Initial Coin Offerings: Issues of Legal Uncertainty

July 2019

www.fmlc.org

Financial Markets Law Committee

Working Group[1]

Arun Srivastava (Chair)	Paul Hastings LLP
Nikita Aggarwal	University of Oxford
Douglas Arner	The University of Hong Kong
Peter Chapman	Clifford Chance LLP
Daniel Csefalvay	Bryan Cave Leighton Paisner LLP
Myriam Daher	Kramer Levin Naftalis & Frankel LLP
Stuart Davis	Latham & Watkins LLP
Scott Farrell	King & Wood Mallesons
Daniel Gabriel	Accenture
Jonathan Gilmour	Travers Smith LLP
Matt Feehily	Sidley Austin LLP
Carolyn H. Jackson	Katten Muchin Rosenman UK LLP
Mark Kalderon	Freshfields Bruckhaus Deringer LLP
Rachel Kent	Hogan Lovells International LLP
Ben Kingsley	Slaughter & May LLP
Sarah Lewis	Cleary Gottlieb Steen & Hamilton LLP
Vladimir Maly	Morrison & Foerster LLP
Hannah Meakin	Norton Rose Fulbright LLP
George Morris	Simmons & Simmons LLP
Wilf Odgers	Sherman & Sterling (London) LLP
Sam Robinson	CMS Cameron McKenna Nabarro Olswang LLP
Penny Sanders	Gowling WLG
Martin Sandler	Ernst & Young LLP
Nicole Sandler	Barclays Bank plc
Wendy Saunders	Herbert Smith Freehills LLP
Phil Smith	Allen & Overy LLP
Stuart Willey	White & Case LLP
Simon Wright	Dechert LLP
William Yonge	Morgan, Lewis & Bockius UK LLP
Joanna Perkins	FMLC Chief Executive
Virgilio Diniz	FMLC Project Manager

[1] 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 EXECUTIVE SUMMARY

1.1. The role of the Financial Markets Law Committee (the "**FMLC**") is to identify issues of legal uncertainty or misunderstanding, present and future, in the framework of the wholesale financial markets which might give rise to material risks and to consider how such issues should be addressed.

1.2. Initial Coin Offerings ("**ICOs**") typically use Distributed Ledger Technology (**"DLT"**) to offer transferable units ("**coins**" or "**digital tokens**") that confer various rights on the holder of record.[2] ICOs can be considered a means of fundraising using blockchain technology. At their outset, ICOs dealt with small amounts of money and small numbers of investors.[3] They have, however, now become a more mainstream way of acquiring funding, particularly for digital businesses.

1.3. The legality of an ICO depends on the jurisdiction in which it is located. China and South Korea have banned or suspended ICOs; some jurisdictions (Malta and the United Arab Emirates) have attempted to regulate them through the creation of new rules, and others, such as the E.U., have issued official warnings about potential dangers in investing in ICOs. In the United States, the Securities and Exchange Commission ("**SEC**") has taken the position that digital tokens issued in ICOs generally fall within the definition of a "security" under U.S. securities laws,[4] has issued a framework for the analysis of digital assets as "investment contracts",[5] as well as pursued a number of enforcement actions against ICOs. The range of regulatory responses across jurisdictions to ICOs—which by their nature are cross-border—has led to regulatory uncertainty and the prospect for regulatory arbitrage.

1.4. The legal characterisation of ICOs has emerged as an integral factor in the discussion around their regulation. Coins issued in an ICO may resemble a digital voucher of receipt in respect of rights. The nature of these rights vary from a license to use a product developed by the issuer ("**utility tokens**"), a financial asset in the form of a cryptocurrency ("**exchange token**") or one that enables participation in an asset or in a

---

2 IOSCO, *Research Report on Financial Technologies* (February 2017), available at: www.iosco.org/library/pubdocs/pdf/IOSCOPD554.pdf

3 Zetzche et all, *The ICO Gold Rush: it's a scam, it's a bubble, it's a super challenge for regulators,* (2017) available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3072298

4 Michaels and Vigna, "SEC Chief Fires Warning Shot against Coin Offerings", The Wall Street Journal, (9 November 2017), available at: https://www.wsj.com/articles/sec-chief-fires-warning-shot-against-coin-offerings-1510247148

5 SEC, "Public Statement "Framework for 'Investment Contract' Analysis of Digital Assets", (3 April 2019), available at: https://www.sec.gov/news/public-statement/statement-framework-investment-contract-analysis-digital-assets

non-asset pool ("**security token**"). The characterisation of any given ICO is, therefore, likely to be fact-dependent. The U.K. Financial Conduct Authority ("**FCA**") and the European Securities and Markets Authority ("**ESMA**") each recently adopted categorisation standards, proposing taxonomy by which cryptoassets may be categorised.[6]

1.5. A closely-related question is whether ICO issuance—or any attendant primary or secondary investment activity—falls within the existing regulatory perimeter. In the U.K., this question may be answered by examining whether an ICO constitutes a regulated activity for the purposes of the Financial Services and Markets Act 2000 (Regulated Activities) Order 2001/544 ("**RAO**") and, if so, whether the coins or tokens themselves constitute a specified investment under that legislation. There is also a debate about whether coins can be considered financial instruments for the purposes of Directive 2014/65/EU on markets in financial instruments ("**MiFID II**"), and whether tokens fit the definition of Electronic Money ("**E-Money**") under Directive 2009/110/EC on the taking up, pursuit and prudential supervision of the business of electronic money institutions (the "**E-Money Directive**").

1.6. When ICOs fall outside the existing regulatory perimeter, there is normative uncertainty as to how, if at all, the interests of consumers and investors might be protected. The answer is likely to be new—perhaps *sui generis*—regulation but that is not likely to be an insignificant undertaking. A vast network of rules is likely to be needed. As distributed token networks grow and ICOs become more mainstream, issues around consumer protection and market stability will become more central and pressing. While the existing regulatory regime may provide traditional safeguards, there are undoubtedly *lacunae* arising from the framework's inability to accommodate ICOs owing to the novel characteristics of the technology involved.

1.7. The FMLC considers that exploratory work on these issues would be of benefit to the financial markets and to regulators that are still assessing tokens on a case-by-case basis. The paper provides, in section 2, an overview of ICOs and the proposed categorisation standards. In section 3, it delves into the legal uncertainties which could arise from framing ICOs under specialised regimes, such as RAO and extended RAO, arising from the limitations of existing product regulation, authorisation requirements, settlement concerns and conflict of laws in cross-border ICOs. The paper considers existing registration/authorisation regimes and whether there are new categories of services

[6] For an explanation of these categorisation standards, see paragraph 2.3.

provider implicated in token issuance (e.g. "operator") for whom there is a case for registering or authorising. It analyses the existence of new market participants that are key to the cryptoasset market value chain ("**new actors**") and whether they should be regulated, including by considering whether activities of these actors that do not map neatly onto traditional regulated securities activities should also be regulated or permissioned ("**new permissions**"). It also analyses the limitations of existing product regulation and activities in this field with examples of regulatory "underlap" and considers what kind of bespoke regime could be constructed from existing financial regulations. Issues relating to conflict of laws with respect to the scope of DLT and ICOs are also considered in section 3 in view of the "distributed" nature of token transactions and the use of "nomad" participants and cloud services. Finally, Section 4 considers the potential impact of such uncertainties and section 5 proposes possible solutions.

2. BACKGROUND: ICOs AND THE EXISTING REGULATORY FRAMEWORK

2.1. An ICO is essentially a fundraising tool. A company planning an ICO creates a coin or digital token on a platform. In return for their capital, which might be in the form of crypto-currencies, investors in ICOs are entitled to a proportion of the new coins. The vast majority of ICOs differ from other fundraising methods, such as initial public offerings ("**IPOs**") or venture capital, where the investor typically gets an equity stake in the company. In some cases, the issue is designed to confer on investors in the ICO what is essentially a credit claim against the issuer; in others investors are intended to spend the tokens on the product created by the company. Investors may profit if they are able to trade the digital token once its value has appreciated.

Characterisation

2.2. In light of the diversity and potential hybrid nature of ICOs, the legal status of cryptoassets must be determined on a case-by-case basis. There have been different trends in "tokenomics" since the inception of the ICO market. For example, a wide range of asset classes have been tokenized and proposals to develop mainstream digital exchanges, such as the SIX Digital Exchange initiative in Switzerland, have emerged.[7]

[7] See *SIX Digital Exchange: The Securities Exchange of the Future* available at: https://www.six-group.com/en/home/blog/six-digital-exchange-future.html

2.3. The FCA, ESMA and the European Banking Authority ("**EBA**") have each attempted to categorise coins in recent publications. Although each authority in its report adopts different language, three main types of coins emerge: exchange, security and utility tokens.[8] Whilst the categories catalogued below are indicative of the main types of cryptoassets, it is important to note that these categories are not mutually exclusive, nor exhaustive. It is also possible that a cryptoasset may, during its lifetime, evolve in its nature and need to be categorised differently. For example, a utility token could initially grant a holder access to a platform, but subsequently become a widespread form of payment, making it resemble an exchange token more closely. The following paragraphs set out brief descriptions of the three main categories of cryptoassets, their interaction with the existing regulatory perimeter and some examples.

Exchange Tokens

2.4. Exchange tokens are intended as a form of payment for goods. In a key distinction from other tokens, they are intended to function independently of the issuer or any underlying business or asset, operating as a unit of inherent value and as an alternative to fiat currency. Exchange tokens operate on a peer-to-peer basis and without the traditional intermediaries associated with the financial system. They are not yet widely accepted as a means of payment, largely owing to market inertia but perhaps also owing in part to the volatility of some of the better known examples. This type of token includes traditional cryptocurrencies such as Bitcoin and Litecoin. In 2017 Filecoin issued a cryptocurrency token by way of an ICO which enabled the prospective holder to swap a range of cryptocurrencies, including Bitcoin, in return for Filecoins. The deal is in the public domain.[9]

2.5. One variety of exchange tokens is the "stablecoin", which is pegged against the value of a fiat currency. As such, these tokens share characteristics of E-money. On 18 June 2019, Facebook announced its plans to launch a new stablecoin called Libra.[10] Regulatory authorities in several jurisdictions have called for close scrutiny of the project. The FCA has expressed concerns about the size and scale of the project and

---

[8] FCA, *Guidance on Cryptoassets—Consultation Paper CP 19/3* and *Advice—Initial Coin Offering and CryptoAssets*, (both January 2019) available at: https://www.fca.org.uk/publications/consultation-papers/cp19-3-guidance-cryptoassets

ESMA, *Advice: Initial Coin Offerings and Crypto-Assets*, (9 January 2019), available at: https://www.esma.europa.eu/press-news/esma-news/crypto-assets-need-common-eu-wide-approach-ensure-investor-protection

[9] Available at: https://icobench.com/ico/filecoin and https://www.ccn.com/257-million-filecoin-prepares-for-impending-launch. The ICO raised U.S.$157,800,000 and allows coin holders to own a distributed electronic currency.

[10] Libra Association, *Libra White Paper* (18 June 2019), available at: https://libra.org/en-US/white-paper/.

has stated that it will monitor Facebook's proposal together with the Bank and HM Treasury.[11] The European Commission has similarly expressed concerns about the potential concentration of personal and financial data.[12] The Chairman of the U.S. Federal Reserve stated that Libra raises many serious concerns regarding privacy, money laundering, consumer protection and financial stability.[13]

Security Tokens

2.6. These cryptoassets have characteristics akin to traditional securities, such as shares or debt instruments. Security tokens are tied to the underlying business of the issuer and will grant the holder some form of rights in the business. These tokens typically provide income to the holder, depending on the profits of the underlying business. In some instances, the holder of the token will also be entitled to vote on matters concerning the business. A security token-holder thus resembles a shareholder in several ways. Issuers often include the rights that an investor may have under a company's articles or shareholders' agreement in the token's white paper. For example, there have been instances where tokens are subject to "drag along" and "tag along" provisions, more readily associated with shareholdings.

2.7. The fact that these tokens are in a more familiar form means that they are more likely to fall within the existing regulatory perimeter, depending on their exact characteristics. For purposes of U.K. law, they are likely to meet the definition of a specified investment as defined in the RAO, or, for the purposes of E.U. law, are likely to meet the definition of a financial instrument as defined in MiFID II. Where such tokens are to be offered to the public (and do not qualify for an exemption), they are likely to be subject to Regulation (EU) 2017/1129 on the prospectus to be published when securities are offered to the public or admitted to trading on a regulated market ("**Prospectus Regulation**").[14] As an example of this, HydroMiner recently published a prospectus in respect of its H3O token, which includes certain share-like rights.[15]

---

11 FCA, Regulating Financial Innovation: Going Behind Scenes, (2 July 2019), available at: https://www.fca.org.uk/news/speeches/regulating-financial-innovation-going-behind-scenes.

12 Helmore, "Facebook's Libra cryptocurrency faces questions from international regulators", *The Guardian* (25 June 2019), available at: https://www.theguardian.com/technology/2019/jun/25/facebook-libra-cryptocurrency-regulation.

13 Chair Jerome H. Powell, *Semiannual Monetary Policy Report to the Congress*, (10 July 2019), available at: https://www.federalreserve.gov/newsevents/testimony/powell20190710a.htm.

14 Please note that this FMLC does not offer legal advice and that this should not be construed as such.

15 HydroMiner, Press Release: HydroMiner's Capital Market Prospectus is approved, (30 November 2018), available at: https://medium.com/@hydrominer/hydrominers-capital-market-prospectus-is-approved-6e4b72896480?source=rss-be0581675b12------2

Utility Tokens

2.8. Utility tokens are typically offered whilst the issuer is developing a platform. The issuer uses the funds received from the sale of the tokens towards the development of the platform. Utility tokens do not generally entitle the holder to any rights in the business. Utility tokens can be structured in a number of different ways, but generally grant the holder (early) access to the platform or the ability to redeem the token for goods or services (or as a discount for such goods or services). In this sense, utility tokens resemble rewards-based crowdfunding, whereby the holder of the utility token retains no ownership rights in the issue.

2.9. These cryptoassets are likely to fall outside the regulatory perimeter, although owing to their ability to be exchanged for goods or services, utility tokens could potentially be considered E-Money and therefore be subject to the E-Money Regulations. Given the limited spending potential of utility tokens, which are only intended to be used within a platform created by the issuer, however, this may be less likely. In 2017, Binance issued a utility token by way of an ICO which enabled the prospective holder to swap a range of cryptocurrencies, including Bitcoin, in return for BNB coins.[16]

ICOs under Existing U.K. and E.U. Regulation

2.10. Carrying out activities involving cryptoassets that fall within the regulatory perimeter requires authorisation by the relevant regulator and compliance with applicable regulations, including the RAO, the financial promotion rules under the Financial Services and Markets Act 2000 ("**FSMA**"), the Prospectus Directive and Directive (EU) 2018/843 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing ("**5MLD**"), which will replace Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing ("**4MLD**").

2.11. In the U.K., whether an ICO is regulated depends on how it is structured and what the token subsequently represents. In other words, when tokens represent a security such as shares or bonds, or other specified investment such as a unit in a collective investment

[16] The deal is in the public domain and documents can be found at https://icorating.com/ico/binance-bnb/ and https://www.binance.com/resources/ico/Binance_WhitePaper_en.pdf . The ICO is believed to have raised in the region of $15,000,000 and provides holders with a discount on any fees which are incurred whilst trading on the Binance trading platform.

scheme ("**CIS**"), the relevant ICO would fall within the FSMA/RAO regulatory perimeter and be subject to regulatory supervision by the FCA. Security tokens that constitute transferable securities will fall within the definition of financial instruments under MiFID II. As the definition of specified investments under the RAO is broader than the definition of financial instruments under MiFID II, a cryptoasset may be a specified investment under the RAO, but not a financial instrument under MiFID II. If the token can be transferred from one person to another—i.e., ownership of the token is transferred, giving the person who acquires the token good legal title to it—the FCA considers the relevant security token negotiable in the capital markets and, therefore, categorised as a transferable security under MiFID II.

2.12. Depending on their specific characteristics, other U.K. and E.U. laws and regulations would apply to activities in cryptoassets. The Electronic Money Regulations 2011 might apply to the extent that utility tokens include features which fall within the definition of E-Money activities, as might the Payment Services Regulations 2017 to the extent the token constitutes "funds" within the meaning of those Regulations or otherwise involves or facilitates payment services in funds (for example where the token is used as a vehicle for remitting fiat currency).

Exploratory Work in the E.U.

European Securities and Markets Authority's Advice on ICOs and Cryptoassets

2.13. ESMA's Advice on ICOs and Cryptoassets (the "**ESMA Advice**") took a technology-neutral approach, attempting to clarify whether the existing E.U. regulatory framework applies to ICOs and cryptoassets and, if yes, whether any clarifications or amendments are required for its effective application.[17] It considered whether new regulations should be introduced to cover any ICOs and cryptoassets that fall outside of the existing E.U. regulatory framework. In ESMA's view, the modest size of the cryptoasset sector does not currently raise financial stability concerns, largely because investments in cryptoassets generally have been made through savings rather than through the use of leverage. Other financial regulators and the Financial Stability Board ("**FSB**"), however, have published reports exploring the possibility that ICOs pose such risks to

17 See ft 8, *supra*.

financial stability and might increase the incidence of financial crime.[18] ESMA considers investor protection and market integrity to be priorities, identifying fraud, cyber-attacks, money laundering and market-manipulation as the most significant risks.[19] On the other hand, ICOs and crypto-assets are considered to provide potential benefits to the E.U. market, including by providing alternative funding sources, raising capital from a diverse group of investors quickly and efficiently, expanding investment opportunities, reducing the need for intermediaries and facilitating a faster and easier transfer of ownership. ESMA identified six cryptoassets that are currently potentially available to E.U. investors, including investment- and utility-type cryptoassets, hybrids of the two as well as payment-type cryptoassets.[20] It considers that cryptoassets with attached profit rights might be considered "transferable securities" or another type of "financial instruments". ESMA notes, however, that E.U. financial securities laws do not contain a definition of cryptoasset (see paragraph 3.5 below).[21]

2.14. With regards to cryptoassets that do not qualify as transferable securities or other financial instruments, ESMA indicated that the National Competent Authorities ("**NCAs**") in many Member States considered utility-type cryptoassets to be outside of existing E.U. financial regulations. ESMA noted that while individual NCAs are considering the rules applicable to such cryptoassets, the lack of an E.U.-wide approach could lead to the creation of an uneven playing field.[22]

---

18 See FSB update on crypto-assets dated 31 May 2019, available at: https://www.fsb.org/2019/05/crypto-assets-work-underway-regulatory-approaches-and-potential-gaps/; and ECB Crypto-Assets Task Force "Crypto-Assets: Implications for financial stability, monetary policy, and payments and market infrastructures" Occasional Paper No 223/May 2019 available at: https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op223~3ce14e986c.en.pdf?f29e06158fa2a6cdb7b909ce3e20ee22

BCBS statement on crypto-assets dated 13 March 2019, available at: https://www.bis.org/publ/bcbs_nl21.htm ; Bank of England Financial Policy Committee statement, from meeting on 12 March 2018, section covering crypto-assets, available at: https://www.bankofengland.co.uk/statement/fpc/2018/financial-policy-committee-statement-march-2018

19 ESMA Advice, pp. 14-17.

20 See Annex I to the ESMA Advice.

21 ESMA notes that the term "virtual currencies" is defined in Directive 2018/843 of the European Parliament and Council of 30 May 2018 amending the Anti-Money Laundering Directive (EU) 2015/849. "Financial instruments" are defined in MiFID II as "inter alia" transferable securities, money market instruments, units in collective investment undertakings and a comprehensive set of different types of derivatives transactions. Article 4(1)(44) of MiFID II defines transferable securities to include negotiable securities such as shares in companies, the equivalent to shares in companies for partnerships and other entities, depositary receipts in respect of shares, bonds, etc. See ibid, pp. 18-19.

22 ESMA Advice, p. 19.

European Banking Authority's Report on Cryptoassets

2.15. Earlier this year, the EBA published a Report (the "**EBA Report**") with advice for the European Commission on cryptoassets.[23] Its purpose was to assess the applicability and suitability of current E.U. laws on cryptoassets, mainly their categorisation under Directive (EU) 2015/2366 on payment services in the internal market ("**PSD2**") and Directive 2009/110/EC on the taking up, pursuit and prudential supervision of the business of electronic money institutions ("**EMD2**"), as well as custodian wallet services and trading in cryptoassets, in a banking context. The EBA's analysis found that cryptoasset-related activity in the E.U. is relatively limited and so their use does not give rise to implications for financial stability. It concludes that, in general, cryptoassets fall outside the scope of E.U. financial services regulation (other than in the limited cases where they may qualify as E-Money), and are not recognised in any Member State as fiat money, deposits or other repayable funds.

2.16. Cryptoassets have been found to fall outside the scope of regulation when traded through digital platforms operated by providers engaged in exchange services between cryptoassets and fiat currencies or other cryptoassets. The provision of custodian wallets services, which safeguard/store private cryptographic keys granting rights to access and transfer cryptoassets is a similarly unregulated activity (although some exchanges provide linked wallets holding fiat currency which are classified as E-Money products). Under current regulation, there are a few other cases where cryptoassets have been treated as E-Money.[24] The regulatory position, however, will change under 5MLD with such activities becoming supervised for anti-money laundering compliance.

The Lifecycle of an ICO

2.17. Importantly, the technologies underpinning ICOs—notably, blockchain (used as a distributed ledger and typically managed by a peer-to-peer network)—have their own governance frameworks and mechanisms that influence and support the functioning of ICOs. For example, Ethereum, the most popular blockchain platform for ICOs, is supported by the "ERC-20" technical standard, which defines a list of rules for implementing Ethereum tokens on Ethereum-based smart contracts. Likewise, all

[23] EBA Report with advice for the European Commission on crypto-assets (January 2019), available at: https://eba.europa.eu/-/eba-reports-on-crypto-assets

[24] Where tokens are used to make payments through a block-chain based payment network. The token are pegged to a given currency (e.g., 1 token = 1 Euro), or the case of the use of tokens on a charitable giving site. A donor credits fiat donations to a platform and in exchange receives tokens to the equivalent value which can be used to make donations to a charity. In both instances, the tokens are issued on receipt of fiat currency and therefore have an intrinsic monetary value. A coin issued as part of an ICO could be treated in the same way, where it has an intrinsic monetary value.

blockchains are governed by consensus protocols or algorithms (such as proof-of-work and proof-of-stake) which manage inter-node communication and the formation of new blocks. Efforts are also being made to develop an ISO certification process for blockchain. The terms and conditions of an ICO are governed by blockchain based smart-contracts, which are becoming increasingly standardised.

2.18. There are various stages in the process of an ICO. An issuer with an idea for which it is seeking funding via an ICO will engage technical advisers in relation to the underlying technology, design and characteristics of the token. A white paper will be prepared setting out the terms of the offering. At the sale stage, wallet providers may be engaged to store public and private keys used to send/receive new tokens. The tokens may then be subject to secondary trading on an exchange. The table below demonstrates the new actors and activities arising in relation to ICO assets which are not covered by the traditional regime applicable to financial instruments but which should be considered in the context of the applicable regulatory framework.

Novel actors	**Role in ICO lifecycle**
Developers	Produce code/protocol creating ICO asset, potentially using smart contract incorporating conditions or criteria set out in white paper.
DLT network	Network on which transfer of assets to investors is recorded[25].
Miner(s) (included within DLT network)	Part of the DLT network that chooses which transactions to verify; these are verified by computing a complex mathematical problem the outcome of which, if criteria are satisfied, is the recording of the transaction to the network. Miners get paid a fee for each transaction processed[26].
Issuer-appointed digital custodian	For holding of investor funds prior to completion.
Digital regulator[27]	Approval of issuance—criteria specific to ICO

[25] For fuller descriptions of what constitutes a DLT network please see paragraph 20 of the ESMA Advice, the definition provided within the Malta Digital Innovation Authority Act 2018, extracted in Appendix 1 to this paper, and the definition within the Gibraltar Financial Services (Distributed Ledger Technology Providers) Regulations 2017, extracted in Appendix II. The Government of Gibraltar and the Gibraltar Financial Services Commission are developing a legal and regulatory framework which will be aligned to the DLT framework, for the sale, promotion or distribution of tokens.

[26] For a fuller description of the activity of miners, see ESMA's 'Advice on Initial Coin-Offerings and Crypto-Assets at paragraphs 29 to 30.

[27] Not all the actors named in this table are essential; some may arise from secondary market practice or the specific model of regulation adopted.

	issuance.
Traditional market participants interact with novel actors as follows:	
Exchange platform—secondary trading	Investors may choose to trade their ICO asset on an exchange. The trade may be effected either: - via the DLT network, or - simply on exchange without being recorded on the DLT network.[28]
Custody service	Storage of private key (private computer code) needed to effect transfer of ICO assets. This may be in cold (not network-connected) or hot (network-connected) storage[29].

3. ISSUES OF LEGAL UNCERTAINTY

3.1. As outlined in the previous section, the application of the current regulatory perimeter to ICOs depends on the characterisation of the coins/tokens issued in the offering. In many instances, the tokens issued in an ICO will be treated as if they are securities. If so, regulatory requirements will apply with consequences for new actors and activities within ICOs. Where the coins are not treated as securities or other forms of regulated investments, they do not fall within the existing regulatory perimeter, and are therefore considered unregulated assets for which other laws and regulations may need to be considered. This section explores uncertainties arising in each of these cases. Issues of legal uncertainty surrounding new actors, technology owners and service providers in the ICO market will also be considered in this section.

U.K. regulatory perimeter: characterisation as an investment for RAO purposes

3.2. The structure of the RAO is such that, to be regulated, a token will need to fall within an existing specified category of investment, such as shares, bonds and debentures, or units in a collective investment scheme.[30] To the extent that tokens are categorised as

[28] As noted in ESMA's 'Advice on Initial Coin-Offerings and Crypto-Assets', Appendix 2, in relation to centralised platforms it is usually only when users deposit/withdraw their crypto-assets at the platform that the transaction is recorded on DLT (on-chain). The rest, eg. matching of orders, the execution of orders and the corresponding transfer of ownership between users, is typically recorded on the books of the platform only (off-chain). This gives rise to hacking risks as platforms are then a single point of failure, and also settlement issues where settlement is not dependent on DLT.

[29] See discussion of digital wallets in ESMA's 'Advice on Initial Coin-Offerings and Crypto-Assets' at paragraphs 25 to 27.

[30] The position can be contrasted with the position in the United States, where regulators have taken a more aggressive approach to enforcement in the cases of ICOs which have not been registered as securities offerings. The regulatory system in the United States applies the "Howey test" to defining whether an asset constitutes a security. This is a broader test than

specified investments under the RAO, it is still not clear whether the regulation of other related activities, such as advising, dealing, arranging and providing custody, will be extended to apply to such activities in relation to tokens and ICOs. Tokens that constitute securities will presumably remain subject to the current framework for the regulation of public offers (and the exemptions that are available under that system). The issue in relation to other tokens is determining the appropriate form of regulation, including whether a prospectus, prospectus-lite or white paper obligation should be introduced, and what mandatory disclosure and risk warning obligations should be imposed. The prevailing form of disclosure for ICOs—the so called white paper—generally offers limited information about the issuer and the project being financed, particularly with respect to the potential financial risks involved. There is, furthermore, no uniformity in the content of white papers between different ICOs.[31]

3.3. With regard to the activities of advertising and financial promotion, the U.K. has a framework for regulating marketing under the financial promotion rules, however there are various exemptions from these restrictions under FSMA. It is, therefore, unclear how the financial promotion rules would be applied to tokens, particularly where they are not in the form of securities. Similarly, the FCA Handbook contains conduct of business rules ("**COBS**") that govern how regulated firms advise, promote and sell investments to their clients. It is unclear how COBS may need to change in the event that tokens become regulated investments. The Financial Services Act 2012 ("**FSA**") contains further provisions preventing persons from making misleading statements or engaging in any conduct which creates a false or misleading impression as to the market in, or the price or value, of any relevant instruments under certain conditions.[32]

3.4. There are also questions as to how market conduct obligations should be extended to ICOs. Directive 2014/57/EU on criminal sanctions for market abuse (the "**Market Abuse Directive**") and other legislation, such as the Criminal Justice Act 1993, regulate market conduct to ensure that parties do not engage in manipulative behaviour, for which there is potential when tokens are traded on an exchange. Likewise, HM Government has drawn attention to anti-money laundering concerns in relation to

---

in the U.K., focusing on whether the investor is investing money in a common enterprise and is led to expect profits from this enterprise generated by a third party. See https://www.sec.gov/news/speech/speech-hinman-061418

[31] There are, however, increasing efforts at self-regulation, such as the platform "Waves" which has established a self-regulatory body to establish standards for the ICO industry, including legal, tax and know-your-client ("**KYC**") requirements

[32] Sections 89 and 90 of the FSA.

ICOs, some of which might be addressed through the 5MLD.[33] The creation of new regulated activities may engender new anti-money laundering and counter-terrorism financing obligations in other contexts.

Cryptoassets that qualify as Transferable Securities or other Financial Instruments

3.5. Whether or not a cryptoasset is a financial instrument is a determination to be made by each individual Member State's National Competent Authority ("**NCA**"). NCAs have defined the term "financial instrument" differently in the transposition of MiFID II into their national laws, leading to a lack of consistency in the definition of "financial instrument" across Member States. This creates uncertainty and gives rise to the risk of regulatory arbitrage in the particular context of ICOs.[34] Moreover, a cryptoasset which has profit rights attached to it would likely be qualified as a transferable security; it would not necessarily need to have ownership rights attached to it. There are concerns, however, about the potential collateral effects of classifying all cryptoassets as some form of financial instrument, including risks arising from potentially granting cryptoassets unwanted legitimacy by regulating them. Furthermore, regulating cryptoassets as financial instruments brings new challenges arising from the unique characteristics of the underlying technology, including its decentralised nature and the risk of forks—i.e., when a single cryptocurrency splits in two owing to a change in the code. Some cryptoassets share the distinguishing characteristics of more than one traditional financial instrument, which might mean that some existing regulations applicable to financial instruments require modification. As such, differences between cryptoassets and more traditional financial instruments could arise in the areas of clearing, settlement, custody and safekeeping, and record of ownership, amongst others.

3.6. In its Advice, ESMA states that for any cryptoasset that qualifies as a "financial instrument", existing E.U. financial regulation could potentially provide a robust regulatory regime. The Prospectus Directive, MiFID II, Market Abuse Directive, Regulation (EU) No 236/2012 on short selling and certain aspects of credit default swaps (the "**Short Selling Regulation**"), Regulation (EU) No 909/2014 on improving securities settlement in the European Union and on central securities depositories (the "**Central Securities Depositories Regulation**") and Directive 98/26/EC on settlement finality in payment and securities settlement systems (the "**Settlement Finality**

[33] See *House of Commons Treasury Committee on Crypto-assets – twenty-second report of session* (2017-19) available at: https://publications.parliament.uk/pa/cm201719/cmselect/cmtreasy/910/910.pdf

[34] ESMA has the view that payment-type crypto-assets re unlikely to be considered "financial instruments" under EU legislation.

Regulation") should apply to such cryptoassets as they would to transactions in any financial instrument. There are, however, certain gaps and therefore potential areas of legal uncertainty which will arise when applying the existing E.U. regulatory framework to those cryptoassets that qualify as financial instruments.

3.7. ESMA identified three areas specific to cryptoassets that merited further consideration and clarification.[35] The first is custody and safekeeping services in a DLT environment, including the safekeeping of private keys. The second is how settlement and settlement finality should be applied to cryptoassets, including determining the role of miners—i.e., individuals engaged in the process of verifying, validating and adding cryptocurrency transactions to the blockchain digital ledger—in the settlement process. The third is the technology underpinning cryptoassets and whether regulation is required to ensure that the underlying protocols, smart contracts and cyber security protections meet minimum reliability and safety standards. This paper considers these issues in more depth below.

Cryptoassets that do not qualify as Transferable Securities or other Financial Instruments

3.8. ESMA is concerned that consumers will be exposed to substantial risks for any cryptoasset that does not either qualify as a financial instrument or is not currently covered by the E-Money Directive, and agrees with the conclusion in the EBA Report that AML regulation should apply to all cryptoassets and related activities.[36] Divergent approaches to the regulation of these activities, however, are emerging across the E.U., which could give rise to potential risks.

Consumer protection issues

3.9. The existence of a relatively liquid secondary market for some ICO tokens grants a level of protection to investors who may, at certain points, trade their tokens on a crypto-currency exchange and thereby cash out their investment.[37] Despite this, the mostly disintermediated nature of the ICO market means that investors are subject to a greater risk of financial loss arising from fraud or manipulation by issuers. In traditional capital markets, information intermediaries such as broker-dealers, underwriters, legal and investment advisers play an important role in overcoming the asymmetry of information

[35] ESMA Advice, pp. 13-17.

[36] ESMA Advice, pp. 5, 36

[37] It is possible, however, that the scope for exit may be more limited in practice, given that it is more difficult to trade tokens in exchange for traditional currencies rather than crypto-currencies.

between issuers and retail investors. While there is a trend towards greater intermediation of ICOs, particularly through the involvement of legal and financial advisers and exchanges in the primary and secondary markets,[38] this remains a concern. The activities described in the previous section might give rise to risks in relation to consumer protection, such as the absence or inadequacy of conduct of business rules (covering risks disclosures), suitability checks, governance arrangements, custody/segregation rules relating to cryptoassets, advertising rules potentially resulting in misleading communications or promotions, compensation schemes such as a deposit guarantee scheme, procedures for handling redress or complaints, and lack of a legal framework determining the rights or obligations of each party, especially liability rules.

The existing registration and authorisation regime and requirements

3.10. To the extent that tokens fall within the regulatory perimeter, authorisation and registration requirements—e.g., under FSMA—will be relevant. Although a comprehensive survey of authorisation and registration requirements under foreign laws is outside of the scope of this paper, it is clear that these requirements are also relevant in a number of other jurisdictions. For instance, tokens offered in connection with an ICO in the U.S. will be classified as securities if the ICO is presented to purchasers as an investment opportunity, whether explicitly or implicitly. Such tokens cannot be lawfully sold without registering with the U.S. Securities and Exchange Commission or utilising a relevant exemption.

Implications of DLT network operations

3.11. Once the ICO asset has been created, it will need to be transferred to investors who have purchased it via the distributed ledger technology network. A report published in July 2018 by a taskforce of representatives from HM Treasury, FCA and the Bank of England (the "**Cryptoassets Taskforce Report**") indicated support for the development of DLT.[39] The authors expressed some concerns in relation to governance challenges particularly in permissionless networks, and in relation to the point of settlement/finality. The key governance challenge in this respect is whether ICO assets on both permissioned and permissionless networks should be brought within the regulatory perimeter.

---

[38] Meng Shi, M., "Germany's second-largest stock exchange is developing an ICO platform", *Coindesk*, (2 August 2018), available at: https://www.coindesk.com/germanys-no-2-stock-exchange-is-developing-an-ico-platform

[39] HM Treasury-Financial Conduct Authority-Bank of England Cryptoassets Taskforce, *Final* Report (July 2018), available at: https://www.fca.org.uk/news/news-stories/cryptoasset-taskforce-publishes-report-uk-approach-cryptoassets

3.12. DLT networks can be either (i) permissioned, whereby only specified users can add and validate entries to the ledger, or (ii) permissionless, whereby anyone can build and verify entries to the ledger. There are advantages and disadvantages applicable to each type of network. Permissioned networks are inherently more secure owing to the control exercised over access and validation by a (more centralised) entity, which can be subject to regulation and governance. As such, more effective oversight can be exercised over participants in a permissioned network. Such networks do, however, require participants to place a higher degree of trust in the centralised entity managing the network, which could discourage some parties from using the network. Furthermore, permissioned networks, being more centralised, are more susceptible to cyber-attacks.

3.13. On the other hand, permissionless networks require significantly more computing power and energy to operate. Given the larger number of nodes in permissionless networks, completion of transactions can be time consuming. Furthermore, anyone can become a miner, thereby increasing the risk of rogue operators. In permissionless networks, making changes to consensus protocols can also be very difficult without serious code rewrites, and it can take a large amount of effort to ensure that new protocol software is effectively distributed.

Lifecycle of actors and activities

Settlement concerns

3.14. A further area of legal uncertainty concerns the settlement of ICOs and whether the underlying DLT network is a "securities settlement system" ("**SSS**"). Legislative requirements and protections for SSS are addressed to the "operator", which may not be identifiable in relation to a decentralised DLT network. Such an operator may need to be authorised as a central securities depository ("**CSD**") or work with an authorised CSD. Participation in an SSS is limited to certain specified entities, whereas participants of DLT networks are typically individuals, which creates both a normative and a descriptive issue for regulation in this area. Moreover, were the legislation for SSS to apply, the network and its participants would also need to comply with settlement timeframes. This would likely give rise to issues relating to settlement finality, particularly considering the consensus validation process and the risk of forks, as well as delivery-versus-payment ("**DvP**") where there is a cash leg of the trade not processed on DLT. As noted by the Cryptoassets Taskforce Report, it can also be time-consuming to ensure that all participants in the DLT network agree on the same version

of the ledger.[40] It is possible that a transaction that appeared to have been successfully completed is overwritten with a different version of the ledger. This would primarily be a concern in permissionless networks, as in permissioned networks consensus mechanisms can be designed to ensure that the point of final settlement is much clearer.

Miners

3.15. The FCA is currently of the view that miners are unlikely to be carrying on regulated activities; it is, however, worth considering whether they should be regulated. Miners perform consensus validation and therefore play a key role in the settlement process. In other jurisdictions, such as Malta, they are categorised as users.[41] However, it is not clear that miners should have the same status as consumers and other network users. Miners do effectively play a key role in settlement, albeit in permissionless networks it may be difficult to identify miners.

3.16. There are several arguments in support of regulating miners: Miners are not subject to price restrictions and therefore can charge high fees for mining transactions. Whilst pricing is not generally the subject of regulation by the FCA, miners are not subject to fair customer treatment principles and so it is conceivable that ICO assets could be rendered worthless if fees for transfer are too high. Potential competition concerns could also arise depending on the nature of the network. Miners also have no obligation to carry out orders that they are instructed to complete and have the power to manipulate the market by carrying out transactions for some but not all instructing parties, in the order they choose. Miners play a key role in forks, when they make a conscious change to the underlying rules of the protocol, which can cause assets to become obsolete. Their decisions to change the underlying rules, particularly in the event of contentious hard forks, can advantage some market participants over others. Market participants are reliant upon miners processing transactions accurately, to prevent duplication of digital assets ("**double spending**"). Collusion among cryptocurrency miners can disrupt the safe and timely transfer of cryptocurrency. If independent miners pool their resources and control enough processing power then they can increase the chance that they will be the first to find a solution and extract higher profits by manipulating the order in which cryptocurrency transfers are recognised on the blockchain.

---

40 Cryptoassets Taskforce Report, p. 10

41 Part 1, section 2 of the Malta Digital Innovation Authority Act 2018

3.17. On the other hand, regulating miners could have disadvantages. It could impede growth in the number of miners, decreasing the speed at which transactions are verified and growth of the sector in general. As a matter of enforcement, identifying miners (especially in permissionless networks) could present practical challenges, particularly where they are located in different jurisdictions that might not be subject to co-operation agreements.

Exchanges

3.18. With regards to exchange-listing criteria, it is important to highlight that given the technological aspects of financial instruments that are ICO assets, it may be necessary to expand listing criteria to take into account requirements that are specific to this particular type of asset.[42]

Custody

3.19. Custody of an ICO asset is another area of legal uncertainty, as the safeguarding of ICO assets presents idiosyncratic challenges. This is illustrated by the loss reported on 6 March 2019 of CA$250m from the wallets of the Canadian cryptocurrency exchange Quadriga.[43] The initial difficulties were about gaining access to the wallets expected to contain the cryptocurrency; however, upon gaining access, the wallets were found to be empty. Therefore, whilst firms may already hold the permission to safeguard financial instruments, it is suggested that there should be a specific permission based on a demonstration of requisite resources and competence to safeguard ICO assets. Technology in this area is still at comparatively early stages and its development will need to be kept under review to make sure that the regulatory framework remains fit for purpose.

Limitations of existing product and activities regulation and regulatory "underlap"

3.20. As seen in the previous sections of this paper, neither the U.K. nor the E.U. considers that all cryptoassets fall within scope of specified investments and financial instruments, as defined respectively. Moreover, even for cryptoassets that are regulated, it may be necessary to extend and, in places, amend, the existing regime to more appropriately

[42] These may include, for example, the technological experience, track record and reputation of the issuer and its development team, the issuer's cybersecurity systems and controls, the availability of a reliable multi-signature hardware wallet solution for the asset, details of the protocol and underlying infrastructure—including whether it leverages a new or existing architecture system and whether it is scalable—the relevant consensus mechanism, whether the ICO asset has any in-built anonymisation functions and if so whether the holder of the ICO asset can be identified, as well as any other technology specific risk factors.

[43] Available at: https://cointelegraph.com/news/canadian-crypto-exchange-quadrigacx-officially-declared-bankrupt

accommodate the types of participants and activities that are undertaken in relation to cryptoassets.

3.21. The House of Commons Treasury Committee on Cryptoassets has opined that cryptoassets and activities in relation to them should be subject to specific regulation as a class and has suggested that the quickest way to do this would be to extend the RAO, so that the issuance of ICOs and the provision of crypto exchange services are included. This would be considerably quicker than creating a new framework of regulation. The U.K.'s Cryptoasset Taskforce has committed to consult further to explore whether the regime needs to be extended so as to ensure that FCA regulation can be applied to all cryptoassets that have comparable features to specified investments, regardless of how they are structured.

3.22. Extending the scope of specified investments under the RAO may not achieve the desired effect without also extending the types of specified activity that can be undertaken in relation to them, given that the participants in DLT structures and the activities they undertake do not fit the existing legislative descriptions very well. Authorisation for regulated activities requires a business to be organised, capitalised and conducted on a day-to-day basis in a way that complies with the applicable detailed rules which would likely need to be adjusted for cryptoassets in a number of respects. The nature of authorisation is that it is designed for the carrying on of the relevant business on an ongoing basis rather than as a one-off event like capital issuance. A company issuing its own shares has traditionally been excluded from the regime, although there are now situations where this is captured by the activity of executing client orders under MiFID II.

3.23. This is not to suggest that token issuers that intend to use the capital they raise to develop a business which involves carrying on a regulated activity should not be regulated in the same way as any other such business. The FMLC considers that it might be helpful to differentiate the activity of issuing and the activity of running a business after the point of issuance.

Conflict of Laws in DLT

3.24. As described in section 2 of this paper, cryptoassets issued through ICOs primarily depend on DLT. In a DLT system, which can be either permissioned or permissionless, the control of the database is typically decentralised; that is, transactions are performed by multiple (or all) network participants, without a central administrator ensuring the consistency or integrity of data across the participants. DLT systems also involve the

"intermediation" of securities; i.e., securities are held indirectly through a chain of intermediaries. As examined in detail in a previous FMLC paper (the "**FMLC DLT Paper**"),[44] and as summarised below, there are significant issues of uncertainty regarding the proprietary effects of DLT transactions in financial instruments or assets.

3.25. The traditional approach under private international law is that a question as to rights or entitlement should be determined by the law of the location of the assets in question (*lex situs*). Given the decentralised nature of DLT systems and the intermediation of securities, however, applying the traditional *lex situs* approach to DLT systems is difficult as complications arise in determining the "location" of the intermediated securities and ascertaining which jurisdiction's laws apply to that DLT system. Further questions of legal uncertainty also arise when applying the traditional *lex situs* approach to DLT systems, including:

- What are the legal nature and effects against third parties of a disposition of an asset recorded on a DLT system?
- What are the requirements—if any—for the perfection of a disposition of an asset recorded on a DLT system?
- What are the requirements—if any—for the realisation of an interest in an asset recorded on a DLT system?

3.26. There has been some development in the *lex situs* approach in respect of intermediated securities, notably the "Place of the Relevant Intermediary Approach" ("**PRIMA**") principle, which was developed during negotiations for the Hague Securities Convention. The PRIMA principle identifies a method to determine the *lex situs* of securities held with an intermediary, by looking to the law of the relevant intermediary securities account to which the securities are credited, instead of the "location" of the intermediated securities.

3.27. Different versions of the PRIMA principle have been implemented in law. The Hague Securities Convention adopted a revised version of the PRIMA principle, by which the law of the account is the law agreed upon by parties in the relevant account agreement (the "**contractual PRIMA approach**"). The contractual PRIMA approach is circumscribed by a "qualifying office" requirement: the intermediary must also have an

[44] FMLC, *Report: Distributed Ledger Technology and Governing Law*, (27 March 2018), available at: http://fmlc.org/report-finance-and-technology-27-march-2018/.

office in the stipulated jurisdiction that meets various requirements with respect to the securities accounts. If the parties do not agree on the law of the account, and/or the qualifying office requirement is not met, then various fallback rules in Article 5 of the Hague Securities Convention take effect. Another version of the PRIMA principle also underpins various E.U. directives and provides that the law of the account is the law of the place where the account is maintained in practice.

3.28. An "elective situs" approach—based on the contractual PRIMA approach under the Hague Securities Convention—would be the most appropriate solution. Under this approach, the proprietary effects of transactions in a DLT arrangement could be governed by the system of law chosen by network participants for the DLT system. There are several advantages to an elective situs approach: (i) the proprietary effects of all transactions on the system are subject to the same governing law, (ii) the applicable law of the transaction is fully transparent to participants and (iii) the applicable law can be accurately reported for regulatory purposes.

3.29. There are, nevertheless, some issues with an elective situs approach, namely: (i) party autonomy is not universally accepted as a choice-of-law principle for proprietary issues, which may create difficulties in adopting a single elective *situs* rule across different jurisdictions or in respect of a permissionless system; and (ii) an elective *situs* approach may pose regulatory risks, e.g. if participants took advantage of the "choice-of-law" approach to choose a jurisdiction that was subject to undue external or private influence.

Conflict of laws in ICOs

3.30. Questions under DLT relate to private law rights between issuers and holders of tokens. These questions are still relevant to ICOs, but the starting question is which regulatory framework applies *prima facie* to ICOs, i.e. which country's laws apply to the offering. A "choice of law" approach is enshrined in European conflict of laws regulation with respect to contractual arrangements. As discussed below, a "choice of law" approach largely remains relevant in the context of ICOs. Nevertheless, there are various uncertainties that arise when applying this approach to ICOs.

Contractual arrangements

3.31. Regulation (EC) No 593/2008 on the law applicable to contractual obligations ("**Rome I**") applies when determining conflict of laws issues in respect of contractual obligations. Article 3(2) sets out the fundamental principle that parties can choose the

governing law of their contract. It seems that, where an investor subscribes to the ICO and agrees to its terms and conditions, a contract is formed. Although ICOs are not contemplated in Rome I, it is arguable that they would fall within its scope: they are contractual arrangements that relate to "civil and commercial matters" (Article 1(1)) and are not expressly excluded under Article 1(2). Assuming Rome I applies to ICOs, issuers would be free to choose the governing law of the ICO and investors would agree to this by signing up to the ICO's terms and conditions. A potential analogy could also be drawn here with the Rome I approach to issuances or offers of securities to the public. Under Rome I, parties can choose the applicable law for such issuances or offers; additionally, Article 6(4)(d) carves out such issuances and offers from the specific rules for consumer contracts, thereby ensuring that they are subject to a unitary legal regime which avoids preferential treatment of certain investors. To the extent that an ICO involved the issuance of tokens classified as securities, it also seems likely that the Article 6(4)(d) carve-out would apply. This analysis would also be consistent with market practice, whereby the standard approach is for the issuer to choose the law applicable to the ICO, and for investors to agree to this by signing up to the terms and conditions.

3.32. It is also worth considering the fallback options if the issuer did not choose the applicable law for the ICO. Again, a comparison may be drawn with the fallback provisions for Article 3(2) under Rome I. Article 4(1) provides criteria for determining the applicable law if one has not been explicitly chosen by the contracting parties. Should none of these provisions be applicable, then the contract will be governed by the law of the country where the party required to effect the characteristic performance of the contract has their habitual residence. It is not entirely clear how this applies in the context of ICOs; one possible argument is that, by offering the token, the issuer effects characteristic performance of the contract (and so the law of the issuer would apply), but this is not certain from a regulatory perspective. A final fallback provision in Article 4(4) provides that the law of the country with which the contract is "most closely connected" should apply; again, however, it is not clear how the "most closely connected country" can be determined given the virtual nature of most offerings and the distributed nature of the underlying DLT systems.

3.33. Furthermore, even where the issuer chooses the applicable law of the ICO, issues similar to those discussed with respect to the elective *situs* approach for DLT systems, still arise, namely that the issuer could choose a system of law that is unrelated to the

ICO or assets issued and subject to undue external or private influence. This is a particular concern in ICOs, where a majority of investors may be retail investors.

Non-contractual arrangements

3.34. Conflict of laws issues may also arise in ICOs with respect to non-contractual disputes, such as prospectus liability or financial promotion. Regulation (EC) No 864/2007 on the law applicable to non-contractual obligations ("**Rome II**")[45] applies to non-contractual disputes arising out of dealings prior to the conclusion of a contract (e.g. consequences arising from tort or delict). The general rule is to apply the law of the place where the damage occurred, or is likely to occur, subject to certain exceptions (the "**Rome II general rule**").[46] Parties can also choose the applicable law in certain circumstances.

3.35. Given the virtual, decentralised nature of tokens, the Rome II general rule may be difficult to apply in the case of non-contractual disputes arising with respect to an ICO. It could be argued that damage occurs (or is likely to occur) in the digital wallet of the potential investor; however, as the wallet is "digital", it remains unclear how the location of the wallet could be determined.

3.36. It is also unclear to what extent parties could choose the location of the applicable law, in the event of a non-contractual dispute relating to an ICO. Under Rome II, parties are allowed to choose the applicable law before the occurrence of the event giving rise to the damage if (i) all the parties are pursuing a commercial activity and (ii) the choice of law is freely negotiated. [47] It is difficult to see, however, how a choice of law could be freely negotiated between an issuer and investors, because (a) many investors will be retail investors, which may create restrictions on whether there can be any 'free' negotiation, and (b) even if the investors are not retail, there will not usually be any negotiation with the issuer (the investor will simply agree to a governing law chosen by the issuer). Parties can also choose the applicable law by an agreement entered into after the damage occurs (without the aforementioned requirements (i) and (ii)). However, where all elements relevant to the situation at the time of the choice of law concern one country, and the parties selected a different country's law, rules of the first country which cannot be derogated from by contract will still be applied.

---

45 Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32007R0864&from=DE

46 Article 4(1). Other specific rules also apply in the cases of unjust enrichment, *negotiorum gestio* and *culpa in contrahendo*.

47 Article 14(1)(b)

4. IMPACT

4.1. Regulatory uncertainty with respect to the status of ICOs risks discouraging productive and innovative investment activity, particularly in cases of conflict and duplication. Most ICOs are conducted by start-ups seeking to attract financial support for new ideas. Access to capital is often constrained for early-stage companies. Compliance with regulation entails costs and one of the risks of increasing the regulatory burden on ICOs—for example, through more robust disclosure requirements—is that it might freeze innovation, creating a disincentive to value creation and inhibiting investment in a potentially transformative technology, notably, blockchain/DLT.

4.2. On the other hand, where confusion leads to regulatory underlap, there may be a consequential increase in the risks to global financial stability. For example, regulatory uncertainty can also facilitate unproductive activity such as scams and frauds.

5. SOLUTIONS AND MITIGANTS

5.1. It has been argued that the next regulatory steps with regard to ICOs would be regional, rather than national.[48] Cross-border cooperation in this context is particularly important, as dependence on technologies such as blockchain make ICOs more likely than traditional rights offerings to straddle multiple jurisdictions. And, as with traditional finance, harmonisation brings about not only a reduction in the risks associated with regulatory divergence and overlap, which can deter productive economic activity, but also those associated with underlap, which can encourage arbitrage.[49] In reality, however, the challenge of a Europe-wide approach to regulating ICOs is likely to be complicated by coordination difficulties that accompany Brexit.

5.2. Equally, the ideal regulatory framework would be a cross-sectoral one, applicable to both innovative/disruptive finance and to the traditional finance sectors. It may be that the latter will, in future, adopt the technology underlying ICOs, for example in relation to E-Money and payment services. By way of analogy, in the payment services sector, when the Competition and Markets Authority ("**CMA**") established the Open Banking

[48] ESMA in its 'Advice on Initial Coin Offerings and Crypto-Assets', at paragraph 7 noted that it had identified gaps and issues in the existing regulatory framework when applied to crypto-assets, and in particular that some of the risks that are specific to their underlying technology may be left unaddressed. Further, that certain existing requirements may not be easily applied or may not be entirely relevant in a DLT framework.

[49] See *Crypto-securities Regulation: ICOs, Token Sales and Cryptocurrencies under EU Financial Law* (2017), available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3075820

Implementation Entity for the design of the Application Programme Interfaces ("**APIs**") that banks and building societies use to provide secure Open Banking, the FCA and HM Treasury noted that the use of APIs and common secure infrastructure in this way could enhance security across the banking industry.[50] This is an early example of a line of thought that token issuance should neither be regulated by the old standards, nor *sui generis*, but should be treated as a testing ground for a rethink on securities regulation altogether. While the FMLC can see the advantages of such an approach, it is beyond the scope of this paper and has not been addressed below.

5.3. One jurisdiction that is positioning itself as an early influencer and adopter with regard to the regulation of innovative finance is Malta.[51] It will be interesting to see whether the Maltese model—which established a dedicated new regulator, the Maltese Digital Innovation Authority—encounters any new and as yet unforeseen difficulties—such as an insufficient number of people in the private sector with sufficient knowledge and expertise to implement compliance protocols and/or a strong demand for additional resources arising out of the creation of new roles under the legislation (i.e. a registered systems auditor and a registered technical administrator). In addition, there are the well-rehearsed problems posed by the geographically distributed nature of the underlying blockchain network, as discussed above.

5.4. The following paragraphs examine areas of ICO issuance not likely to be covered by traditional financial regulation which could benefit from bespoke UK regulation, beginning with "novel actors".

Novel actors and the lifecycle

Developers

5.5. To satisfy the consumer protection and market integrity objectives in relation to ICO assets that constitute financial instruments, most commentators think it important to put in place mechanisms providing sufficient regulatory oversight concerning the standard of the code used by developers to design and develop the ICO asset.[52] This can be done

---

50 HM Treasury and Financial Conduct Authority, *Expectations for the third party access provisions in Payment Services Directive II*, (July 2017), available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/630135/Expectations_for_the_third_party_access_provisions_in_PSDII.pdf.

51 To assist in informing possible approaches and solutions, reference is made in this section to various provisions of the Maltese regime governing innovative technology arrangements and virtual financial assets. A list of legislative definitions underpinning the Maltese regime can be found in Appendix I.

52 ESMA's observations at paragraph 62 and 174 of its Advice on Initial Coin-Offerings and Crypto-Assets.

via direct oversight by a regulator, or by delegating such oversight to individual persons associated with the ICO enterprise (*qua* regulated actors) approved by the regulator to perform such functions.[53]

Custodians

5.6. A custodian is not a novel actor per se but custody of ICO tokens involves innovative types of property entitlement and security requirements, including, for example, the holding of the private key. A custodian must have appropriate systems and controls to ensure that an investor's funds are reimbursed if the ICO is cancelled for any reason, including where the set soft cap stated in the issuer's white paper is not reached. Custody should also be performed through a smart contract: where regulation introduces a systems auditor, one of their functions will be to certify the use of smart contracts for custody. Where custody is carried out by a third party, the public key to the assets should be retained by a systems auditor to enable custody by the third party. Further, consideration should be given to insurance requirements particularly in relation to risks associated with "hot" storage.[54]

5.7. More generally, specific regulatory responsibility might be given to a new regulator to keep under review technological developments including digital assets and their issuance, cryptography in the context of technology arrangements and uses thereof, and the development of standards within the industry. Consideration should be given to which body in the U.K. would take on responsibility for technological oversight, and the extent of those responsibilities.

Activities that do not fall within the existing regulatory perimeter

5.8. If E.U. policymakers were to develop a bespoke regulatory regime for those cryptoassets that do not qualify as financial instruments, ESMA advises that the rules should be tailored to the specific issues and risks posed by such assets. In line with the EBA's conclusions and ESMA's survey of NCAs, ESMA recommends that the AML regime should be expanded to apply to all activities. ESMA also recommends that risk disclosure requirements are put into place.

---

53 The Maltese model adopts the latter approach; however, this activity of overseeing the development of the code is not specifically overseen as a standalone function but rather is part of the broader landscape covered by "innovative technology arrangements" (see Appendix I for definition), and is the subject of further checks prior to listing.

54 "Hot storage": the fastest storage, designed to be accessed frequently. It might be, for example, flash memory in hybrid or tiered storage environments.

5.9. Before adopting any new regulation, it is important to clarify the objectives of such regulation. The U.K. authorities have identified, *inter alia*, risks relating to consumer protection, market integrity and financial crime. The most commonly cited mitigant to these risks, discussed below, is authorisation. Authorisation has the advantage of bringing the ICO operator, issuer and other actors into the regulatory fold but it would require the definition of new specified investments. It is useful to consider whether requiring issuers to be authorised is necessary to, or even would be capable of, mitigating these risks.

Consumer protection

5.10. A major concern for regulators, where tokens do not fall within the existing regulatory perimeter, is to protect consumers from financial loss due to fraud or insufficient understanding of the risks and volatility of investing in cryptoassets. Although the FCA has issued warnings about the risks of participating in ICOs, these have been criticised as being inadequate.

5.11. In contrast, there are multiple mechanisms to protect the buyers of regulated investments. Some pieces of legislation which include disclosure obligations, such as Regulation (EU) No 1286/2014 on key information documents for packaged retail and insurance-based investment products (the "**PRIIPs Regulation**"), are designed to ensure that investors understand what they are buying. Other requirements, such as product governance and the duty for financial advisers to assess the appropriateness or suitability of the investment for the buyer, aim to prevent them being sold investments that may be unsuitable for them.

5.12. The full extent of these rules only applies to a person that is FCA-authorised or FCA-regulated but some regimes are wider in scope. In particular, the restrictions on financial promotion apply to any person (wherever they are and whether authorised or not) that communicates an invitation or inducement to engage in investment activity. Although there are numerous exemptions from the financial promotion regime, very few of them enable an unauthorised person to communicate cryptoassets to retail clients without engaging with the FCA and complying with regulation. Therefore, where cryptoassets do qualify as specified investments, there is a degree of protection available irrespective of authorisation.

Market integrity

5.13. The government has recognised the rapid emergence of cryptoasset exchanges and is concerned about the fact that cryptoassets can be sold without an authorised person needing to be involved. The fact that neither the exchange operators nor the investments are regulated also means that there is no effective market surveillance. The market abuse regime applies to any person in any location in respect of financial instruments that are traded on trading venues and related investments and also, in some cases, to spot commodity derivatives. In order to extend this regime to cryptoassets using the same structure, not only would they need to be classified as specified investments, the exchanges on which they are traded would also need to be regulated as trading venues. Given the scope of unregulated cryptoassets and the fact that they are not traded on regulated platforms, it may therefore be more proportionate to extend the market abuse regime to include another type of instrument in the same way as spot commodities were brought into the regime.

Money laundering

5.14. There is a natural concern that ICOs could be used for the purposes of money laundering and other financial crime—natural, because tokens can be issued and traded anonymously in a permissionless system. The FCA's Know Your Client ("**KYC**") anti-money-laundering requirements apply to a wider set of persons than just those that are authorised or otherwise involved with specified investments but it is still unlikely that an ICO issuer would fall within scope of the KYC requirements under current English law. The regime will be extended to reflect 5MLD ahead of January 2020, when the Directive comes into force.[55] Although this includes custodian wallet providers and exchanges, it does not include issuers. That said, it remains to be seen whether the U.K. will implement it on a wider basis. This could therefore be done without extending the RAO to cover issuing cryptoassets.

Extending the regulatory perimeter; self-regulation and other approaches

5.15. An alternative model of regulation to those discussed above might be the securities offering regime. This essentially requires that a person offering securities to the public must publish a prospectus which has been approved by the FCA in its capacity as the

[55] According to FMLC analysis of relevant definitions in 5MLD, however, this extension may raise concerns about regulatory underlap. The issues are more likely to arise in respect of exchange tokens, making the analysis less relevant to ICOs which tend to issue security tokens. A fuller exploration of the legal uncertainties may be found in a letter sent by the FMLC to HM Treasury: FMLC, *Letter to HM Treasury on 5MLD and Cryptoassets*, (30 July 2019), available at: http://fmlc.org/letter-to-hm-treasury-on-5mld-and-cryptoassets-30-july-2019/.

UKLA, unless the offer falls within an exemption. Exemptions apply, for example, when the offer is made to or directed at qualified investors only, or fewer than 150 U.K. persons other than qualified investors. The U.K. prospectus regime as it exists in its current form may not be a perfect solution, not least because the required content for a prospectus is designed with different types of transferable securities in mind and may not lend itself well to the types of information a potential investor may want to know about a token. However, the provision of sufficient information to enable the investor to make an informed assessment of the issuer and the rights attaching to the tokens in a form which is comprehensible and easy to analyse, with a summary in concise, non-technical language, would have some value in terms of consumer protection. The directors of the company issuing the prospectus must take responsibility for the accuracy and completeness of its contents, which may be a useful way of encouraging ICO issuers to focus their attention on the information they provide to investors.

5.16. The prospectus requirement has been adopted in the laws that countries such as Malta and the Bahamas have designed specifically for ICO issuance. Some of these have also incorporated requirements that are specific to cryptoassets such as those relating to the scrutiny of the cryptographic design and the security of the cryptoassets being issued and mechanisms through which they will be sold. If this were to be considered a useful approach for the U.K., it may be possible to adapt the existing regime to accommodate cryptoassets as a new type of investment.

5.17. A further alternative is to allow the industry to self-regulate by creating voluntary codes of conduct and develop best practices. While such arrangements doubtless provide many benefits, the House of Commons Treasury Committee on Cryptoassets was skeptical that all firms would comply with them without there being an authority that could enforce them and hold the industry to account.

Conflict of Laws in DLT

5.18. To help mitigate conflict of laws risks, one possible solution might be to set restrictions on the elective *situs* approach: for instance, the parties' choice of *situs* could be restricted to a choice of law that is connected to the DLT system or could be limited to a choice of law that is subject to approval by the regulators. Arguably, there is some precedent in Rome I for regulators placing restrictions on party autonomy with respect to choice of law, although it should be noted that difficulties could still arise in identifying the relevant competent authority for a distributed system.

5.19. If an elective *situs* approach cannot be properly implemented, some appropriate fallback solutions could be identified. These include (i) looking to the location of the relevant administrator or operating authority of the DLT system (which could only apply for a permissioned DLT system that is not decentralised); and (ii) looking to the location of the transferor of the asset subject to the transaction in the distributed ledger (although this would not resolve questions of entitlement in the case of joint transferors or chains assignment, and would artificially split up the distributed ledger record).

5.20. It is clear from the solutions summarised above that any approach adopted will also have to adapt to expected changes in DLT technology, particularly the advent of permissionless, fully decentralised DLT systems. Nevertheless, at the present stage of DLT development, an elective *situs* solution (with appropriate modifications) seems the most appropriate approach to addressing conflict of laws questions in DLT systems.

Conflict of laws in ICOs: Non-contractual arrangements

5.21. One possible solution might be to look through to the residence of the person who owns the wallet or, in a situation where a company is managing the digital wallets of potential investors, to the jurisdiction where that company is established. However, taking this approach could lead to potential fragmentation of the regulatory framework, as investors could be located in numerous locations worldwide.[56]

6. CONCLUSION

6.1. The objective of the FMLC's most recent work on tokens has been to identify, and engage with issues of legal uncertainty which may arise in the context of applying regulation to, or drafting regulation for, ICOs. The legal characterisation of ICOs has been considered in the course of the FMLC's analysis, as have some of the challenges of addressing activities, functions and assets hitherto unknown to the law. An exploration of the existing regulatory framework for specified investments in the U.K. and the E.U. has been undertaken and this paper comments briefly on the application of existing laws to ICOs.

[56] In the case of *Kolassa v Barclays Bank plc* [2015] EUECJ C-375/13, which related to jurisdiction in a prospectus liability claim, it was held that place where the damage occurred includes where an investor suffers loss. Additionally, it was held that such damage is suffered in the country where the applicant is domiciled, particularly when the loss occurred directly in the investor's bank account located in that same jurisdiction. Therefore, both the domicile of the investor and the location of the investor's bank account were relevant factors in determining the location of the damage suffered. Extrapolating from this case to ICOs, one could argue that the digital wallet of an investor (arguably the closest analogy to a bank account) and/or the investor's residence are relevant factors in determining the location of the damage (or potential damage).

6.2. The paper addresses some of the challenges posed by the current environment for regulators, providers and market participants alike. First, there is a lack of international and regional harmonisation in relation to the categorisation of tokens issued in ICOs, let alone in relation to regulatory treatment. Where ICOs do fall within the U.K. or E.U. regulatory perimeter, further uncertainties emerge about the application of existing registration and authorisation regimes to the ICO-specific actors and activities. Where ICOs fall outside the regulatory perimeter, there are questions about whether and, if so, how, the regime(s) might be extended to prevent any regulatory underlap. Finding answers to all these questions is made more challenging by the non-physical, a-geographical nature of token issuance. For this reason, the paper also explores the conflict of laws issues which may arise owing to the likely cross-border nature of ICOs and DLT.

6.3. In the final section of the paper, the FMLC refers to existing attempts to regulate ICOs and provides some recommendations which might inform further work in this rapidly-evolving area. It explores in brief some models that might be adopted in adapting legal and regulatory frameworks to accommodate ICOs. In this context, the FMLC recommends that particular attention be given to the aspects of ICOs that are innovative and non-aligned with traditional financial services and which are thus unfamiliar to, or unrecognised by, existing law and regulation.

APPENDIX I

Maltese legislative definitions

Act No. XXXI of 2018 – Malta Digital Innovation Authority Act 2018[57]

"DLT", "distributed ledger technology", "decentralised ledger technology" means a database system in which information is recorded, consensually shared, and synchronised across a network of multiple nodes, or any variations thereof, as further described in the First Schedule of the Innovative Technology Arrangements and Services Act, 2018, and the term "node" means a device and data point on a computer network;

"innovative technology arrangements" means the intrinsic elements including software, codes, computer protocols and other architectures which are used in the context of DLT, smart contracts and related applications as well as other arrangements as may be further defined in the Innovative Technology Arrangements and Services Act, 2018;

"innovative technology services" are those services in relation to innovative technology arrangements as are designated in the Innovative Technology Arrangements and Services Act, 2018;

"smart contract" means a form of innovative technology arrangement consisting of:

(a) a computer protocol; and, or

(b) an agreement concluded wholly or partly in an electronic form, which is automatable and enforceable by execution of computer code, although some parts may require human input and control and which may be also enforceable by ordinary legal methods or by a mixture of both.

Act No. XXXIII of 2018 – Innovative Technology Arrangements and Services Act 2018

"systems auditor" means a person who, upon a written engagement accepts to review and, or audit innovative technology arrangements and smart contracts or parts thereof who may not necessarily be an accountant or auditor with a practicing certificate under the Accountancy Profession Act;

"technical administrator" means the person who, upon a written engagement accepts to carry out specific functions relating to the operation, of the whole or a designated part, of an innovative technology arrangement as are established in this Act, in guidelines issued by the Authority, as the same may be supplemented by the conditions applicable to the certification of the particular certified innovative technology arrangement.

FIRST SCHEDULE

(Articles 2 and 8)

Innovative Technology Arrangements

[57] The Act is available online at https://mdia.gov.mt/wp-content/uploads/2018/10/MDIA.pdf.

The following shall be considered to be innovative technology arrangements for the purposes of this Act:

1. software and architectures which are used in designing and delivering DLT which ordinarily, but not necessarily:

(a) uses a distributed, decentralised, shared and, or replicated ledger;

(b) may be public or private or hybrids thereof;

(c) is permissioned or permissionless or hybrids thereof;

(d) is secure to a high level against retrospective tampering, such that the history of transactions cannot be replaced;

(e) is protected with cryptography; and

(f) is auditable;

2. smart contracts and related applications, including decentralised autonomous organisations, as well as other similar arrangements;

3. any other innovative technology arrangement which may be designated by the Minister, on the recommendation of the Authority, by notice from time to time.

SECOND SCHEDULE

(Article 2)

Innovative Technology Services

The following shall be considered to be innovative technology services for the purposes of this Act:

1. the review or audit services referred to in this Act with reference to innovative technology arrangements provided by system auditors;

2. the technical administration services referred to in this Act with reference to innovative technology arrangements provided by technical administrators.

APPENDIX II

Gibraltar legislative definitions

FINANCIAL SERVICES (DISTRIBUTED LEDGER TECHNOLOGY PROVIDERS) REGULATIONS 2017[58]

SCHEDULE 1

AMENDMENTS TO THE PRINCIPAL ACT

In schedule 3 to the Principal Act, after paragraph 9 insert–

"10. Providing distributed ledger technology services.

(1) Carrying on by way of business, in or from Gibraltar, the use of distributed ledger technology for storing or transmitting value belonging to others.

(2) For the purposes of sub-paragraph (1)–

"distributed ledger technology" or "DLT" means a database system in which–

(a) information is recorded and consensually shared and synchronised across a network of multiple nodes; and

(b) all copies of the database are regarded as equally authentic; and

"value" includes assets, holdings and other forms of ownership, rights or interests, with or without related information, such as agreements or transactions for the transfer of value or its payment, clearing or settlement.

…

(6) In this paragraph–

a "DLT Provider" means a person licensed to carry on the controlled activity of providing distributed ledger technology services;

SCHEDULE 2

THE REGULATORY PRINCIPLES

1. A DLT Provider must conduct its business with honesty and integrity.

2. A DLT Provider must pay due regard to the interests and needs of each and all its customers and must communicate with them in a way that is fair, clear and not misleading.

3. A DLT Provider must maintain adequate financial and non-financial resources.

[58] The Regulations are available online at: https://www.gibraltarlaws.gov.gi/articles/2017s204.pdf.

4. A DLT Provider must manage and control its business effectively, and conduct its business with due skill, care and diligence; including having proper regard to risks to its business and customers.

5. A DLT Provider must have effective arrangements in place for the protection of customer assets and money when it is responsible for them.

6. A DLT Provider must have effective corporate governance arrangements.

7. A DLT Provider must ensure that all of its systems and security access protocols are maintained to appropriate high standards.

8. A DLT Provider must have systems in place to prevent, detect and disclose financial crime risks such as money laundering and terrorist financing.

9. A DLT Provider must be resilient and have contingency arrangements for the orderly and solvent wind down of its business.

FINANCIAL MARKETS LAW COMMITTEE MEMBERS[59]

Lord Thomas of Cwmgiedd (Chairman)

David Greenwald (Deputy-Chairman)

Andrew Bagley, Goldman Sachs International

Sir William Blair, Queen Mary, University of London

Raymond Cox QC, Fountain Court Chambers

Hubert de Vauplane, Kramer Levin Naftalis & Frankel LLP

Michael Duncan, Allen & Overy LLP

Simon Firth, Linklaters LLP

Bradley J Gans, Citigroup

Kate Gibbons, Clifford Chance LLP

Richard Gray, HSBC Bank plc

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

Sean Martin, Financial Conduct Authority

Jon May, Marshall Wace LLP

Sinead Meany, Bank of England

Chris Newby, AIG

Jan Putnis, Slaughter and May

Barnabas Reynolds, Shearman & Sterling LLP

Peter Spires, Lloyd's of London

Sanjev Warna-kula-suriya, Latham & Watkins LLP

Pansy Wong, J.P. Morgan

Mr Justice Zacaroli

Joanna Perkins (Chief Executive)

[59] Note that Members act in a purely personal capacity. The names of the institutions that they ordinarily represent are given for information purposes only. Whilst the Bank of England, the Financial Conduct Authority and HM Treasury participate in the FMLC, the views expressed in this paper are not necessarily those of the three institutions.