



## **Response: Law Commission Call for Evidence on Digital Assets**

**July 2021**

[www.fmlc.org](http://www.fmlc.org)

**Registered Charity Number: 1164902.**

"The FMLC" and "The Financial Markets Law Committee" are terms used to describe a committee appointed by Financial Markets Law Committee, a limited company ("FMLC" or "the Company"). Registered office: 8 Lothbury, London, EC2R 7HH. Registered in England and Wales. Company Registration Number: 8733443.

## Financial Markets Law Committee

### Working Group<sup>1</sup>

John Salmon (Chair)	Hogan Lovells International LLP
Diego Ballon Ossio	Clifford Chance LLP
Anne Bodley	Queen Mary University of London
Dorothy Delahunt	Delahunt and Associates
Jonathan Gilmour	Travers Smith LLP
Ben Kingsley	Slaughter and May
Ernest Lima	xReg Consulting
Matthew Nyman	CMS Cameron McKenna Nabarro Olswang LLP
Rosali Pretorius	Simmons & Simmons LLP
Bradley Rice	Ashurst LLP
Jason Rix	Allen & Overy LLP
Deborah Sabalot	Deborah A. Sabalot Regulatory Consulting
Adam Sanitt	Norton Rose Fulbright LLP
Sarah Smith	Dechert LLP
Julia Smithers Excell	White & Case LLP
Harriet Territt	Jones Day
Peter Werner	International Swaps & Derivatives Association
Brian Gray	FMLC Interim Chief Executive
Venessa Parekh	FMLC Research and Communications Manager
Katja Trela-Larsen	FMLC Researcher

---

<sup>1</sup> Note that Members act in a purely personal capacity. The names of the institutions that they ordinarily represent are given for information purposes only.

## TABLE OF CONTENTS

1.	INTRODUCTION AND BACKGROUND	4
2.	NOMENCLATURE	5
3.	A THIRD CATEGORY OF PROPERTY	11
4.	QUESTION ONE	13
5.	QUESTION TWO	19
6.	QUESTION THREE	21
7.	QUESTION FOUR	25
8.	QUESTION FIVE	26
9.	QUESTION SIX	28
10.	QUESTION SEVEN	31
11.	QUESTION EIGHT	36
12.	QUESTION NINE	39
13.	QUESTION 11	43
14.	QUESTION 12	46
15.	CONCLUSION	56

## 1. INTRODUCTION AND BACKGROUND

- 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, affecting the wholesale financial markets which might give rise to material risks and to consider how such issues should be addressed.
- 1.2. The Law Commission has undertaken to review the law of England and Wales and consider reforms to ensure that the law can accommodate digital assets (the “**Digital Assets Project**”). As a first step, the Law Commission has issued a Call for Evidence (the “**Call for Evidence**”).<sup>2</sup> The Digital Assets Project builds on the Legal Statement on the Status of Cryptoassets and Smart Contracts published in 2019 by the U.K. Jurisdiction Taskforce of the LawTech Delivery Panel (the “**UKJT**”) which concluded that virtual currencies have all the characteristics of property and any novel features—such as cryptographic authentication, decentralisation and rule by consensus—do not disqualify them from such categorisation.<sup>3</sup> The Digital Assets Project goes on to ask respondents to consider the implications of possible law reform. The Call for Evidence aims to identify how digital assets are used, treated, and dealt with by market participants; how the law might accommodate digital assets now, and in the future; and where the law might be inhibiting particular use cases, innovation, or development. The responses to the Call for Evidence will be used to inform future proposals for law reform.
- 1.3. The FMLC has previously considered the legal characterisation of digital assets. In a report published in 2016 (the “**2016 Report**”), the FMLC considered how to allocate virtual currencies to the traditional categories of property and personal rights developed by the common law (explored in further detail below).<sup>4</sup> Building on the 2016 Report, the FMLC has considered issues of legal uncertainty surrounding exchange tokens and the legal characterisation of initial coin offerings.<sup>5</sup>

---

<sup>2</sup> Law Commission, Digital Assets Call for Evidence (30 April 2021), available at: <https://www.lawcom.gov.uk/project/digital-assets/#digital-assets-call-for-evidence>

<sup>3</sup> UKJT, Legal Statement on cryptoassets and smart contracts (November 2019), available at: <https://technation.io/lawtechukpanel/>

<sup>4</sup> FMLC, Issues of Legal Uncertainty Arising in The Context of Virtual Currencies (July 2016), available at: [http://fmlc.org/wp-content/uploads/2018/03/virtual\\_currencies\\_paper\\_-\\_edited\\_january\\_2017.pdf](http://fmlc.org/wp-content/uploads/2018/03/virtual_currencies_paper_-_edited_january_2017.pdf)

<sup>5</sup> FMLC, Exchange Tokens: Issues of Legal Uncertainty (October 2019), available at: <http://fmlc.org/wp-content/uploads/2019/10/Exchange-Token-paper-FINAL-3.pdf>

FMLC, Initial Coin Offerings: Issues of Legal Uncertainty (July 2019) <http://fmlc.org/wp-content/uploads/2019/07/ICOs-paper.pdf>

- 1.4. This paper responds to the questions posed in the Call for Evidence.

## 2. NOMENCLATURE

- 2.1. It might be useful to consider, as a preliminary issue, the meaning and scope of the term “digital asset”. The Call for Evidence does not define the term “digital asset”, remarking that it uses the term broadly “to cover assets that are represented digitally or electronically, including cryptoassets”.<sup>6</sup> Without refinement, the term “digital asset” is an umbrella term that, as noted by the Law Commission, extends to a wide array of items of value, including social media accounts, online bank accounts, photography, software applications, databases, logos, illustrations, animations, audio-visual media, presentations, spreadsheets, cryptocurrencies and DLT tokens, digital paintings, electronic documents, electronic mail, and websites.<sup>7</sup> The term “digital asset” includes established and innovative technology, as well as established technology being used in wholly new ways for novel purposes.
- 2.2. The purpose and form of a digital asset will inform, to some extent, its treatment under English law. Any reflections on how digital assets may be dealt with under English law need to take into consideration the complex components of any particular asset. Given this, the Law Commission’s decision not to define the term “digital asset” in the Call for Evidence may give rise to unintentional legal complexities and ambiguities. Some forms of digital assets, for example, are already protected by existing laws and regulations, including intellectual property law and certain pieces of financial services legislation. For example, the much-debated question of whether digital assets are possessable is redundant in relation to online bank accounts held with U.K. banks supervised by the Prudential Regulation Authority and backed by the Financial Services Compensation Scheme. It could therefore be misleading to suggest that the law of England and Wales does not provide certainty on the legal status of “digital assets” as a whole. Rather, the degree of legal certainty depends on the nature of the digital asset itself.<sup>8</sup> The term is also so broad so as potentially include dematerialised securities, such

---

<sup>6</sup> Paragraphs 1.5 and 1.20 of the Call for Evidence, see footnote 2.

<sup>7</sup> See Betsy Simmons Hannibal, *What Are "Digital Assets"?* (accessed 8 July 2021), available at: <https://www.nolo.com/legal-encyclopedia/what-are-digital-assets.html>

<sup>8</sup> A wider approach has been adopted by other commentators. Business Telegraph defines digital assets as “anything that exists in binary data which is self-contained, uniquely identifiable, and has a value or ability to use”. (See Business Telegraph, *What are Digital Assets?—Securities.io* (5 March 2020), available at: <https://www.businesstelegraph.co.uk/what-are-digital-assets-securities-io/>)The American advocacy group, the Chamber of Digital Commerce, uses the term in a far narrower context: “...the term "digital asset" refers to an asset that is issued

that any law reform which is not more specific could cause conflict with the existing legislative framework governing securities, increasing uncertainty.<sup>9</sup>

- 2.3. By contrast, the UKJT Legal Statement on Cryptoassets and Smart Contracts (the “**Legal Statement**”) is narrowly focused on a sub-class of digital assets—i.e., cryptoassets—that possess the following attributes: (a) intangibility; (b) cryptographic authentication; (c) use of a distributed transaction ledger; (d) decentralisation; and (e) rule by consensus.<sup>10</sup> These distinctive component parts describe the value arc enjoyed by the user; if any one feature were missing, this value arc would change significantly. The UKJT further observes that cryptoassets:

...can in that respect be contrasted with other digital assets, such as databases or digital photographs or computer programmes...<sup>11</sup>

Upon reviewing the existing body of case law on personal property, the UKJT concludes “cryptoassets are therefore to be treated in principle as property”.<sup>12</sup>

The Call for Evidence is based heavily on the UKJT’s Legal Statement.<sup>13</sup> It is important, however, to note that the UKJT’s analysis was restricted to cryptoassets, distributed ledger technology, and smart contracts, which form, as described above, a small subset of the larger group of digital assets.

- 2.4. It would seem to follow that, insofar as a digital asset’s technical features, or combination of technical features, are unique, each technical feature or combination of factors carries implications for the asset’s legal and proprietary status. For example, one could view a Bitcoin created within a peer-to-peer, permissionless system as a part of a collectivised or co-operative ownership: its value derives from every transaction that came before it, and the legitimacy of its “block” determines the viability of all the

---

and/or transferred using distributed ledger or blockchain technology ..., including, but not limited to, so-called “virtual currencies,” “coins,” and “tokens.” See also Ms. Vanessa A. Countryman Secretary Securities and Exchange Commission, Email Re: File No. 87-25-20; Custody of Digital Asset Securities by Special Purpose Broker-Dealers (Release No. 34-90788) (5 April 2021) available at: <https://www.sec.gov/comments/s7-25-20/s72520-8634796-230930.pdf>

<sup>9</sup> For example, ssecurities would be subject to regulation under Directive 2014/65/EU on markets in financial instruments (“MiFID II”). Financial instruments covered by MiFID II are also subject to Regulation (EU) No 909/2014 on improving securities settlement in the European Union and on central securities depositories (“CSDR”) and Regulation (EU) No 648/2012 on OTC derivatives, central counterparties and trade repositories (“EMIR”).

<sup>10</sup> See footnote 3.

<sup>11</sup> Paragraph 61 of the Legal Statement, see footnote 3.

<sup>12</sup> Paragraph 15(d) of the Legal Statement, see footnote 3.

<sup>13</sup> Paragraphs 1.17 to 1.20 of the Call for Evidence, see footnote 2.

transactions that follow it (if any). No one individual or entity controls the platform, yet all participants, and the processes they perform, are co-dependent. To abstract technology, or the lack of it, from this undertaking could potentially confuse the existing state of the law, as well as stakeholders and market participants. Extrapolating the UKJT's narrow conclusion to digital assets in the broadest sense of the term is therefore likely to give rise to impractical consequences, including legal uncertainty for financial markets participants as well as creators and consumers of digital assets.<sup>14</sup>

- 2.5. Given this risk, for the purposes of this paper, the term “digital asset” has been used to refer solely to what have come to be known as “cryptoassets” in the sense used by the Legal Statement. In the FMLC's view, the truly novel legal questions which are best addressed by the Call for Evidence relate to such cryptoassets rather than digital assets in the broadest sense. The latter have generally been assimilated to existing legal concepts and/or been the subject of existing legislation whereas the former lay genuine claim to be *sui generis* as outlined in paragraph 5.3 below. That said, there is still a wide variety of types of asset within this sub-category and there have been a number of attempts by regulators to define and classify them.

#### *The FCA*

- 2.6. The Financial Conduct Authority (“FCA”) classifies tokens into regulated and unregulated tokens. Within the ambit of regulated tokens are: (a) security tokens, which are tokens that amount to Specified Investments under the Financial Services and Markets Act 2000 (Regulated Activities) Order 2001 (the “RAO”), and may also be deemed transferable securities or other financial instruments under Directive 2014/65/EU on markets in financial instruments (“MiFID II”); and (b) E-money tokens which are tokens that meet the definition of e-money under the Electronic Money Regulations 2011.
- 2.7. Unregulated tokens by comparison are tokens which are neither security tokens nor e-money tokens. This includes (a) utility tokens which can be redeemed for access to a specific product or service that is typically provided using a Distributed Ledger Technology (“DLT”) platform; and (b) exchange tokens such as Bitcoin and Litecoin

---

<sup>14</sup> It is also possible that this conflation between a legal rationale for cryptoassets and digital assets more broadly stems from the proximity of the Law Commission's electronic trade documents project. The FMLC observes that while electronic trade documents are a class of digital asset, there are analytically distinct from those digital assets that possess all of the characteristics listed by the UKJT.

See Law Commission, Consultation Paper No 25: Electronic Trade Documents (2021), available at: <https://www.lawcom.gov.uk/project/electronic-trade-documents/>

which are decentralised and designed to be used primarily as a medium of exchange.

### *HM Treasury*

- 2.8. In HM Treasury’s consultation and call for evidence on cryptoassets and stablecoins the term “token” is used interchangeably with “cryptoasset”.<sup>15</sup> HM Treasury largely follows the classification of tokens set out by the FCA although it recognises the need for a new category of regulated tokens: stable tokens. The regulated category of stable tokens would refer to tokens which stabilise their value by reference to one or more assets, such as fiat currency or a commodity and could therefore be reliably used as a store of value. In defining stable tokens, HM Treasury recognised that whilst stable tokens are typically underpinned by DLT, they could also be underpinned by other types of technology. On this basis the definition aims to be neutral to the technology underpinning its use.

### *E.U. Proposal for a Markets in Cryptoassets Regulation*

- 2.9. The E.U.’s Proposal for a Regulation on Markets in Cryptoassets (“**MiCA**”) introduces 28 cryptoasset related definitions. MiCA defines cryptoassets as

a digital representation of value or rights which may be transferred and stored electronically, using distributed ledger technology or similar technology

### *Basel Committee on Banking Supervision*

- 2.10. The Basel Committee issued a Consultative Document on the prudential treatment of cryptoasset exposures.<sup>16</sup> The Consultative Document proposed a classification system that divides cryptoassets into three broad categories: (a) tokenised traditional assets such as derivatives; (b) cryptoassets with a stabilisation mechanism/underlying traditional assets; and (c) cryptoassets that do not fall within (a) or (b) such as Bitcoin.

### *Financial Action Task Force*

- 2.11. Cryptoassets (or “virtual assets”, as they are referred to by the Financial Action Task Force (“**FATF**”)) are defined as any digital representation of value that can be digitally

---

<sup>15</sup> HM Treasury, *UK regulatory approach to cryptoassets and stablecoins: Consultation and call for evidence*, (6 January 2021), available at: [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/950206/HM\\_Treasury\\_Cryptoasset\\_and\\_Stablecoin\\_consultation.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/950206/HM_Treasury_Cryptoasset_and_Stablecoin_consultation.pdf).

<sup>16</sup> Basel Committee on Banking Supervision, *Consultative Document: Prudential treatment of cryptoasset exposures*, (June 2021), available at: <https://www.bis.org/bcbs/publ/d519.pdf>



traded transferred or used for payments but does not include digital representation of fiat currencies.

2.12. The FMLC recommends that the Law Commission take into consideration the definitions proposed by these authorities but that it should seek to create narrower, more focused definitions of cryptoassets when recommending legal reform.<sup>17</sup> This is integral to providing market participants with the legal certainty that the markets require. All-encompassing wording such as that found in MiCA, which refers to “...or similar technology”, can be confusing. It is important that the Law Commission clearly and accurately defines the subject of its examination and recommendation even if that should result in comparatively narrow definitions. The FMLC considered the risk of technology outpacing the legislative definition of cryptoassets, if a narrower range of definitions were adopted. It concluded, however, that the risk of legal uncertainties owing to wide, inaccurate definitions is greater and that, ultimately, the definitions could be reviewed and updated if necessary in the future.

2.13. Turning, again, to the subject of this paper, it is important to note that digital assets which are “cryptoassets” may range from those used as a means of payment to those which may be redeemed for access to a specific product, service or right that is typically provided using a DLT platform, or those representing fungible and tradable assets or utilities that reside on their own DLT systems, or those recording ownership of a digital item.<sup>18</sup> Within this range of cryptoassets, the legal analysis will also differ when considering a digital asset which: (1) only exists in digital form and has no real-world counterpart (for example, a bitcoin) (herein referred to as a “**Digital Only Asset**”); (2) is a direct digital representation of a “real-world” asset (for example, a 1:1 digital asset representing a single company share) (herein referred to as a “**Real-world Digital Asset**”); or (3) is a digital asset which is referable to a real-world asset but is not a 1:1 representation of that asset (such as a 1/100<sup>th</sup> fractionalised ownership share in a painting) (herein referred to as a “**Referable Digital Asset**”). In particular, for the latter two categories, in addition to the legal framework applicable to digital assets, it will be

---

<sup>17</sup> Part of the FMLC’s response to the European Commission’s Consultation on MiCA considered the classification of cryptoassets based on their function, including how the underlying technology may affect the resulting characteristics. The response also considered whether a cryptoasset is the asset or is merely evidence of a legal right or claim to an asset and analysis of means of holding and transfer of cryptoassets. See FMLC, Response to European Commission Consultation: Framework for Markets in Cryptoassets (17 March 2020), available at: [http://fmlc.org/wp-content/uploads/2020/03/FMLC\\_UP\\_11706611\\_v\\_1\\_Part-I-Response-to-EC-Consultation-on-regulating-cryptoassets-taxonomy.pdf](http://fmlc.org/wp-content/uploads/2020/03/FMLC_UP_11706611_v_1_Part-I-Response-to-EC-Consultation-on-regulating-cryptoassets-taxonomy.pdf)

<sup>18</sup> Blockchain is a specific application of a technology known as Distributed Ledger Technology (“DLT”)—a virtual system that relies on peer-to-peer networking, distributed data storage, and cryptography. For that purpose, this paper consistently refers to DLT.

necessary to consider whether any proprietary or contractual interest in the underlying real-world asset is valid, binding and enforceable against third parties. In the case of Real-world Digital Assets, it will normally be important for the rights and obligations attaching to both the underlying asset and the related cryptoasset to be identical or at least substantially similar so that the two interests can move “hand in hand”. This is particularly the case when the underlying asset—such as securities—is itself subject to its own legal regime or legal requirements. In this case, it is important that any new regime for digital assets does not overcome or somehow replace those existing legal requirements simply as a result of the underlying asset being tokenised. In contrast, Referable Digital Assets will essentially represent divisible interests in a single underlying asset (such as a share), which may not have been envisaged to be divisible, and where there is no such expectation of equivalent rights and obligations as between the real-world asset and its digital representation.

- 2.14. Finally, it is also important to reference or otherwise distinguish between the different elements which together may either comprise a digital asset or, more likely, are required to access, transfer or otherwise control a digital asset. As a high-level summary, current cryptoasset technologies typically require some combination of the following elements: a wallet (which itself can be desktop, hardware, online or just a piece of paper); a wallet address; a public key; and a private key. Each element is addressed in more detail below.

### *Wallet*

- 2.15. A wallet is a means of holding the collection of addresses and information necessary to receive, access or transfer digital assets. It is important to note that the wallet itself does not hold the digital assets (for example, if a wallet is lost or destroyed, but the information contained in it is accessible by other means, the digital asset can still be accessed and transferred by the owner), but the wallet is the primary means of storing the information necessary to control and deal with the underlying asset.<sup>19</sup> The wallet also stores a separate log of all incoming and outgoing transactions. Every transaction linked to a wallet address will be stored by the wallet to give users an overview of their

---

<sup>19</sup> There are a number of possible variations of “wallets”. At its most basic, a wallet could be a piece of paper with the relevant information written down or a USB key with the information recorded in a document stored on that key. More securely, and increasingly common, are software or mobile app “wallets” that store the relevant information locally on the computer or device running the relevant program and which interface directly with the relevant ledger on which the digital assets are stored. A further variation is an online wallet that can be accessed via a webpage, but which does not store the underlying information on the device used to access that page. Hardware wallets are typically separate, physical devices that must be plugged into a computer or connected to another system. Once connected, the information contained on the wallet is not visible to the user but can be used to automatically approve and execute digital asset transactions.

spending and receiving habits.

#### *Wallet address*

- 2.16. The wallet address is a randomly generated set of alphanumeric characters, often (but not always) a one-time link generated by a wallet. The wallet address is used to send or receive digital assets and can be freely shared with third parties for these purposes. Both the public and private key are needed to create a wallet address.

#### *Public key*

- 2.17. The public key is used to ensure that a person who is the owner of a wallet address can receive funds. This can cause some confusion as it is sometimes assumed that a wallet address and the public key are the same. That is not the case, although they are mathematically related. A wallet address is a hashed version of the relevant public key.<sup>20</sup>

#### *Private key*

- 2.18. Finally, there is a private key, which is normally the most critical element required to own, possess, or transfer digital assets. In the same way as the public key and the wallet address, the private key is a randomly-generated alphanumeric string used to verify access to and control or transfer the relevant digital asset. A private key is always mathematically related to the wallet address and public key but is thought to be impracticable to reverse engineer using current technologies due to the nature of encryption.

### **3. A THIRD CATEGORY OF PROPERTY**

- 3.1. Some background comment on the understanding of “property” under common law may help to frame the analysis below. Personal property has traditionally been divided into two broad categories—(1) things in possession and (2) things in action—with the assumption that all things must fall within one or other of the two categories.<sup>21</sup> As the Law Commission acknowledges in its related consultation on electronic trade documents, it was logical in the past for the law to assume that only physical or tangible

---

<sup>20</sup> A hash is similar to a one-way algorithm which encodes a message in an output of predetermined and unvarying size.

<sup>21</sup> This was considered in *Colonial Bank v Whinney* (1885) 30 Ch D 261 at 285, referring to Sir William Blackstone, Commentaries on the Laws of England (vol 2) p 389. Fry LJ said: “All personal things are either in possession or action. The law knows no tertium quid [“third thing”] between the two”.

things could be possessed.<sup>22</sup> The UKJT Legal Statement concluded that a cryptoasset cannot be a "thing in possession"—because it is intangible and cannot be physically possessed—and does not easily sit within the definition of a "thing in action"—a term generally used to mean a right of property that can be enforced by way of legal action, but which has also been used more broadly as a catch-all for any property that is not a thing in possession.<sup>23</sup> Developments in technology may have already moved beyond this traditional assumption and therefore, as the UKJT concluded, cryptoassets are not precluded from being treated as property even if they are not characterised as a thing in possession or a thing in action on a narrow definition.

- 3.2. The Call for Evidence recognises that uncertainty remains as to whether a third category of property, separate from a thing in possession and a thing in action exists and, if it does, how that category should be defined. As mentioned above, the FMLC's 2016 Report considered this question in relation to cryptocurrencies<sup>24</sup>. It concluded that, if a choice must be made as to whether cryptocurrencies are a thing in possession or a thing in action, the legal uncertainty arising if virtual currencies are classified as things in action is likely on balance to be greater than if they are acknowledged to share the essential characteristics of things in possession. However, given that some digital assets, at least, share certain characteristics of both intangible property and things in possession, the 2016 Report suggested there is an argument for acknowledging the new reality of the digital world and extending the traditional legal categories to a third type of property. The 2016 Report proposed recognising a kind of hybrid: "virtual choses in possession"; that is, intangible property with the essential characteristics of things in possession.
- 3.3. That a digital asset cannot be categorised within the existing common law understanding of property as a thing in possession or a thing in action should not, however, preclude it from being treated as property and enjoying property rights under English Law. To address this, the FMLC proposes the creation of a third category of personal property which addresses the distinct attributes of digital assets (the "**Third Category**"). A more detailed look at this proposal is set out in the answer to question two, below.
- 3.4. The parameters around and characterisation of the Third Category, for the purposes of

---

<sup>22</sup> Law Commission Consultation Paper No 25: Electronic Trade Documents (2021), available at: <https://www.lawcom.gov.uk/project/electronic-trade-documents/>

<sup>23</sup> See footnote 3.

<sup>24</sup> FMLC considers that its views on this question in its 2016 Report in relation to cryptocurrencies (see footnote 4) apply equally to the broader class of digital assets as defined in this paper.

this paper, have yet to be set and potentially open fundamental questions that would need considerable exploration.<sup>25</sup> A key consideration is the pace of change and technological advancement. To accommodate this, any change in the law should not only be technology-neutral but should assume that the technological means of creating, storing, and transferring digital assets will continue to develop beyond current concepts. Any change in the law around digital assets therefore needs to be designed to remain "fit for purpose".

#### 4. QUESTION ONE

4.1. Question one of the Call for Evidence asks what the legal or practical implications would be if digital assets were possessable under the law of England and Wales. As it is generally and increasingly accepted that digital assets constitute property under English law<sup>26</sup>, the potential classification of digital assets as a thing in possession would go to the precise nature of that property, not to the essential question of whether digital assets are property at all. The classification of digital assets as possessable would embed the treatment of digital assets as personal property under English law. However, careful consideration would need to be given to some of the practical issues outlined in this paper.

4.2. Even if the Law Commission concludes that Digital Only Assets, such as cryptocurrencies, should not be considered possessable, the FMLC considers that it could significantly reduce legal uncertainty if Real-world Digital Assets were classified as possessable, in the same way as the underlying real-world tangible asset to which the digital asset refers. This would avoid a situation in which the Real-world Digital Asset could be subject to a different regime in respect of (for example) transfer by delivery or be the subject of a possessory lien, whereas the digital representation would have to be the subject of a legal or equitable assignment for an effective transfer to take place and could not be the subject of a lien. There is also a clear and direct link between the Real-

---

<sup>25</sup> The City of London Law Society has made a similar observation. See: Financial Law Committee of the City of London Law Society, Response to the consultation, dated 9 May 2019, by the UK Jurisdiction Taskforce of the LawTech Delivery Panel in relation to cryptoassets, distributed ledger technology and smart contracts (June 2019), available at: <https://www.citysolicitors.org.uk/storage/2019/06/Financial-Law-Committee-response-Personal-Property-20-06-19.pdf>

<sup>26</sup> As discussed above, this is set out in the UKJT Legal Statement (see footnote 3) and subsequently approved/adopted by the English courts in a limited number of cases: *AA v Persons Unknown* [2019] EWHC 3556 (Comm), [2020] 4 WLR 35 (High Court of England and Wales), *Robertson v Persons Unknown* (15 July 2019, unreported) (High Court of England and Wales) and *Ion Science Ltd and Duncan Johns v Persons Unknown* (21 December 2020, unreported) (High Court of England and Wales).

world Digital Asset and the underlying real-world asset which makes the arguments in favour of treating such assets as possessable even stronger.

- 4.3. Nevertheless, the consequences of digital assets being characterised as possessable/personal property should not be underestimated.<sup>27</sup> The general range of issues that could be implicated include:
- a) availability of security rights over digital assets;
  - b) rights relating to succession and inheritance of digital assets;
  - c) impact on limitation;
  - d) tax consequences; and
  - e) accounting treatment – including depreciation.

#### **Elements of digital asset technologies**

- 4.4. As explained in paragraphs 2.14 to 2.18, current digital asset technologies typically require some combination of a wallet, a wallet address, a public key and a private key. The question arises whether any of these elements is an essential aspect of a possessable digital asset. Each of these elements has a different role in the creation, storage or transfer of digital assets, and each can be separately characterised as possessable in its own right. For example, a person may have physical possession of a hardware wallet, which is plainly recognised as property. If the user cannot access the digital asset (the code or bytes accessible via the wallet) without the physical wallet, there appears to be a strong argument that the relevant digital asset cannot be separated from the physical form of the wallet and should be considered possessable in that particular case.<sup>28</sup> Other wallets may be virtual only; the determination of their possessability should turn on fundamental characteristics of ownership rights and control, independent of rights attaching to a physical wallet. The wallet address is one step further removed as a storage space for the wallet, which is no longer a physical asset but a dematerialised “signature”. In the same way, a public key is part of an encrypted address and may be held/possessed by any number of people whereas the private key is presumably

---

<sup>27</sup> c.f. Dr. Joanna Benjamin, *Financial Law*, Chapter 21, “The adaptation of property rights in the Financial Markets” (Oxford University Press, 2007).

<sup>28</sup> This notwithstanding, the Committee acknowledges that, even in this case, it is normal to have recovery mechanisms for hardware wallets (typically a backup recovery code or “seed phrase”) which allow the wallet to be reconstituted (although typically this requires the wallet to be reconstituted on a similar physical device).

possessed only by the “owner/holder” of the asset. Even in this situation, the use of “multi-signature” wallets can require the creation and use of two or more private keys to sign and approve a transaction and/or multiple cryptographic signatures to access the relevant wallet, as discussed below, so that the possession of a single private key may still not be determinative of ownership or control of the relevant asset.

- 4.5. Each of the elements is a typical part of holding, owning, transferring or otherwise controlling digital assets, and each element is capable of taking multiple physical forms as well as digital-only forms. Any change in the law relating to the nature of digital assets will need to be drafted in such a way as to take account of these (potentially independently possessable) elements but in a way that is also sufficiently independent of the definitions of each element identified below.

### **Control**

- 4.6. Control of each of these elements is an observable fact which may indicate or evidence the owner of a digital asset, but control is not necessarily determinative of ownership—keys may be stolen, wallets may be hacked, etc.<sup>29</sup> It is important that the definition of a “digital asset” is not limited in practice to the approach taken by current technological systems. In addition, it will be critical that elements that are needed to control the digital asset (such as the private key, the wallet, or the wallet address) are not conflated with the underlying digital asset itself.
- 4.7. The complexity of drafting a law which separates an underlying digital asset from the possessable elements needed to create, hold or transfer such assets in a technology-neutral way should be balanced against the potential benefits of such a law. Stakeholders have raised the growing market for crypto-custody services, whereby a party may offer various kinds of storage arrangements for digital assets and/or one or more private keys as a service to customers. These crypto-custody services are useful to market participants that do not have the technical capability or infrastructure to hold digital assets directly and, further, can provide an added layer of security against theft or the diversion of digital assets.
- 4.8. Even in this niche (but growing) market, the traditional financial market concept of “holding assets” in the context of custody or “possessability” may need to be reconsidered and redefined for digital assets. The FCA’s regulatory regime for the safe

---

<sup>29</sup> The UKJT observes at paragraph 28 that “Knowledge of the private key confers practical control over the asset”, see footnote 3.

custody of assets, set out in the Client Assets Sourcebook (“**CASS**”), is designed to ensure that a regulated firm must introduce adequate organisational arrangements to minimise the risk of the loss or diminution of clients' safe custody assets, or the rights in connection with those safe custody assets, as a result of the misuse of the assets, fraud, poor administration, inadequate record-keeping or negligence when held by the firm.<sup>30</sup> Some of those CASS principles are very relevant to digital assets; in particular, the risk of fraud or theft has led to the development of so-called cold storage solutions which are entirely offline and disconnected from the internet, limiting the risk of a wallet hack, but others are far less relevant. There is also a generally accepted structure for safe custody of different classes of financial assets, whereas stakeholders report the structure of crypto-custody implementations to be more varied.

- 4.9. Where a digital asset is placed with a crypto-custody service, typically the ownership of the asset does not typically change but all of the above elements may—the wallet, wallet address and public key may all be moved to the custody and control of a crypto-custody provider (and the private key will also often be within the control of the crypto-custody provider). In this situation, the owner of the asset is protected by contract but in practice has limited non-contractual control of the asset. The Committee notes that the German implementation of Directive (EU) 2018/843 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives (known as the “**Fifth Money Laundering Directive**”) has defined crypto-custody as:

the safekeeping, administration and safeguarding of crypto assets or private cryptographic keys used to hold, store or transfer crypto assets for others.<sup>31</sup> (emphasis added)

- 4.10. In addition, the advice on cryptoassets the European Securities and Markets Authority (“**ESMA**”) published in January 2019 states that:

having control of private keys on behalf of clients could be the equivalent to custody/safekeeping services, and the existing [regulatory] requirements should apply to the providers of those

---

<sup>30</sup> FCA, FCA Handbook, CASS 6.2.2, available at: <https://www.handbook.fca.org.uk/handbook/CASS/6/2.html>

<sup>31</sup> BAFIN, *Guidance notice – guidelines concerning the statutory definition of crypto custody business (section 1 (1a) sentence 2 no. 6 of the German Banking Act (Kreditwesengesetz – KWG)*, (2 March 2020), available at: [https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Merkblatt/mb\\_200302\\_kryptoverwahrgeschaef\\_en.html](https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Merkblatt/mb_200302_kryptoverwahrgeschaef_en.html).



services.<sup>32</sup>

Both of these guidance notes effectively equate custody of digital assets to the holding and storage of private keys. The FMLC would caution that this approach may reflect current practices in the non-institutional markets, but crypto-custody solutions are rapidly developing and, in particular, there are increasing number of services which allow owners to retain private keys and/or require multiple approvals (for example, from custody provider and asset owner) before assets are transferred or moved out of custody. This emerging complexity is an additional reason why the control of the elements cited above is a relevant factor in establishing ownership but not determinative (on a case-by-case basis).

#### **Legal and practical consequences of classifying digital assets as "possessable"**

- 4.11. Turning to the Law Commission's main question, the Call for Evidence document already addresses a number of specific legal/practical consequences of classifying digital assets by statute as "possessable". The FMLC has set out below some further general comments on the legal and practical impact, and on those specific issues (such as creation of security interests and conversion) which will follow.
- 4.12. The issue of whether a particular digital asset is a thing in possession or a thing in action typically arises in the context of taking security over the asset, or within crypto-trading and crypto-storage projects—when digital assets are held by and potentially controlled by third parties to the owner—and when considering insolvency risk. As discussed further below, an example of a project where the classification of a relevant asset would be material would be the taking of security over a digital-only artwork or digital asset representing a real-world artwork. There are certain types of English law security interests which are typically only created over things in possession because they involve the transfer of physical possession of the asset, which is seen as impossible to do with a thing in action. In particular, an English law pledge involves the actual or constructive delivery of possession of a physical asset as security until payment. While ownership remains with the pledgor, the pledge confers a power of sale (in the event of default) for the pledgee. In a similar way, a lien (whether a legal or statutory lien) arises out of a creditor's right to retain possession of a debtor's property until the debt has been repaid. Such liens provide a passive right to retain the property, and deprive the debtor of it, but

---

<sup>32</sup> ESMA, Advice: Initial coin offerings and crypto-assets (January 2019), available at: <https://www.esma.europa.eu/press-news/esma-news/crypto-assets-need-common-eu-wide-approach-ensure-investor-protection>

do not give the creditor the right to sell the property and use the proceeds of sale to pay the outstanding debt.

- 4.13. An exception to the general position that a pledge or lien can only be taken over a thing in possession exists. It is possible for a pledge or lien to be created over a thing in action which is represented by a document which, if transferred, transfers title to the asset—for example, a bearer bond or promissory note. The Court of Appeal has considered whether it is possible for a possessory lien to be created over an intangible asset such as a database in *Your Response Ltd v Datateam Business Media Ltd*.<sup>33</sup> In concluding that it could not,<sup>34</sup> the Appeal judges rejected four arguments in support of the extension of the scope of a possessory lien to the content of databases, including an argument that such intangible assets should be considered as a “third class of thing” (labelled, an “intangible chose in possession”) in just the same way as the UKJT—and the FMLC’s 2016 Report—has suggested.<sup>35</sup> In his judgment, Moore-Bick LJ acknowledged that an extension of the law of possessory liens to intangible objects would be a matter for Parliament. This decision, in combination with the risk that a higher court might not follow the approach of current case law in relation to digital assets—and the Legal Statement in considering digital assets as “property”—weighs in favour of a change in the law to make the position clear.
- 4.14. One potential consequence of a reclassification of digital assets as possessable is that it would be legally possible to pledge or subject such assets to a lien. Practical issues would still arise in terms of establishing a sufficient process to deliver the asset to the creditor and perfect the pledge or lien, but these issues could be overcome from a technical perspective and on a case-by-case basis. Other practical issues remain—including considerations around what elements (listed in paragraph 2.14) a holder would have to “possess” in order to be able to grant a possessory lien over a digital asset. It is possible that the answer as to the key component underlying the grant of such a lien differs, depending upon the nature of the digital asset.

---

<sup>33</sup> [2014] EWCA Civ 281.

<sup>34</sup> This position may be distinguished from *Armstrong DLW GmbH v Winnington Networks Ltd* [2012] EWHC 10 (Ch), [2013] Ch 156 [58], [94] (Stephen Morris QC) where it was noted:

An EU emissions allowance could be intangible personal property (not necessarily a chose in action and not a chose in possession), in respect of which a proprietary claim may be brought.

<sup>35</sup> The FMLC 2016 Report also suggested that it might be useful to understand virtual currencies as “virtual choses in possession”, i.e., intangible property with the essential characteristics of choses in possession. See footnote 4 and further analysis set out in section three and the response to question two, below.

- 4.15. Granting security interests over digital assets is likely to be the most important (and difficult) issue for market participants raised in the Call for Evidence. While it is possible for other forms of English law security to be created over digital assets, including mortgages and legal or equitable charges, these forms of security may not be available or suitable for all types of digital asset. More detail is given in relation to this point below in the response to question nine of the Call for Evidence.
- 4.16. A change in the law expressly to provide that digital assets are “possessable”, therefore, could provide an incremental further benefit in terms of certainty and confidence in the treatment of such assets under English law. The market for developing and engaging in digital asset businesses is inherently cross-border and, subject to the form of asset, not required to be located in the local jurisdiction where the digital assets are made available. The classification of digital assets as “possessable” under English law would provide more certainty and confidence in the treatment of such assets for market participants. As digital asset classes develop and become more common—and in the event digital asset systems become the primary means of transacting in a particular asset class—the classification of such assets as possessable is likely to become more important.
- 4.17. As noted above, there are other potential consequences of the characterisation of digital assets as possessable, including their treatment under tax, inheritance and criminal law. Each of these aspects will need to be thought through carefully so as to avoid unintended consequences.

## **5. QUESTION TWO**

- 5.1. Question two of the Call for Evidence considers whether the transfer of a digital asset is more analogous to a transfer of a thing in possession, such as cash, or a transfer of a thing in action, such as bank money, and whether a different analysis should apply for different types of digital assets (including the various subsets of digital assets) or methods of transfer. In order to address the inability for digital assets to be easily categorised as a thing in possession or a thing in action, as explained in section three above, the FMLC proposes the creation of a Third Category of personal property which addresses the distinct attributes of digital assets.
- 5.2. Despite this analysis of digital assets as a Third Category of property separate from both things in action and things in possession, the introduction of a legal concept analogous

to possession applying to digital assets would allow them to be treated analogously to things in possession where, and to the extent, appropriate. While those digital assets that are controlled by an individual entity or group, by virtue of a contractual arrangement to which all affected are party,<sup>36</sup> may be analysed using traditional contractual concepts, different analysis is needed for Digital-Only Assets that are subject to a cryptographically secure decentralised consensus mechanism.<sup>37</sup> In this context, a transfer of a thing in possession provides a closer analogy than a transfer of a thing in action.

- 5.3. The key distinction is not between assets that are tangible and assets that are intangible, but between assets that have a purely legal existence and assets that have an existence independent of any law. The concept of possession applied to a thing in possession is a means of accommodating the non-legal facts that apply to it: for instance, that it is *somewhere* in the world and *somebody* has it. A similar concept is needed for digital assets. It may be noted that no legal rule can on its own create or destroy a digital asset independent of the underlying facts; no court decision can say that it has ceased to exist. Contrast this with an online bank account—which may seem superficially similar to a cryptocurrency account. A court can hold that a balance in a bank account is zero—that is, the debt owed by the bank should cease to exist—irrespective of any password or bank security. The debt owed by the bank is a thing in action which the court can extinguish. If the bank fails to change its records, then its records are wrong. However, if a digital asset provider records an account on its DLT system, then that digital asset exists on the DLT system and no court decision can destroy it—although courts might decide, for instance, who legally owns it.
- 5.4. Similarly, a transfer of possession of a physical object can be accomplished by moving it from one person to another person. The courts have considered this in numerous contexts so as to allow for the fundamental reality that physical objects can move from place to place. Things in action can move from one place only to the extent that the law specifically allows it. Absent compliance with a legal rule, a thing in action cannot be transferred, irrespective of any facts in the real world. By contract, a digital asset can be moved from one account, address or wallet to another account, address or wallet, irrespective of legal rights. Whether this is characterised in law as a deletion followed by the creation of a new asset or a transfer (discussed below in the response to question

---

<sup>36</sup> Hyperledger Fabric is an example of a private DLT system where all participants are known and permissioned.

<sup>37</sup> The “consensus mechanism” is the method of authenticating and validating a value or transaction on a DLT system without the need to trust or rely on a central authority.

four), legal rules must accommodate the reality that a change in account balances has taken place. Dwelling on whether a digital asset has moved or been deleted and recreated misses the point—the law must cater for the fact that a digital asset is in a different place, however it got there and whether or not its identity is the same. Whether a digital asset has moved or been replaced is a factual question. It is the fact that a digital asset can move or be replaced, without legal intervention, which suggests it should be seen as analogous to a thing in possession rather than a thing in action.

- 5.5. The consequences that flow from this treatment of digital assets affect security, bailment and insolvency, amongst other areas; these are dealt with further below. Generally speaking, the FMLC’s proposal of a Third Category of property needs to be considered in respect of not only Digital Only Assets, but also when creating Real-world Digital Assets or Referable Digital Assets where the underlying asset may be categorised as a thing in possession (or as a thing in action). An example may be when tokenising interests in shares which are held via a central security depository. In particular, the Committee would suggest that the Law Commission should specifically consider the potential impact of its proposals on existing legal and regulatory regimes that may already apply to the underlying asset in respect of Real-world Digital Assets, as this seems to us to have the greatest risk of unforeseen consequences and/or impacts on existing legal requirements.

## **6. QUESTION THREE**

- 6.1. Question three of the Call for Evidence asks whether there are practical circumstances in which it would be useful to distinguish, or to separate, the ownership and the possession of a digital asset, particularly in relation to transfers; whether such circumstances arise on-chain and/or off chain for digital assets; and whether other technical or practical solutions or market practice make these distinctions less important.
- 6.2. To be things in possession, digital assets need to be capable of being possessed. Corporeal objects satisfy the core criteria which are hallmarks of possession: one or more persons have the ability to hold, transfer and destroy them to the exclusion of others. Digital assets do not, however, have a physical manifestation. They are intangible and incorporeal: a digital asset’s existence in any meaningful sense is evidenced by the combination of its public and private keys.
- 6.3. Arguments against treating digital assets as things in possession include that they consist

solely of information—digital assets are essentially just unique bits of data recorded on a specific DLT protocol (used by nodes to establish communication with one another). Bitcoins, for example, are essentially rewards for operating nodes on the Bitcoin DLT that have helped to ensure the accuracy and permanence of the record of all transactions on that DLT system.

- 6.4. Even if digital assets were “merely” information, however, they are qualitatively different from other generic forms of information which can easily be shared among many people, forgotten, or corrupted. Data on DLT systems is distinguishable in its immutability and permanence, as well as often carrying a high degree of reliability and transparency.<sup>38</sup> These characteristics make DLT data in the form of digital assets susceptible to differential treatment for legal purposes. Of particular relevance to their legal characterisation is that DLT data in the form of digital assets is typically controlled to the exclusion of others by the holder(s) of the private key for the digital asset. Digital assets can be sold and (in some cases) destroyed, characteristics already considered indicative of ownership at law. Unlike cash in the form of coins and notes, digital assets are not readily accessible. Rather, as with bank money, combinations of public and private information are required for access.<sup>39</sup>
- 6.5. Many crypto-custodians offer similar services: the public key is a bit like bank account details; and gives one “view access” to the “wallet” (in this instance the updated record of all transactions related to the digital assets associated with the relevant public key). To access the wallet for transactional purposes, a pair of keys—both a public and a private key—is needed. The keys depend on public key cryptography. The public and the private key are linked, so it is possible to create public keys from the private key, but not vice versa. The private key functions like a digital signature. To control digital assets, the holder needs access to the private key for those specific digital assets.
- 6.6. Practice varies hugely in relation to private keys. “Hot wallets” refer to keys stored online. These are susceptible to hacking and generally not considered secure. “Cold wallets” are offline digital records. Some custodians offer old fashioned solutions to

---

<sup>38</sup> The immutability and permanence of the data recorded by most DLT protocols is probabilistic rather than absolute. For example, Bitcoin is vulnerable in circumstances where a group of miners who control more than 50% of the network's mining hash rate coordinate to invalidate or orphan a chain of recorded blocks, forcing miners back to a point where they have to start again from a specific block height. The risk of 50.1% of miners colluding maliciously is limited in practical terms by the actual distribution of hashing power and in economic terms by the incentives shared by all miners. Twice in the past, in 2010 and 2013, bitcoin has been “rolled back” in this manner to resolve disputes in the developer community.

<sup>39</sup> In the case of bank money, this would be a combination of the bank and account details, as well as the customer's PIN.

digital assets and store the private key information in traditional vaults—like those used by banks for gold, accessible only through multiple keys made available to different individuals within an institutional customer.

- 6.7. Private keys are not necessarily single pieces of information or data. In recent years, crypto-custodians and others have sharded or split keys so as to achieve greater levels of security. For example, crypto-custodians may offer multiparty computation so each private key is split in three parts: one held by the customer, another by the custodian and the third by an independent third party, all held in cold wallets. Two of the three components of the private key are needed to effect a transaction. Normally one of these will be the customer's key, but where the customer has lost their key, that of the independent third party.
- 6.8. If the digital asset embodies a form of chose in possession, a proprietary right, and if parties can enforce rights in relation to it, it is necessary to establish rules governing which governing law and jurisdiction will apply. For things in possession, this is usually the place of the thing—the *lex situs*.<sup>40</sup> This concept is difficult to apply in the case of completely decentralised systems. Unlike bank accounts, which do not exist in a single location in any physical sense but for legal purposes can be said to be located where the bank branch is established, wallets on decentralised systems are not records associated with a single administrating entity/bank. Wallets exist as collections of data on the DLT system and are accessible via the nodes of that system from anywhere in the world. Some crypto-custody providers have sought to remedy this issue contractually by providing expressly in legal agreements with their customers that digital assets, their associated private keys and other assets will be treated as being located in a particular jurisdiction.
- 6.9. The FMLC suggests that where a digital asset is *not* associated with an identifiable obligor, the law could deem the digital asset to be located in the place from where it is controlled. As stated above, *control* is usually exercised by the person who has *possession* of the private key: without the private key, no transactions—buying, selling or (in the case of some permissioned systems, burning/destroying)—are possible.
- 6.10. Some custodians provide that they are to retain possession and ownership of the keys, but that the customer, as owner of the digital asset, is the only person able to have *direct*

---

<sup>40</sup> For more in-depth analysis, see FMLC, Report: *Distributed Ledger Technology and Governing Law* (27 March 2018), available at: <http://fmlc.org/report-finance-and-technology-27-march-2018>

*use of, and control of* the keys; this is then assured by issuing another, cryptographically assured, key to the customer to direct application of the private key. In this way, the customer is exercising those control rights usually associated with ownership and possession of the private key.

6.11. The legal basis on which crypto-custodians hold digital assets and keys for customers may be one of the following two models:

- a) often, under English law crypto-custody agreements, digital assets and keys are held by the wallet provider on trust for their customers. The wallet provider has possession and legal title; the customer has beneficial title. In this capacity, the trustee owes duties to the customer under the Trustee Act 2000; or
- b) another variation builds on the way shares are commonly held in England, under which the custodian holds the digital asset and the associated private key as nominee or bare trustee for customers, so that customers again retain only an equitable interest. What is different in this context from intermediated securities holding is that the custodian itself does not, unlike in the case of shares, have rights against an issuer.

To avoid the costs of fees associated with on-chain transactions, some crypto-exchanges have adopted the bare trustee model. The custodian would hold the public and private keys, and therefore the digital asset, as nominee for its customer. If customers want to trade with others on the exchange, settlement is effected by the provider holding for another customer. The provider changes its records, rather than effecting a transaction on the DLT system.

6.12. In this context, circumstances arise in which ownership must be split from possession and control. One situation which may arise in practice, wherein possession and ownership may need to be separated, concerns coins held in a wallet by a custodian. While it is plain that possession of the digital assets lies with the custodian, to determine ownership one might need to consider other aspects of the custodian's services. If the digital assets in the wallet are considered separate from any other digital assets held by the custodian for itself or for other customers, and if the custodian—either owing to lack of access to the private key or inability to apply the private key without direction from the customer—was unable to alienate the digital assets, then the custodian's customer is likely to be considered to have ownership of the digital assets.

6.13. In summary, therefore, the separation of possession from ownership—particularly in



relation to the private key through which all actions (including transfers) in relation to digital assets can be effected—would be useful. A further concept, that of control of the private key and thus of all actions in relation to the digital asset, should also be recognised.

## 7. QUESTION FOUR

- 7.1. Question four of the Call for Evidence asks how an on-chain transfer of a digital asset is typically characterised. The UKJT characterises the transfer of a digital asset as involving the creation of a new asset in the hands of the transferee rather than the transfer of the same asset. The Legal Statement states:

...the transferor typically brings into existence a new cryptoasset, with a new pair of data parameters: a new or modified public parameter and a new private key.<sup>41</sup>

While it is possible that this accurately describes the technological sequence of events, it is not necessary—and in the view of the FMLC is unhelpful—to consider a transfer of an asset in such terms from a legal perspective. Indeed, the UKJT recognises, later in the Legal Statement, that data should not be considered as constituting the digital asset but rather as being:

...the record of it and the key to dealing in it. Thus, the commercial value of a cryptoasset is not in the recorded data itself but in the fact that the person possessing that data is able to effect and authenticate dealings in the cryptoasset in accordance with the rules of the system.<sup>42</sup>

- 7.2. In a lecture given to the Insolvency Lawyers' Association on 17 October 2019, Mr Justice Zacaroli stated that, in his view, "Bitcoin is an entirely imaginary thing" and it is that imaginary thing "that is the subject matter of the transfer".<sup>43</sup> On the basis that a digital asset is best understood as an "ideational construct", any attributable value rests

---

<sup>41</sup> UKJT Legal Statement, paragraph 45 (footnote 3). David Fox in his chapter in D. Fox and S. Green (ed.), *Cryptocurrencies in Public and Private Law* (Oxford, 2019), adopts a similar characterisation.

<sup>42</sup> UKJT Legal Statement, paragraph 60 (footnote 3).

<sup>43</sup> South Square Barristers, *South Square Digest*, "Crypto-currencies and insolvency" (November 2019) at p.53ff., available at: <https://southsquare.com/wp-content/uploads/2019/11/Digest-Nov-2019.pdf>

on consensus building amongst a network of participants and the broader economy. The FMLC would suggest that it is the “ideational construct”, or its perceived economic value—and not the data—that is being transferred between parties. In the same way that English law does not currently regard a new entry in the register of members in a U.K. company as entailing the creation of a new data string, it should not do so for the transfer of digital assets.

- 7.3. There are a number of reasons for adopting an understanding of digital assets as an “ideational construct” with a perceived economic value, including:
- a) this is what market participants believe and intend to be happening;
  - b) it avoids the risk of unintended consequences, which may flow from the UKJT’s “destruction-creation” analysis, from a tax and financial regulatory perspective as well as questions as to how that analysis could be compatible with the concept of taking security over a digital asset or the theft of a digital asset;<sup>44</sup>
  - c) it could be more easily applicable to a variety of technological contexts, possibly even as the technology develops in the future; and
  - d) it could apply to the different types of cryptocurrencies, crypto-collectibles, stablecoins and other digital assets identified in paragraph 2.41 of the Call for Evidence.

## 8. QUESTION FIVE

- 8.1. Question five of the Call for Evidence concerns the practical consequences of characterising digital assets as “goods” under the Sale of Goods Act 1979 as well as views on these issues in the context of the Supply of Goods and Services Act 1982 and the Consumer Rights Act 2015.
- 8.2. Section 61(1) of the Sale of Goods Act 1979 defines goods as “all personal chattels other than things in action and money”. The 2016 Report considered whether virtual currencies might constitute “goods” for the purposes of sale of goods legislation and identified a risk that anything deemed to be a “virtual chose in possession”—

---

<sup>44</sup> See for instance Leigh Sagar, “Disposals of cryptoassets, tax & the UKJT Legal Statement” (January 2020), available at: <https://www.scl.org/articles/10801-disposals-ofcryptoassets-tax-the-ukjt-legal-statement>

intangible/incorporeal and yet somehow capable of being held “in possession”, without (at least, in the case of cryptocurrencies) qualifying as money—would naturally fall to be classified as “goods” in England but not in Scotland. The 2016 Report concluded that this question is primarily one of consumer policy, rather than legal classification, and may be dealt with accordingly by statutory amendment.<sup>45</sup>

- 8.3. There are, however, a number of practical issues which arise should digital assets be classified as goods. The legal regime which underlies such classification may be incompatible with the nature of certain digital assets. One instance of this is the result of the volatility of certain digital assets which makes adherence to the Sale of Goods Act difficult. For example, section 6 of the Sale of Goods Act 1979 provides:

Where there is a contract for the sale of specific goods, and the goods without the knowledge of the seller have perished at the time when the contract is made, the contract is void.

- 8.4. “Perished” has previously been interpreted to mean “damaged so that they no longer fit the contract description”.<sup>46</sup> The difficulties around determining when a digital asset has perished are apparent. For example, the volatility of digital assets, including the possibility that the price of a digital asset may suddenly plummet, means that classifying them as “goods” may give rise to disagreement and disruption around whether the loss in value may be interpreted as “perishment”. Perhaps a better example to demonstrate the uncertainties is by considering whether the loss of a private key could be interpreted as causing the digital asset to have “perished” for the purposes of the Sale of Goods Act. As described above, knowledge of the private key is critical to be able to access or transfer the digital asset. Loss of the private key of a crypto-wallet means that access to all the associated data and financial assets in the wallet are also permanently lost. In this context, it is possible that a court takes the view that the private key is an essential element of the digital asset and its loss or destruction could be considered perishment. Alternatively, it is arguable that the key is not part of the digital asset, such that the key being lost or destroyed will not be considered perishment, as the digital asset itself is still intact (though it may be incapable of transfer). Even if digital assets are to be considered “goods” under the Sale of Goods Act, consequent uncertainties exist around the manner in which courts interpret the legislation.

---

<sup>45</sup> Annex II of the 2016 Report considers whether computer software is goods or services, see footnote 4.

<sup>46</sup> Gooch, G. and Williams, M. ‘A Dictionary of Law Enforcement’ (Oxford University Press 2014)

- 8.5. Another uncertainty is evident by considering section 9 of the Sale of Goods Act, which provides stipulations in relation to the price to be paid by the buyer, and which would be difficult to apply given the frequent fluctuations in the price of various digital assets. Similarly, section 14 of the Sale of Goods Act implies in a contract for sale of goods a term that the goods are of satisfactory quality. Digital assets, however, are often not benchmarked by their “quality” but instead by their monetary value. The reasons for the exclusion of “money” in the definitions of goods under the Sale of Goods Act are also likely to be true for some types of digital assets: for example, those which can be used for payment—i.e., “cryptocurrencies”—do not have additive value, only monetary value (in which case, it is analogous with money and therefore not caught by the definition of “goods”). Similar issues arise under the Supply of Goods and Services Act 1982.
- 8.6. Under the Consumer Rights Act 2015, goods are defined as “tangible moveable items”, which would disqualify digital assets. The Act contains, however, a separate definition for “digital content”—data produced and supplied in digital form—and created protection for digital rights which it recognised as being neither goods nor services. Contracts for the supply of digital content are expressly included in the Consumer Rights Act 2015, where digital content is defined “as data which are produced and supplied in digital form”. As explored above, however, digital assets are more akin to things in possession, placing them in contrast to the rights extended to digital content. If the conceptualisation of digital assets under English law coalesces around a Third Category of property, then it would be feasible for consumer protection around digital assets to be provided in a way similar to the protection created for digital rights, with the least risk of unintended consequences, by statutory amendment of the Consumer Rights Act 2015.

## 9. QUESTION SIX

- 9.1. Question six of the Call for Evidence asks about practical or legal difficulties or problems that may be encountered in relation to the transfer of title to a digital asset. Under English law, title transfers are guided by the general principle of “*nemo dat quod non habet*” or “no one can give what they do not have” (the “*nemo dat principle*”). The Call for Evidence contemplates that the impact of the *nemo dat* principle may be different across different digital asset classes and functions. This seems to accurately reflect the experiences of stakeholders who have observed to the FMLC that the application of the *nemo dat* principle varies considerably depending on the type of digital asset, including

## Digital-only Assets and Real-world Digital Assets.

- 9.2. Typically, *nemo dat* issues are seen as limited in practice for Real-world Digital Assets because the transfer of the digital asset is linked to the underlying physical asset and the chain of title can be established by reference to the physical asset. The risk of improper or incomplete transfer of title of the digital asset is equal to that which arises in relation to the transfer of the underlying asset—albeit the mechanism required to manage control of a digital asset will be different from that of a physical asset. Practically, such issues do not generally arise as the two assets—one physical, one digital—can be said to "travel together".
- 9.3. In some respects, the same analysis will apply in respect of Referable Digital Assets. The chain of title in the underlying asset can generally be established and/or risk assessed by reference to the nature of the underlying asset and, although there is an additional risk represented by the transfer of the partial ownership, given the current niche applications of this ownership structure, the risks are seen as limited and manageable. This is the case whether the transactions are fully on-chain or partly on-chain and partly off-chain.
- 9.4. In contrast, transfers of Digital Only Assets appear to raise more material *nemo dat* issues, for both technical and practical reasons. Cryptocurrencies which have achieved status as a medium of exchange within a significant user community have a good claim to be regarded as money.<sup>47</sup> Although some would consider current cryptocurrency iterations as more a store of value, the future development of Central Bank Digital Currencies (“**CBDCs**”) will likely also raise this issue. Cryptocurrencies are not, however, legal tender in the U.K. and do not obviously fall within the category of documentary intangibles (such as money) which are exempt from the *nemo dat* principle. This raises a number of practical issues for parties that either use exchanges to change fiat currency into cryptocurrency or engage in trading of cryptocurrencies for value. Such transactions are normally undertaken using a third party, such as a digital assets exchange or trading platform, which will normally execute transactions from a pool of assets under their control, without reference to the individual owners of those assets. Current exchanges and trading platforms treat digital assets as fungible, notwithstanding the fact that individual holdings of cryptocurrency are traceable, and each holder needs to be reviewed for anti-money laundering and related purposes. This exposes exchange

---

<sup>47</sup> See the 2016 Report at 14–15, footnote 4.

and trading platform users to the risk that they could be allocated cryptocurrency in a legitimate transaction, which could subsequently be subject to challenge under the *nemo dat* principle due to activities taking place further up the chain, even as a *bona fide* purchaser for value of the relevant assets.<sup>48</sup>

9.5. There are exemptions from the *nemo dat* principle, and it may be important to consider whether they may apply to digital assets. One such exemption becomes relevant if digital assets can be classified as negotiable instruments. While the Call for Evidence is concerned with a wider set of assets than just cryptocurrencies, it may be useful to note the FMLC's 2016 Report concluded that cryptocurrencies should not be understood as negotiable instruments, even by distant analogy with other financial innovations, such as vouchers and in-game "bank notes", which more closely resemble documentary intangibles. The 2016 Report raised two issues against using negotiable instruments as an analogy in an attempt to understand the legal nature of cryptocurrencies. First, it highlighted an objection to shoehorning modern technology into concepts defined by Victorian legislation (i.e., the Bills of Exchange Act 1882) as retrogressive and, without amendment, precluded by the legislation itself. Second, there are a number of defining features shared by all negotiable instruments which are not, or not necessarily, replicated in cryptocurrencies. Further, negotiable instruments are, by virtue of section 83 of the Bills of Exchange Act 1882, to be executed in writing and signed by the obligor. Not only are the concepts of writing and signature not applicable to cryptocurrencies but units may be wholly anonymised.

9.6. Another category of negotiable instruments is that of transferable securities as defined under Directive 2014/65/EU on markets in financial instruments ("MiFID II") as onshored in the U.K. by the Markets in Financial Instruments (Amendment) (EU Exit) Regulations 2018.<sup>49</sup> To be a "transferable security", a digital asset must fulfil the following requirements:<sup>50</sup>

- a) the digital asset must belong to a class of securities—to form a class, digital assets must be fungible with one another, issued by the same issuer, show similarities

---

<sup>48</sup> Which may bring the discussion back to *Re London Wine (Shippers)* [1986] PCC 121 and whether "ownership" is identified when the assets are held "in bulk".

<sup>49</sup> See Martin Hobza, "ICOs, Cryptoassets and MiFID II: Are Tokens Transferable Securities?", Charles University in Prague Faculty of Law Research Paper No. 2020/III/1 (November 2020), available at: [https://www.researchgate.net/publication/345807153\\_ICOs\\_Cryptoassets\\_and\\_MiFID\\_II\\_Are\\_Tokens\\_Transferable\\_Securities](https://www.researchgate.net/publication/345807153_ICOs_Cryptoassets_and_MiFID_II_Are_Tokens_Transferable_Securities)

<sup>50</sup> Per Article 4(1)(44) of MiFID II.

and give access to the same rights to the same group of investors;

- b) the class of securities must be capable of being negotiated on the capital markets—this is not always clear. Generally, the abstract possibility of the digital asset being traded could be considered sufficient for it to be "capable of being traded", even if there is not yet a specific market for the product or there is a temporary lock-up. Moreover, the term "capital markets" may be broad enough to include any place where buying and selling interests meet (including an online exchange); and
- c) the digital asset must not be a payment instrument—examples of a payment instrument include a cheque or bill of exchange.

9.7. The analysis above raises the possibility that certain kinds of digital assets will have characteristics of negotiable instruments and may therefore be considered by analogy as exempt from the *nemo dat* principle, but this characterisation cannot be applied to all such assets. The risks of an "unfair" application of the *nemo dat* principle appear to be greatest in respect of Digital Only Assets for the reasons set out above.

9.8. The Committee also notes the analysis of the UKJT on this issue (see paragraph 47 of the Legal Statement) and, in particular, their conclusion that the *nemo dat* principle will not apply to cryptoassets, because (on each transfer) they are a newly created thing. While the simplicity of this approach is attractive, as noted above, the *nemo dat* principle is capable of broad and more flexible application. The UKJT's analysis on this point seems to be driven by consideration of Digital Only Assets, without necessarily considering Real-world or Referable Digital Assets and the differences that may arise as a result. Even in the case of Digital Only Assets, for the purposes of the criminal law, it is possible in some cases (such as Bitcoin) to trace through from a tainted address to all other unspent transaction outputs derived from those tainted funds, and it is difficult to see why the *nemo dat* principle should not apply in that situation.

## 10. QUESTION SEVEN

10.1. Question seven of the Call for Evidence is concerned with what was referred to earlier as Real-world Digital Assets, in particular, how the characterisation of the relationship between a digital asset and the underlying tokenised asset may affect transfers of either the digital asset or the underlying tokenised asset. Unlike cryptocurrencies, such as

Bitcoin or Ether, which are the “native asset” of a DLT system, a “token” is computer code bestowed with a distinctive asset reference and unique digital properties, as determined by the issuer, built onto an existing DLT system. The token may be encoded with certain legal rights, depending on the smart contract that generated it. The properties of a token depend in part on design choices and features of the underlying software; several projects have been established to attempt to define and classify tokens. For example, the Blockchain Research Institute states that tokens share five common characteristics. First, the token must be valuable (for example, measurable by reference to a global standard such as the US dollar or with reference to a Bitcoin or Ethereum DLT or another cryptocurrency exchange. Second, tokens are representative in the sense that they stand for the holder’s claims to an asset, resource, or right. Finally, tokens must be digital, distinct, and authentic.<sup>51</sup>

- 10.2. The common threads running through the technical, commercial and industry definitions of “token” are the concepts of ownership and representation of a thing of value, and transferability. Token ownership does not, however, automatically include the concept of token possession suggesting that tokens both in customary usage and in conception are perceived as binary: you either own one, or you do not. This view is consistent with that of the UKJT. Whilst stating that digital assets have all the “indicia” of being property and therefore being owned, the UKJT stopped short of hypothesising on whether, as a class of intangibles, they are capable of being possessed.
- 10.3. Question 7(1) of the Call for Evidence asks if this characterisation has any impact on the transfers of tokens or of the underlying asset. Transfers of tokens follow the same stages involved in the transfers of traditional securities, involving the creation, distribution, trading, settlement, clearing, custody, and storage of tokenised assets through DLT. Tokens may affect or disrupt the existing techniques and processes supported by financial markets infrastructure if they are substituted for traditional means of payment or for the assets themselves. Specifically, the transfers of tokens on DLT may not require the current infrastructure of third-party intermediaries, thereby streamlining costs and processes. The trading of tokens on the secondary market offers several other benefits. For example, valuable assets can remain securely in storage yet be transferred quickly and easily through its tokenised equivalent. An indisputable “proof of provenance” can be easily and cheaply provided by the DLT.

---

<sup>51</sup> Don Tapscott and the Blockchain Research Institute, *Token Taxonomy: The Need for Open-Source Standards Around Digital Assets* (February 2020), available at: [https://www.blockchainresearchinstitute.org/wp-content/uploads/2020/02/Tapscott\\_Token-Economy\\_Blockchain-Research-Institute.pdf](https://www.blockchainresearchinstitute.org/wp-content/uploads/2020/02/Tapscott_Token-Economy_Blockchain-Research-Institute.pdf).



- 10.4. Question 7(2) of the Call for Evidence asks whether the current legal characterisation of a transfer gives rise to practical or legal difficulties. If it is accepted that a digital asset is a form of property and that, within that “bucket” of property, Real-world Digital Assets and Referable Digital Assets are characterised as being relatable to real-world assets, then the current legal characterisation of a legal or equitable transfer of property as applied to these sub-classes needs further exploration. First, however, it is essential to consider how the market standard digital token is created and operates. Multi-layered and complex, it transcends any traditional conception of financial instruments by being at once co-dependent on a particular community and technological environment, whilst also self-executing.
- 10.5. As discussed above, digital assets as a class typically have attributes of a wallet, wallet address, public key, and private key. The prerequisite technical feature is the distributed ledger itself, a public infrastructure that provides a distributed record of transactions in which each wallet address is assigned to each token. These are the external technical features of a digital asset. But for a digital token or simply “token” in particular, there are two additional equally important characteristics that collectively form the composite asset. One is the technical set of characteristics that are innate in the digital token itself, which might be described as “internal” technical features: cryptographic tokens represent a set of rules, encoded in a smart contract or “token contract”. The other is the identifiably original features of a token which reside in the ecosystem in which the token was created and in which it exists: the “ecosystem features”.
- 10.6. Regarding the first, it is impossible to write about tokens without discussing the Ethereum Request for Comments 20 (“ERC-20”). The Ethereum Request for Comments (“ERCs”) are technical documents used by Ethereum smart contract developers that define a mandatory set of rules to implement tokens for the Ethereum ecosystem. These documents are typically created by developers and include protocol specifications and contract descriptions. First proposed by Fabian Vogelsteller in November 2015, the ERC-20 is a token standard implementing an application programming interface (“API”) for tokens within smart contracts. If a smart contract implements the stipulated functions and events, it can be called an ERC-20 token contract.
- 10.7. Once deployed, the ERC-20 token contract embeds a property that makes each token exactly the same in type and value as another token. As the most widely used fungible token standard, the ERC-20 not only facilitated the widespread creation of tokens but also has ensured interoperability of tokens within the Ethereum ecosystem of

decentralized applications.<sup>52</sup> For non-fungible tokens, which are by definition individually unique, a comparable industry standard was designed (ERC-721).

- 10.8. Whilst other token creation standards now exist in addition to ERC-20, the majority of tokens have been built on top of the community-run Ethereum DLT network.<sup>53</sup> For many commentators, the key differentiator between “tokens” is that these are built onto an existing DLT whereas cryptocurrencies are “native” to a DLT. The final component of a token is the ecosystem in which it resides. The ERCs and standards-setting are examples of the wider Ethereum ecosystem. Located on the application layer within this Ethereum ecosystem are dApp and DAO token communities that are self-governing. The characteristics of an “ecosystem” have been defined as:

...alignment structure of a multilateral set of partners for a defined period of time, who pursue a common goal, and by the active shaping of relationships, create a common added value for all actors by a focal value proposition.<sup>54</sup>

- 10.9. The nature of these ecosystems is less relevant here, other than to note that these self-governing DLT communities exert significant influence over the threshold behaviours of their members. Without these behavioural incentives, consensus building, could not be achieved. Thus, behavioural engineering is as essential to the operation and performance of the token ecosystem as the DLT infrastructure itself. The above analysis underlines the inherent complexity of tokenisation and digital assets more generally. No single set of factors, whether external technical features, (such as, the distributed ledger, wallet, public key, etc.), internal technical features (for example, token contract design, white paper product specifications, etc.) or ecosystem rules of engagement and consensus-based mechanisms, is separable from the others.

- 10.10. Within the virtual domain, the current legal characterisation of a transfer—including legal, or equitable assignment or novation—appears largely irrelevant to token communities. From before the point of creation, the digital asset token is intended for

---

<sup>52</sup> Cryptopedia, ERC-20: The Definitive Ethereum Token Standard: How can a token drive an entire ecosystem? (17 May 2021) available at: <https://www.gemini.com/cryptopedia/erc20-token-standard-ethereum>

<sup>53</sup> William Entriken, Dieter Shirley, Jacob Evans, Nastassia Sachs, "EIP-721: ERC-721 Non-Fungible Token Standard," Ethereum Improvement Proposals, no. 721 (January 2018), available: <https://eips.ethereum.org/EIPS/eip-721>.

<sup>54</sup> Tönnissen, S., Beinke, J.H. & Teuteberg, F., Understanding token-based ecosystems – a taxonomy of blockchain-based business models of start-ups. *Electron Markets* 30, 307–323 (2020). Available at: <https://doi.org/10.1007/s12525-020-00396-6>

transfer and programmed for transfer, based on the notional relationship between the token and the asset or value it represents. Like the token itself is stacked within multiple outer protocol layers, such as the white paper, the ERCs, the token community, the Ethereum ecosystem, and so forth. These largely self-sufficient and self-regulating organised systems have proved extremely adaptive and efficient in solving technological and security challenges, and the business use cases are proliferating. Within these purely virtual peer-to-peer parameters in which innovation thrives, “established mercantile usage” appears to have taken root and any intervention by law bodies has not been a limiting factor in development except in isolated cases of regulatory intervention.

- 10.11. The picture shifts with the introduction of more “friction” into the token economies, either in the form of intermediaries, creditors, agents, custodians and other third parties. In those circumstances, possessability and the exact legal classification of a digital asset becomes more pressing, and these questions are dealt with elsewhere in this paper.
- 10.12. As alluded to above, a tokenised asset is in many cases not virtual but physical in the form of Real-world Digital Assets and Referable Digital Assets. In such cases, these digital assets must be considered not only in their virtual context but also in a physical world governed by established law. Like the law of a foreign jurisdiction, questions arise as to which “law” or custom has precedence and how any conflicts should be dealt with. Also, more practical concerns, such as: how a purchaser of a Real-world Digital Asset could extinguish the token if so desired; whether the token and physical object can be transferred separately, or only together; how a would-be purchaser of a physical object could be assured that a physical object was not tokenised or, if it were, that the token was subsumed in passing of title to the physical object; whether competing claims (token versus physical possession) could arise; and similar. It is at this juncture where legal uncertainty is most apparent.
- 10.13. Question 7(3) of the Call for Evidence asks whether the ability to possess a digital asset would help to clarify this analysis. As outlined in our response to question two above, the Committee considers that it would so help, particularly in the case of Real-world Digital Assets and Referable Digital Assets.
- 10.14. Whilst assigning the legal attribute of possessability to Real-world Digital Assets and Referable Digital Assets, the functionality of legal possessability is likely to be of more immediate practical value. This would appear to involve some technical means of linking the token with the underlying physical asset (which is possessable) which would serve, in turn, to integrate the “legal” framework with the tenets of the English law.

Whether smart contracts can embed tokens with “possessability” features will be a question for technologists and the markets.

## 11. QUESTION EIGHT

- 11.1. Question eight of the Call for Evidence asks in what practical circumstances, were a digital asset possessable, would bailment arise. A “bailment” occurs when one person is voluntarily in possession of a tangible thing that belongs to (is owned by) another, usually for a specific purpose. Commonly, bailment arises where physical goods are delivered in contemplation of a service—a textbook example being goods delivered to a repairer, or cleaner or transporter of the goods. With the exception of staking, it is hard to imagine a useful or practical application where this sort of bailment would apply to digital assets. Staking arrangements give rise to novel questions of law and legal uncertainties. Staking occurs when digital asset owners in a DLT system perform the service of validating transactions alongside locking some of their assets in the protocol, for an agreed period of time. The locked assets are used achieve consensus and ensure honest validation. In return for their participation, these “validators” are rewarded with new digital assets from the network but a DLT system may decrease (“slash”) a validator’s stake for dishonest or malicious behaviour. To avoid dealing with the requirements that DLT systems place on validators, owners of the digital assets may opt to delegate their digital assets to a validator running a staking pool, who in turn will share the rewards with their delegators. This arrangement is typically set up and administered by smart contracts automatically but the underlying legal relationship might be best characterised as one of bailment. In the event of a loss of digital assets after a slashing event, how would responsibility be allocated—i.e., does the answer differ depending on the validator’s level of fault (negligence vs. gross negligence vs. recklessness) or on the type of slashing event (double-signing vs. downtime)?
- 11.2. Other types of staking exist, some of which may require the use of legal contracts. For example, in custodial liquidity staking, a custodian (like a traditional cryptocurrency exchange) will hold tokens on behalf of a staker. A legal agreement which defines the parties’ respective rights and obligations as part of that relationship must be established, and the custodian must define therein the type of custody arrangement—whether a trust, bailment, escrow, etc.—which will apply to the staking tokens entrusted to the exchange. Other legal definitional questions also arise, including whether the digital assets subject to staking are transferable legal instruments or a mere certificate of deposit

from the custodian.

- 11.3. A bailment could also be used to constitute a pledge, where possession of the asset by the pledgee is set up to secure some obligation entirely unrelated to the asset—for example, an unrelated debt obligation. If this “possession” were deemed feasible for digital assets then it would, in theory at least, allow borrowers to pledge digital assets as collateral. A contractual lien would also be possible. Moreover, *possessory* security can have a number of advantages over other forms of security, such as charges. For instance, possessory security is generally agreed to fall outside the scope of the charge registration rules for U.K. companies (although the Companies Act 2006 is silent on this point). It might also be relevant to consider the multiple advantages that would flow from a pledge over a digital asset constituting a "security financial collateral arrangement" under the Financial Collateral Arrangement (No. 2) Regulations 2003. However, finance market participants (outside specialist units) are generally unfamiliar with security over digital assets and, as noted in the Call for Evidence, the UKJT Legal Statement concluded that “because a cryptoasset cannot be possessed, neither can it be the object of a bailment”.<sup>55</sup>
- 11.4. The feasibility of "possession" (and hence bailment) is going to require technical solutions. Financial institutions are also likely to look to either a legislative structure or some well-formed market guidance in order to get comfortable with it. A practical hurdle that arises is that many things that may be construed as a "digital asset" are not readily identifiable or monetizable. In many cases, the digital asset is a ledger or accounting statement arising via participation in a network.<sup>56</sup> To quote an example from a recent article:

Thus, when, in everyday terms, we speak of Alice as owning 64.36 Bitcoin, in technical terms this means Alice has a legitimate expectation that, until she decides to spend any of her bitcoin, the Bitcoin blockchain continues to record that 64.36 bitcoin are attributed to public addresses to which Alice is entitled. The essential point is, however, that the blockchain does not attribute 64.36 bitcoin to *Alice*, but to one or several pseudo-anonymous public addresses participating in the Bitcoin network as an attribute of a node. There is nothing to confirm that Alice is entitled to the bitcoin attributed to

---

<sup>55</sup> See paragraphs 17 and 87-88 of the Legal Statement, footnote 3.

<sup>56</sup> Paragraphs 24-34 of the Legal Statement may provide a better understanding of this point, see footnote 3.

the relevant public addresses, nor whether she has the direct means to control those Bitcoin through access to the corresponding private keys.<sup>57</sup>

The introduction of legislative framework might provide a resolution to this problem in limited contexts. Its use could be significantly limited, however, from a conflict of laws perspective since the *situs* of digital assets is difficult to ascertain (see paragraph 6.8 above).

- 11.5. Question 8 of the Call for Evidence also asks about "other technical or practical solutions" which might make the debate about bailment redundant. If parties want to grant or take security over a digital asset, it may be possible for a mortgage or equitable charge to be created over it without the need for possession, but there could still be technical hurdles to overcome.<sup>58</sup> As noted in the Call for Evidence (at paragraph 2.69), much depends on whether the difficulties in exercising control over a digital asset reduce the efficacy of taking a mortgage or charge over digital assets.
- 11.6. For the vast majority of Bitcoin owners, participation in the network is typically intermediated by cryptoasset exchanges through an exchange-hosted wallet. Bitcoin trading, for instance, is largely carried out through an intermediary company (for example, Coinbase or Gemini). If the "owner" of some Bitcoin wanted to put up collateral, it might be easier for the collateral giver to assign its contractual rights against that intermediary/custodian. In this sort of context, the assignment (by way of security) of contractual rights might be more readily acceptable to a financier than trying to engineer "possession" of a digital asset. A similar approach is adopted when a chargor grants security over securities (shares, bonds, etc) held in a clearing system. However, it is probably not that simple, because of the nature of the trading wallets and the way trades occur in practice (many trades occur "off chain"). In addition, owing to the different standards governing each platform, it would not be appropriate to equate, for example, bitcoin trading on a platform with bond trading via Euroclear. As explained by Amy Held:

The consequent risks to exchange users thus mirror those recognised in the context of omnibus securities accounts: the absence of any requirement that exchanges maintain sufficient 'balances' of

---

<sup>57</sup> Amy Held, Does situs actually matter in disputes concerning bitcoin? (2021) 4 JIBFL 269.

<sup>58</sup> See paragraphs 103-106 of the Legal Statement, footnote 3.

cryptoassets, termed here as 'participation values', attributable to their public addresses in the blockchain network to cover the sum of their users' entitlements. In the case of shortfalls, the strength of users' ownership rights in 'their' cryptoassets will depend on, not only a consideration of cryptoassets per se as property, but analyses of the exchanges' own practices in submitting signed transactions to the other nodes in the crypto network, and the agreements between the exchange and the user as matter of law.<sup>59</sup>

Another aspect to consider is the governing law of these platforms.<sup>60</sup>

- 11.7. The Call for Evidence refers (at paragraph 2.63) to Wyoming Blockchain Laws, which provide that digital assets held by qualified custodian intermediaries are held in a bailment relationship. This approach might be helpful in considering security over digital assets but it is unlikely to be a solution which is capable of being deployed simultaneously in multiple jurisdictions. It could therefore give rise to a range of conflict of laws issues and would require a financier to accept the risks and costs of an additional cross-border element in the relevant finance transaction. Finally, a solution focused on the "rights against the intermediary" may only be possible where the digital assets in question are considered fungible in the same way as shares or bonds. It is unlikely to be appropriate for other types of digital assets, such as smart contracts, non-fungible tokens or crypto-collectibles.

## 12. QUESTION NINE

- 12.1. Question nine of the Call for Evidence asks about how security over digital assets is granted or taken in practice. There is no standard method of taking security over digital assets. The four forms of consensual security in English law are underpinned by

---

<sup>59</sup> Amy Held, *Intermediated cryptos: what your exchange-hosted wallet really holds* (2020), 8 JIBFL 540.

<sup>60</sup> Amy Held (*ibid*), for example, includes an analysis of the contractual arrangements in the UK for Coinbase and in the US for Gemini. In the UK, **an account with Coinbase** is governed by a User Agreement which comprises an Agreement with each of Coinbase UK Ltd and CB Payments Ltd. CB Payments provides services in respect of E-Money, which is typically purchased with fiat currency in a standard bank transfer. Coinbase UK, on the other hand, provides Digital Currency services through a Digital Currency Wallet, which enables users to store, track, transfer, and manage balances of certain supported Digital Currencies. Similar to Coinbase, **a Gemini account** comprises a number of sub-accounts: one or more of a "Fiat Account" that reflects its fiat currency balance; and a "Digital Asset Account" that reflects its Digital Asset balance. Gemini Trust Company LLC (Gemini) is a fiduciary under §100 of the New York Banking Law in respect of both Fiat and Digital Asset Accounts.

ownership, possession or control of the asset by the security taker, but the nature of digital assets means that it may be difficult to achieve any of these based on existing law and techniques. Where digital assets are held on an exchange or by a custodian, it is expected that security would be taken over the claims of the "owner" against the exchange operator. Such security is common in respect of other tradeable assets, and existing practices should be applicable to digital assets. Question nine also asks whether respondents consider mortgages and charges to be effective methods of taking security over digital assets.

### **Mortgage**

- 12.2. In the case of a mortgage, equitable or legal title to the asset will need to be transferred to the mortgagee. The issues raised by the *nemo dat* rule as discussed in the response to question six may inhibit the creation of an effective mortgage. The multiple components of a digital asset mean that multiple transfers of title may be needed in order to ensure that the security is complete, unless there is legal recognition of the "package" of assets that constitutes a single digital asset (see paragraph 2.14 in respect of the elements of a digital asset). This approach has been taken in the context of intellectual property, where section 30(1) of the Patent Act 1977 and section 22 of the Trade Marks Act 1994 define the nature of patents and trademarks respectively as personal property in order to establish how transfers and mortgages of those assets can be effected in an enforceable manner.
- 12.3. Problems may arise for a mortgagor in ensuring their interest in the asset is adequately notified to third parties in order to prevent unlawful transfers of the mortgaged assets by the mortgagee. Mortgages of other classes of asset typically allow the mortgagor to retain some control over the asset (for example, chattel mortgages) or have their interest recorded on a public register (for example, real property).

### **Charge**

- 12.4. As the charge is a construct of an agreement between the chargee and the chargor, it affords a more flexible means of creating security over digital assets, provided that the asset can be adequately defined to enable the attachment of the security. Problems may arise, however, in ensuring that third parties are on notice as to the existence of the charge, as discussed below.

### **Pledge/Lien**



12.5. As noted in previous answers and in particular paragraphs 4.12 to 4.16, the nature of digital assets means possessory security is not feasible at present. If, however, a Third Category of possessable property was adopted for digital assets, these types of security would be available. Thought will then need to be given to determining how one possession, ownership and control are ascertained, as discussed in previous sections above.

### **Statutory security interests**

12.6. Legislation has been used to create distinct security interests under English law. For example, the Law of Property Act 1925 created the charge by way of legal mortgage, and The Financial Collateral Arrangements (No.2) Regulations 2003 created the concept of a security financial collateral arrangement. The definition of security financial collateral arrangement makes it clear that such arrangements can extend beyond the forms of English law consensual security. A similar approach could be followed in the case of digital assets.

### **Perfection and Priority**

12.7. A significant issue for security takers is how they preserve priority of security over digital assets. In this regard, a mortgage is perhaps the most effective security, with the mortgagee being recognised as the owner of the digital asset, preventing further interests in the asset from being created by the mortgagor. A registration system for digital assets similar to that proposed by the Secured Transaction Law Reform Project would ensure that third parties are on notice as to the existence of security interests.<sup>61</sup>

### **Situs of the digital asset and conflict of laws concerns**

12.8. A significant issue in taking security over digital assets is that elements of the asset may exist simultaneously in multiple jurisdictions in circumstances where no single element is dispositive of its *situs* for conflicts of laws purposes. A general conflict of law principle is that *lex situs* will determine the governing law applicable to security over an asset. Foreign jurisdictions may refuse to recognise English law security over a digital asset or treat the asset in a manner that prevents the security from being enforced.

12.9. One way in which this uncertainty may be mitigated is by establishing an international

---

<sup>61</sup> Louise Gullifer, Secured Transactions Law Reform Project: Registration Discussion Paper (January 4, 2017), available at: <https://ssrn.com/abstract=3148886> or <http://dx.doi.org/10.2139/ssrn.3148886>

registry of third-party interests in digital assets with a single enforcement regime upheld by all states. In the case of aircraft assets, for example, this is achieved through the Cape Town Convention on International Interests in Mobile Equipment 2001 and the supporting International Registry of Mobile Assets, which ensures that signatory states uphold security interests recorded in the Registry irrespective of competing local law.

- 12.10. The FMLC does not underestimate the significance of the challenge in creating an international registry of third-party interests in digital assets, not least because the aviation sector is narrower than the universe of digital assets, which is continuing to evolve. Such a registry could be a DLT-based registry that could interact with other DLT systems and act as a single source of truth for security interests. An international approach also appears to be in line with HM Treasury's wider policy proposals, which recognise the importance of global regulatory standards.<sup>62</sup>
- 12.11. If an international approach is not on the agenda, then a national registry—similar to, for example, the Land Registry—could add legal certainty and transparency. This could be developed by industry in a similar way to how Open Banking standards were formed and developed, albeit with the force of the Competition and Markets Authority's Order behind them.
- 12.12. A public-private partnership with statutory footings could be an ideal option, possibly supported/incentivised by HM Treasury through the British Business Bank or similar body in a similar way to how the European Investment Bank is supporting and incentivising the innovation in European capital markets.

### **Possessory security over a digital asset**

- 12.13. Question nine of the Call for Evidence also asks whether there are practical circumstances in which the creation of possessory security over a digital asset might be used if the digital asset were possessable. To the extent that a simple means of granting security analogous to pawning could be created, it could create a means for borrowers to access a wider pool of potential lenders and remove complexity from taking security. However, the burdens that possessory security place on both the security beneficiary, through its duty of care while the asset is in its possession, and the security provider, in terms of ceasing to have the asset available to it, may make it an unattractive

---

<sup>62</sup> See, for example, paragraph 2.4 of HM Treasury's consultation and call for evidence on the UK regulatory approach to cryptoassets and stablecoins, January 2021, available at: [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/950206/HM\\_Treasury\\_Cryptoasset\\_and\\_Stablecoin\\_consultation.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/950206/HM_Treasury_Cryptoasset_and_Stablecoin_consultation.pdf)

proposition.

### **Other technical or practical solutions or market practice**

- 12.14. Question nine of the Call for Evidence also asks if other technical or practical solutions or market practice, including the creation of quasi-security, make the ability to take possessory security over a digital asset less important. The flexibility of the equitable charge means that, if there were suitable means of imposing actual or constructive notice of the charge on third parties, this may remove the need for the creation of a mechanism for possessory security to arise. Flawed asset arrangements or repo transactions could perform the function of possessory security—although the attractiveness of these would depend on tax treatment and the ease of transferability of the relevant digital assets.

Overall, rather than deeming digital assets to be possessory and applying existing security principles to them, ideally it would be better to create a specific class of digital asset security together with a unilateral registration regime to provide security providers with more flexibility in dealing with assets than requiring transfer of possession or title to a third party for the duration of the security period.

## **13. QUESTION 11**

- 13.1. Question 11 of the Call for Evidence welcomes comments on the aspects of the Liechtenstein Blockchain Act and the Wyoming Blockchain Laws relevant to the questions in this Call for Evidence. It also asks for suggestions of other jurisdictions the Law Commission should consider.

### **Wyoming**

#### *Categorisation of Digital Assets*

- 13.2. Inspiration for the Third Category, as proposed in section three and the response to question two above, may be drawn from U.S. State of Wyoming's treatment of digital assets. The U.S. State of Wyoming enacted Senate File SF0125 ("**SF0125**"), which has three elements relevant to this submission: (1) created a set of definitions for digital assets; (2) identified digital assets as enjoying property rights; and (3) outlined how

perfection and priority of security operates.<sup>63</sup>

### *Definitions*

13.3. SF0125 recognises digital assets as having property rights. The legislation categorises digital assets into three mutually exclusive subclasses:

- a) digital securities: which are treated as securities and investment property;
- b) virtual currencies: which are treated as money; and
- c) digital consumer assets: which are treated as “general intangibles”.

The term “general intangibles” is a term which has long existed in Wyoming’s commercial code.<sup>64</sup> Any asset which falls within one of these three categories is defined as “intangible personal property”, which is a term used in Wyoming’s 2011 tax law.<sup>65</sup>

### *Perfection of Security, Ownership and Control*

13.4. Under SF0125, perfection of security in a digital asset may be achieved through the newly established concept of “control”.<sup>66</sup> Before a secured party can take control of a

---

<sup>63</sup> Wyoming State, enacted Senate File SF0125 (2019), available at: <https://www.wyoleg.gov/Legislation/2019/sf0125>

<sup>64</sup> The term “general intangibles”, in Wyoming’s commercial code, means:

any personal property, including things in action, other than accounts, chattel paper, commercial tort claims, deposit accounts, documents, goods, instruments, investment property, letter-of-credit rights, letters of credit, money and oil, gas or other minerals before extraction. The term includes payment intangibles and software.

See WY Stat § 34.1-9-102, available at: <https://law.justia.com/codes/wyoming/2011/title341/section341-9-102/>

<sup>65</sup> The term “intangible personal property” has come from Wyoming’s 2011 tax law, and means:

personal property that lacks mass and cannot be seen, felt, weighed, measured or otherwise perceived by the senses; property that has no physical existence beyond merely representational. Intangible property’s value lies chiefly in what it represents, and its existence may be evidenced by a document.

See Wyoming State, enacted Senate File SF0031, available at: <https://www.wyoleg.gov/Legislation/2006/SF0031>

<sup>66</sup> In this context, “control” of a digital asset means:

a secured party, agent, custodian, fiduciary, or trustee of the party has the exclusive legal authority to conduct a transaction relating to a digital asset including by means of a private key or the use of a multi-signature arrangement authorized by the secured party.

See SF0125 (footnote 52)

digital asset, it must enter into a control agreement with the debtor. “Control” of a digital asset is equivalent to “possession” and signifies priority of interest, which may be pledged by written agreement, and for which a financing statement may be filed with the state.

- 13.5. As well as creating a comprehensive property classification of digital assets, SF0125 integrates with existing Wyoming commercial laws. The FMLC would strongly recommend that, were a Third Category of property to be recognised under English law, the framework around it must not be created in a vacuum, removed from existing legislation. For the Third Category to be effective, it must work both with and within the existing legal framework.

### *Bailment*

- 13.6. With reference to issues considered in the response to question eight above, Wyoming’s SF0125 is unique in that it enables custody of digital assets via bailment. SF0125 establishes an opt-in regime which allows banks to provide custodial services. SF0125 states that digital assets held in custody are not depository liabilities or assets of the bank. The bank maintains control and custody of the digital asset under bailment. The concept of bailment is more nuanced than expressed in SF0125, as recognised in a letter from the State of Wyoming Department of Audit Division of Banking, which stated that the law surrounding custody, particularly for digital assets, “is not fully developed”.<sup>67</sup> Although digital assets themselves may not be subject to bailment, it may nonetheless be taken over the underlying asset. When drafting U.K. legislation, regard should be given to the unique features of digital assets examined in the preceding sections of this paper, such as the delineation between the conceptualisation, possession and ownership of private keys, the underlying assets and wallets.

## Liechtenstein

### *Characterisation*

- 13.7. As explored in the response to question seven above, there is confusion surrounding the different types of assets that can be represented by a token, the difference between the digital asset tokens and the underlying asset and the rights attributed therein. The Liechtenstein Blockchain Act incorporates a treatment of digital assets which helps

---

<sup>67</sup> State of Wyoming Department of Audit Division of Banking, Two Ocean Trust No-Action Letter (23 October 2020), available at: <https://docs.google.com/viewer?a=v&pid=sites&srcid=d3lvLmdvdnxiYW5raW5nfGd4OjU2MDk2ZGQyYjg1ZDUzYTc>

resolve this confusion. As set out in the Call for Evidence, the Liechtenstein Blockchain Act introduced the “Token Container Model”, whereby a token can represent “claims or rights of memberships against a person, right to property or other absolute or relative rights”, meaning that nearly any right or asset can be packaged into a token. This includes “real” assets such as real property, shares, bonds and access rights and money; but the container can also be “empty” and include digital codes and digital assets. Creating a container for a right or asset allows for the separation of (a) the right and the asset and (b) the token technically running on a DLT-based system. The container model allows binding transfers of the underlying rights, whether that is a right to real or digital assets.

### *Practical application*

- 13.8. Liechtenstein’s regulators have recognised the gap between the online and the offline world and addressed it by creating, under the Liechtenstein Blockchain Act, roles such as that of “Physical Validator”, which ensures that the physical object and associated rights to be tokenised actually exist. For example, if an individual were to invest in a token representing a fraction of a painting, it would be the role of the Physical Validator to guarantee the ownership rights to that fraction. Furthermore, the Liechtenstein Blockchain Act provides guidelines in the event that a user holding a token embodying a right loses access to their token, such as the loss or theft of a private key, as well as authorising mechanisms for the burning of tokens that are rendered invalid.<sup>68</sup>

## **14. QUESTION 12**

- 14.1. Question 12 of the Call for Evidence seeks suggestions as to other issues which arise in practice, or other areas of law which could be affected, and which should be included in the scope of the Digital Assets Project. Certain issues of legal uncertainty which arise in this context are set out below. Given the remit of the FMLC, the issues considered have arisen in the context of financial market transactions and financial market infrastructures. The implications of any changes in law in these areas on matters outside financial markets should be considered further, especially given the breadth of the definition of digital assets used in the Call for Evidence.

---

<sup>68</sup> Article 10 of Liechtenstein Law of 3 October 2019 on Tokens and TT Service Providers (“Token and TT Service Provider Act” or “TVTG”), available at: [https://www.lcx.com/wp-content/uploads/2020\\_Liechtenstein\\_Blockchain\\_Laws\\_Translation\\_English.pdf](https://www.lcx.com/wp-content/uploads/2020_Liechtenstein_Blockchain_Laws_Translation_English.pdf)

## Settlement risk

- 14.2. In financial markets, settlement broadly refers to the process of delivering securities from seller to buyer to complete a trade. Payment usually passes in the opposite direction in a settlement process known as delivery versus payment (or “**DvP**”). In legal terms, settlement refers to the point in time at which title to the underlying property passes from seller to buyer. Until settlement occurs, the buyer of securities has a contractual right to have the securities delivered to them from the seller in consideration for the payment and receipt of the purchase price. Since this contractual right is a personal right, the buyer's rights to the securities are at risk of the seller's insolvency or other causes of non-delivery, even if the buyer has paid for them. Settlement turns these personal rights into proprietary rights and therefore protects the buyer from the risk of default of the seller or other counterparties.
- 14.3. Settlement risk exists outside financial markets, but it is more acute in financial markets, especially with intra-day trading, netting between multiple participants and interaction between different payment and security settlement systems, where property can change hands multiple times a day. Settlement can (now) be done in real time, as with payment systems operating real-time gross settlement systems, or it can take a few days to occur. The longer the settlement period, the greater the risk of settlement failures. To address this risk, financial markets often require a central counterparty to sit in the middle of each trade—the central counterparty is buyer to every seller, and seller to every buyer. By intermediating in this way, settlement risk passes to, and is contained within, the central counterparty (i.e. a centralised body) on whom regulatory and legal obligations are imposed to ensure the stability and soundness of financial markets. Markets for digital assets exhibit many of the features of traditional financial markets and, therefore, settlement risk has to be considered in these markets, but the existing law dealing with financial markets and digital assets representing or resembling financial instruments or securities poses a number of barriers to further innovation due to legal uncertainties.
- 14.4. In the U.K., financial market settlement is dealt with through various pieces of legislation affecting payment systems and security settlement systems. For present purposes, this paper will focus on the U.K. version of Regulation (EU) No 909/2014 on improving securities settlement in the European Union and on central securities depositories (the “**CSDR**”) as “onshored” by the Central Securities Depositories (Amendment) (EU Exit) Regulations 2018 (the “**U.K. CSDR**”) and the Financial Markets and Insolvency Settlement Finality Regulations 1999 (the “**SFRs**”), which

implemented the Directive 98/26/EC on settlement finality in payment and securities settlement systems into U.K. law (this Directive and the SFRs are referred to together as the "**SFD**").

14.5. The SFD seeks to reduce systemic risk associated with participation in payment and security settlement systems, particularly the risk linked to the insolvency of a participant in such a system.<sup>69</sup> The SFD applies to systems which are designated. Designation occurs by application to the relevant authority; although, there are instances when a designating authority may require designation, particularly where a system could be systemically important.

14.6. The CSDR aims to:

Harmonize certain aspects of the settlement cycle, settlement discipline and provide a set of common requirements for [central securities depositories] operating securities settlement systems in order to enhance cross border settlement in the EU.<sup>70</sup>

The U.K. CSDR requires the participation of a Central Securities Depository ("**CSD**") in two situations: (i) where transferable securities are listed on an in-scope trading venue; or (ii) where the DLT system is a security settlement system within the scope of the SFD.

14.7. The current settlement regimes for financial markets create legal uncertainty for new forms of digital assets, even where these represent tokenised forms of traditional securities. The FMLC has previously considered issues of legal uncertainty in the context of DLT and settlement.<sup>71</sup> The FMLC previously observed that the SFD excludes natural persons from the list of persons authorised to take part in a designated system. This means that DLT implementations which provide for direct access to retail "customers" are unlikely to qualify for designation. A lack of designation means that transactions remain subject to the insolvency and other risks noted above, which settlement legislation seeks to remove or mitigate. This is more likely to be an issue for DLT implementations that reach a level of systemic importance or risk. It also supports a conclusion that the SFD is more likely to be compatible with a centralised and

---

<sup>69</sup> ESMA, Advice: Initial Coin Offerings and Crypto-Assets (9 January 2021), at paragraph 141, available at: [https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391\\_crypto\\_advice.pdf](https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf)

<sup>70</sup> *Ibid* at paragraph 142.

<sup>71</sup> See footnote 40.



permissioned system than a decentralised and permissionless one. While the SFD and issues concerning settlement finality may be better suited to centralised, permissioned DLT systems, any legislative steps to regulate digital assets may need to distinguish between the different DLT systems, because prohibiting decentralised, permissionless networks could stifle some innovations. Clarity in scope and the use of consistent taxonomy will be vital in these areas.

14.8. ESMA's Advice on Initial Coin Offerings and Cryptoassets also highlighted various issues for DLT platforms that qualify as a securities settlement system.<sup>72</sup> For example:

- a) the scope of the current regime will not apply to all digital assets, so consideration needs to be given to whether a broader range of digital assets and DLT platforms need, or would benefit from, the certainty that settlement legislation offers;
- b) any securities settlement system must be operated by a system operator who is responsible for the operations of the system. ESMA correctly notes that it can be difficult to identify such an operator in the case of decentralised DLT platforms. If settlement laws are extended to a wider class of digital assets and/or DLT platforms, consideration will need to be given to how one identifies such an operator;
- c) designation as a securities settlement system requires the appointment of a CSD, which must comply with specific governance and organisational requirements to comply with the requirements of the CSDR. The role of miners under the CSDR is another area that ESMA rightly points out needs to be considered, given the novel role they play in the settlement process; and
- d) the potential issues in relation to settlement finality and DvP in a DLT system. In particular, how to define and achieve settlement finality with DLT from an operational and legal perspective. ESMA notes that this needs to take into account the different “consensus” validation methods within, and still emerging in, DLT systems and the risk of “forks” to the concept of finality and irrevocability. Consideration also needs to be given to how DvP is achieved, notably when the payment leg is off-chain. Any legislation in this area needs to future-proof against the possibility of CBDCs and private, permissioned DLT

---

<sup>72</sup> See footnote 69.

systems interoperating with one another so as not stifle current thinking and innovation.

14.9. The concept of settlement finality has also been widely discussed in relation to the use of digital assets and DLT in financial markets, including by the FMLC.<sup>73</sup> Settlement finality refers to the point in time at which a transaction is deemed to be final and irrevocable, even in the event of insolvency proceedings against participants in the system. Settlement finality protects both parties from transactions being unwound if one party become insolvent intra-day. This certainty adds to users' confidence in payment and securities settlement systems and, in turn, adds to the stability of such systems. The international framework for Financial Market Infrastructures ("FMIs") provided by the Principles for Financial Market Infrastructures established by the Committee on Payment and Settlement Systems (now the Committee of Payments and Market Infrastructures ("CPMI")) and the International Organization of Securities Commissions ("IOSCO") (the "CPMI-IOSCO Principles") also includes settlement finality as one of its core principles for FMIs.<sup>74</sup> The CPMI-IOSCO Principles are intended to:

enhance safety and efficiency in payment, clearing, settlement, and recording arrangements, and more broadly, to limit systemic risk and foster transparency and financial stability.<sup>75</sup>

If settlement finality is not ensured in any proposed legislation concerning digital assets, then issues of legal uncertainty in this area may remain. Settlement finality may not be necessary in all DLT implementations, but its benefits to FMIs are clear and any new legislation should address settlement finality within DLT implementations used in financial market infrastructure, both in the traditional sense and in the context of any new financial market infrastructure that could emerge as a result of the innovations in

---

<sup>73</sup> FMLC, *The Regulation of Cryptoassets: Response to European Commission Consultation—Part II* (March 2020), available at: [FMLC UP 11706609 v 1 Part-II-Response-to-EC-Consultation-on-regulating-cryptoassets-existing-regulation.pdf](https://www.fmlc.org.uk/11706609/v1/Part-II-Response-to-EC-Consultation-on-regulating-cryptoassets-existing-regulation.pdf)

<sup>74</sup> The CPMI-IOSCO Principles are available at: <https://www.bis.org/cpmi/publ/d101a.pdf>

Principle 8 on Settlement finality (page 64) states:

An FMI should provide clear and certain final settlement, at a minimum by the end of the value date. Where necessary or preferable, an FMI should provide final settlement intraday or in real time.

Operators of multilateral systems of participating institutions used for clearing, settling, or recording payments, securities, derivatives, or other financial transactions, regardless of the legal structure or technological foundation of that system.

<sup>75</sup> *Ibid* at paragraph 1.15.

digital assets.

- 14.10. It should be noted that some DLT systems cannot offer settlement finality in the way required by the SFRs. This is true of the Bitcoin DLT system and its proof-of-work consensus protocol, whereby there is never absolute certainty of settlement (or settlement finality) but, rather, an ever-reducing likelihood of the transaction being unwound as each block is added to the chain until it becomes a negligible risk. The position above in relation to Bitcoin's DLT system is not true of all DLT systems. It should be technically possible to create a DLT system that meets the requirements of the SFRs, albeit this is most likely at present to be a permissioned, centralised system. As such, settlement finality should not be an absolute barrier to digital asset adoption, but legal uncertainties remain with regard to the current scope of the regime when applied to DLT systems and digital assets (especially those that are not securities), and whether a similar regime offering finality or irrevocability would be desirable in DLT systems and for digital assets that sit outside the traditional financial markets, given the similarities some of them have with traditional financial markets.
- 14.11. It has been argued that the introduction of CBDCs and continued innovations in DLT systems could even eliminate the need for the complexity around settlement finality.<sup>76</sup> According to The Whitechapel Think Tank:

The immutable nature of DLT gives rise to embedded settlement finality at the point of exchange – with no further oversight or set-aside of funds in cash collateral accounts required. In other words, the use of DLT in a retail CBDC system offers “atomic settlement”: irrevocable, final, and real-time settlement of retail transactions, using central bank-backed digital fiat currency, and eliminating credit risk between the instigator and the beneficiary of the relevant payment. The existing tripartite process of payment, clearing and settlement would be collapsed into one simple, trustable and assured digital process.<sup>77</sup>

- 14.12. If, or when, atomic settlement using CBDCs becomes a tried and tested reality, it may no longer be necessary for such prescriptive rules on settlement of digital asset

---

<sup>76</sup> The Whitechapel Think Tank, *The Impact of Digital Currency of the Future of Payments* (December 2020), available at: <http://www.whitechapelthinktank.co.uk/wp-content/uploads/2020/12/WTT-FPWG-Paper-Final-Singles.pdf>

<sup>77</sup> *Ibid.*

transactions which make use of CBDCs. If digital assets legislation is to be truly future-proofed, thought will need to be given to issues such as these further advances in technology. If settlement laws are to be expanded to a wider class of digital assets and amended to apply to tokenised financial markets, it is more likely that a mandatory centralised system will be more achievable than a truly decentralised model. The Law Commission will also, no doubt, consider the European Commission’s proposal for a DLT Pilot Regime when considering a regime for the U.K.<sup>78</sup>

## Insolvency

- 14.13. What happens on the insolvency of holders of digital assets or a DLT system is another issue that requires consideration in any law relating to digital assets. The UKJT set out in its Legal Statement that it had no doubt that digital assets could fall within the very wide definition of property in s. 436(1) of the Insolvency Act 1986.<sup>79</sup> The High Court judgment in *AA v Persons Unknown* supports this view.<sup>80</sup> A number of cases outside the U.K. have considered digital assets to form part of insolvent estates, bringing them within the powers of insolvency practitioners.<sup>81</sup>
- 14.14. The areas of legal uncertainty relating to insolvency seem to relate more to the categorisation of digital assets as property, money, commodities, debt claims, etc. and to practical issues relating to digital assets—for example, how one obtains control of a digital asset or the private key, how one can trace real life holders etc—rather than material issues with insolvency law itself.<sup>82</sup>

---

<sup>78</sup> European Commission, A Proposal for a Regulation on a pilot regime for market infrastructures based on distributed ledger technology (September 2020), available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0594&from=EN>

<sup>79</sup> See footnote 3.

<sup>80</sup> [2019] EWHC 3556 (Comm)

<sup>81</sup> See, for example, the helpful overview provided by Norton Rose Fulbright, *Cryptocurrency and insolvency: 2018 the year in review* (January 2019), available at: <https://www.nortonrosefulbright.com/en/knowledge/publications/39f45394/cryptocurrency-and-insolvency-2018-the-year-in-review>

<sup>82</sup> See, for example, Insolvency Lawyers’ Association, *Crypto-currencies and Insolvency Lecture* delivered by Mr Justice Zacaroli to the Insolvency Lawyers’ Association on 17 October 2019, available at: [https://www.ilauk.com/docs/ILA\\_-\\_AZ\\_Talk\\_Crypto-currencies\\_and\\_insolvency.pdf](https://www.ilauk.com/docs/ILA_-_AZ_Talk_Crypto-currencies_and_insolvency.pdf) and Corporate Rescue and Insolvency, *Dealing with crypto-assets in a downturn: Lessons from London and other jurisdictions* (1 June 2020), 3 CRI 90, which concludes:

Much remains to be settled in the public eye, but the UK’s insolvency legislation, together with the pragmatism of the UK courts, would appear to place this jurisdiction in a prime position to deal with the likely convergence of crypto-assets and corporate failure. The focus now appears to rest more on the practical issues of how to identify, take control of and realise crypto-assets.

14.15. Some of the issues of uncertainty concern:

- a) What it means to be the “owner” of a digital asset, including whether it is the person who controls the private key. The issue of control is discussed in more detail above. The Law Commission's paper on electronic trade documents puts forward the notion that possession (of property) is linked not only to tangible things, but also to factual control.<sup>83</sup> If this notion is adopted for digital assets, then consideration needs to be given to how this interacts with the notion of public/private key encryption. For example, if the private key is known by more than one person, the digital asset can be factually controlled by more than one person; does this amount to a form of shared or joint ownership, or is there only one 'owner' and, if so, how is this determined?
- b) How do you locate or trace the owner in a decentralised system where owners' real-world identities are not stored? This may be possible by tracing the transaction on the DLT system, but it takes time and requires expert input, which could delay and add to the cost of insolvencies. Even where you can trace the asset, you may still need the private key to regain control of it.
- c) Many digital assets can now be traded on exchanges, put up as collateral in staking programmes or lent in decentralised finance (“DeFi”) transactions. All these various uses of digital assets mean that they could be subject to other proprietary claims from third parties at any time; for example, are they held on trust or have they been assigned?
- d) There are also questions of value. Given the volatility of some digital assets, would an insolvency practitioner have to ascertain the value of the digital assets in terms of real-world assets, the date on which any digital asset is sold, the impact of increases in value, whether the digital asset can be distributed or if it has to be converted into fiat currency?

### **Section 53(1)(c) and section 136 of the Law of Property Act 1925**

14.16. Paragraphs 2.53 and 2.54 of the Call for Evidence explain the transfer of "tokenised" assets, noting that digital asset platforms or systems (including those that use DLT) are convenient for trading those tokens, and that parties operate with an expectation that when the tokens transfer on the system, so does the title to the digital or physical things

---

<sup>83</sup> See footnote 14.

represented by the token or the legal rights in that thing.

- 14.17. There are many legal structures that can be relied on in order to tokenise assets. These range from creating a contractual right to the delivery of the underlying asset—or benefits obtained under it—in favour of the token holder, recognising an equitable right of redemption similar to a security interest of the underlying asset in favour of the token holder and/or recognising a beneficial (equitable) interest in the underlying asset through an express or implied trust on behalf of the token holder similar to how "depository receipts" are normally structured in the financial markets. In many cases, a combination of contractual and beneficial ownership rights may be created in order to tokenise assets. This is particularly true in the context of tokenising securities.
- 14.18. However, under section 53(1)(c) and section 136 of the Law of Property Act 1925, an equitable interest (which an intermediary's customer has) and certain contractual rights must be transferred/assigned in compliance with certain written formalities. Section 53(1)(c) states:

a disposition of an equitable interest or trust subsisting at the time of the disposition, must be in writing signed by the person disposing of the same, or by his agent thereunto lawfully authorised in writing or by will

Section 136(1) states:

(1) Any absolute assignment by writing under the hand of the assignor (not purporting to be by way of charge only) of any debt or other legal thing in action, of which express notice in writing has been given to the debtor, trustee or other person from whom the assignor would have been entitled to claim such debt or thing in action, is effectual in law (subject to equities having priority over the right of the assignee) to pass and transfer from the date of such notice:

- a) the legal right to such debt or thing in action;
- b) all legal and other remedies for the same; and
- c) the power to give a good discharge for the same without the concurrence of the assignor:
- d) Provided that, if the debtor, trustee or other person liable in

respect of such debt or thing in action has notice

- e) that the assignment is disputed by the assignor or any person claiming under him; or
- f) of any other opposing or conflicting claims to such debt or thing in action;
- g) he may, if he thinks fit, either call upon the persons making claim thereto to interplead concerning the same, or pay the debt or other thing in action into court under the provisions of the Trustee Act, 1925

14.19. Whilst it remains unclear exactly how the property law analysis of tokens will operate, it is likely that English courts may characterise wallet providers and similar services as trusts. If this approach is taken, then the transfer of a token held within such a wallet is very likely to be characterised as a transfer of an equitable interest in the trust property. This creates the risk that English law may refuse to recognise the transfer for want of formality. The mere risk that this outcome could be reached will operate as a significant disincentive to use English law to govern legal relations in respect of tokens.

14.20. In the context of intermediated securities, there are arguments which may support the conclusion that these sections of the Law of Property Act 1925 would not apply as a matter of law to transfers of intermediated securities.<sup>84</sup> However, this remains a source of uncertainty and has not been addressed fully by the courts. In the context of tokenised assets, the sections in the Law of Property Act 1925 exacerbate legal uncertainty and in practice can be a contributing factor to avoid English law when considering the creation of tokenised trading platforms.

14.21. The Call for Evidence, at paragraph 2.39, refers to the UKJT observation that:

[an on-chain transaction] is not really analogous to the delivery of a tangible object or the assignment of a legal right, where the same thing passes, unchanged, from one person to another. Instead, the transferor typically brings into existence a new cryptoasset, with a new pair of data parameters: a new or modified public parameter and

---

<sup>84</sup> Some cite obiter comments of Hildyard J. in *SL Claimants v Tesco PLC* [2019] EWHC 2858 (Ch.) at [116] to support this.

a new private key.

This factual description of on-chain transactions has been relied on to suggest that sections 53(1)(c) and 136(1) of the Law of Property Act 1925 can be ignored in respect of transfers of digital assets representing underlying assets because the digital assets (or interests in the underlying assets) are not transferred at all. Instead, they are extinguished and new ones are created. This line of argument may be based on the idea that there is a novation, not a transfer, of digital assets—similar to *R v Preddy*, although *Preddy* concerned payments between deposit accounts (i.e. debts owed), not property rights.<sup>85</sup> In the response to question four above, the FMLC rejects this line of argument.

- 14.22. This analysis creates many practical problems, including in the context of theft (by hacking) or wrongful acquisition, and raises difficult questions, such as how security can be created over an asset which will change on purported transfer. There is legislative power to disapply section 53(1)(c) and section 136 of the Law of Property Act 1925 under section 8 of the Electronic Communications Act 2000, and such general disapplication should be made in favour of electronic transfers of tokenised assets or at least in favour of securities transfers (including in tokenised form or not). There is a precedent for this in Regulation 38(5) of the Uncertificated Securities Regulations 2001 (SI 2001/3755).

## 15. CONCLUSION

- 15.1. There is considerable legal uncertainty surrounding digital assets and the FMLC welcomes the Law Commission’s Digital Assets Project and the prospect of law reform which can help to provide legal certainty and predictability for digital assets. In the Committee’s view, attempting to reform the law in a way that addresses “digital assets” in the “very broad sense” identified in paragraph 1.20 of the Call for Evidence is likely to prove impracticable and to give rise to more uncertainty rather than less.
- 15.2. The need for law reform is most acute in respect of the narrower category of digital assets, as defined in this paper, since both the technologies underpinning these and the means by which they are being used in practice are novel and are not assimilated readily with other assets familiar to law and practice.

---

<sup>85</sup> [1996] Crim LR 726



15.3. On the overriding question of whether the law needs to recognise digital assets as capable of being in possession, the Committee's view is that it does. This should be done in a manner which is sensitive to those features of digital assets which are distinct. For this reason, the FMLC has proposed the recognition of a Third Category of property recognising digital assets as both intangible and yet capable of possession.

## FINANCIAL MARKETS LAW COMMITTEE MEMBERS<sup>86</sup>

Lord Thomas of Cwmgiedd (Chairman)

David Greenwald (Deputy-Chairman)

---

Andrew Bagley, Goldman Sachs International  
Sir William Blair, Queen Mary, University of London  
Claude Brown, Reed Smith LLP  
Raymond Cox QC, Fountain Court Chambers  
Michael Duncan, Allen & Overy LLP  
Simon Firth, Linklaters LLP  
Kate Gibbons, Clifford Chance LLP  
Carolyn H. Jackson, Katten Muchin Rosenman U.K. LLP  
Mark Kalderon, Freshfields Bruckhaus Deringer LLP  
Rachel Kent, Hogan Lovells (International) 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  
Rob Price, Bank of England  
Jan Putnis, Slaughter and May  
Barnabas Reynolds, Shearman & Sterling LLP  
Peter Spires, Lloyd's of London  
John Tribolati, J. P. Morgan Chase  
Sanjev Warnakula-suriya, Latham & Watkins LLP

---

Brian Gray (Interim Chief Executive)

<sup>86</sup> Note that Members act in a purely personal capacity. The names of the institutions that they ordinarily represent are given for information purposes only.