2018) chapter 6.

¹⁷ Summary at 15-16.

¹⁸ Geva & Peari (2018) chapter 7.

¹⁹ Summary at 16-17.

(b) **The three-fold classification of private international law methods**- the presumption according to which private international law should be classified into the following three methods: (1) ‘supernational law’, (2) ‘unilateralist approach’, and (3) ‘multilateralist approach’²⁰ is equally problematic. *First*, the methods and approaches to private international law are highly debatable in the literature; there no consensus with respect to the list of the leading approaches/methods. *Second*, it’s not clear to what degree and extent the three-fold classification applies to each one of the three questions of private international law. These are not the same questions. Each question (jurisdiction, applicable law and recognition) is analytically distinctive, what requires an extensive exercise of delineation and adjustment to each one of the three methods. *Third*, the link between the three methods and the suggestions made by the Commission is somewhat vague. One would wonder whether the three-fold classification can actually assist the Commission in its inquiry. The Commission could simply reject (as suggested) the sovereignty/territoriality axiom and state the underlying principles of the traditional private international law rules. The Commission does not need to commit itself to suggested three-fold classification of the discipline.

3. Section 72 of the Bills of Exchange Act

I believe that the future of payment mechanisms belongs to electronic negotiable instruments which have a significant advantage over other mechanisms. The advantage of negotiable instruments is the accumulated wisdom and self-reflection of centuries, their internal balance within the risks and expectations of the parties and consumer protection considerations.²¹ The *Electronic Trade Documents Act 2023* made a critical step towards the legitimisation of negotiable instruments; the adjustment and qualification of their traditional paper-based form towards their full paperless digitalisation.²²

It is impossible to restate in this submission the entire *International Negotiable Instruments* monograph (OUP, 2020)²³ which dealt in great detail with section 72 of the *Bills of Exchange Act*. The monograph focused on this section, elaborating on its history, doctrine, comparative outlook, theory, possible interpretations and most importantly- the required reform of it.

While the manuscript makes some extensive observations on the proper interpretation of the conflict of laws rules set in section 72 of the BEA, covering such complex issues as ‘issue’ and ‘delivery’,²⁴ our principal position is that Section 72 is **ripe for reform**.²⁵ As Professor Benjamin Geva and I discuss in detail, section 72 has been left behind the major developments in the private international law doctrine of the last centuries, which **moved away from the connecting factor of the place of contracting**. While this connecting factor was justifiable in the context of the 18th and 19th centuries, it was precisely the technological advances related to contract formation and the growing phenomenon of mobility of goods and people which led to reconsideration of the ‘place of contracting’ outside of negotiable instruments. Put simply, as we show in the monograph, due to some mythical arguments about ‘distinctive’ and/or overly ‘complex’ character of negotiable instruments,²⁶ this law has been unfortunately left behind the sustained qualification and adjustment of the private international law doctrine, which took place precisely due to the ongoing shifts in technology and our social reality.

So, ironically, and in sharp contrast to the main thesis of this submission with respect to other areas of law, it is submitted that Section 72 of BEA does not require qualification or adjustment of their conflict of laws rules (as the other areas of law do) - but an elimination. This is indeed the ‘**radical overhaul**’²⁷ of section 72 which we suggest in the monograph. The draft of the alternative appears in the Appendix of the *International Negotiable Instruments*.²⁸

²⁰ *Call for Evidence*- chapter 2.

²¹ Sagi Peari, ‘Negotiable Instruments Law: Two Layers of Harmful Discrepancy’ (2023) in Gulati et al eds, *Elgar Companion on the United Nations Commission on international Trade Law* (Elgar, 2023) 462- 479.

²² *Electronic Trade Documents Act 2023*, sections 2-5.

²³ Geva & Peari (2018).

²⁴ Geva & Peari (2018) chapter 4.

²⁵ Geva & Peari (2018) chapters 5-8.

²⁶ Geva & Peari (2018) chapters 1-2.

²⁷ Geva & Peari (2018) *General Editors’ Foreword; Introduction*.

²⁸ Geva & Peari (2018) *Appendix*.

From: Luminita Procopie [REDACTED]
Sent on: Thursday, May 16, 2024 5:47:17 PM
To: conflictoflaws <conflictflaws@lawcommission.gov.uk>
Subject: Digital assets and ETDs in private international law: \Which court, which law? Call for Evidence

[REDACTED]

To my mind, the only reasonable solution to developing a legal framework that could address the questions on which law and which court to apply to digital assets and DLTs is an international convention such as an amended Rome Convention to address this new phenomenon or a set of similar reforms on legislation of many countries similar with the development of the netting legislation and legal framework governing the use of internet.

In particular, I would like to mention one point that should be considered under the new legal framework i.e. the issue of domestic contracts that cannot be placed under foreign law even if a choice of law is expressed in the terms agreed by contract as the ***doctrine of the foreign element*** is viewed as mandatory law aspects related to the sovereignty of a country of civil law tradition (jurisdictions which represent the majority of the global population). Therefore, in all continental European countries, the general position is that the Rome Convention cannot apply to pure domestic contracts which are not a matter of private international law that the Rome Convention covers and this is a matter where the conclusions presented in Dicey and Morris diverge from the actual conclusions of the Giuliano and Lagarde Report.¹

The point is particularly important for digital assets and DLT where there is no doubt that there will be domestic transactions on the chain and these cannot be placed under the jurisdiction of a different state unless the law is amended. Therefore, an English court decision over a pure domestic transaction of a different country will not be recognized under current legislation of the respective civil law country as it will be seen as displacing the local law and it is a point that touches upon sovereignty/mandatory law spectrum. Furthermore, if the respective on-chain transactions are related to consumers, the mandatory laws of the consumer's country are displacing any choice of foreign law or foreign courts.

In respect to development of the national legislation, it might be an idea to coordinate the efforts with the countries where similar initiatives are made to determine the scope for national legal framework in a similar manner and make it easier to agree on the common ground for the international convention.

Kind regards,

Luminita Procopie

[REDACTED]

[REDACTED]

[1] The French version of the Giuliano and Lagarde report does not confirm that the choice of law is sufficient to bring domestic contracts in scope of the Rome Convention contrary to the conclusion expressed in Dicey, Morris & Collins, Conflicts of laws 14th Edition Sweet & Maxwell Volume 2 pg.1563.

Submitted to Law Commission Call for Evidence on digital assets and ETDs in private international law
Submitted on 2024-05-16 10:40:31

About you

What is your name?

Name:
Camilla Slater

What is your email address?

Email:
[REDACTED]

What is your telephone number?

Telephone number:

Questions on applicable law - negotiable instruments, bills of lading, and the exclusions from the Rome Regulations (Chapter 10)

Question 13: We seek evidence, particularly from market participants, on how market practice in respect of bills of lading has been affected, or how it is likely to be affected, by the introduction of the Electronic Trade Documents Act 2023.

Please share your views and evidence below::

Question 14: We seek evidence on market sentiment relating to use of DLT platforms for electronic bills of lading.

Please share your views and evidence below::

Question 15: We seek evidence on the difficulties, if any, of incorporating the Hague-Visby Rules where an electronic bill of lading has been used.

Please share your views and evidence below::

We have no comment to Question 15 (1).

In relation to Question 15 (2), ii) it is the expectation of the International Group of P&I Clubs (IG P&I), that where the governing law of an electronic bill of lading gives legal recognition to bills of lading in electronic form, then the Hague Visby rules should apply to the same extent that they would have applied had the bill of lading been in paper form. In our view, the form or media of the bill of lading should not matter provided the law recognises the document as a bill of lading. There is however a difference between electronic bills of lading under the ETDA and those under some current contractual systems. Not all documents regarded as bills of lading issued pursuant to the terms and conditions of those contractual systems would be recognised as bills of lading under the governing law of the document purporting to be a bill of lading (as opposed to the law of the contractual system). Therefore, the Hague Visby rules would not apply to those documents which in law are not bills of lading, as they are not within the scope of the Hague Visby Rules. The Hague Visby Rules, however, can be applied by contractual incorporation and an agreement by users of the systems not to dispute the status of the electronic "bill of lading".

Question 16: We seek evidence on market practice to help us identify where it could be said that an electronic bill of lading is "issued" for the purpose of the Hague-Visby Rules, as implemented in the UK by the Carriage of Goods Act 1971

Please share your views and evidence below::

Whilst many bill of lading forms typically provide for a place of issue to be inserted, in the absence of such a provision (or in the case of subsequent – re-issue) we consider it helpful to identify the place of issue of an electronic bill of lading as this may be significant in the application of the Hague Visby rules. Place of issue of a bill is a distinct criterion to that of port of shipment. We believe that due to the uncertainty of where servers may be and that cyber is borderless, not to mention operating personnel in modern remote working practices, it is important to strive for some degree of certainty perhaps by a deeming provision determining the place of issue.

S



The Society of Scrivener Notaries

11 Old Jewry, London, EC2R 8DU,
England

www.scrivener-notaries.org.uk

notary@scrivener-notaries.org.uk

City of London,
15 May 2024

Response of the Society of Scrivener Notaries

Law Commission Call for Evidence

Digital assets and ETDs in private international law: which court, which law?

1. The Society of Scrivener Notaries (“the Society”) is the professional body representing the interests of scrivener notaries practising in the City of London and beyond. Scrivener notaries are a specialised branch of the profession of notaries public generally.

The role of notaries in the English legal system generally

2. Notaries in England and Wales exercise the important public office and duty of preparing and authenticating legal documents, whether in paper or digital form, creating or affecting rights, duties and obligations chiefly outside the United Kingdom. The notarial system is an integral part of the legal structure of jurisdictions founded under civil law and, in these jurisdictions, the notary’s intervention is necessary to consummate many of the most important legal transactions. In England and Wales, as in other common-law jurisdictions, the notarial system is less deeply rooted, and notaries primarily exist in order to enable parties to give effect to legal transactions outside the United Kingdom. This role is nonetheless an important one and integral to the United Kingdom’s status as a trading nation and, in particular, to the maintenance of the City of London as an international financial and trading centre.

The role of Notaries in relation to of bills of exchange

3. Notaries have an important function in relation to of bills of exchange. Under s.51(2) and (4) Bills of Exchange Act 1882 (“the 1882 Act”), in the event of dishonour of a foreign bill, either by non-acceptance or for non-payment, the holder is obliged, in order to protect their right to sue on the bill, to have the bill duly noted and protested. It is also possible, though not compulsory, to protest inland bills for non-acceptance or non-payment, or to protest a bill for better security in the event that the acceptor becomes insolvent. As confirmed by s.51(7) of the 1882 Act, the noting and protesting of bills of exchange are, with certain exceptions, activities reserved to notaries public. There are also other, more marginal notarial activities associated with bills of exchange, including the act for honour *supra protest*. In former times, the business of notarial

presentment and noting, followed by extension of a notarial protest, was a core part of the practice of scrivener notaries. Over the course of this century, the significance of this work in most notaries' day-to-day practice has declined. However, s.51(7) of the 1882 Act remains in force, and an understanding of bills of exchange and notarial protest thereof remains a compulsory part of the academic training required for admission as a notary public¹ and for the further qualification of scrivener notary.²

4. A full account of the procedure of notarial presentment, noting and protest may be found in *Brooke's Notary*.³ For these purposes, a brief summary of the procedure in the case of non-payment is given here. The notary:
 - Attends at the place at which the bill is payable
 - Formally re-presents the original bill with a demand for payment
 - Records the response given (if any), or any other relevant fact (e.g. that the premises were empty, the building demolished, etc.)
 - Notes the bill; which is to say, makes a hand-written minute on the face of the original bill, recording the identity of the notary, date of attendance and brief details of the response given
 - Records the relevant facts in the notarial register
 - Later, "extends" (writes out) a notarial instrument of protest, under signature and seal of office, certifying as to the facts above and annexing a copy of the dishonoured bill.
5. It should be borne in mind that strict time limits apply in order for the presentment, noting and subsequent protest to be valid. By s.51(6) of the 1882 Act, a bill must be protested at the place where it is dishonoured. However, where "authorised by agreement or usage", the Act allows presentment to be made by post (s.45(8)). In such cases, a bill returned by post that is dishonoured may be protested at the place to which it is returned.
6. It is also important to note that the original of the bill must be presented. Under the 1882 Act, s.51(8), it is clear that protest may only be made on a copy of a bill of exchange in circumstances where the original bill is "lost or destroyed or is wrongly detained from the person entitled to hold it".
7. As will be evident from the foregoing, this procedure is heavily dependent on the existence of a paper bill of exchange as a physical object, and on acts being carried out at a prescribed place. Now that the Electronic Trade Documents Act 2023 ("the 2023 Act") has come into force, the Society understands that electronic bills of exchange are already circulating in the market. We suggest that it is regrettable that this is so without any clarity having been established as to how such bills might validly be protested in the event of dishonour.

¹ Notaries (Qualification) Rules 2017, Sch.2, para.11

² Scriveners (Qualifications) Rules 2019, Sch.5

³ Nigel Ready ed., *Brooke's Notary*, 15th ed (2021), chapter 7, in particular para. 7-52 ff.

8. Many issues arise here which fall within the scope of domestic law, but we consider that private international law issues are also engaged. As the Commission is aware, s.72 of the 1882 Act addresses the conflictual issues relating to bills of exchange. In particular, s.72(3) provides that:

“The duties of the holder with respect to presentment for acceptance or payment and the necessity for or sufficiency of a protest or notice of dishonour, or otherwise, are determined by the law of the place where the act is done or the bill is dishonoured.”

Question 16

9. We have no relevant expertise to offer in relation to bills of lading, but we would suggest that similar questions, *mutatis mutandis*, ought to be asked and considered in relation to the issue of bills of exchange.

Question 17(5)

10. Notaries may be instructed to protest purported bills of exchange which do not satisfy the stringent formal requirements or time limits set by the 1882 Act. In such an event, or indeed if the notary is unsure, it is considered good practice for the notary to protest the bill urgently in any case; if the notary were to refuse, or delay, but the bill was later held to be valid – for example, under the law of another jurisdiction – the notary might be liable to their client for the damage caused.⁴ In this sense, the notary is not enjoined to enquire as to the formal validity of the purported bill. In any case, the notary’s involvement in the matter of a dishonoured bill will generally cease once the protest has been extended, and the notary would not be involved in any subsequent litigation on the bill. For these reasons, we do not have the necessary experience to comment on how often this question actually arises in practice in relation to paper bills.
11. We might speculate that the risk of the formal validity of electronic bills’ being challenged may be heightened in the early years of their existence, before they have fully bedded down into commercial practice and a useful corpus of case law has developed.

Question 17(6)

12. We would suggest that electronic bills of exchange pose significant issues in regard to conflict of law rules surrounding presentment, dishonour and protest.

Location of presentment

13. In relation to s.72(3) and (5) of the 1882 Act, you say that “as the place where ... an act relating to presentment is done, or where the bill is dishonoured do not seem to relate directly to the location of the bill of exchange itself, we are of the preliminary view that it will not make a difference whether the bill of exchange takes electronic or paper form”.⁵ We would demur from

⁴ See *Brooke’s Notary*, paras. 7-63 to 7-65.

⁵ Call for Evidence, para. 11.36

this view.

14. As set out above, in the traditional procedure, except in cases where the bill has been presented by post, presentment involves the physical presentation of the bill of exchange to the acceptor with a formal demand for payment. In the case of an electronic bill of exchange, it is not immediately obvious how this can be replicated. We have tentatively identified the following plausible routes for presentation of an electronic bill of exchange:
 - The electronic bill is converted to paper under s.4 of the 2023 Act; the entire procedure then proceeds in the traditional way.
 - A human-readable representation of the bill could be loaded on the screen of an electronic device, and then the device could be physically presented in the same way as a paper bill.
 - The “reliable system” contemplated by the 2023 Act could provide a mechanism for the notary to formally “e-present” the bill within the system. Such a mechanism would form part of the contract between the system provider and the users of the system. This would undoubtedly involve some electronic act initiated by the notary which brings the bill to the attention of the person who is liable to pay on it, incorporating a demand for payment.
15. In the first case, it is unlikely that any new difficulties arise. In the second case, we would suggest that it is doubtful whether this amounts to “presenting” the bill itself, or rather a copy of it (see para.6 above). This consideration apart, the question as to whether this constitutes a valid presentment or not would fall to be determined by the law of the place where the purported presentment is attempted. In the third case, if an “e-presentment” can be valid, knotty private international law questions would certainly arise in determining the location at which this “e-presentment” has taken place. We suggest that at least three *loci* are potential contenders: the place where the act of e-presentment is done (i.e. the location of the notary at the time of “e-presentment”), the place where the e-presentment is received, or the location of the “reliable system”. In our view, this question should be clarified by legislation. Sections 45(8) and 51(6) of the 1882 Act provide a useful example of legislative intervention to adapt to changing commercial realities.

Location of issue

16. Another possible issue we identify is how connecting factors in relation to “location” might interact with the requirement to determine whether a bill is a “foreign” or an “inland” bill. As explained above, in English law this difference affects whether notarial protest in case of dishonour is required in the first place, and therefore the true position is important to establish in order to preserve the holder's right to bring suit against antecedent parties to the bill.
17. By s.4 of the 1882 Act, a bill is “inland” if it “is or on the face of it purports to be (a) both drawn and payable within the British Islands, or (b) drawn within the British Islands upon some person resident therein. Any other bill is a foreign bill.” We suppose that, since the Act includes the words “on the face of it purports to be”, the drawer can simply state a location within the British

Islands on the face of the electronic bill in order to make it an “inland” bill, even if that is not the location of drawing according to whatever connecting factor may be settled on.

18. However, the Society is not familiar with how “reliable systems” that have been or are being developed work in practice, and therefore we are not able to comment on whether the functionality posited in the preceding paragraph is in fact being incorporated into such systems. In the absence of such a system, where the bill is deemed to be drawn will be the operative question.
19. We stress, therefore, that determining the *locus* where an electronic bill of exchange is drawn, and hence the need or otherwise for notarial protest, is essential in order to preserve the liability of the drawer and indorsers in the event of dishonour.

Conclusion

20. We hope that our comments are of use to your work, and we look forward to hearing from you if you require any further clarification or assistance with the points that we have raised.

STEP Consultation Response: The Law Commission of England and Wales' Consultation on Digital Assets in the Context of Private International Law

About Us

STEP is the worldwide professional association for those advising families across generations. We help people understand the issues families face in this area and promote best practice, professional integrity and education to our members.

Today we have over 22,000 members in over 100 countries and over 8,000 members in the UK. Our membership is drawn from a range of professions, including lawyers, accountants and other specialists. Our members help families plan for their futures: from drafting a will or advising family businesses, to helping international families and protecting vulnerable family members.

We take a leading role in explaining our members' views and expertise to governments, tax authorities, regulators and the public. We work with governments and regulatory authorities to examine the likely impact of any proposed changes, providing technical advice and support and responding to consultations.

Purpose of this paper

STEP responds to the Law Commission of England and Wales' (the Law Commission's) Call for Evidence on digital assets and electronic trading documents (ETDs) in the context of private international law. This consultation examines the issue of which courts have jurisdiction and what law is applicable in the context of a dispute concerning digital assets in a cross-border context.¹

Our members advise primarily in relation to non-contentious tax and estate planning issues. They are not all litigators. We do not therefore address most of the issue raised in the call for evidence.

However, there is one important issue we wish to address. The location of digital assets is relevant not only in relation to issues concerning jurisdiction or applicable law for disputes about digital assets but also for other purposes; for example, tax, determining the formalities required for dealing with such assets after a person has died and, in some jurisdictions (but not in England and Wales), determining the law that governs who is entitled to inherit an asset on the death of the owner.

¹ Law Commission, Digital assets and ETDs in private international law: which court, which law?: <https://lawcom.gov.uk/project/digital-assets-and-etds-in-private-international-law-which-court-which-law/>

Therefore, even if there is an alternative approach to determining jurisdiction/applicable law in relation to disputes, this does not necessarily eliminate the need to have rules that determine where a digital asset is located. It might be said that it follows that, if there is a need to assign a location to a digital asset for some purposes, it would be appropriate to use that location for private international law purposes. For example, it could be used in determining whether the courts of a particular country have jurisdiction over a dispute and the applicable law that should be applied in determining the dispute.

Location for tax purposes could, of course, be determined by inserting a specific provision in any relevant tax legislation. There are specific statutory rules in the capital gains tax legislation dealing with the location of some types of asset (but not digital assets). However, there are no statutory provisions for inheritance tax (IHT) purposes, which relies on the common law in determining if an asset is situated in the UK.

However, a piecemeal statutory approach limited to specific tax purposes will not help in resolving other questions, such as determining whether a person is entitled to deal with an asset of a deceased person.

Providing clarity of location of digital assets based on immediate control of the asset would be an effective approach to take, as it would allow courts to know which rules they need to apply in regards to disputes, as well as in issues of tax and inheritance of assets.

The current lack of clarity in the law causes serious problems for individuals. This can be illustrated with a simple example. Alice is domiciled in Canada but resident in the UK (and has not acquired a deemed UK domicile for tax purposes). She has a Canadian will leaving her assets outside the UK to her son Bob and an English will leaving her assets in the UK to her daughter Carol. She owns a sum of Bitcoin, which is held on her behalf in a trust account operated by a cryptocurrency exchange located in the US.

When Alice dies, three legal problems will arise:

- There is a dispute between Bob and Carol over who inherits the Bitcoin, which depends on whether it is located in the UK. Bob argues that since Alice was the beneficial owner of the Bitcoin and resident in the UK, the Bitcoin was located in the UK. Carol argues that there is no legal basis for this argument, and that since the exchange holding the Bitcoin for Alice was located in the US the Bitcoin was not located in the UK.
- It is unclear whether the Bitcoin will be subject to UK IHT. As Alice was not domiciled in the UK, her estate is subject to UK IHT only to the extent that it is located in the UK. HMRC argues that as Alice was the beneficial owner of the Bitcoin and resident in the UK, the Bitcoin was located in the UK and so subject to UK IHT. Alice's executors argue that since the exchange holding the Bitcoin for Alice was located in the US, the Bitcoin was not located in the UK and UK IHT does not apply.

- The US exchange will not know whether it is the UK executors or the Canadian executors who have the right to take control of the Bitcoin.

The issues in this example are likely to arise all the more regularly as more individuals die holding crypto-tokens. At some point the question of crypto-token location will inevitably have to be considered by the courts. We believe that it would be beneficial for legislation to clarify the position before then to the extent that this is possible, so that individuals have greater certainty.

Even if it is not settled by legislation, we believe that any decision by the court setting a common-law precedent would benefit considerably from the detailed analysis that could be provided by the Law Commission, rather than relying on the specific parties to a dispute to present all arguments.

We therefore consider it appropriate (and hopefully helpful in the context of the call for evidence) to make some comments as to the rules which could be applied by an English court in determining where digital assets are located.

Determining the location of digital assets

The nature of digital assets means that the principles that courts may apply in relation to the location of other assets are less relevant. In the case of a chose in possession, it is straightforward to identify the physical location of the object. In the case of a chose in action, this would generally be based on where it can be enforced (for example, where the debtor resides, in the case of an ordinary debt), although there are particular exceptions (for example, the location of the instrument in the case of a specialty debt).

Digital assets are commonly a decentralised asset and are therefore tracked by a computerised database maintained by a network of computers that may be located all around the world. There is no physical location, as in the case of a chose in possession, nor is there a legal claim to be enforced, as in the case of a chose in action. A token is represented by a public key that is linked to a private key. This can make it difficult for courts to apply principles that they would normally apply to determine location, which raises questions of how courts determine location of digital assets.

However, more recently there has been a move towards centralised digital assets, as seen in the Bank of England's proposal for a central bank digital currency (CBDC). With these assets being centrally administrated, this would make it easier to determine the location of the assets with a clear link to a jurisdiction. For example, provided the computer recording ownership of the Bank of England's proposed CBDC was located in England then all units of this CBDC would be located in England.

In the absence of a central administrator, it is STEP's view that the location of a digital asset can be determined by the residence of the person who has immediate control over them, as explained in our guidance note on location of crypto-assets.²

The person with immediate control will be the person (whether an individual or a corporation) who has knowledge of the private keys necessary to initiate a transaction using the crypto-token. This may be the beneficial owner, where the beneficial owner holds their own private keys. However, there are situations where a beneficial owner may not directly participate in the system, such as where the keys are held by a custodian (such as an exchange). In this situation, the residence of the custodian will determine the location of the asset.

Determining the location of digital assets

The question of the location of cryptocurrency has been considered by the English courts in *Ion Science Limited v Persons Unknown* (2020, unreported).³ The court apparently considered that it was arguable that the location of the cryptocurrency was the place where the participant in the cryptocurrency system is domiciled. This conclusion is said to be based on the arguments put forward by Professor Andrew Dickinson in chapter 5 of the book *Cryptocurrencies in Public and Private Law*.⁴

In fact, in that chapter, Professor Dickinson is dealing with the question as to which law governs the proprietary aspects of any rights relating to cryptocurrency. The reason this is connected with the location of cryptocurrency is that, normally, the law that governs property rights in relation to an asset is the law of the jurisdiction in which the asset is located. In the absence of any location for cryptocurrency, Professor Dickinson suggests in paragraph 109 in chapter 5, that the law of the place of residence of the participant is the appropriate law to govern any proprietary questions relating to the cryptocurrency.

The important point to note from this analysis is that the governing law is based not on the residence of the beneficial owner but on the residence of the participant in the relevant cryptocurrency system. The reason for this is that Professor Dickinson's conclusion that the value of cryptocurrency derives from a claim or legitimate expectation to be associated with and have the power to engage in transactions in relation to particular units of cryptocurrency within the system. In practice, this means controlling the public address to which the cryptocurrency has been allocated and holding the private key which is needed to authorise transactions in relation to that cryptocurrency.

Although Professor Dickinson's focus is on determining the law governing proprietary aspects relating to cryptocurrency. It might be expected that a UK court would consider

² STEP guidance note, *Location of Cryptocurrencies – an alternative view*:
https://www.step.org/system/files/media/files/2021-09/step_note_location_of_cryptocurrencies-an_alternative_view_0.pdf

³ This is recorded by the solicitors who acted for the claimant in that case – *Ion Science Ltd v Persons Unknown Explained. Cryptocurrency Fraud & Asset Recovery* (rahmanravelli.co.uk)

⁴ Edited by David Fox and Sarah Green, Oxford University Press (2019)

similar principles in relation to the location of cryptocurrency. Indeed, that is what the court in *Ion Science* appears to have done.⁵

In our view, the approach taken by Professor Dickinson and adopted by the court in *Ion Science* seems a sensible approach for the courts to take in relation to the question of location as it builds on existing principles (control, ability to deal and, by extension, enforceability) rather than introducing a completely new principle based on beneficial ownership which has no precedent in determining the artificial location of an intangible asset.

It is worth noting that the UK jurisdiction taskforce agrees that the law governing any proprietary aspects in relation to cryptocurrency is not to be determined by looking at the location of the cryptocurrency (as it has none) but by reference to other factors. The only factor they identify which is relevant to cryptocurrency (at paragraph 99(c)) is ‘whether a particular cryptoasset is controlled by a particular participant in England and Wales (because, for example, a private key is stored here)’.

Although expressed in slightly different terms, this leads to the same conclusion as that reached by Professor Dickinson, which is that the applicable law is linked not to the beneficial owner but to the participant in the relevant cryptocurrency system who will be the person who has control over the private key.

Of course, the beneficial owner may also be a direct participant in the cryptocurrency system and, in that capacity, may hold the private key. In those circumstances, the cryptocurrency will be located where the beneficial owner is resident.

However, 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.

In these circumstances, 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.

In this context, where the beneficial owner has an account with the cryptocurrency exchange, the nature of the relationship with the exchange must be carefully analysed. In some cases, the wallet that represents the public address and the associated private key will be held by the beneficial owner and the exchange merely facilitates transactions. However, in other cases, the wallet and the private key will be held by the exchange itself on a pooled basis for all of its clients with the rights of the beneficial owner being limited to the holding of

⁵ The decision in *Ion Science* has been followed in *Fetch.ai Limited v Persons Unknown* [2021] EWHC 2254 (Comm)

an account with the exchange in which the holding of units of cryptocurrency are recorded in the form of book entries made by the exchange itself. This was, for example, the position in relation to the Cryptopia Exchange, which was the subject of the New Zealand case of *Ruscoe v Cryptopia* [2020] NZHC 728.

One objection to this conclusion in the tax context might be that, in the case of other types of intangible property, the location of a custodian does not affect the location of the underlying asset. For example, if shares in an English company are held by a custodian in Switzerland, the beneficial owner would still be treated for UK tax purposes as holding a UK asset, being his beneficial interest in the shares in the English company. However, the position is different as the shares in the English company have an independent location based on the place where the company share register is kept (which has nothing to do with the status of the custodian or the beneficial owner). In the case of cryptocurrency, if the suggested analysis is right, this has no independent location separate from the residence of the actual participant in the relevant cryptocurrency system.

We can see that the position might be different if cryptocurrency is held by a dedicated nominee for the beneficial owner – i.e. the cryptocurrency is not pooled as part of a commercial arrangement. Where there is a dedicated nominee, it would be open to the beneficial owner to require the nominee to give them control of the private key (which would relate only to the cryptocurrency held for the benefit of the beneficial owner). This might be said to give the beneficial owner sufficient control over the cryptocurrency to be treated as if it were directly held by them. This is not however the case where cryptocurrency is held on a pooled basis for multiple participants as none of the participants would be in a position to require the operator of the arrangement to disclose the private key to them.

One important point to note is that, whether the location of the cryptocurrency is based on the residence of the beneficial owner or on the residence of the participant in the cryptocurrency system, residence must surely be tested by reference to relevant common-law principles and not by reference to the tax definition contained in the statutory residence test (Finance Act 2013, Schedule 45). The reason for this is that, as explained above, the location of an asset is a general common law concept and is relevant for purposes which go beyond taxation. If the statutory residence test is to be used in order to determine residence for this purpose, this would need to be provided for by statute.

Where a person is resident in more than one jurisdiction, Professor Dickinson suggests that the governing law should be based on the jurisdiction with which the relevant participant has the closest connection. We would suggest that this is also the most sensible approach to apply to determining the location of cryptocurrency.

One particularly difficult issue that arises is what the position is where cryptocurrency is jointly owned. In the tax context, this is provided for in relation to capital gains tax in section 275C TCGA 1992. This provides that the location of an asset should be determined on the basis that the taxpayer in question is the sole owner. The effect of this is that, if a UK

resident jointly owns cryptocurrency with a non-UK resident and those individuals are direct participants in the cryptocurrency system (both having access to the wallet containing the public address with which the cryptocurrency is associated and to the private key) the share of the cryptocurrency owned by the UK resident will be located in the UK and the share owned by the non-UK resident will be located outside the UK.

Where there is no statutory provision (for example in relation to IHT or succession/probate issues), we would again endorse Professor Dickinson's suggestion that the location of the cryptocurrency should be determined by identifying the place of residence with which the participation in the cryptocurrency system is most closely connected.

**Submitted by STEP UK Technical Committee and Digital Assets Special Interest
Group, 16 May 2024**

An Opinion About Applicable Law and Jurisdiction of the Courts for Bills of Lading (B/L), Issued in Blockchain, in English Private International Law

Göker Tataroğlu*

When the trade documents have started to become electronic, some legal disputes have arisen. Such determination is important in international commerce because some legal issues are hard to determine when there is a dispute arisen from the electronic trade documents (ETDs). Especially, when it comes to the applicable law and jurisdiction of the courts, the significant importance meets the eyes. However, it would be appropriate to start by giving general information about how the English Private International Law rules will be applied.

Generally, when looked at in English Law, in order for English courts to apply the law of a foreign state other than English law in such a dispute that¹;

1. English Law must in principle allows the application of foreign law,
2. There should be no precludes regarding the application of foreign law,
3. The party who relies on the necessity of foreign law to find application area must plead this claim (or application) and,
4. The party claiming to rely on foreign law must prove its claim of relying on foreign law to the satisfaction of the court with an expert testimony.

However, this rule is effective only if the foreign law is the applicable law of the dispute (*lex causae*).²

This rule generally covers contracts and trade documents (TDs) drawn up on paper. On the other hand, the main issue starts with the electronic documents as we mentioned above. The importance of determining which law is going to apply and which courts or arbitral tribunals have their jurisdiction is getting much harder in ETDs. The reasons of this could be sortable like this;

1. If the both parties have different nationalities, but such one of the party use “VPN” to manipulate its IP Address and makes the dispute seems not international,
2. Parties agree to issue the blockchain document such as blockchain bill of lading (B/L)³ regarding to their contractual relationship, and due to pseudonymity of the blockchain structure, the company names of the parties could not be able to determined,
3. Also, when there is a blockchain trade document issued by both parties, blockchain technology can be accessed from anywhere due to its decentralized and distributed structure.

¹ Burrows A, ‘Private International Law’ [2013] English Private Law 1183., p. 1884.

² Ibid., p. 1187.

³ For explanation, see above., p.2

As, Electronic Trade Documents Act (ETDA), some documents considered to be trade documents (TDs) in English Law. According to Art.1 (2) of ETDA;

- a bill of exchange;
- a promissory note;
- a bill of lading;
- a ship's delivery order;
- a warehouse receipt;
- a mate's receipt;
- a marine insurance policy;
- a cargo insurance certificate etc.

regarded as TDs. ETDs can be issued and has the same effect of the paper TDs according to Art.4 of ETDA as well.

Blockchain Bills of Lading (B/L) is an electronic B/L issued with using Blockchain Document Transfer (BTD) platforms⁴. In our perspective, Blockchain B/Ls are also regarded as an ETD via ETDA, Factors Act and Public Records Act in English Law. Due to this, Blockchain B/Ls has same effects of paper TDs according to Art. 4 of ETDA.⁵

With the spread of electronic B/Ls and moreover blockchain B/Ls, the legal problems mentioned above have started to increase and various debates have begun to arise about the law to be applied. Since this proposal will only put forward our views on *lex causae*, the question “*Digital assets and ETDs in private international law: which court, which law?*” will be answered through the VPN problem.

One Such Party Is Using “VPN” to Manipulate Its IP Address

Using a VPN plays a critical role, especially when the law applicable to the B/L is not determined between the parties. Because VPN allows people to browse the internet by keeping their IP secret.⁶ For instance, a person in France can use a VPN to browse the internet as if they were in the USA. That is, it completely hides the IP address of the person using the Internet, making it difficult to find his location. Well, using this system in international trade can also lead to danger. Because, in the case of a dispute specific to private international law, the judge who will resolve the dispute may make a mistake due to the VPN used by one of the parties. Moreover, the law that should be applied may not be applicable to that dispute.

However, before examining possible solutions, it would be appropriate to talk about the Rome I Regulation, of which the UK is a member, in terms of documents using BTD.

⁴ A structure that enables the transfer of a commercial document issued using blockchain from the issuer to the other party. For more information, see. WCO_ OMD, ‘Blockchain Document Transfer: Understanding the Technology and Its Uses’ (*WCO News*) <<https://mag.wcoomd.org/magazine/wco-news-97-issue-1-2022/blockchain-document-transfer/>> accessed 28 April 2024

⁵ For more, see. Tataroğlu G and Çağlayan Aksoy P, *Karşılaştırmalı Hukukta Tokenize Edilmiş Konişmentolar* (1st edn, On İki Levha Yayıncılık 2023)., p. 56 & p. 73 – 75.

⁶ ‘What Is a VPN? Virtual Private Network Meaning’ (*NordVPN*, 16 April 2024) <<https://nordvpn.com/what-is-a-vpn/>> accessed 28 April 2024

It is normal for the parties not to choose the law to be applied, because in this case it is an indication of the parties' freedom of will (or party autonomy). In this case, Rome I Art.5 or generally, Art.4 will apply.

It is already seen that crypto assets are described as goods both by the UK Law Commission⁷ and in several court decisions⁸. In light of this framework, it seems that Rome I Art.4 can generally be applied to blockchain B/Ls if the parties have not chosen the applicable law. However, it can be said that Art.5 can be applied to blockchain B/Ls, as it is stated in Article 4 “*without prejudice to Articles 5 to 8*” and B/Ls can also be evaluated as contract of carriage⁹ when necessary.

In my opinion, the following solutions are needed to determine the applicable law regarding blockchain B/Ls within the framework of English Private Law rules:

- If the use of VPN is detected while issuing a blockchain B/L issue with the integration of blockchain based document tracking system (BBDTS) and VPN Tracker System, and if the dispute has started to be resolved by the English Courts, **the Court must apply English Law**. In my opinion, this may be the case if applicable law has been chosen by the parties and one of the parties brings the dispute before the English Courts. In my opinion, this situation I mentioned should be applicable even if no law is chosen by the parties.
- If the parties have not chosen any law, in my opinion, a code should be added to any Digital Standard created for the B/Ls that the parties will separately arrange between them, as an evidence that there is an element of foreignness. This code must include the place where the B/L was issued and the place where it will be delivered. At the same time, it is necessary to add a code that allows it to be tracked when issued by a reliable VPN Tracker, which I mentioned above. Thus, even if one of the parties uses a VPN, the real IP address can be determined and the applicable law can be determined according to Rome I Art.5 (or Art.4 in general) due to the element of foreignness.
- Due to both the hiding of the IP address with VPN and the pseudonymity feature of the blockchain, it will be very difficult to determine who the other party is and therefore whether there is an element of foreignness. For this reason, in my opinion, it may be mandatory to use vLEI¹⁰ systems when issuing B/Ls (or blockchain documents in general), especially in order to eliminate pseudonymity to some extent. If this obligation is not complied with by the parties, English Law must again be applied regarding disputes arising from such B/Ls.

⁷ ‘Digital Assets as Personal Property Short Consultation on Draft Clauses’ (*Digital assets as personal property – draft clauses*, 2024) <<https://cloud-platform-e218f50a4812967ba1215eaecede923f.s3.amazonaws.com/uploads/sites/30/2024/02/Feb-2024-digital-assets-and-personal-property-CP.pdf>> accessed 28 April 2024., p.3 – 8 & p. 29.

⁸ ‘Osbourne v Persons Unknown & Anor [2022] EWHC 1021 (Comm) (10 March 2022)’ (*England and Wales High Court (Commercial Court) decisions*, 2022) <<https://www.bailii.org/ew/cases/EWHC/Comm/2022/1021.html>> accessed 28 April 2024. In this case, NFT’s, which are also crypto-assets, are regarded as a property.

⁹ Dubovec M, ‘The Problems and Possibilities for Using Electronic Bills of Lading as Collateral’ (2006) 23 Arizona Journal of International and Comparative Law 437., p. 448.

¹⁰ vLEI is a cryptographically evolved and more advanced form of the traditional LEI. For more information, see. ‘Vlei - Verifiable Legal Entity Identifier’ (vLEI Verifiable Legal Entity Identifier, 22 February 2024) <<https://vlei.com/>> accessed 28 April 2024

- Finally, comprehensive provisions regarding the solution methods I mentioned above can be introduced into the Civil Procedure Act and/or ETDA (which, in my opinion, should be introduced).

References

Burrows A, ‘Private International Law’ [2013] English Private Law 1183.

‘Digital Assets as Personal Property Short Consultation on Draft Clauses’ (*Digital assets as personal property – draft clauses*, 2024) <<https://cloud-platform-e218f50a4812967ba1215eaecede923f.s3.amazonaws.com/uploads/sites/30/2024/02/Feb-2024-digital-assets-and-personal-property-CP.pdf>> accessed 28 April 2024.

Dubovec M, ‘The Problems and Possibilities for Using Electronic Bills of Lading as Collateral’ (2006) 23 Arizona Journal of International and Comparative Law 437

‘Osbourne v Persons Unknown & Anor [2022] EWHC 1021 (Comm) (10 March 2022)’ (*England and Wales High Court (Commercial Court) decisions*, 2022) <<https://www.bailii.org/ew/cases/EWHC/Comm/2022/1021.html>> accessed 28 April 2024

Tataroğlu G and Çağlayan Aksoy P, Karşılaştırmalı Hukukta Tokenize Edilmiş Konişmentolar (1st edn, On İki Levha Yayıncılık 2023).

‘Vlei - Verifiable Legal Entity Identifier’ (*vLEI Verifiable Legal Entity Identifier*, 22 February 2024) <<https://vlei.com/>> accessed 28 April 2024

WCO_ OMD, ‘Blockchain Document Transfer: Understanding the Technology and Its Uses’ (*WCO News*) <<https://mag.wcoomd.org/magazine/wco-news-97-issue-1-2022/blockchain-document-transfer/>> accessed 28 April 2024

‘What Is a VPN? Virtual Private Network Meaning’ (*NordVPN*, 16 April 2024) <<https://nordvpn.com/what-is-a-vpn/>> accessed 28 April 2024

Submitted to Law Commission Call for Evidence on digital assets and ETDs in private international law
Submitted on 2024-05-10 09:48:21

About you

What is your name?

Name:
Jasper Verstappen

What is your email address?

Email:
[REDACTED]

What is your telephone number?

Telephone number:

Questions on international jurisdiction - specific issues (Chapter 5)

Question 1: In this question, we seek views and evidence on jurisdiction over consumer contracts.

Please share your views and evidence below::

Question 2: In this question, we seek views and evidence on jurisdiction founded on the basis that a contract was concluded in England and Wales.

Please share your views and evidence below::

I believe that, generally speaking, the European private international law rules (including those in England and Wales) are well-prepared to deal with issues that might arise in the context of smart contracts. Blockchain-technology that underpins smart contract platforms might be used to hide information that is relevant to the contracting parties. This might create an information asymmetry amongst the parties. Private international laws apply connecting factors that rely on information that is shared automatically by the parties in the execution of the agreement. Hence, the mere execution of the legal agreement breaks this information asymmetry.

This means that, as far as gateway 6(a) is concerned, a connecting factor based on a geographical location or real-world actor can be used, provided that the execution of the particular type of agreement requires the parties to share the information that enables them to determine the applicable law on the basis of that connecting factor. The habitual residence seems most obvious.

Considering that the technology in question can be implemented with great variety and for many different purposes, there is no guarantee of a certain degree of transparency (meaning that, whilst it is likely that the execution of an agreement forces parties to share the information relevant to the connecting factor, there is no guarantee). In light of that, a waterfall-model in which a connecting factor based on a geographical location or real-world actor is supplemented with a more generalised connecting factor provides a more comprehensive solution.

Question 3: In this question, we seek views and evidence on jurisdiction founded on the basis that damage or detriment was suffered in England and Wales.

Please share your views and evidence below::

Question 4: In this question, we seek views and evidence on jurisdiction founded on the basis that an unlawful act was committed in England and Wales.

Please share your views and jurisdiction::

Question 5: In this question, we seek views and evidence on jurisdiction founded on the basis that the claim relates to objects within England and Wales.

Please share your views and evidence below::

Question 6: In this question, we seek views and evidence on the types of claims and causes of action relied upon in applications to serve proceedings relating to crypto-tokens out of the jurisdiction.

Please share your views and evidence below::

Questions on applicable law - non-consumer contracts (Chapter 7)

Question 7: In this question, we seek views on applicable law and decentralised finance (DeFi).

Please share your views and evidence below::

Question 8: This question concerns the applicable law for non-consumer contracts.

Please share your views and evidence below::

Yes; I believe that the provisions of the Rome I Regulation can be applied to contracts involving crypto-tokens without undue difficulty. There might be some edge-cases in which the information necessary to determine the applicable law is not available to the parties (e.g. this might occur in quite radical implementations of the technology in which pseudonymity is implemented in a rather absolute manner). However, this is indicative of a more severe underlying problem: the cause of which is technological and the symptoms felt, although not exclusively, in the area of applicable law.

The situations in which the provisions cannot be applied, or cannot be applied without undue difficulty, will (in my opinion) turn out to be exceptionally rare. Firstly because most smart legal agreements will force parties to share the information necessary to determine the applicable law during the executing of the agreement. Secondly because the amount of smart contracts that exist only on a blockchain-platform (and are not accompanied by an off-chain legal agreement) that has implemented its pseudonymity in such a manner that the information necessary to determine the applicable law is masked for parties and judges will be extremely rare.

However, for those (extremely rare) edge-cases, I believe, prevention rather than intervention is key: discouraging the creation of such platforms, discourage parties from contracting on such platform, especially parties such as consumers, and implement measures to render the implementation of very pseudonymous platforms more difficult. Any attempts to regulate such platforms should not be limited to the area of private international law, as this issue is broader than PIL alone: the symptoms are pronounced within this area of the law, but not limited to it exclusively.

Questions on applicable law - non-consumer contracts (Chapter 8)

Question 9: This question concerns the applicable law for consumer contracts.

Please share your views and evidence below::

Question 10: This question concerns the exclusions in Articles 6(4)(d) and (e) of the Rome I Regulation.

Please share your views and evidence below::

Question on applicable law - property (Chapter 12)

Question 19: We seek views on the law applicable to property disputes in relation to digital assets and ETDs. Where possible, we ask that stakeholders contextualise their responses, for example, give details as to whether it relates to a pledge over an ETD or property entitlements in crypto-token litigation.

Please share your views and evidence below::

Digital assets and ETDs in private international law: which court, which law?
Call for evidence.

Date of submission: 16 May 2024

Sent via email to: conflictoflaws@lawcommission.gov.uk

From: W Legal Limited

W Legal Background

W Legal ('the Firm') is a unique law firm mostly based in London, but also has a presence in USA, Paris, Israel, and Poland, specialising in Blockchain, Digital Assets, Regulation, Compliance, AML, Corporate Law, Commercial Litigation, Financial Crime, GDPR and Data Handling.

Exceptionally, three of our Firm's members are senior retired Judges; a former Master in the High Court of Justice in London; a former Judge of the First Tier Tribunal, and a former Circuit Judge. Another member of our Firm is a Professor of Law and currently a Fellow of Keble College, Oxford.

Our diverse group of lawyers have experience in tracing and recovering lost/stolen digital assets, Initial Coin Offerings, Non-Fungible Tokens ("NFTs") and the 'Metaverse', fraud, and cyber-security. We have been involved in drafting of legislation and working closely with central governments and Parliamentary authorities. The Firm has represented Members of UK Parliament.

The Firm dealt with Worldwide Freezing Injunctions on the Blockchain and was involved in the first ever Worldwide Freezing Order granted on the blockchain by the High Court in Singapore, permitting service of a Freezing Injunction by an NFT including Cold Wallets. The Firm has dealt with establishing standards in smart contract programming and represents blockchain business, programmers and entrepreneurs.

W Legal is interested and willing to be involved in more in-depth discussions planned for any private international law projects in the future.

Executive Summary

We have critiqued a number of the "theories" around Evidential Gateways, Universal and Multi-lateral approaches as well as reviewing the application of the Rome Conventions I and II, but a theme of our recommendations is that simplified clarity in this complex new area of digital assets would be promoted by broadly clarifying legislation (akin to that for digital asset property rights); by developing specialised commercial courts/arbitration fora; and specialist judges/arbitrators to deal with the detailed technology elements in conjunction with law and regulations that underlie the new assets.

There will be a need for judicial decisions and commentary through common law/equity case law around the novel technical features of "gas fees", "staking" and "minting" issues,

complexities around the development of layers of coding that sit on the underlying Ethereum and other digital networks. Legal solutions need to develop in tandem with clearer regulatory treatment, particularly in financial areas under the FCA's jurisdiction and under the jurisdiction of regulators such as ICO and Ofcom.

W Legal's Responses:

Question 1: In this question, we seek views and evidence on jurisdiction over consumer contracts.

Whist overall, we consider that digital consumer contracts can be fully accommodated in section 15B, we have provided more nuanced answers to the specific points below. Section 15B is drafted sufficiently clearly to indicate that the critical factor is the domicile of the buyer. There should be no difference for crypto business in terms of directing the sale of goods/services to different jurisdictions, as compared with any other regular goods/services. The key issue will be to identify the seller and its jurisdiction, although we envisage considerable potential difficulties in doing so as highlighted below.

➤ **To what extent can the issue of jurisdiction over consumer contracts in the digital and decentralised contexts be accommodated by section 15B of the Civil Jurisdiction and Judgments Act (CJJA) 1982?**

Section 15B of CJJA 1982 provides a framework for determining jurisdiction in consumer contract disputes. Consumers are protected in the course of allowing them to bring a claim in their domestic courts which prevents them from being bound by jurisdiction clauses that would force them to litigate internationally.

In digital and decentralised contexts, such as transactions made over the internet or on blockchain platforms, the issue of jurisdiction becomes complex. Traditional notions of jurisdiction rely on geographical markets and the physical presence of businesses, which do not easily apply in these contexts.

The application of Section 15B in these scenarios requires an adaptation of its principles to the realities of digital commerce. This might involve considering the digital presence of a business, such as the use of language, currency, marketing targeted at consumers in a specific jurisdiction, or the use of technology that enforces legal agreements and transactions in a decentralised manner.

➤ **Does the fact that the business is a crypto-business, as opposed to any other business, change the analysis of whether a business has directed its services to consumers located in the UK?**

The core question is whether a crypto-business, by virtue of its nature, alters the analysis of the jurisdiction based on "directed activities". The principle underpinning jurisdiction in consumer contracts often, but not always, involves determining if the business has "directed its activities" to the country in question.

For crypto-businesses, this analysis might include factors such as whether the blockchain platform targets UK consumers specifically (through marketing, language, availability of services etc), and whether it accepts payments in GBP or offers services that comply with UK regulations.

The decentralised and borderless nature of many crypto-businesses adds complexity. Although the fundamental analysis does not change, it requires consideration of the specific ways in which crypto-businesses interact with and target consumers in different jurisdictions.

➤ **Are there any changes or clarifications that are needed in respect of the issue of jurisdiction over consumer contracts?**

Legal frameworks often lag behind technological advancements. As such, there may be a need for changes or clarifications (by statute or judicial decisions) to existing laws, including Section 15B, to accommodate the nuances of digital and decentralised commerce.

Potential areas for clarification might include broadening or clarifying the definition of "directed activities" in a digital context, the treatment of decentralised autonomous organisations (DAOs), and the applicability of consumer protections in the context of smart contracts and crypto-transactions.

➤ **To what extent does this issue cause problems in practice (or is likely to in future)?**

Disputes involving digital and decentralised transactions can present significant challenges in determining jurisdiction. Consumers may find it difficult to enforce their rights, and businesses may face legal uncertainty regarding their obligations across different jurisdictions.

As digital commerce and crypto-businesses continue to evolve, these jurisdictional issues are likely to become more prevalent. The international legal community may need to develop new frameworks or agreements to address these challenges effectively.

Question 2: In this question, we seek views and evidence on jurisdiction founded on the basis that a contract was concluded in England and Wales.

➤ **How should the courts apply gateway 6(a) to a smart contract? Should the relevant connecting factor be the participating computer, or the real-world actor?**

It would seem to be preferable to use the real-world actor domicile/situs rather than a computer location – particularly as laptops/computers and other PDAs can travel independently of the real actor's domicile/normal location.

If the relevant "connecting factor" was to be the participating computer, this would suggest that jurisdiction could be established based on the physical location of the computer (or node) that executes the smart contract. This approach might align with traditional notions of jurisdiction being tied to a tangible, geographical location, but the reality of multiple nodes

and the portability of computers, particularly laptops and PDAs, would make this approach rather impractical.

Given the decentralised nature of blockchain networks, where a contract's execution might involve multiple computers across the globe, pinpointing a single jurisdiction could be problematic. This method might lead to jurisdictional uncertainty and potentially hinder the efficacy and appeal of using smart contracts for international transactions.

Alternatively, focusing on the real-world actor as the connecting factor—meaning the parties who created, offered, or accepted the contract—anchors the jurisdiction to traditional legal principles that emphasise the parties' intentions, actions, and expectations.

This approach would consider where the offer was made or accepted by the parties involved, regardless of where the contract was digitally executed. It maintains consistency with the principle that contractual rights and obligations ultimately reside with the parties themselves, not the technology used to facilitate the contract.

- **If gateway 6(a) should use a connecting factor based on the real-world actor, how should their location be determined? Should it be by their habitual residence, their domicile, or at the place where they happen to be at the time the contract was formed?**

All three factors are usable with the primary jurisdiction being the habitual residence, then the place where the real actor was located at the time of the contract being formed and, lastly and far less relevant, the real actor domicile.

The application of gateway 6(a) should ideally be consistent with the fundamental principles of contract law, which focus on the intentions and interactions of the parties involved in the contract. Considering the real-world actors aligns with these principles, it emphasises the importance of human agency and intent in establishing contractual relationships.

From a practical standpoint, focusing on real-world actors may provide greater predictability and clarity for parties engaging in transactions involving smart contracts. It helps to establish jurisdiction based on clear and understandable criteria related to party behaviour and choices, rather than the technically complex and fluid operations of decentralised networks.

The legal system's approach to emerging technologies like smart contracts requires adaptability and an understanding of the technology's unique characteristics. While traditional legal concepts remain relevant, their application may need to be re-interpreted or evolved to effectively address the novel contexts created by these technologies.

- **Has the question of where a smart contract is made arisen in legal and commercial practice? If so, please provide details.**

As a firm, we have not had to address this issue to date—save for in the context of discussions concerning the development of property real estate smart contracts which we have been involved in.

➤ **To what extent is it likely that the question of where a smart contract is made will become prevalent in practice?**

We consider that it is highly likely in terms of potential litigation issues surrounding the law/jurisdiction governing smart contracts will need to be addressed.

Blockchain's decentralised nature means that transactions can involve parties from multiple jurisdictions, simultaneously. Unlike traditional contracts, where the parties' locations might be clear and stationary, the execution of smart contracts involves nodes spread across the globe. Smart contracts often facilitate cross-border transactions, making it challenging to determine where the contract is made. This global aspect can lead to jurisdictional complexities and conflicts of law. The legal frameworks governing smart contracts and blockchain technology are still developing issues. It is our view that there is a growing need for legal clarity on issues such as the applicability of existing laws to smart contracts, the recognition of digital signatures, and the enforcement of smart contract terms.

As more disputes arise from smart contract transactions, courts and legal systems worldwide will increasingly need to address the question of jurisdiction. The outcome of these early cases will likely set precedents that shape the future legal landscape for smart contracts. The adoption of smart contracts in growing number of commercial areas is expected to grow, driven by their efficiency, automation capabilities, and lower transaction costs. As their use expands, so too will the instances where jurisdiction needs to be determined. Technological advances may also influence how jurisdiction is determined. For example, developments in digital identity verification or geolocation tagging within blockchain networks could offer new ways to establish where a contract is made.

Governments and regulatory bodies are beginning to draft and enact legislation specifically addressing digital assets, smart contracts, and blockchain technology. These laws may include provisions that directly or indirectly address jurisdictional questions. We recently attended a conference (based in Vienna) of the IACPIL, Vienna University and EBI, which comprehensively and excellently addressed many of the issues at an international cross border level that the Law Commission is seeking answers on and we would encourage access to and reading of the papers delivered. The cross-border nature of blockchain may encourage greater international cooperation and the development of treaties or agreements that provide a more standardised approach to jurisdiction over smart contracts.

In practice, we have come across issues relating to 'gasless minting', intellectual property, and author rights arising as a result of smart contracts and issues around to whom do IP rights belong to and in relation to these are the operations of the companies that are raising funding.

Question 3: In this question, we seek views and evidence on jurisdiction founded on the basis that damage or detriment was suffered in England and Wales.

➤ **Do you consider the approach of the courts of England and Wales so far in the crypto litigation when localising damage or detriment for the purposes of jurisdiction to be theoretically sound?**

Yes. However, as crypto-related litigation becomes more prevalent, the courts may need to refine their approach to address the unique challenges posed by cryptocurrency transactions and their global nature when localising damage or detriment.

Whilst we see considerable theoretical soundness in many cases, there is an element of inconsistency or at least a range of divergent connecting factors being employed. We would suggest that a range of “localising” factors could be developed and placed in an order of cascading/descending importance.

- **To what extent can it be said that the tortious damage pleaded in the crypto-token litigation are not cases of pure economic loss? How else could tortious damage in the crypto-token context be conceptualised?**

To the extent of defamation, brand and reputation damage, employability, and the ability to function and fund raise in the world of technology. We are somewhat surprised that, based on our understanding of the judgments in *Brownlie I* and *II*, the view is that private international law and the coverage of economic loss arising in negligence cases follows the logic that there needs to be underlying physical damage. We would feel that the basis of financial statement economic loss established in the cases that follow on from *Hedley Byrne v Heller* would give more credibility to coverage of economic loss in digital asset cases and that this broader principle would be followed going forward.

It can be conceptualised by applying the normative concepts through the digital asset’s world, especially paying special attention to the fact that opinions and trends are formed quickly, if not to say instantly. Social media gossip and verified statements broadcasted on the internet are almost impossible to rectify. Offences such as malicious communications, then become impossible to deal with via law enforcement.

- **If the crypto-token cases are cases of pure economic loss, to what extent would it be desirable that a consistent approach is taken in England and Wales to localising pure economic loss as between jurisdiction and applicable law?**

It would be desirable to the extent of making it pragmatic for the courts to focus on quantum rather than on a multiplicity of variables. It would permit all levels of the judiciary to feel comfortable in the route of reaching a decision on quantum. That extent would not be desirable in the circumstances where matters other than pure economic loss are of relevance.

Please share your views and evidence below:

N/A

Question 4: In this question, we seek views and evidence on jurisdiction founded on the basis that an unlawful act was committed in England and Wales.

- **To what extent is the approach so far of the courts of England and Wales in localising a crypto token for the purposes of jurisdiction theoretically sound? What would be the relative merits and demerits of any alternatives?**

To date, the courts have approached the test of unlawful act on a broad and somewhat inconsistent basis, in our view, as we discussed under the previous question relating to negligence – testing both the location of the act and consequential damage. Similarly, where the act underlying the crime has taken place as well as where the harm has been caused are both relevant tests that we consider have been applied. We also have seen that the policy and CPS have struggled to assist in investigating and prosecuting cases of financial loss through fraud and linked crimes where bitcoins/digital assets on a distributed/cross border basis have been involved.

It is sound to the extent of establishing a clear nexus but localising digital assets is a counterproductive stance for any consideration. It may be theoretically sound because it seeks to begin its analysis with the correct locality for that jurisdiction, but it needs to now consider multiplicity of issues such as constantly travelling directors (“digital nomads”).

The merits of any alternatives would be to secure a better and fairer approach to access to justice. The demerits are essentially opening floodgates through litigation tourism and impossibility of enforceability.

- **To what extent does the question of where an unlawful act is committed or event occurs for the purpose of jurisdiction arise in practice?**

To a minor extent because location is not a prime consideration in such matters.

Please share your views and jurisdiction:

N/A

Question 5: In this question, we seek views and evidence on jurisdiction founded on the basis that the claim relates to objects within England and Wales.

- **To what extent is the approach so far of the courts of England and Wales in localising a crypto-token for the purposes of jurisdiction theoretically sound? What would be the relative merits and demerits of any alternatives?**

Localising crypto-token transactions in terms of contractual and tortious liability is theoretically and practically feasible in terms of certain “connecting factors”, that is, governing law stated in any related smart/real contract; the location of the buyer; the location of performance of service/delivery of product and location/type of breach or damages involved.

We have answered this question in more detail by considering a number of key factors below as well as the merits and demerits of seeking a uniform universal approach.

In terms of theoretical soundness, this approach allows the courts to apply established legal principles flexibly to new technologies, ensuring a degree of continuity and predictability. By adopting a case-by-case basis, decisions based on the specific facts of each case can accommodate the vast diversity of scenarios involving crypto-tokens, from straightforward ownership disputes to complex issues involving decentralised finance (DeFi) and non-fungible tokens (NFTs).

The current approach of the courts ensures consistency with existing law. This approach seeks to integrate crypto-tokens within the existing legal framework, ensuring that the principles of justice and equity that underpin the law are extended to digital assets. It provides a pragmatic solution to the challenge of applying traditional concepts of jurisdiction to inherently global and decentralised digital assets. Nevertheless, given the novelty of the technology and the evolving nature of the law, there remains a degree of legal uncertainty for parties dealing with crypto-tokens. This can make risk management difficult.

Alternatives and Their Relative Merits and Demerits:

Creating Specific Legislation for Digital Assets

Merits: This could provide clear, specific guidelines for the localisation of crypto-tokens, reducing uncertainty and potentially fostering a more favourable environment for innovation and investment in digital assets.

Demerits: The rapid pace of technological development may outstrip the ability of legislation to keep up, resulting in laws that quickly become obsolete or are overly prescriptive and inhibit innovation.

International Agreements

Merits: Given the global nature of blockchain technology, international agreements could offer a harmonised approach to jurisdiction, providing clarity and predictability.

Demerits: Reaching consensus on international standards can be a slow and complex process, and such agreements may lack the flexibility to address the nuances of specific cases.

Adopting a Universal Jurisdiction Principle for Digital Assets

Merits: A principle of universal jurisdiction could sidestep the issue of localising a token by establishing a common legal framework applicable to disputes involving digital assets, regardless of where they arise.

Demerits: This could lead to jurisdictional overreach and conflicts with national sovereignty, as well as practical challenges in enforcement.

- **What point in time is relevant for gateways 11 and 15(b)? Do these gateways require that a crypto-token is within England and Wales: at the time of proceedings, at the time of misappropriation, or some other time?**

Overall, we do not consider that location of the digital asset is the necessary factor. The actual location of a the crypto-token (its custody wallet), could be quite different from the buyer's/owner's location.

The unique characteristics of crypto-tokens require a nuanced approach to determining their "location" for legal purposes. Unlike physical assets, their location might be conceptualised based on various factors, including the legal domicile of the parties, the location of relevant nodes, or other connecting factors that tie the digital asset to a specific jurisdiction.

The approach to gateways 11 and 15(b), in the context of crypto-tokens, may evolve as courts gain more experience with such cases and as legal frameworks adapt to technological advancements. For gateway 11, the relevant time is when the damage was suffered, and for gateway 15(b), it is the time of commencing proceedings, requiring the property to be within the jurisdiction at that point.

➤ **To what extent does the question of where a crypto-token is located for the purpose of jurisdiction raise issues in practice?**

The test should not be the location of the crypto-token as this could be quite academic. It should be addressed by the location of the buyer or possibly the seller and certainly where the service is to be performed and where any loss or damage is sustained.

The decentralised nature of blockchain technology means that crypto-tokens do not reside in a single, physical location. This challenges traditional jurisdictional rules based on geographical location, leading to complexities in determining which court has authority over a dispute involving crypto-tokens.

There is still relatively limited case law on this matter, leading to uncertainty and variability in how different jurisdictions and courts approach the question of a crypto-token's location. This inconsistency can complicate cross-border disputes and enforcement of judgments.

Even if a court successfully asserts jurisdiction and issues a judgment involving a crypto-token, enforcing that judgment presents practical challenges. The anonymous and borderless nature of blockchain technology can make it difficult to compel compliance from an unwilling party or to seize digital assets without cooperation from intermediaries like exchanges or wallet providers.

The location of a crypto-token can impact taxation, including which jurisdiction has the right to tax gains from crypto transactions. The lack of clarity around the location of digital assets creates uncertainty around tax obligations and reporting requirements extending also to areas of money laundering, sanctions and corruption regulations and proceedings.

The cross-border nature of crypto-tokens may encourage greater international legal cooperation and the development of harmonised standards or agreements to address jurisdictional and enforcement challenges. We can see this in terms of UNIDROIT principles and the international conferences that are taking place within legal and technological circles which we endeavour to have our legal team attending in order to understand how best to advise clients operating in multiple different jurisdictions and in more and more innovative ways.

Question 6: In this question, we seek views and evidence on the types of claims and causes of action relied upon in applications to serve proceedings relating to crypto-tokens out of the jurisdiction.

- **To what extent can it be said that there is a serious issue to be tried where claimants allege that exchanges are constructive trustees in the circumstances pleaded in Piroozzadeh v Persons Unknown and comparable cases?**

We suggest that the remedy should not focus on the constructive trustee, but on the underlying beneficiary and its bona fides in order not to obstruct proceedings that are essentially targeted at unknown defendants who have obtained digital assets either by fraud or negligence.

- **Is there any further practical evidence we could consider in relation to the ways in which exchanges defend or intend to defend applications and/or claims alleging they are constructive trustees at the return date of these applications?**

We suggest finding a remedy to look through the constructive trusteeship in order to seize the digital assets. This should be available in equity or through legislation.

- **Are there similar problems with causes of action under any of the other gateways?**

Yes, similar problems with causes of action may arise under other gateways. In cases involving contractual disputes, tort claims, or breaches of statutory duty, determining the appropriate jurisdiction can be complex, especially when transactions occur across borders or involve parties from different jurisdictions.

- **Are these cases indicative of a need to consider more carefully the “serious issue to be tried” limb of the three-stage test for service out of the jurisdiction?**

Yes, not only that, but it could also accommodate a multiplicity of factors involved in accepting exchanges (being the entry point i.e. the de facto custodian bank behind closed doors) and thereby producing an unintended effect of a facilitating a ‘mixing’ stage. This, in effect, permits funds to come in on a trackable and defined format which can then be controlled by mixing them with other illegitimate funds away from the public eye, and releasing the funds which are no longer trackable, facilitating money laundering.

Question 7: In this question, we seek views on applicable law and decentralised finance (DeFi).

- **Do you agree that contractual disputes in the context of DeFi are not likely to come before the courts?**

We suggest that the answer is more nuanced. New types of claims based on defective code; deficient administrative procedures not working as planned and less around intentional breach and more around mis-administration.

We feel that such disputes require specialist arbitration – it being more likely to be resolvable between the parties without litigation but there will be exceptional cases to adjudicate on.

We consider below certain factors which may mean such disputes do not reach the courts:

Why might they not reach courts?

Self-Executing Contracts: DeFi contracts are often smart contracts that automatically execute the terms agreed upon by the parties. The automated nature of these contracts reduces the scope for disputes over performance, as execution is triggered by the code itself rather than requiring manual intervention or interpretation.

Anonymity and Pseudonymity: Participants in DeFi transactions often operate under pseudonyms or with a degree of anonymity. This can make it challenging to identify and bring claims against counterparties in a traditional legal setting.

Jurisdictional Challenges: The decentralised and borderless nature of blockchain technology complicates jurisdictional questions. Determining which court has authority over a dispute, especially when parties are dispersed globally, can be a significant hurdle.

Preference for Arbitration and Mediation: The blockchain community often favours alternative dispute resolution mechanisms, such as arbitration or mediation, over traditional court proceedings. These methods are seen as more in tune with the decentralised ethos of the blockchain space.

Technical Complexity: The technical complexity of DeFi and blockchain technology can make it difficult for traditional courts to adjudicate disputes. Specialised knowledge is often required to understand the intricacies of a dispute fully.

Why might they reach the courts?

Significant Financial Losses: In cases of substantial financial losses, especially those involving fraud, theft, or significant flaws in smart contract code, affected parties might seek legal recourse through the courts, especially if other avenues for resolution are ineffective.

Regulatory Actions: Regulatory bodies may intervene in DeFi activities deemed to violate securities laws or other financial regulations, potentially leading to court cases. These actions could involve disputes over the classification of tokens, compliance with anti-money laundering (AML) standards, or enforcement of investor protections.

Smart Contract Flaws: While smart contracts are designed to execute automatically, flaws in their code can lead to unintended consequences. In such cases, parties might seek court intervention to resolve disputes over liability and losses, especially if the contractual terms were ambiguous or if there was a significant misalignment between the parties' understanding and the contract's execution.

- **Do you agree that, as a result, these disputes will not be resolved with reference to private international law and the question of applicable law?**

We feel that it is likely to need separate arbitration to decide where the technical mal-administration arises and need technology expertise as well as legal/regulatory expertise to address these matters.

Reasons Why DeFi Disputes Might Sidestep Traditional Legal Frameworks

Autonomous Execution: DeFi contracts, being self-executing and governed by code, are designed to operate independently of traditional legal frameworks. Theoretically, this minimises the reliance on external legal systems to interpret or enforce agreements.

Decentralisation and Anonymity: The global, borderless nature of blockchain technology, coupled with the anonymity of participants, challenges the application of national laws and the determination of jurisdiction in traditional senses.

Community Governance: Many DeFi platforms operate under community governance models, where disputes are resolved through consensus mechanisms or pre-defined protocols, rather than through legal proceedings.

Use of Code as Law: In the DeFi space, a strong ethos of "code is law" has developed, where the written code's execution is considered the final arbiter of disputes, potentially sidelining traditional legal interpretations and enforcement mechanisms.

Why Private International Law and Applicable Law may still be Relevant:

As DeFi Interfaces with traditional finance, it continues to intersect with traditional finance, so that the regulatory scrutiny and legal frameworks governing traditional financial transactions may extend to DeFi operations, necessitating considerations of applicable law and jurisdiction.

Cross-Border Disputes: Despite the decentralised nature of DeFi, disputes involving parties across borders may still raise questions of private international law, especially when issues of enforcement against assets or entities in specific jurisdictions arise.

Regulatory Compliance: Regulatory bodies worldwide are increasingly focusing on DeFi, suggesting that compliance with national laws and international regulations will become more critical. This regulatory landscape may lead to disputes that involve questions of applicable law, especially concerning anti-money laundering (AML), know your customer (KYC) regulations, and securities laws.

Contractual Failures and Externalities: Not all aspects of DeFi transactions can be entirely encoded or anticipated by smart contracts. Failures, such as those due to bugs, external manipulation, or unforeseen legal issues, may necessitate recourse to traditional legal mechanisms, including considerations of private international law to resolve disputes.

Evolution of Legal Frameworks: Legal frameworks are evolving to address the unique challenges posed by digital assets and decentralised platforms. This evolution may include the development of new principles in private international law specifically tailored to the blockchain and DeFi contexts.

- **Would the law applicable to these kinds of disputes benefit from further clarification?**

It is our view that there is a need for a new general principle to allow the parties in the first instance to rely on General Agreed Resolution principles applicable for all disputes and for all jurisdictions in way that reduces the need to enter into jurisdictional dispute issues.

The law applicable to disputes in the context of Decentralised Finance (DeFi) and other blockchain-based transactions would greatly benefit from further clarification. As DeFi continues to grow in popularity and sophistication, it intersects more frequently with traditional financial and legal systems, exposing various gaps and ambiguities in existing legal frameworks.

Clarification of the laws applicable to blockchain and DeFi disputes is not just beneficial but necessary for the continued growth and integration of these technologies into the broader economic system. Such clarifications could come through legislative action, judicial decisions, or regulatory frameworks, ideally in a manner that involves dialogue between technologists, legal experts, regulators, and the community at large. Ensuring that the law keeps pace with technology is essential for protecting stakeholders and supporting the healthy evolution of the financial landscape.

Question 8: This question concerns the applicable law for non-consumer contracts.

- **Can the provisions of the Rome I Regulation for identifying the applicable law for non-consumer contracts be applied to contracts involving crypto-tokens without undue difficulty?**

Yes. Although, we believe that there is a need to dispense with or extend the concept of “money consideration” to include digital assets.

- **If the provisions cannot be applied, or can only be applied with significant difficulty, what are the possible solutions?**

We do consider that there is a need to re-define or expand on “money consideration” to avoid unnecessary complications in bringing digital asset cases to court.

- **If the provisions can be applied easily or without undue difficulty, are there any areas that would benefit from further clarification?**

Again, our key point would be to re-define or expand on “money consideration”.

- **To what extent is the application of these provisions problematic in practice?**

It may be problematic to reach a broad consensus on expanding the concept which in turn could take time and may not be a widely shared view.

- **If the issue is prevalent in practice, what would be the consequences if it were not resolved adequately as a matter of law?**

It may cause considerable confusion between parties reaching settlements and in court litigation/appeals to resolve the matter. It may also lead to 'litigation tourism'.

Question 9: This question concerns the applicable law for consumer contracts.

- **Can the provisions of the Rome I Regulation for identifying the applicable law for consumer contracts be applied to contracts involving crypto-tokens without undue difficulty?**

Yes. We suggest that, in the first instance, to let the vendor state the law and/or the relevant custodian/exchange where the asset is held. We accept that the consumer purchaser should be able to bring the case in its home jurisdiction and that complications will arise where asset-backed tokens are involved and there is a further different lex situs relating to the underlying asset.

- **If the provisions cannot be applied, or can only be applied with significant difficulty, what are the possible solutions?**

"Lex Cryptographia", as a solution, should be developed as a separate set of legal principles for these contracts.

- **If they can be applied easily or without undue difficulty, are there any areas that would benefit from further clarification?**

Further clarification should be focused on existing grey areas of international consumer contract law.

- **To what extent is the application of these provisions problematic in practice?**

We envisage a wide range of service/remedy issues, aside from the governing law and acceptable court jurisdiction.

- **If the issue is prevalent in practice, what would be the consequences if it were not resolved adequately as a matter of law?**

There would be inevitable disagreements on remedies – some would use common arbitration principles and others would end up with intractable arguments on how the dispute should be resolved.

- **We seek views on whether the provisions of the Rome I Regulation for identifying the applicable law for consumer contracts can be applied to contracts involving crypto-tokens without undue difficulty.**

In principle, yes but in practice, we envisage considerable issues.

The English law should offer certainty within its own remit, and it should contain mechanisms irrespective of the Rome I identification.

Consumer contracts that apply to crypto tokens should be clear and stay relevant law. The blockchain community must not, as a starting point, look for mechanisms such as Rome I to then proceed identifying the applicable law. The position of law should be clear from the outset and should consider the location and intention of the parties.

Question 10: This question concerns the exclusions in Articles 6(4)(d) and (e) of the Rome I Regulation.

- **Do the exclusions of financial instruments and transferable securities, as set out in Articles 6(4)(d) and (e) of the Rome I Regulation, apply to crypto-tokens?**

Yes, but Rome I is not the correct vehicle for this. We suggest that digital assets, or at least certain such tokens and assets, are to be seen as financial assets and subject to financial instrument product regulations which form an exclusion from Rome Convention regulations.

- **What would be the positives and negatives of interpreting these provisions in an international way, bearing in mind guidance from the European Securities and Markets Authority?**

The positives would be a clear pathway and framework of reference in line with an established position concerning the so-called international law and the EU based guidance from ESMA.

The negatives would be the difficulties in applying a large number of complex principles of international law in line with the ESMA guidance, which not binding. Reliance on a large number of rules and interpretations will open matters up for argument.

- **Should the courts simply apply the Financial Services and Markets Act 2000 (Regulated Activities) Order 2001 in line with Financial Conduct Authority guidance?**

Yes, in the usual way.

- **To what extent do these exclusions cause problems in practice (now or in the future)?**

These exclusions cause problems of interpretation, jurisdiction, enforcement, although no more than other exclusions. There may also be a lack of expertise in this field and create an “open season in case law”.

- **If these exclusions are problematic in practice, what would be the consequences if they were not addressed as a matter of law?**

Legal chaos and a distinct possibility that the courts would make contradictory decisions when faced with the same facts.

- **What kind of reform is needed?**

It is our view that a Blockchain Act should be considered and implemented, with specialist blockchain judges and specialist courts dealing with specific and complex matters.

Question 11: We seek views and evidence on localising damage arising in tortious claims relating to crypto-tokens for the purposes of applicable law.

- **To what extent is it likely that claims in tort, such as those pleaded in the crypto-token litigation for the purposes of service out of the jurisdiction, will proceed to trial before the courts of England and Wales? Is it likely that the question of applicable law will be in dispute between the parties?**

To a high extent. There will likely be a dispute between the parties would be establishing the jurisdiction and it is very often in crypto fraud cases that the respondent party is absent.

- **If it becomes necessary for the courts of England and Wales to determine the question of applicable law, how could the courts approach the question of localising tortious damage in the broader digital asset and electronic trade documents context? Please indicate whether your response should be considered in the context of the CJEU jurisprudence or in the context of a potential common law approach.**

The courts approach should be focussed on the location and the nexus of the parties, conduct of business of the claimant, the damage having occurred in the jurisdiction, and representations made by the defendant as they relate to the jurisdiction.

Given the post-Brexit system, common law is, in our view, a better alternative, but the solution of introducing a Blockchain Act, with Blockchain Judges and Blockchain Courts should be considered.

Question 12: We seek views and evidence on recourse to the “escape clause” in Article 4(3) of the Rome II Regulation.

- **In what circumstances in the digital assets and electronic trade documents contexts would it be appropriate for the courts of England and Wales to have recourse to the escape clause on the basis of a pre-existing contractual relationship?**

The escape clause is by its nature counterproductive and overly legalistic.

England and Wales should not be in a position to exercise the escape clause, as much as this clause is helpful, but it at least pins down the jurisdiction in which the litigating parties may have agreed in an underlying contract.

- **To what extent would the parties in a tort claim involving digital assets and electronic trade documents have a pre-existing contractual relationship? Would these represent the vast majority of cases?**

Little to no extent, as much as it may suit the legal establishment to be pushing this argument forward. It is our view that the point of such a claim is to start from the beginning.

- **If the parties to a tort claim do not have a pre-existing contractual relationship, when else would it be appropriate for the courts of England and Wales to have recourse to the escape clause? What factors should the courts consider when identifying the country “manifestly more closely connected” to the tort?**

The Court should treat digital assets related disputes without desperately trying to base them on pre-existing contractual relationships. The court should not have to exercise the escape clause but, if need be, complete discretion should be adopted by the judge to find as broadly as possible a necessary connection.

Question 13: We seek evidence, particularly from market participants, on how market practice in respect of bills of lading has been affected, or how it is likely to be affected, by the introduction of the Electronic Trade Documents Act 2023.

Please share your views and evidence below:

As a Firm with some involvement in shipping law and disputes, we have not encountered directly cases, either in commodity trading or in shipping, involving an electronic bill of lading.

We do not consider that at this time, this is particularly surprising. According to a press release last year by the Digital Container Shipping Association, to which most of the major container carriers belong, ocean carriers issue around 45 million bills of lading a year, but in 2021, only 1.2% of these were electronic.

Moreover, most cargoes are carried without mishap. In practice, if there is a claim in connection with a (paper or electronic) bill of lading, typically for loss or damage to cargo, it will be raised in the first instance with insurers: the cargo owner will claim under cargo insurance, while the carrier is likely to refer the claim to its P & I Club, which insures it against third-party liabilities. Most claims are settled without recourse to lawyers.

Questions 13 to 16 seek evidence on market practice and market sentiment respectively and we do not have the necessary background or experience in these specific areas to provide answers.

For example, Question 15 asks for evidence on the difficulties of incorporating the Hague Visby Rules where an electronic bill of lading has been used, and specifically, how often disputes arise, and are likely to arise in the future, on the incorporation of the Rules. It also asks whether there are concerns in the market, in the marine insurance and shipping sectors, regarding the incorporation of the Rules. Again, we do not have the relevant

background at this time to answer these questions but would be ready to work with the Law Commission to investigate these areas further.

Therefore, we have not attempted to answer questions 14-16 in this submission:

Question 17: We seek views on the most appropriate connecting factor for determining where an electronic bill of exchange is “delivered to a first holder” for the purposes of section 72(1) of the Bills of Exchange Act 1882.

➤ **As the connecting factor for determining where an electronic bill of exchange is “delivered to a first holder”, what are the relative merits and demerits of recourse to: (i) the reliable system, and (ii) a relevant person?**

In selecting the “reliable system” we consider the following:

Merits

- (i) Defining the system in terms of the exchange; custodian and potentially the DAO would give all parties involved a clear and objective connecting factor;
- (ii) The system could be located in a legally/regulatory satisfactory jurisdiction for the purposes of dispute resolution/litigation. If not, then other connecting factors should operate, which is discussed in terms of the demerits;
- (iii) A reliable system often involves automated processes that can handle the transfer and storage of electronic bills of exchange efficiently and quickly, minimising human error and delay and providing a more satisfactory jurisdiction/applicable law determination;
- (iv) Digital systems usually have robust logging and tracking mechanisms, making it easier to audit and trace the history of a bill of exchange, which is beneficial for resolving disputes and proving authenticity; and
- (v) Using a standardised system can help ensure consistency in how of exchanges are handled across jurisdictions.

Demerits

- (i) The system jurisdiction could be located in a far-off tax advantaged jurisdiction with less developed administration procedures, judicial system, laws, regulations and arbitration rules;
- (ii) The system can be seen as quite arbitrary jurisdiction in relation to the relevant person(s) or relevant asset (s) – i.e. it could be seen as the effective “motorway” along which the relevant “car/digital asset” is travelling and, therefore, quite incidental to where the parties are travelling to or located; and

- (iii) Technology evolves rapidly and a system that is used can become obsolete quickly which can be costly and difficult to migrate personal data.

➤ **If the reliable system were used as the connecting factor, should it make a difference whether the reliable system is a central registry or a DLT system? Is it desirable for a single connecting factor to be used for all types of reliable systems?**

In our view it should not matter, *prima facie*, whether the system is centralised, decentralised or a DAO; it should be developed as broadly as circumstances require.

Again, we would favour a cascade of connecting factors to allow a broad and evolving jurisprudence around the types of reliable systems that are covered.

While having a uniform standard for the connecting factor in reliable systems could simplify transactions and legal interpretations, it is also crucial to allow flexibility to choose the most appropriate technology based on specific needs and circumstances. This approach can leverage the strengths of different systems while mitigating their weaknesses, tailored to the particular requirements of the users and regulatory environments involved.

➤ **Can we assume that the “reliable systems” that are or will be used in the context of bills of exchange will largely be comparable to those used in the context of bills of lading?**

In principle, we would say “yes”, but with the caveat that our shipping law team are hesitant to be definitive around the evolution of the PIL around electronic bills of lading. Therefore, we prefer to confine our views to the area of bills of exchange as they are currently still used in general commercial and financial fields.

The assumption that “reliable systems” used for electronic bills of exchange might be largely comparable to those used for electronic bills of lading is reasonable in several respects, especially considering their shared purposes and the benefits of digitisation. Both types of documents function as critical instruments in trade and finance, with bills of exchange used primarily for payment processes and bills of lading for the shipment of goods.

While we can assume some level of comparability between the systems due to their shared goals of enhancing security, efficiency, and compliance, we consider it is important to recognise the unique requirements and regulatory contexts of each document type. This means that while there might be technological and conceptual overlaps, specific adaptations will be necessary to address the unique challenges and needs of each domain. Hence, system developers and users should not assume a one-size-fits-all approach but rather should consider the specificities that might necessitate adjustments or specialised features.

➤ **If a relevant person were used as the connecting factor, what are the relative merits and demerits of recourse to (i) the transferor; and (ii) the transferee?**

Merits

- (i) Transferors typically control the initiation of the transaction and can ensure that all necessary steps are taken to validate the transaction. They are responsible for the accuracy and authenticity of the document at the time of transfer;
- (ii) Transferors are usually familiar with terms and conditions reducing the risk of error or disputes;
- (iii) Transferees have the opportunity to verify the bill of exchanges and ensure it meets all eligibility criteria before accepting it; and
- (iv) The transferee's involvement in the validation process can increase their confidence in the transaction, as they have the ability to confirm all aspects of the bill directly.

Demerits

- (i) Since transferors are in control, there is a risk that they might misrepresent the terms or conditions of the bill, intentionally or unintentionally;
- (ii) If the transferor's systems are compromised, this can affect the integrity of the bill's transfer, especially if they lack adequate security measures;
- (iii) The transferee may not always have the same level of expertise or access to information as the transferor, which can lead to inefficiencies or errors in validating the bill of exchange; and
- (iv) Relying on the transferee to verify and accept the bill can lead to delays, especially if the transferee needs additional time to conduct due diligence or if they are not equipped with efficient systems for such verification.

➤ **To what extent does the question of the formal validity of a paper bill of exchange arise in practice? How likely is it that the question of the formal validity of an electronic bill of exchange will arise in practice?**

While the formal validity of paper bills of exchange still arises in practice, especially in less technologically advanced settings, the frequency and severity of such issues are generally manageable with current banking practices. For electronic bills of exchange, although there might be an initial increase in disputes related to their formal validity owing to the novelty and evolving legal standards, this is expected to decrease as legal frameworks mature and technology standardises.

The key to minimising such disputes lies in the development of robust legal frameworks and the adoption of standardised technologies that ensure the security and authenticity of electronic bills of exchange.

➤ **Do electronic bills of exchange pose any other issues for section 72 of the Bills of Exchange Act 1882 that we have not considered here?**

Proof of Authenticity: Ability to establish a genuine system that cannot be tampered with;

Digital Signatures: Are all forms of possible digital signatures now legally binding?

Endorsement systems: There needs to be a legally binding and recognisable endorsement system that recognises a more digital framework;

Chain of Custody: Blockchain solutions providing a clearer and immutable record of transactions;

Time Stamping: Ensuring that timestamps are accurate, so they are not manipulated;

Rapid system checks: System should allow for rapid checks and also simultaneously reduce errors; and

Fraud Detection, Sanctions evasion and Anti-Money Laundering: Techniques for detecting fraud and breaches of financial law/regulation that must develop to keep pace with more digitally sophisticated methods of forgery, evasion and deception.

Please share your views and evidence below:

The above views have been based on the Firm's legal, financial and compliance advisory work across a broad range of areas in which Bills of Exchange operate in a traditional non-digital format. The ideas advanced are based around digital asset advisory and litigation work involving bitcoin and other digital assets, rather than specifically relating to digital Bills of Exchange and Electronic Trade documents.

Question 18: We seek views on whether it would be desirable to have a single conflict of laws regime to cover all types of electronic trade documents that fall within the scope of the Electronic Trade Documents Act 2023.

- **Would it be preferable for electronic bills of exchange, cheques, and promissory notes to continue to be governed by the Bills of Exchange Act 1882 through an extended application of section 72; or for them to fall within a new rule for all electronic trade documents under the 2023 Act?**

Extended Application of the Bills of Exchange Act 1882

Advantages

Continuity and Stability: Extending the 1882 Act maintains continuity with established legal principles, which can provide stability and predictability for financial transactions.

Precedent and Interpretation: Courts are familiar with the 1882 Act, and there is a wealth of case law interpreting its provisions, offering clear guidelines for application to disputes.

Disadvantages

Outdated Framework: The 1882 Act was conceived long before the digital age, and its provisions may not fit well with the nature and technical specifics of electronic documents.

Adaptation Limitations: While s 72 allows for adaptations to enable electronic forms, continuous patching of an old act might lead to a patchwork of rules that are difficult to apply cohesively in a modern context.

Proposed New Rule for All Electronic Trade Documents Under the 2023 Act

Advantages

Modern Framework: A new act specifically designed for electronic trade documents can be tailored to address the unique aspects of digital transactions, including security, authenticity, and transferability issues that are central to electronic instruments.

Flexibility and Innovation: New legislation can incorporate flexibility to adapt to future technological changes and innovations in financial technology.

Unified Approach: Having a single, comprehensive rule for all electronic trade documents could simplify the legal landscape, making it easier for users to understand and comply with the law.

Disadvantages

Implementation Challenges: Drafting and implementing a new legislative framework involves significant time and resources. There's also the risk of unforeseen consequences that could disrupt existing financial practices.

Lack of Precedent: A new act would not have the benefit of established case law, leading to initial uncertainties in how courts will interpret the new rules.

- **If a single conflict of laws regime for all electronic trade documents under the 2023 Act is preferable, what should be its scope? Should it cover contractual obligations only, or both contractual and proprietary obligations arising within the reliable system?**

If the decision is to establish a single conflict of laws regime for all electronic trade documents under the 2023 Act, defining its scope is crucial to its effectiveness and relevance. This regime would need to address the unique characteristics of electronic transactions while ensuring legal clarity and certainty.

Contractual obligations are fundamental to trade documents and include the rights and duties of each party involved in the transaction. Since electronic trade documents like electronic bills of lading, promissory notes, or letters of credit primarily serve as means to enforce contracts, it is essential that the regime comprehensively covers these aspects.

The electronic element introduces complexities related to the verification of parties' identities, the integrity and authenticity of signatures, and the enforceability of terms. A conflict of laws regime should address where a contract was formed, which law applies to interpret the terms, and how disputes are resolved.

Proprietary rights concern ownership and other property rights that might be transferred or affected by the trade documents. In digital transactions, determining the location and ownership of a digital asset can be particularly challenging due to the decentralised and often intangible nature of these assets.

Proprietary issues in electronic documents might involve questions about the transfer of ownership rights, the effects of such transfers on third parties, and the jurisdictional implications of these transfers. These issues are critical in ensuring that electronic documents provide the same level of security and certainty as their paper counterparts.

Ideally, the conflict of laws regime under the 2023 Act should cover both contractual and proprietary obligations arising within reliable systems. This approach ensures that all essential aspects of electronic trade document transactions are legally recognised and protected. By providing a comprehensive legal framework, the regime can facilitate international trade, reduce legal uncertainties, and foster trust in electronic transactions, which are increasingly prevalent in global commerce.

- **If a single conflict of laws regime for all electronic trade documents under the 2023 Act is preferable, what approach should we take to any new regime and what broader objectives of the conflict of laws should we keep in mind? Stakeholders may wish to refer back to Chapter 6 from paragraph 6.103.**

When establishing a new conflict of laws regime for electronic trade documents under the proposed 2023 Act, it is crucial to design a system that not only addresses specific legal and practical issues but also aligns with the broader objectives of conflict of laws. This approach should consider the unique dynamics of electronic transactions while ensuring robustness, fairness, and adaptability.

Below, we have considered specific factors:

Flexibility: Adopt a principle-based rather than a rule-based approach to accommodate future technological developments without the need for frequent legislative updates.

Clarity and Simplicity: Ensure the principles are clear and easily understandable to encourage compliance and facilitate enforcement across different jurisdictions.

Adaptability: The regime should apply to various forms of electronic documents and digital transactions, regardless of the underlying technology, to prevent obsolescence as new technologies emerge.

Harmonisation: Align the regime with international standards and practices to facilitate cross-border enforcement and recognition. Engaging with international bodies like UNCITRAL or the Hague Conference on Private International Law can help ensure that the regime supports global trade.

Consultation: Involve a wide range of stakeholders in the drafting process, including legal experts, technology providers, businesses, and consumer representatives to ensure the regime meets diverse needs and minimises unintended consequences.

Security and Privacy: Address data protection and privacy concerns, ensuring that the regime respects these rights while facilitating the secure and efficient transfer of electronic documents.

The approach to establishing a new conflict of laws regime for electronic trade documents under the 2023 Act should be comprehensive, forward-looking, and aligned with international norms to ensure effectiveness and broad acceptance. By balancing these considerations with the broader objectives of conflict of laws, the new regime can provide a robust legal framework that supports the evolving landscape of digital transactions while promoting fairness, efficiency, and security in international commerce.

Question 19: We seek views on the law applicable to property disputes in relation to digital assets and ETDs. Where possible, we ask that stakeholders contextualise their responses, for example, give details as to whether it relates to a pledge over an ETD or property entitlements in crypto-token litigation.

- **To what extent would recourse to contractual principles obviate the need for us to consider the lex situs rule?**

Recourse to contractual principles, instead of relying on the lex situs (law of the place where the property is located) rule, can potentially simplify and streamline the legal considerations for transactions involving intangible assets, like those typical in finance and digital transactions. The lex situs rule is traditionally important in determining which laws govern the transfer and ownership of property, especially in cross-border situations. However, the suitability of this rule for modern, digital, or intangible assets can be limited.

While recourse to contractual principles can significantly reduce the reliance on the lex situs rule, particularly for intangible or digital assets, it does not completely eliminate the need for this traditional legal doctrine. The choice between contractual principles and the lex situs rule should be guided by the nature of the asset involved in the transaction, the goals of the parties, and the legal outcomes they wish to achieve. For modern, fast-paced, and technologically driven transactions, especially those lacking physical dimensions, contractual agreements often provide a more adaptable and appropriate framework.

However, for traditional assets and particularly in real estate, the lex situs rule remains indispensable.

- **Do permissioned networks and/or cases where there is clearly a contractual or hierarchical relationship between the parties represent the vast majority of DLT applications for digital assets and ETDs?**

The landscape of Distributed Ledger Technology (DLT) applications for digital assets and Electronic Trade Documents (ETDs) includes a mix of both permissioned and permissionless networks. Whether permissioned networks, which often involve clear contractual or hierarchical relationships between participants, represent the vast majority of applications depends largely on the specific sectors and use cases being considered.

Whether permissioned networks represent the vast majority of DLT applications for digital assets and ETDs largely depends on the context and specific sectors in question. In environments requiring strict regulatory adherence and operational control, permissioned networks are more prevalent, whereas, in broader, more innovative contexts that value decentralisation and open participation, permissionless networks thrive.

- **Should we need to consider a new conflict of laws regime for property rights in digital assets and ETDs, what approach should we take to any new regime and what broader objectives of the conflict of laws should we keep in mind? Stakeholders may wish to refer back to Chapter 6 from paragraph 6.103.**

Developing a new conflict of laws regime for property rights in digital assets and Electronic Trade Documents (ETDs) requires a nuanced approach that takes into account the unique properties of these assets and the technological environment in which they operate. This initiative should aim to address the specific challenges posed by the digital and decentralised nature of these assets, while also aligning with the broader objectives of conflict of laws to ensure clarity, predictability, and fairness in legal resolutions.

Creating a new conflict of laws regime for property rights in digital assets and ETDs is a complex but necessary task to address the unique challenges of the digital age. The approach should be forward-looking, inclusive, and aligned with international standards, in the way that Model Universal Codes have been developed in other novel areas. Such an approach needs to ensure it is robust, fair, and capable of fostering growth and innovation in the digital economy. By focusing on these objectives, the regime can provide a strong legal foundation that enhances trust and stability in the market for digital assets and electronic trade documents.

- **To what extent would recourse to a distinct rule based on the connecting factor of the "owner" or "transferor" for cases where parties have voluntarily dealt with one another obviate the need for us to consider further the application of the lex situs rule to cases where the parties to the dispute are strangers?**

Incorporating a distinct rule based on the connecting factor of the "owner" or "transferor" for resolving disputes in transactions where parties have voluntarily interacted with each other presents a potentially effective alternative to the traditional lex situs rule, particularly for digital assets. This approach can offer several benefits, especially in simplifying the jurisdictional complexities associated with digital transactions that do not neatly fit into the territorial frameworks established by the lex situs rule.

While a distinct rule focusing on the owner or transferor can streamline jurisdictional determinations in many cases involving digital assets, especially between parties who have voluntarily transacted with one another, it does not entirely eliminate the relevance of the lex

situs rule, particularly in complex scenarios involving third parties or broader property rights issues. A nuanced approach, potentially incorporating elements of both rules, could provide a more comprehensive legal framework that accommodates the diverse scenarios encountered in modern digital transactions.

In many ways, a unified universal set of principles would make a great deal of sense for the unique aspects of certain digital assets and smart contracts, and we could envisage a route through an international court that could arbitrate/decide disputes which potentially involve many disparate jurisdictions and laws in addition to our own jurisdiction and courts.

- **In what circumstances could a rule based on the “owner” or “transferor” be satisfactorily used? Do creditors taking security over ETDs typically require, as a matter of contract, that the debtor warrants their title to grant the security interest?**

A rule based on the "owner" or "transferor" primarily focuses on the identity and legal standing of the parties involved in a transaction rather than the location of the asset. This approach can be particularly effective in several scenarios that are common in digital transactions and modern commerce. Additionally, discussing the practices of creditors in taking security over Electronic Trade Documents (ETDs) can illuminate how such a rule can be practically applied.

The rule based on the "owner" or "transferor" can be satisfactorily used in scenarios where digital or intangible assets are involved, in cross-border transactions, and where parties prefer to establish clear legal and jurisdictional expectations upfront. Regarding creditors securing interests in ETDs, ensuring the debtor's title to the assets is a standard and critical requirement, serving as a foundational element of the security agreement. This practice aligns with the broader legal principles ensuring that all parties have clarity about the rights and obligations concerning the asset in question.

- **To what extent is it 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”?**

The scenario where courts might be asked to determine disputes relating to wholly decentralised digital assets held on permissionless Distributed Ledger Technology (DLT) networks, especially in cases of "involuntary dispossession" (such as theft or loss due to hacking), is becoming increasingly likely due to several factors associated with the growth of these technologies and their adoption.

Below is a breakdown of the factors that contribute to this likelihood:

Asset Value Fluctuations: The high volatility of digital assets can lead to significant fluctuations in value, which might increase the stakes in disputes over asset ownership and dispossession.

Anonymity and Pseudonymity: Permissionless blockchains often allow users to operate anonymously or under pseudonyms. While this feature is prized for privacy reasons, it complicates legal processes when disputes arise, especially when trying to identify parties involved in a dispute.

Decentralisation: The decentralised nature of these networks means there is no central authority to intervene in disputes, unlike in traditional banking or financial systems. This lack of oversight mechanism increases the likelihood that parties will turn to the courts for resolution.

Involuntary Dispossession: This can occur through hacking, fraud, or errors in smart contracts. Such dispossession raises complex legal questions about the recovery of assets and compensation for losses.

Jurisdictional Challenges: Determining which court has jurisdiction over a dispute involving decentralised, borderless assets can be inherently challenging. Courts may need to establish jurisdiction based on the location of parties involved or other connecting factors, which may not be straightforward.

Legal Uncertainty: The rapidly evolving nature of DLT and the lack of specific regulatory frameworks in many jurisdictions create uncertainty that often leads parties to seek judicial clarification and intervention.

The likelihood that courts will need to address disputes related to wholly decentralised digital assets on permissionless DLT networks is significant and growing. These cases will challenge traditional legal concepts, particularly concerning jurisdiction, property rights, and the enforcement of judgments. As the digital asset landscape continues to evolve, the legal system will likely see an increasing number of these complex cases, necessitating judicial intervention and potentially new legal precedents.

- **How should courts approach the question of applicable law in such disputes relating to decentralised digital assets held in permissionless DLT networks where the parties have not dealt with one another and there has been an “involuntary dispossession”?**

When courts are faced with disputes involving decentralised digital assets on permissionless Distributed Ledger Technology (DLT) networks, particularly those involving involuntary dispossession where parties have not directly interacted, they encounter unique challenges. These challenges stem from the decentralised and often international nature of blockchain technology, which complicates the determination of applicable law.

Courts addressing disputes over decentralised digital assets held in permissionless DLT networks must navigate several complex legal and technical issues. The lack of direct interaction between parties and the international, decentralised nature of the technology requires innovative legal thinking and possibly the development of new legal frameworks. As this field evolves, so too will the legal approaches to resolving these disputes, potentially

influencing broader aspects of law including property, contract, and international legal cooperation.

We need to be clearer on what situations will be classified as “involuntary dispossession”. There are ever-expanding ways in which hacking is being practised and in which AI-enhanced frauds are being deployed to directly de-fraud and to attack custodians as well as exchange wallets. In light of this diversification of attack, there is less likely to be a one fit solution that the courts should use in dealing with such cases and instead a range of remedies in damages, enforcement of injunctions and freezing orders on a cross-jurisdiction basis will be needed.

Contributors at W Legal Ltd:

*Raf Demczuk
David Ellis
Raphael Uribe
Sophie Ashworth
Elliot Shear*

The views and responses provided in this document reflect opinions of some but not necessarily of all the legal advisers at the Firm and mentioned above. They are provided as preliminary subjects for further discussion which would be welcomed by the above legal team members should the Law Commission wish to do so, and, in all cases, the views expressed are subject to review and amendment and should not be relied on as definitive advice.

The UK Law Commissioner Call for evidence: Digital assets and ETDs in private international law which court, which law?

Wave BL Response

16.5.24

Dear Prof Sarah Green, Law Commissioner,
Law commission team,

We are delighted to enclose our response to the call for evidence.

| Question | Response |
|---|---|
| <p>13.13 We seek evidence, particularly from market participants, on how market practice in respect of bills of lading has been affected, or how it is likely to be affected, by the introduction of the Electronic Trade Documents Act 2023.</p> | <p>Like all eBL platforms, if order for carriers to enjoy insurance coverage, IGPANDI approval of a multi-party agreement is required - in Wave BL this agreement is called the Bylaws ("Bylaws"). The Bylaws have always been governed by English Law and therefore the introduction of ETDA has helped removed ambiguity regarding the potential questions arising around legality of the eBL under English law. As an eBL is a document which involves at least two jurisdictions (if not more), the issue of litigation risk management, especially with an electronic version of a document of title remains very high prioritized by our customers. We advocate for seeing the Bylaws as a tool that mitigates this risk an provides certainty to all parties regarding the jurisdiction and legal system that the "question of electronic validity" will be settled at. Although we see a constant increase in adoption, other issues are seen as barriers for adoption such as: Willingness of Banks to receive e-presentations and the quest for an</p> |

| | | |
|-------|--|---|
| | | <p>interoperable eBL. Interoperability discussion held by the entire community of eBL platforms is negotiating a framework which will create a multi-platform agreement together with a standard annex that would govern that would be added to the multi-party agreements of the interoperable platforms, thus facilitating legal relations between parties using different platforms.</p> <p>Two issues that have risen from the ETDA: 1) The 'Reliable Platform' and the risk of a platform been classified differently under different law in different jurisdictions having different criteria. 2) An understanding that MLETR compliant laws merely exist around the world and it would be wise to stall adoption until the vast majority of countries adopt similar laws.</p> |
| 13.14 | We seek evidence on market sentiment relating to use of DLT platforms for electronic bills of lading. | <p>To the best of our knowledge, except for the two first eBL platforms which were approved before the introduction of blockchain technology, all platforms today (over 12) utilize DLT technology. There is a difference between the way these services are designed and the way they are marketed. Wave BL offers a combination of : 1) Legal Framework 2) SaaS solution 3) DLT ledger which Proof of Work permissioned mining under a provided ledger which is provided and managed by a Service Provider (Wave BL).</p> |
| | (1) Is it likely that market participants will move towards a wholly decentralized DLT platform for bills of lading? | <p>When we consider what is a "wholly decentralized DLT platform", one should analyze what is the difference between a "wholly" or "partial" DLT platform.</p> <ol style="list-style-type: none"> 1. <u>Public or Private ledger</u> - As a an eBL Service Provider is expected to provide full liability of 'system failure' cases and parties do not to introduce external uncontrolled dependencies risks and costs, we see it highly unlikely that parties would like a platform to utilize a public ledger like Ethereum e.g. |

| | | |
|--|--|---|
| | | <p>2. <u>Proof of Stake vs Proof of Work</u> – Mining in a privately managed platform is an issue under the control and management of the Service Provider and there is no sense (and imposes additional risks) to work under Proof of Work mining.</p> <p>3. <u>On Prem Installation vs Cloud based managed solution</u> - the idea that all platform users' nodes on the network (ledger) would install the platform application locally (on their own self-managed server) and communicate directly in a peer-to-peer manner with other applications is highly unrealistic. From our experience not only that most Companies around the world do not want to install 'on prem' applications on their own servers but also in terms of issuers role out and go to market strategies the use of a defaulted platform cloud-based management SaaS combined with a DLT is the only solution that could work. Nevertheless, the 'On prem' Installation offering, is retained for Parties who wish to do so (mainly carriers). The biggest benefit for an on prem installation is the fact the party controls its data on its own server but this benefit seems not to interest most of our customers.</p> |
| | <p>(2) To what extent can we assume that market participants will be reluctant to join a DLT platform that does not at least offer a user agreement setting out the terms on which the DLT platform will operate, and the rights and obligations of all users of the platform?</p> | <p>There is no way that carriers could enjoy insurance coverage over issuance of eBLs on platforms that have not been actively approved by IGPANDI as this is a mandatory requirement of their insurers. As part of the approval process, the legal framework of the platform which is based on a multi-party contract between all parties (and potential future parties such as endorsees) is examined and approved by IGPANDI. Carriers cannot enjoy insurance coverage in regards to eBLs issued on a</p> |

| | | |
|-------|--|---|
| | | <p>platform that is operates without approved Bylaws (User Terms).</p> <p>Should be noted that IGPANDI requirements for such an agreement shall be:</p> <ol style="list-style-type: none"> 1. Addressing the liability of the platform's managing service provider in case of 'system failure'. 2. A full description of the flow of rights and liabilities deriving from descriptive wording regarding the flow of Possession and Title. 3. Choice of the legal venue – it should be noted that a platform creates a flow of possession and title based on the specific b/l law applicable in a jurisdiction (e.g COGSA 1992 in case of English law) which could differ between different jurisdictions. <p>Another point to be mentioned, the users need to receive a license to use the service (EULA in case of ON PREM installation) and also expect a Service Level Agreement to receive support in case of troubleshooting and system failure.</p> <p>It is un realistic to expect companies would use an eBL platform without these legal frameworks in place.</p> |
| | (3) Other than wholly decentralized DLT platforms, how else might DLT be used to issue and transact with electronic bills of lading (under the 2023 Act or otherwise)? | <p>Platforms that utilize a DLT ledger (Blockchain technology) while allowing 'on prem' installations upon request alongside with a defaulted cloud based managed by service provider server (SaaS) for hosting the customer's account and data. This is how WaveBL operates and to the best of our understanding, the offering of all other blockchain platforms is the same.</p> |
| 13.15 | We seek evidence on the difficulties, if any, of incorporating the Hague-Visby Rules where an electronic bill of lading has been used. | <p>The assumption made by WaveBL is that incorporation of treaties such as HV rules is legally performed through the contract of carriage which is not mandated by the platform rules and is drafted freely by the Issuer. Nevertheless, we mandate as part of Bylaws the need to issue an eBL</p> |

| | | |
|-------|---|--|
| | | evidencing the applicable Contract of Carriage. In any case, we don't see a need to positively address this issue through Bylaws. |
| | (1) How often do disputes arise as to incorporation of the Hague-Visby Rules, specifically because an electronic bill of lading has been used, and how likely are they to in future? | We are not familiar of any such dispute. |
| | (2) Are there concerns in the market, both in the marine insurance and shipping sectors, regarding the incorporation of the Hague-Visby Rules in electronic bills of lading? Please provide detailed examples in your answer and, where possible, distinguish between electronic bills under the Electronic Trade Documents Act 2023 and electronic bills held within contractual "approved systems." | <p>We haven't encountered any rejections of concerns regarding the way we addressed this topic (as described above).</p> <p>We don't see an IGPANDI platform "approved system" as such that doesn't operate under ETDA. We see the platform Bylaws as the best way to reduce the risk of parties from different jurisdictions to challenge the "question of electronic validity" in different jurisdictions (event if they have an MLETR based local law in place, which could deem the validity of the same eBL differently). The idea of the Bylaws is to "put" users from around the world on the same page and agree to English Law and to the way the platforms transfers rights and liabilities based on its COGSA 1992 design.</p> <p>The idea of an eBL platform which is not approved is still theoretical is no carrier would ever agree to work on such platform as it introduces risks and doesn't enjoy insurance coverage. In addition, there is even a bigger question regarding the fact that banks would be willing to receive documentary presentations not by an "Approved Platform".</p> |
| 13.16 | We seek evidence on market practice to help us identify where it could be said that an electronic bill of lading is "issued" for the purpose of the Hague-Visby Rules, as | On WaveBL, eBLs will always bear an issuance signature of the carrier, digitally representing the carrier's legal entity on the platform in form of a "Platform Node" address. The accurate analogy would compare the Company details to the |

| | | |
|--|---|--|
| | <p>implemented in the UK by the Carriage of Goods Act 1971.</p> | <p>stamp and the 'Platform Node' to 'the 'Physical Office' signing with this stamp. As part of the digital identity of a 'Platform Node' a full physical address is a mandatory public field.</p> <p>On platform level, a Company could not exist twice, as our Platform Identities are aimed to digitally identify a company only once. A company has one or more "Platform Nodes" which represent a "physical post box" and its defined place of issuance (would be carrier's agency at port of loading).</p> <p>As the digital world does not have any 'physical location', it is advised that the Issuer would retain the ability to self-define the place of issuance by defining the issuing identity's address.</p> |
| | <p>(1) How, in practical terms, does a carrier wishing to issue an electronic or tokenized bill of lading do so within the respective electronic "approved" system or DLT system? What steps must a carrier take within the system?</p> | <ol style="list-style-type: none"> 1. Establish an account on the platform either 'on prem' or hosted on SaaS server managed by service provider (this choice has GDPR implications as data controlled by carrier is processed by the Service providers managed cloud). Establishment means creating under that account 'companies' and linking each company to one or more 'nodes' (a node must be irrevocably linked only to one company). 2. Approve Platform's legal framework (Bylaws). 3. Approve SaaS Agreement or EULA (in case of on prem installation) and Service level Agreement). 4. Start mapping digital identities on Platform of Shippers and Consignees to carrier's trade management system. In case they are not already onboarded to platform, there is a need for a 'role out' a joint strategy with the Platform's Service Provider to easily onboard the Shippers and Consignees usually creating accounts on SP's managed Cloud for the newly identified shippers and consignees. |

| | | |
|--|--|---|
| | <p>(2) How, in practical terms, does a shipper “receive” an electronic or tokenised bill of lading within an “approved” system or DLT system? What steps must a shipper take within the system?</p> | <p>Shipper (and Consignee + Endorsee) need to preapprove Bylaws/SaaS Agreement/DPA as a condition for receiving an eBL. This could be done once for permanent onboarding or alternatively upon election of Issuer sent to deemed email by Shippers Freight forwarder and becoming a Single Document User specifically in regard to that eBL. We have removed the need to pre onboard shipper/consignees as a condition for issuance but they will always be required to approved the bylaws even in regards to one specific eBL they gain access to via email.</p> |
| | <p>(3) Does the issue of an electronic or tokenised bill of lading between carrier and shipper involve the platform provider, or do the systems allow for electronic or tokenised bills to be sent directly from carrier to shipper?</p> | <p>Legally - our Bylaws facilitate the relations but do not deem the Platform provider as an agent or escrow for the transfer of rights and liabilities.</p> <p>Technologically - both kind of installation (On Prem/SaaS) will always require connectivity with providers servers for technical reasons that cannot be achieved otherwise and the use (and maintenance) of the designated software needed to issue and handle eBL.s</p> <p>Businesswise – Users rely on the ongoing services including identity management services.</p> <p>We don't see any realistic possibility these conditions could be different.</p> <p><u>Comment:</u> Without involvement of platform's cloud solution, it almost unrealistic to expect shippers/consignees to have an 'on prem' installation as that is a very unconventional and difficult process required from such party. It involves a lot of internal approvals and ongoing management of such an installation by Customer is very complicated. It does not sufficiently interest a party which isn't a carrier to perform such installation and</p> |

| | | |
|-------|---|--|
| | | would take months for internal approvals unlike an SP cloud based managed solution which could be created within minutes with hardly any approvals needed. On top of that we also have the SDU solution which doesn't require any pre actions from shipper but could only be done using the Bylaws and the legal framework that releases the carrier from any liability in regard to freight forwarder sending an single-document user invite email to the Shipper (which is the freight forwarder's customer). |
| 13.17 | We seek views on the most appropriate connecting factor for determining where an electronic bill of exchange is "delivered to a first holder" for the purposes of section 72(1) of the Bills of Exchange Act 1882. | We do not have clear advice on this issue except we advise to apply the logic of the 'relevant place' of each digital identity of a party to be predefined by such party upon creation of the digital identity on the relevant platform. |
| | (1) As the connecting factor for determining where an electronic bill of exchange is "delivered to a first holder", what are the relative merits and demerits of recourse to: (i) the reliable system, and (ii) a relevant person? | <p>1. Reliable system should have the freedom to be addressed in accordance with the platform's referral to a specific venue in Multi Party platform agreement (Bylaws) as that SP is adhering to comply with reliable system requirements in a specific jurisdiction (no matter if these requirements turn out to be the same).</p> <p>2. Relevant person- again this should be pre-defined by the person himself upon creation of digital identity.</p> <p>We believe Relevant Person should be the answer.</p> |
| | (2) If the reliable system were used as the connecting factor, would it make a difference whether the reliable system is a central registry or a DLT system? Is it desirable for a single connecting factor to be used for all types of reliable systems? | <p>We do not see any difference between the type of technology 'central registry' or DLT as the idea should be to leave the rights to the platform and all parties to be governed by a multiparty contract if they wish to do so (due to a requirement by insurer or for purposes of risk management).</p> <p>The rules will have to be the same for all platforms offering a registry ledger managing possessory documents.</p> |

| | | |
|-------|--|--|
| | (3) Can we assume that the “reliable systems” that are or will be used in the context of bills of exchange will largely be comparable to those used in the context of bills of lading? | The rules will have to be the same for all platforms offering a registry/ledger managing possessory documents. |
| | (4) If a relevant person were used as the connecting factor, what are the relative merits and demerits of recourse to (i) the transferor; and (ii) the transferee? | We believe the transferee would obviously be the ‘connecting factor’. Again as long as we allow the person to self-define the ‘physical’ place of the digital identity it creates to represent him. |
| | (5) To what extent does the question of the formal validity of a paper bill of exchange arise in practice? How likely is it that the question of the formal validity of an electronic bill of exchange will arise in practice? | We have no opinion on this question. |
| | (6) Do electronic bills of exchange pose any other issues for section 72 of the Bills of Exchange Act 1882 that we have not considered here? | <p>Clause 72 of BoA 1882 refers to different jurisdictions, as such it become even more eminent that a separation between:</p> <ol style="list-style-type: none"> 1. ‘Question of Electronic Validity’ – freedom needs to be left for platform to bind an interpretation to the applicable jurisdiction in each case through multi-party agreement. 2. As this clause raises some various interpretations in the paper world, we believe we should accommodate a digital environment that would not introduce further uncertainties. The place of the digital identity needs to accommodate be predefined, in addition the parties should have the freedom of interpreting these places just with a contract of carriage in case of b/l with the applicable legal framework that would apply in the paper world whether the law requires it be part of a document or somehow implicit. |
| 13.18 | We seek views on whether it would be desirable to have a single conflict of laws regime to cover all | Please see our responses above. In addition: |

| | | |
|--|---|--|
| | <p>types of electronic trade documents that fall within the scope of the Electronic Trade Documents Act 2023.</p> | <ol style="list-style-type: none"> 1. The most important question is 'electronic validity question', the fact that the service provider's company is registered at cannot be the criteria. We advise stating that <u>"Unless otherwise expressly agreed by the service providers and parties in advance</u> (to accommodate multiparty agreement), the conflict of laws regime should apply in regard to the question of electronic validity in accordance to the place digitally defined by the party that would have been the party upon which this question should have been settled assuming the ETD was issued on paper." 2. In regard to the substantial law regarding the instrument, this should be excluded from the question above and left to the freedom of parties to decide or to be addressed in according to any other conditions that would have implicated on this issue if this document was printed in paper. <p>Please note that this is how this is done today. All platform are IGPANDI Approved and include a Single Conflicts law which pertain to English law (in some cases with an ability to apply Singapore law to a specific eBL) but in any case as far as WaveBL understands it, and definitely as it is on our platform, the contract of carriage itself is not part of this arrangement as it will force the entire commercial transaction to become subject to English Law although this is clearly not the goal of the parties to the commercial dealing that prefer to remain under the jurisdictions they are used to doing business under for a variety of other personal reasons.</p> |
| | <p>(1) Would it be preferable for electronic bills of exchange, cheques, and promissory notes to</p> | <p>Please see our above responses which answer this question. We do not believe there is a need for such change.</p> |

| | | |
|--|--|---|
| | continue to be governed by the Bills of Exchange Act 1882 through an extended application of section 72; or for them to fall within new rule for all electronic trade documents under the 2023 Act? | |
| | (2) If a single conflict of laws regime for all electronic trade documents under the 2023 Act is preferable, what should be its scope? Should it cover contractual obligations only, or both contractual and proprietary obligations arising within the reliable system? | <p>We are in a position that separating between proprietary obligations through single conflict of laws regime and contractual obligations to be decided between the parties with no relations to the digital aspect of the transaction, follows what we have described above. Nevertheless, again, it should be left out to the parties to reach an agreement positively regarding the proprietary obligations for the reasons described above.</p> <p>It should also be noted that the flow of possession and title in WaveBL was designed to perfectly mirror the flow described in English Law – COGSA 1992. So even if the Bylaws would apply to a different legal venue, the entire flow of rights and liabilities (technologically) would need to change to accommodate the applicable law in the different legal venue. This is why it should be up to the platform to decide what law applies regarding proprietary rights and to positively provide a description of the entire flow. This is imperative as today over 10 platforms are approved by IGPANDI, subject to English law, claim to “mirror” COGSA 1992 but in reality, in terms of flow of possession and title, rights and liabilities, perform it differently.</p> |
| | (3) If a single conflict of laws regime for all electronic trade documents under the 2023 Act is preferable, what approach should we take to any new regime and what broader objectives of the conflict of laws should we keep in mind? Stakeholders may wish to refer | It should allow a clear and practically undisputable way to eliminate risks of using digital instruments in comparison to paper ones, not adding any new ones (even if it won't be a mandatory way). |

| | | |
|-------|--|--|
| | back to Chapter 6 from paragraph 6.103. | |
| 13.19 | We seek views on the law applicable to property disputes in relation to digital assets and ETDs. Where possible, we ask that stakeholders contextualise their responses, for example, give details as to whether it relates to a pledge over an ETD or property entitlements in crypto-token litigation. | Comment: ETD are a digital manifestation of a possessory document which by itself would and is governed by a different applicable law – using non fungible tokens that pair an RWA asset. Crypto tokens on the other hand, are based on fungible tokens and exist only in the digital world. Crypto-Token litigation issues and cases have nothing to do with ETD's which could in theory not even use a crypto token to singularize the ETD (e.g. central registry platform) and should be treated the same, by the substantial asset they are trying to represent, ETD and not the token itself representing then. |
| | (1) To what extent would recourse to contractual principles obviate the need for us to consider the lex situs rule? | N/A |
| | (2) Do permissioned networks and/or cases where there is clearly a contractual or hierarchical relationship between the parties represent the vast majority of DLT applications for digital assets and ETDs? | Yes. |
| | (3) Should we need to consider a new conflict of laws regime for property rights in digital assets and ETDs, what approach should we take to any new regime and what broader objectives of the conflict of laws should we keep in mind? Stakeholders may wish to refer back to Chapter 6 from paragraph 6.103. | Nothing further to add. |
| | (4) To what extent would recourse to a distinct rule based on the connecting factor of the “owner” or “transferor” for cases where parties have voluntarily dealt with one another obviate the need for us to consider further the application of the lex situs rule to cases where the | Nothing further to add. |

| | | |
|--|--|--|
| | parties to the dispute are strangers? | |
| | (5) In what circumstances could a rule based on the “owner” or “transferor” be satisfactorily used? Do creditors taking security over ETDs typically require, as a matter of contract, that the debtor warrants their title to grant the security interest? | We can only say that the we believe interfering in commercial question regarding instruments that are only digitized should remain at minimum. |
| | (6) To what extent is it 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”? | Not sure we understood the exact scenario. Would be happy to answer if further elaborated. |
| | (7) How should courts approach the question of applicable law in such disputes relating to decentralised digital assets held in permissionless DLT networks where the parties have not dealt with one another and there has been an “involuntary dispossession”? | Nothing further to add. |

Boaz Lessem

Chief Legal Regulation and Partnerships Officer

WAVE BL

Please feel free to contact me directly with any further enquires [REDACTED]