THE INTERNATIONAL JOURNAL OF BLOCKCHAIN LAW

Volume 12

June 2025

GBBC
Global Blockchain
Business Council


GBBC
Global Blockchain
Business Council

TABLE OF CONTENTS

NOTE FROM THE EDITOR-IN-CHIEF

DR. MATTHIAS ARTZT
SENIOR LEGAL COUNSEL, DEUTSCHE BANK
GERMANY

Dr. Matthias Artzt is a certified lawyer and senior legal counsel at Deutsche Bank AG since 1999. He has been practicing data protection law for many years and was particularly involved in the implementation of the GDPR within Deutsche Bank AG. He advises internal clients globally regarding data protection issues as well as complex international outsourcing agreements involving data privacy related matters and regulations.

Welcome to the 12th edition of the IJBL, featuring a wide range of blockchain- and crypto-related topics across Europe, Turkey, UK, Malaysia, Japan, Hong Kong and the United States.

We begin with an article by Umut Gün, LL.M., Legal Counsel and Data Protection Officer at BtcTurk, a cryptocurrency trading platform in Turkey. He examines the interaction between two significant EU regulations—MiCA and PSD2, also considering the latest EBA opinion. Given that the transfer of e-money tokens (as defined under MiCA) must be treated as a payment service subject to PSD2, a key legal question arises: which framework takes precedence? Umut concludes that ensuring compliance with overlapping regulations will prove challenging for both e-money token issuers and crypto asset service providers. Applying traditional payment rules to blockchain ecosystems may clash with the very foundations of decentralization.

Next, Edmund Yong, Managing Partner at Celebrus Advisory in Malaysia, along with Ming Chiek Gan and Kelvin Wong, Partners at GLT Law, delve into digital asset custody (DAC) in Malaysia. They investigate the custody requirements outlined in the 2020 Guidelines on Digital Assets (as revised in 2024) and examine the legal challenges linked to custodial services.

From Mayer Brown's Singapore and Hong Kong offices, Amita Haylock and Justin W. J. Lai shed light on Hong Kong's licensing regime for stablecoin issuers (the Stablecoins Bill). Any entity issuing stablecoins within Hong Kong—or backed by Hong Kong dollars—will require a license from the Hong Kong Monetary Authority. The article highlights the bill's key objectives, including safeguards aimed at mitigating financial and monetary risks posed by fiat-backed stablecoins. The authors suggest that Hong Kong's approach may become a model for regional regulatory standards. A follow-up piece on this topic is slated for our next issue.

Together with Yumi Ahn and Masayuki Otake (Tokyo International Law Office), I explore the legal and governance implications of autonomous AI agents from both EU and Japanese perspectives. The connection to blockchain technology lies in the idea of a decentralized AI agent registry. As this emerging field known as agentic AI takes shape, it demands unique legal frameworks to handle liability for autonomous digital agents acting without direct human intervention and control. We've included this piece as AI increasingly intersects with blockchain applications—and vice versa.

Also in this issue, Daniel J. Davis, Carl E. Kennedy, and Alexander C. Kim from Katten's NYC and DC offices discuss a recent CFTC Staff Advisory Letter ("Letter").

The Letter offers clarity on whether entities trading digital asset derivatives outside the U.S. fall under the CFTC's jurisdiction. Interestingly, the Letter signals a possible retreat from aggressive extraterritorial claims made in past enforcement actions—potentially pointing to a more balanced approach to global regulation.

Contributors from Clifford Chance London—Diego Ballon, Monica Sah, Sara Evans, Laura Nixon and Madeleine Yates—review the UK government's draft order (published April 29) to establish a comprehensive regulatory framework for crypto-assets, including stablecoins. They evaluate which activities and assets will be covered and flag areas where clarification may be needed. The authors close with practical guidance on how firms can begin preparing.

Finally, we wrap up this edition with a write-up of the "2025 Future of Finance" conference hosted in London by GBBC and Norton Rose Fulbright. Special thanks to the NRF team for sharing their coverage. I especially want to point readers to the fireside chat "Exploring Digital Assets and the Impact of AI" which beautifully links to the article on agentic AI mentioned above. It underscores how AI agents could streamline complex DeFi functions such as staking and token trading.

And last but not least, I would like to thank Riley Fay and Philip Gant for their incredible support to bring this edition as well as the previous editions over the finish line.

Happy reading!

Dr. Matthias Artzt
Editor-in-Chief

ABOUT THE CO-EDITORS

LOCKNIE HSU

PROFESSOR, SINGAPORE MANAGEMENT UNIVERSITY

SINGAPORE

Locknie Hsu received her legal training at the National University of Singapore and Harvard University, and is a member of the Singapore Bar. Locknie specializes in international trade and investment law, including areas such as paperless trade, FTAs, digital commerce, and business applications of technology.

ELÇIN KARATAY

MANAGING PARTNER, SOLAK&PARTNERS LAW FIRM

ISTANBUL, TÜRKIYE

Elçin Karatay, is a partner at Solak&Partners Law Firm, who specializes in corporate law, commercial law and IP law with a keen focus on technology and Fintech sectors. She advises local and international clients on agreements, regulatory aspects of IT law and M&As, particularly within tech-driven domains. Elçin works intensively on creating legal structures for new technological developments including blockchain area.

STEPHEN D. PALLEY

PARTNER, BROWN RUDNICK

WASHINGTON, DC, USA

Stephen Palley is a litigation partner and co-chair of Brown Rudnick's Digital Commerce group. He has deep technical and U.S. regulatory knowledge, particularly in the digital asset space, and assists clients working on the frontiers of technology, including on deal work for blockchain and other technology enterprises.

NINA MOFFATT

PARTNER, PAUL HASTINGS

LONDON, UK

Nina Moffatt is a partner in the London office of Paul Hastings providing legal and commercial advice on regulatory requirements across Europe. She has particular expertise in large cross border offerings and product design. She also regularly assists clients with their relations with the U.K. regulators, including applications for authorization and supervisory issues.

JAKE VAN DER LAAN

CO-AUTHOR, "HANDBOOK OF BLOCKCHAIN LAW"; BARRISTER AND SOLICITOR

NEW BRUNSWICK, CANADA

Jake van der Laan teaches within the Faculty of Computer Science at the University of New Brunswick, Canada and served as the Director, Information Technology and Regulatory Informatics and the Chief Information Officer with the New Brunswick Financial and Consumer Services Commission (FCNB). Prior to joining FCNB he was a trial lawyer for 12 years, acting primarily as plaintiff's counsel.

GARY D. WEINGARDEN

PRIVACY OFFICER AND DIRECTOR OF IT SECURITY COMPLIANCE, TUFTS UNIVERSITY

BOSTON, MA, USA

Gary Weingarden is the Privacy Officer and Director of IT Security Compliance at Tufts University. Gary has multiple certifications in privacy, security, compliance, ethics, and fraud prevention from IAPP, ISC2, ISACA, SCCE, and the ACFE, among others. Before Joining Tufts, Gary served as Data Protection Officer for Notarize, and Senior Counsel at Rocket Mortgage.

ARTICLE I

INTEROPERABILITY CHALLENGES BETWEEN MICA AND PSD2

UMUT GÜN
LEGAL COUNSEL & DATA PROTECTION OFFICER
BTCTURK

The European Union has enacted one of the most significant regulatory frameworks in the world with respect to crypto-assets. Markets in Crypto-Assets (MiCA) was adopted by the European Union Parliament and Council, and it has entered into force on December 30, 2024. MiCA is a framework that governs crypto-asset markets across Europe and, in some cases, beyond the EU borders.

In general, MiCA differentiates crypto-assets into different types, imposes certain obligations for crypto-asset service providers, regulates the crypto-asset market and sets technical infrastructure standards.

While MiCA is still in its early stages of implementation, Payment Services Directive 2 (PSD2) which was implemented on September 14, 2019 has become a point of contention for the crypto-asset market. PSD2 is a regulation that introduced open banking to Europe, regulates payment systems and payment institutions and introduces technical standards.

As the European Union strengthens its regulatory landscape for digital finance, the intersection of crypto-asset regulation under MiCA and traditional payment oversight under PSD2 has emerged as a complex legal frontier.

For example, e-money tokens[1] and asset-referenced tokens[2] (as defined below) can be used by the holders of these assets for payments and similar transactions, placing them at the convergence of these two regimes. While crypto-assets are already regulated under MiCA, PSD2 regulates payment transactions within European borders. Therefore, it is of great importance to ensure MiCA and PSD2 work in coherence on this basis. The challenge lies in the practical implementation and interoperability of MiCA and PSD2 where their scopes overlap. What can be the solution to all these difficulties and what can be done? This article explores key challenges and proposes practical solutions.

IDENTIFICATION OF PROBLEMS

Problems related to concepts and definitions

In order to explain the first problem regarding the interoperability of MiCA and PSD2, it is necessary to define some concepts. In Article 3 of MiCA entitled Definitions, e-money token is defined as *"a type of crypto-asset that purports to maintain a stable value by referencing the value of one official currency"*.

1 A type of crypto-asset that purports to maintain a stable value by referencing the value of one official currency.

2 A type of crypto-asset that is not an electronic money token and that purports to maintain a stable value by referencing another value or right or a combination thereof, including one or more official currencies.

The concept of crypto-asset is defined in the same article as *"a digital representation of a value or of a right that is able to be transferred and stored electronically using distributed ledger technology or similar technology"*.

Electronic money is defined as a fund under PSD2 and Article 4 of the PSD2 regulation titled Definitions explains the concept of fund where it is defined as *"banknotes and coins, scriptural money or electronic money as defined in point (2) of Article 2 of Directive 2009/110/EC"*.

Even through the review of the definitions a key legal issue emergers

Can e-money tokens be accepted as funds under PSD2? The answer to this question is very important. Because, if this question is answered as "yes", then the transfer of e-money tokens can also be considered as a payment service at the point of fund transfer, and in this case, PSD2 can be applicable for e-money tokens, almost mandatorily.

Problems related to applicability of overlapping regulations

This leads to a second, closely related issue. If e-money tokens are recognised as funds and subsequently accepted to be within the scope of PSD2, it becomes unclear which legal framework applies to a crypto-asset service provider in transactions such as the issuance and transfer of e-money tokens. Which licence or regulatory approvals will it obtain? If this question cannot be answered, companies providing e-money tokens may find themselves subject to overlapping and potentially conflicting obligations. Navigating this regulatory duality would impose significant compliance burdens and it will be difficult for companies to survive.

Problems related to transfer of crypto-assets:

Another problem is related to the transfer process in the crypto-asset ecosystem. In the crypto-asset market, each individual is actually their own bank. Everyone carries their vaults in their pockets with ledgers. These assets can be transferred from peer to peer when necessary. The problem here is what is the legal nature of this transfer? Is the transfer between wallets a payment transaction? Or is it an asset transfer? It would be appropriate to provide a brief clarification to better distinguish the concepts.

Payment transactions and asset transfers are fundamentally different. A payment transaction involves the settlement of funds in exchange for goods or services. In contrast, an asset transfer refers to the conveyance of an asset or value to another party, which does not necessarily have to involve funds. The answer to this question is also very important. Because, if such transactions are characterised as payment transactions, crypto-asset service providers, ledger companies and in some cases even individuals will be covered by PSD2. This will bring additional obligations, costs and sanction risks to the relevant parties. Moreover, a question begs a question here. For example, according to the discussion here, can ledgers be considered a payment account? Another question: Do ledger companies provide payment services?

Problems related to applicability of different regulatory frameworks

MiCA and PSD2 also impose different obligations on the companies subject to them. For example, the founding principles of these companies, the policies and procedures to be followed, and the internal processes are different. For instance, identity verification requirements also differ between the two types of providers. Which legal framework should apply to companies operating at the intersection of these two regimes?

FINDING AND DISCUSSING SOLUTIONS

Responding to Conceptual and Qualitative Challenges: To answer the questions introduced above, it is important to determine the legal nature of e-money tokens.

If e-money tokens are recognised as electronic money, they will also be accepted as funds. In this case, organisations issuing e-money tokens will also have to comply with PSD2 requirements. There is no definition of the concept of electronic money under the PSD2 regulation.

However, as stated in PSD2, this concept is defined within the scope of Directive 2009/110/EC. According to this definition, electronic money is be defined as electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions and which is accepted by a natural or legal person other than the electronic money issuer.

When this definition is analysed, we can state that the elements of electronic money are: electronically, including magnetically, stored monetary value, representing a claim on the issuer, issued on receipt of funds, the purpose of making payment transactions and accepted by a natural or legal person other than the electronic money issuer. Within the scope of these elements, the concept of e-money token should be evaluated. Considering the current use of e-money tokens, it can be clearly stated that e-money tokens are issued against funds, stored electronically, can be used in payment transactions, can be accepted as a means of payment and give rise to a right of claim against the issuer. It should be noted here that whether electronic money can be used in payment transactions or not is a situation that varies from person to person or from organisation to organisation.

Article 48 of MiCA clearly states that *"e-money tokens shall be deemed to be electronic money. An e-money token that references an official currency of a Member State shall be deemed to be offered to the public in the Union"*. As can be seen, within the scope of the European Union directives, the acceptance of e-money tokens as electronic money may be a legally justified view. The consequence of the view is that the e-money issuer must comply with the obligations under PSD2 and Directive 2009/110/EC in addition to MiCA.

It will be extremely challenging for e-money token issuers and users to comply with multiple regulatory frameworks. Therefore, the boundary between these two concepts should be clearly defined. In parallel with this view, the European Banking Authority (EBA) has published its opinion. According to this opinion, e-money tokens also qualify as e-money. However, e-money does not qualify as an e-money token. Therefore, both MiCA and PSD2 will be applicable to e-money tokens. Nevertheless, complying with two different regulatory frameworks for the same subject is challenging and impractical. For this reason, MiCA should be reformed, or PSD3 should be revised accordingly.

Parallel Problems, Parallel Remedies

Although MiCA does not set a minimum capital requirement for e-money token issuers, PSD2 and Directive 2009/110/EC set this requirement at €350,000. This is an example of a major problem. The fact that an e-money token issuer, which is not planned and issued for payment transactions, is subject to such a minimum capital requirement will be very disadvantageous for new actors to enter the sector. While PSD2 regulated entities are not required to issue whitepapers, MiCA imposes such an obligation. Such differences will also manifest themselves in issues such as the way companies operate, audit and supervision.

The two issues discussed so far are in fact interrelated. Based on this interest, a single answer and solution can be given for the two questions. The solution here may be a decision of inaction to be taken by the public authorities, or it may be the exemption of legal entities that comply with one of the legislation from certain parts of the other legislation. Under the No Action Letter published by the European Banking Authority, important messages have been conveyed to national competent authorities. Accordingly, crypto-asset service providers involved in activities related to electronic money tokens should avoid dual authorisation that would result from separate authorisations under both MiCA and PSD2.

The EBA advises that such authorisation should only be applied from 2 March 2026 onwards. Additionally, a crypto-asset service provider that transacts with e-money tokens may be required to hold a total capital of €250,000, consisting of €125,000 separately under both MiCA and PSD2.

Is It a Payment or a Transfer of Assets?

The transfer made with ledgers in the crypto world shows us another discussion. According to the PSD2 regulation, a payment transaction is defined as *"an act, initiated by the payer or on his behalf or by the payee, of placing, transferring or withdrawing funds, irrespective of any underlying obligations between the payer and the payee"*. As seen in this definition, in order for a transaction to be considered a payment transaction, the elements of placing, transferring or withdrawing funds, payer and payee must be present. In crypto-asset transfers, sender, receiver, deposit, withdrawal and transfer operations are performed. For example, crypto-asset investors usually make deposits and withdrawals when sending an asset from ledgers or transacting with crypto-asset service providers. However, the main question here is that are the crypto-assets funds?

The classification of such transfers as either payment transactions or asset transfers depends on how this question is answered. According to the definition of fund under PSD2, crypto-assets are not funds. However, if e-money tokens are to be considered as electronic money, crypto-assets that have the characteristics of e-money tokens will be considered as funds. **As such, the transfer, deposit or withdrawal of e-money tokens or the sending of e-money tokens via peer-to peer network will be considered as payment transactions. In this scenario the problem we face is that crypto-asset service providers or ledger platforms should be considered as a payment service provider.** However, crypto-asset service providers and payment service providers have many different requirements such as licence, establishment, working conditions and principles.

Considering such transactions as payment transactions also requires PSD2 compliance for crypto-asset service providers and ledger platforms, which will be a very challenging aspect for industry participants. Moreover, treating such transfers as payment transactions would conflict with the nature of the crypto-asset ecosystem and the foundational principles of blockchain technology. At this point, the required action is clear. Transfers between crypto-asset service providers, ledgers and individuals should not be considered as payment services. The European Banking Authority also provides clear guidance on this matter. National Competent Authorities are advised not to consider as payment services the "exchange of crypto-assets for funds" and "exchange of crypto-assets for other crypto-assets" as defined in MiCA. Additionally, the European Banking Authority advises National Competent Authorities not to regard as a payment service cases where crypto-asset service providers intermediate the purchase of any crypto-assets with e-money token.

FINAL REMARKS

We would like to briefly enumerate possible solutions to the various problems between PSD2 and MiCA. Possible solutions include a no-action letter, an exception to some provisions in the other legislation in case of full compliance with one of the legislation, clear distinction between e-money tokens and electronic money, and an exception to payment services in terms of crypto-asset transfers.

The European Banking Authority advises avoiding dual authorisation for electronic money token transactions under PSD2 and MiCA. PSD2 authorisation should only apply to certain crypto-asset service providers after 2 March 2026, with simplified procedures. Some PSD2 rules will be deprioritised, but key protections like strong customer authentication and fraud reporting remain mandatory. Exchanges of crypto-assets for funds or other crypto-assets and e-money token-facilitated crypto purchases are not considered payment services under PSD2. This approach reduces regulatory burdens but acknowledges that MiCA alone is insufficient to manage all risks related to e-money token transactions.

ARTICLE II

A BRIEF LEGAL TOUR OF DIGITAL ASSET CUSTODY (DAC) IN MALAYSIA

EDMUND YONG
MANAGING PARTNER
CELEBRUS ADVISORY

MING CHIEK GAN
PARTNER
GLT LAW

KELVIN WONG
PARTNER
GLT LAW

Any person who "provides the services of safekeeping, storing, holding or maintaining custody of digital assets for the account of another person" is regulated in Malaysia as a digital asset custodian (DAC).[1] At present, there are three such custodians registered with the main regulatory body, the Securities Commission (SC).[2] Crypto exchanges and licensed trustees may also provide these services in the country if they meet the requirements to SC's satisfaction.

Background information: Digital asset ownership in Malaysia is high at 19.9% of its online population.[3] In absolute numbers, there are an estimated 4.7 million owners this year or 13.3% of the total population.[4] The country is situated in the continental tip of Southeast Asia which has some of the highest national adoption rates in the world.[5]

Malaysia inherited the English common law system along with its principles relating to equity and trusts, and legislates through a bicameral parliament. Islamic law is also practiced in certain areas. That being said, the *Trustee Act 1949 (revised 1978)* and *Trust Companies Act 1949* are the main laws governing the administration of conventional trusts in Malaysia.

Having a regulated environment is needful and conducive to the high-growth crypto industry. However, it also underscores the challenges of imputing trust obligations on a transactional system that is designed to be trustless, and circumscribing geo limits on blockchain wallets that are by nature decentralized.

OVERVIEW OF CUSTODY GUIDELINES

First off, it is useful to point out that regulated DACs are a subset of a much broader custodial landscape that is currently unregulated or unregulatable (e.g. self-custody where the owner is responsible for the private keys to his own wallet).

1 Digital Assets - Guidelines | Securities Commission Malaysia (revised 19 August 2024).
2 Digital Assets | Securities Commission Malaysia (last accessed 28 February 2025).
3 Malaysia ranks 7th in cryptocurrency ownership out of 27 countries - Focus Malaysia
4 Cryptocurrencies - Malaysia | Statista Market Forecast
5 Crypto Adoption in Southeast Asia is On the Rise - Fintech Singapore

Existing regulations only cover custodial services that are offered in Malaysia. This article walks through the relevant custody provisions in the *Guidelines on Digital Assets 2020 (revised 2024) ("the Guidelines")* and some of the legal considerations to look out for:

1. Securities

'Digital assets' is the generic term applied to cryptographic-based digital currencies and digital tokens, both prescribed as securities (note: 'tokenized securities' are scoped out in an amendment, possibly treated as a third category).[6] The Guidelines do not delve into the custodial handling of financial instruments as book-entry securities (which are more nuanced than digitized bearer assets) to support various capital market services including fund management.[7]

2. Counterparty

To qualify as custody, it should be a 'managed service' provided by counterparties for the digital asset owner. By this logic, centralized exchanges that open wallet accounts for their users may be providing custody even though the former engages third party DACs to manage their cold wallets. The Guidelines specifically exclude systems or protocols that merely host or facilitate storage (e.g. wallet-as-a-service), where the owner retains "full control" and is able to make transfers unilaterally (more on this later).[8]

3. Activity

From straight reading of the Guidelines, the DAC primarily plays a safekeeping role and is specified as a custodian for purposes of the capital market.[9]

However it is not spelt out how the DAC conducts detailed identification, attribution and history of ownership; and whether the DAC is expected to perform normal custodial functions such as processing the settlement of transactions, servicing corporate actions related to tokens (including capital distribution, burning/buyback, forced transfers, and proxy voting for governance), or exercising entitlements and obligations throughout the asset lifecycle.

4. Arrangement

The custodial arrangement must bear the hallmarks of a trust, such as the segregation of client assets and safeguard from misappropriation. While this helps to ensure bankruptcy remoteness, it should be noted that unlike trust accounts which are held in a bank, there is no bank to claim against – the DAC creates blockchain wallets for storage but the blockchain is not a legal person. **These wallets are not regulated in the same vein as online accounts or e-money purses,[10] though they could and should be.**

5. Compliance

Malaysia is compliant or largely compliant with nearly all FATF recommendations (38 out of 40).[11] The country is an early adopter of the Travel Rule and goes further e.g., by mandating it for transfers without any 'de minimis' threshold (cf. USD/EUR1000 for FATF) and requiring all unhosted wallet owners to be identified and sanctions screened before transfer.[12] Aside from the breadth of anti-money laundering laws, DACs are also required to protect personal data privacy and prevent corruption across the organization.[13]

6 Capital Markets and Services (Prescription of Securities) (Digital Currency and Digital Token) Order 2019, P.U.(A) 12/2019 incorporating amendment P.U.(A) 6/2025. Also, Public Consultation Paper 1/2025: Proposed Regulatory Framework for Offering and Dealing in Tokenised Capital Market Products.

7 See Guidelines on Compliance Function for Fund Management Companies

8 Guidance to paragraphs 23.01 and 23.02, Guidelines on Digital Assets 2020

9 Practice Note No.1/2024 – Digital Asset Custodian Specified As "Custodian" Under Section 121(G) Of The Capital Markets And Services Act 2007. Also Section 23.01, Guidelines of Digital Assets 2020, citing Section 76A(1) therein.

10 See Electronic Money (E-Money) | Bank Negara Malaysia

11 FATF Global Network | Malaysia (Follow-up Report 2018).

12 Chapter 9, Guidelines on Prevention of Money Laundering, Countering Financing of Terrorism, Countering Proliferation (revised 13 June 2024).

13 Namely Anti-Money Laundering and Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001, Personal Data Protection Act 2010, and Guidelines on Adequate Procedures issued pursuant to section 17A (5) of the Malaysian Anti-Corruption Commission Act 2009.

6. Jurisdiction

Foreign DACs who operate in a "comparable jurisdiction with whom the SC has regulatory arrangements" may be registered if it is in the best interest of the country to do so.[14] Notwithstanding this, comparable jurisdictions (e.g. equivalent or substantially equivalent to Malaysia) may still pose inconsistent requirements to foreign DACs, particularly if the law of more than one jurisdiction applies to the same digital assets.[15] In other words, domestic owners may not be assured of the same protection for recovery.

7. Technology

The emphasis is on organizational resilience with sound tech risk management.[16] Hence the Guidelines are tech-neutral and do not specify a preferred model of wallet architecture and hot-warm-cold apportionment, other than having "effective policies and procedures for key generation and management".[17] The fault lines for legal liability need to be scrupulously assessed as loss incidents aren't just caused by technology itself, but more often than not, due to counterparty failures or contributory negligence.

FULL CONTROL AND OWNERSHIP

The factual concept of 'full control' is crucial in determining ownership as the Guidelines state: *"An asset owner is considered as having full control of his digital assets when he holds the private key(s) to the wallet and the DAC does not have the ability to effect a unilateral transfer of the digital assets"*.[18] However in practice, the DAC's control is not always exclusive.

For secure formats like multi-party computation (MPC), the keys are divided between different signers; while for multi-signature, the set of keys are shared among different signers – which may include representatives of the client, sub-custodian and DAC.

If the DAC only holds one part of the keys, it arguably has 'partial control' not 'full control' – ergo custody is shared or joint at best.[19] As for MPC, if the architecture requires user authentication to cryptographically trigger a signing process, then the control rests with the user and logically no custodian service exists![20] In hardware security modules (HSM), it is an authorized signing to a key management system rather than holding the actual private keys.

Does the legal threshold for 'full control' have to be 100% or can it accommodate user-controlled configurations and delegations? How will this work in the context of sub-custody? One approach is to refine the concept of 'full control' so that it does not have to be fully exclusive (*erga omnes*) for the custody arrangement to take effect, and for the rightful controlling party to be registered and identifiable.[21] Alas the word 'control' is not defined, and could mean authorization or knowledge, presumably with consent. Furthermore, 'full control' cannot be absolute since the Guidelines allow nearly all processes including transfers to be outsourced, except for decision-making and client interaction.[22]

If control is equated to ownership, a hacker or thief who finds the keys, by lawful means or not, may become the owner of the entrusted digital assets. Inasmuch as control can be distinguished from proprietary rights e.g. DAC holds legal control of digital assets for the equitable interest of its beneficiaries, this is not established in the country's jurisprudence yet. As it stands, claimants in a dispute would have to rely on control as (unperfected) security interests. **It would also be interesting to see whether the courts will transpose 'full control' vs 'partial control' into a hierarchy of rights.** And when it comes to inheritance and intestacy cases, control is far from ideal as it does not guarantee the intended continuity of ownership.

14 Section 23.05(b), Guidelines of Digital Assets 2020.

15 See *Svalbard Holdings Ltd v Khoo Boon Gui [2025] MLJU 578*, Penang High Court.

16 See Technology Risk - Guidelines | Securities Commission Malaysia

17 Section 28.01-03, Guidelines on Digital Assets 2020.

18 Supra note 8.

19 The multisig model is adopted by at least one registered DAC in Malaysia.

20 See Christopher Grilhault des Fontaines (Dnfs), Custodial or Non-Custodial Under MICAR (8 April 2025).

21 Principles 6.10 and 7.1, UNIDROIT Principles on Digital Assets and Private Law. Note: Malaysia is not a member of UNIDROIT Statute, the International Institute for the Unification of Private Law.

22 Section 28.10, Guidelines on Digital Assets 2020.

LOCATION AND DIGITAL EVIDENCE

The location (*lex situs*) of digital assets is not covered in the Guidelines. Even though DACs are registered locally, the digital assets are domiciled in blockchain networks which are generally cross-jurisdictional – and may complicate the determination of territoriality and applicability of property laws. The use of foreign DACs might also present conflict of laws which would need to be reconciled in the custody agreement.

Nevertheless, the standing rules in the industry so far have centered on the 'place of the relevant intermediary approach' (PRIMA),[23] or the 'primary residence of the encryption private master keyholder' (PREMA).[24] Applying the former, it is the DAC, duly incorporated and regulated by the laws of Malaysia. As for the latter, "the employees that are involved in the key generation process" for onshore cold wallets are likely based in Malaysia as well,[25] though it is less certain how it applies to HSMs with colocation (for backup storage) and global key distribution. One local High Court case has ruled that a person's control of the wallets may determine "assets within jurisdiction" even if the wallet service providers are outside Malaysia.[26]

Location may also have bearing on the law of digital evidence. Digital assets in custody are susceptible to search and seizure for investigations under the country's *Criminal Procedure Code 2018*. When summoned, the DAC has to provide "access" to law enforcement agencies (LEA) such as "the necessary password, encryption code, decryption code, software or hardware and any other means required to enable comprehension of the computerized data",[27] including private keys presumptively; and this can be done without obtaining a warrant.[28]

Consequently, the seized digital assets will be transferred to an LEA-controlled address, along with freezing of the custodial wallet.[29] For foreign DACs, mutual legal assistance, warrants and subpoenas may be required. The procedures for forfeiture and recovery must be done "in accordance with the law, including if required with the order of the court",[30] and notice to third parties by way of gazette.[31] Though this could possibly run into challenges on location and ownership as discussed above.

REGULATORY COLLABORATION

Custody is the cornerstone of modern banking and finance; and the areas of regulation are well-established for decades. Therefore it is important for peer regulators in other sectors to collaborate so that regulations are harmonized.

For instance, the financial regulator may have to focus on asset quality and market integrity – even though 'key management' is the linchpin of a DAC setup which is much better regulated from personal data and cybersecurity angles – and not in derogation to other integral DAC components like trustees and e-wallets. Alas all these areas are overseen by separate regulators! Not to mention that there is a plurality of Islamic views – even though the SC has its own Shariah position, the respective state-level Fatwa Committees have their own as well.

Along with this, a "minimalist approach" is being practiced for digital assets so as not to stifle innovation.[32] It's supposed to provide a wide berth of flexibility for DACs and invite them to dialogue or propose solutions towards compliant outcomes.

23 Law Applicable to Certain Rights in Respect of Securities Held With an Intermediary 2006, Hague Convention.

24 See *Cheong Jun Yoong v Three Arrows Capital Ltd & Ors. [2024] SGHC 21*, Singapore High Court.

25 Section 28.02(b), Guidelines on Digital Assets 2020.

26 See *Sim Kwang Kai, Adrian v Johnathan Wong Futt Po & Ors [2024] MLJU 3396*, Malaysia High Court.

27 Section 116B(3), Criminal Procedure Code [Act 593].

28 Section 116A, ibid.

29 Section 2.7, Policy and Procedures for Seizing Cryptocurrencies 2023.

30 Section 1.4.1, Policy and Procedures for Seizing Cryptocurrencies 2023.

31 Section 61(2), Anti-Money Laundering and Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001. For instance, *Public Prosecutor v Joseph Lee Fook Heng (Kuala Lumpur Criminal Case No. WA-44-33-04/2024).*

32 Ismail Nawang N. and Abdul Ghani I.M., "Cryptocurrency: An Insight into the Malaysian Regulatory Approach", *Psychology and Education Journal*, Vol. 58 No. 2 (2021) pp 65-77.

Nonetheless, **custody itself is not an innovation even though novel technologies are used. The same discipline should apply to an old dog performing new tricks.** DACs could benefit from more prescriptive rules – such as security audits and standard of liability – in the wake of so many breach of trust cases, including mass data leakage of a national wallet registry,[33] and the largest ever heist of a custodial wallet?[34]

Digital asset custody is a risky business, and this article merely treads on the surface. Market participants should sort through the regulatory maze and legal ambiguity. Losses or threats cannot be fully prevented, but at least legal exposures can be anticipated and minimized.

33 "Leaked Personal Info of Over 5 Million Salvadorans Apparently Linked to Chivo Wallet", Bitcoin.com News, 11 April 2024.

34 "Hackers steal $1.5bn from crypto exchange in 'biggest digital heist ever'", The Guardian, 23 February 2025.

THE HONG KONG STABLECOINS BILL AND ITS IMPACT ON THE CRYPTO LANDSCAPE

AMITA HAYLOCK
PARTNER
MAYER BROWN

JUSTIN W.J. LAI
ASSOCIATE
MAYER BROWN

Stablecoins, digital currencies pegged to other conventional assets like fiat money or commodities, have become widely used in areas ranging from cross-border payments and remittances to decentralized finance. They are often perceived as the bridge between traditional finance and cryptocurrencies, offering faster, cheaper transactions while reducing price volatility and associated risks.

However, stablecoins still face challenges such as inadequate asset backing and insufficient transparency, and potential systemic risks persist. These challenges were highlighted by the collapse of TerraUSD in 2022, which revealed vulnerabilities and led to calls for regulatory oversight.

Against this context, on 6 December 2024, Hong Kong gazetted its Stablecoins Bill ("Bill"), following from a Discussion Paper and a Consultation Paper issued by the Hong Kong Monetary Authority ("HKMA") on 12 January 2022 and 27 December 2023 respectively. The Bill marks a significant step in Hong Kong's proactive regulation of stablecoins.

HIGHLIGHTS OF THE STABLECOINS BILL

The Stablecoins Bill establishes a comprehensive framework seeking to regulate the issuance of stablecoins, and the conduct of stablecoin-related activities, in Hong Kong.

As a starting point, the Bill's scope is determined with reference to the following definitions:

- *"stablecoin"*, defined as **"a cryptographically secured digital representation of value that –**

(a) is expressed as a unit of account or store of economic value;

(b) is used, or intended to be used, as a medium of exchange accepted by the public for any one or more of the following purposes – (i) payment for goods or services; (ii) discharge of a debt; (iii) investment;

(c) can be transferred, stored or traded electronically;

(d) is operated on a distributed ledger or similar information repository; and

(e) purports to maintain a stable value with reference to – (i) a single asset; or (ii) a pool or basket of assets",

but which excludes a digital representation of value that is issued by a central bank (or an entity performing the functions of, or authorised by, a central bank) or a government (or an entity authorised by a government to issue currency) or otherwise falls within the scope of other regulation.[1]

1 Namely: the Anti-Money Laundering and Counter-Terrorist Financing Ordinance (which applies to limited purpose digital tokens); the Securities and Futures Ordinance (which applies to securities or futures contracts); the Payment Systems and Stored Value Facilities Ordinance (which applies to floats or SVF deposits); and the Banking Ordinance (which applies to deposits).

- "specified stablecoin", defined as: (a) a stablecoin that purports to maintain a stable value with reference wholly to one or more official currencies (and/or units of accounts or stores of economic value specified by HKMA); or (b) a digital representation of value (or value of a class) specified by the HKMA.

- "regulated stablecoin activity", where a person is deemed to carry on a regulated stablecoin activity if: (a) he issues a specified stablecoin in Hong Kong in the course of business; (b) he issues a specified stablecoin in the course of business which purports to maintain a stable with reference (whether wholly or partly) to Hong Kong dollars; or (c) he carries on an activity specified by HKMA by notice published in the Gazette.

These terms, previously undefined under Hong Kong law, are foundational to the Bill. They dictate the specific digital assets and activities that are subject to the new regime – clarifying the scope of the Bill and establishing boundaries for regulatory oversight. This in turn enhances certainty for market participants and industry stakeholders from the perspectives of compliance and enforcement.

Businesses engaged in regulated stablecoin activity are subject to regulation under the Bill and should be familiar with its key features:

- Licensing and Registration Requirements: The Bill establishes a licensing regime under which a license must be obtained from the HKMA to carry on regulated stablecoin activity (or advertise oneself as carrying on regulated stablecoin activity). Once licensed, the licensee will be listed on a register maintained by the HKMA and subject to duties as stipulated under the Bill.[2] Most pertinently, the Bill sets out the minimum criteria that a licensee must fulfil:

- Corporate status: The licensee must be a company or an authorised institution incorporated outside Hong Kong.

- Financial resources: The licensee is obliged to have "adequate financial resources and liquid assets to meet its obligations … as they will or may fall due". Further, the licensee must have paid-up share capital of not less than HKD 25M (or equivalent in other currency) or other financial resources as approved by the HKMA equivalent to or exceeding HKD 25M (or equivalent in other currency).

- Reserve assets management: The licensee must maintain a pool of reserve assets, separate from any other pool of assets or funds held by the licensee, which "must be of high quality and high liquidity with minimal investment risks", must be "adequately protected against claims by other creditors", and the market value of which must at all times be at least equal to the par value of the outstanding specified stablecoins of the type in circulation.

- Redemption: The licensee must provide the stablecoin holders with redemption rights that are not subject to any unduly burdensome conditions or unreasonable fees. **Further, in the event of the licensee's insolvency, stablecoin holders have the right to direct the disposal of the specified reserve assets pool for the purposes of redemption on a pro rata basis and to claim against the licensee for any shortfall if proceeds from disposal of the specified reserve assets pool are insufficient to cover redemption in full.**

- Risk management and systems of control: The licensee must implement adequate and appropriate risk management policies and/or systems of control in relation to matters including the management of reserve assets, appointment of key personnel and officers, preventing anti-money laundering and counter-terrorist financing, the conduct of stablecoin

2 For example: the duty to pay the license fee; the duty to display its license number on its advertising material and consumer-facing interfaces of its software; the duty to ensure that it fulfils the minimum criteria established; and the duty to report to the HKMA matters including an inability to meet its obligations, a change of address, and material changes of circumstances.

activities, conflicts of interest, complaints handling and redress mechanisms, and business continuity and contingency planning.

- Disclosure and reporting obligations: The licensee is obliged to publish "a white paper to provide comprehensive and transparent information" about each type of specified stablecoin it issues and must make adequate and timely disclosures in relation to matters including the management of reserve assets and redemption rights. **The licensee is also required to seek the HKMA's consent to appointment of key personnel and notify the HKMA of changes to such personnel.**

- Prohibited Stablecoin Activities: The Bill outright criminalises certain harmful activities involving stablecoins. Broadly, these activities are: engaging in fraud and deception in relation to a specified stablecoin; and making a fraudulent misrepresentation or reckless misrepresentation for the purpose of inducing another person to enter into a transaction in respect of a specified stablecoin.

- Enforcement: The Bill grants broad enforcement powers to the HKMA as the primary regulatory authority. Aside from issuing, suspending, and revoking licenses, the Bill confers upon the HKMA the power to require the licensee to take remedial action, the power to appoint a statutory manager to manage the licensee's affairs, broad powers of investigation (including search and seizure under a warrant), and the power to impose sanctions for contravention of statutory provisions (including in relation to former licensees and officers of a licensee).

- Administration and Judicial Review: The Bill establishes the Stablecoin Review Tribunal ("Tribunal"), with jurisdiction to review decisions made under the purview of the Bill on application by aggrieved persons. Further, decisions made by the Tribunal may be appealed to the Hong Kong Court of Appeal.

IMPLICATIONS FOR HONG KONG AND THE BROADER CRYPTO INDUSTRY

As set out in the Consultation Paper, the key policy objectives sought to be achieved under the Bill are: to put in place appropriate safeguards to address potential monetary and financial stability risks posed by fiat-referenced stablecoins; to provide adequate protection to such stablecoin users; to maintain Hong Kong's status as an international financial centre by putting in place an appropriate regulatory regime for FRS issuers that is in line with international regulatory recommendations; and to foster sustainable and responsible development of the virtual asset ecosystem in Hong Kong by providing legal and regulatory clarity.

To meet these key objectives, the Bill imposes strict licensing, asset backing, and consumer protection measures. While critics may argue that these features increase compliance costs and stifle innovation (especially for smaller or emerging stablecoin issuers), the Bill may still be viewed as a necessary step to safeguard digital finance. Clear regulatory standards have the potential to enhance investor and consumer confidence in stablecoins, encouraging greater market participation and innovation in digital payment systems and decentralised finance. Without such standards, long-term market stability and consumer trust would be difficult to achieve in the rapidly evolving digital asset ecosystem.

For those interested in conducting stablecoin-related activities, the Bill provides transparency in the licensing process, establishing clear application and compliance procedures. The HKMA must provide written notice, including the grounds for its decisions, when granting, refusing, or attaching conditions to licenses or consents for key personnel. Further, any decision by the HKMA in this context may be subject to independent review by the Tribunal.

While the requirement for the HKMA's prior consent to the appointment of key personnel may introduce additional regulatory scrutiny and could be seen as a hurdle for some businesses, this requirement is balanced against the implementation of procedural safeguards and the availability of a review mechanism.

The Bill is one of the most advanced legislative efforts in the Asia-Pacific region in the cryptocurrency space. Jurisdictions such as Singapore and Australia have thus far relied on soft law instruments, combined with existing legislation, to mitigate risks.[3] Hong Kong's initiative may serve as a benchmark for regional regulatory standards and inform compliance strategies for businesses moving forward.

The Bill was presented to the Hong Kong Legislative Council for First Reading and commencement of the Second Reading debate on 18 December 2024. It was passed by the Legislative Council on 21 May 2025 and will come into force on 1 August 2025.

3 Singapore, see e.g.: the Response to Public Consultation on Proposed Regulatory Approach for Stablecoin-related Activities (proposing that single-currency stablecoins be regulated under a new framework while other stablecoins remain subject to the existing regulatory regime under the Payment Services Act 2019); Australia, see e.g. Consultation Paper 381 (proposing that the existing information sheet on the applicability of the Corporations Act 2001 and Australian Securities and Investment Commission Act 2001 to crypto-assets be updated to include further guidance relating to stablecoins.

LEGAL AND GOVERNANCE ISSUES REGARDING AGENTIC AI IN THE EU AND JAPAN

DR. MATTHIAS ARTZT
SENIOR LEGAL COUNSEL
DEUTSCHE BANK AG

YUMI AHN
COUNSEL
TOKYO INTERNATIONAL LAW OFFICE

MASAYUKI OTAKE
COUNSEL
TOKYO INTERNATIONAL LAW OFFICE

INTRODUCTION

Artificial intelligence is rapidly reshaping industries globally, and at the core of this transformation lies AI agents, posing unique and novel legal challenges for developers, deployers and users of AI agents as well as policymakers worldwide. This paper discusses certain legal issues AI agents present in light of current laws or regulatory frameworks in the EU and Japan - the EU adopting a codified and prescriptive approach and Japan adopting a non-binding and agile principle-based approach. Policy and practical recommendations are considered to mitigate the identified legal risks and promote innovation and voluntary governance based on principles of transparency and accountability.

WHAT IS AGENTIC AI?

An AI agent or agentic AI is an autonomous AI system that can plan, execute tasks, and work towards some pre-defined objectives without human intervention, i.e. making autonomous decisions based on real-time data and adapting its output based on past experiences.

Agentic AI is driving automation, enhancing decision-making, optimizing performance and user experience across various sectors, such as finance, healthcare, manufacturing, entertainment and beyond, creating new efficiencies and possibilities.

What sets agentic AI apart from monolithic ("stand-alone") large language models (LLMs) is its ability to interact with external systems, such as APIs, IoT devices, enterprise tools as well as other AI agents. While traditional LLMs typically require human instructions for each task, agentic AI can retrieve real-time information, access databases, interact with other software tools, and take initiatives to execute based on such context. More advanced AI agents continuously refine their decision-making processes using machine learning techniques, as seen in self-driving cars that autonomously navigate roads, make decisions and adapt to road conditions through an accumulated set of data.

WHAT LEGAL CHALLENGES DOES AGENTIC AI PRESENT?

There are potential cybersecurity and legal challenges surrounding AI and, particularly, agentic AI.

Security remains a paramount concern, as vulnerabilities in AI algorithms or models could lead to exploitation by bad actors or agents autonomously making unintended harmful decisions. Since AI agents have some discretion on how to achieve their given tasks, they may tend to explore and pursue the easiest path to optimize their results. For example, an AI agent may decide to share information with other AI agents pursuing the fastest route to achieve certain tasks, which may infringe data protection or IP rights of those affected by that disclosure. Also, when it comes to liability concerns, without a clear disclosure on the part of an AI agent, it may not be clear to the counterparty that they are acting or transacting against an AI agent. Another legal problem with AI agents could be a lack of transparency over how an AI agent has arrived at a certain decision or outcome, making it difficult to prove causation for any claims for losses or damages allegedly caused by an AI agent.

The EU AI Act

The EU AI Act classifies AI systems into different categories according to their risk profile – prohibited, high-risk, limited or minimal risk. **AI agents are not specifically mentioned in the EU AI Act. However, the autonomous nature of an agentic AI system may increase the risk profile under the EU AI Act significantly when compared with a monolithic LLM. Given the autonomous and self-transformative nature of AI agents, they may alter their activities without being instructed to do so which may trigger a re-assessment of their initial risk classification.** For example, if an AI agent has been classified as a high-risk system, in the course of interacting with other agents, its particular activity may fall into the scope of prohibited AI practices. The EU AI Act does not regulate this type of scenario explicitly. However, Article 5 of the EU AI Act stipulates, amongst others, that the use of an AI system shall be prohibited that deploys purposefully manipulative or deceptive techniques with the objective, or the effect of materially distorting the behaviour of a person.

If an AI agent's activity falls under the prohibited category under Article 5 (1) (a) of the EU AI Act, violations will entail heavy penalties under the EU AI Act amounting to 35 million Euros or up to 7% of the total worldwide annual turnover of the offending company.

This implies that the violation needs to be allocated to a specific offender, such as the provider or the deployer of an AI agent being launched in the EU.[1] Against this background, we need to be able to track the company or person that developed or deployed the AI agent.

Given that the EU AI Act is essentially a product safety regulation, this provision needs to be interpreted broadly to cover all relevant use cases. This is also underpinned by the definition of the deployer under Article 3 of the EU AI Act. A deployer means a natural or legal person, public authority, agency or other body using an AI system under its authority. This implies that the deployer is accountable to others for any losses or damages caused by the AI system under its authority. To that end, all activities rendered by an AI agent, even those which go beyond the initial scope of tasks attributed to such agent, are under the control and authority of the deployer. Personal or non-professional usage of AI systems is excluded from the scope of the deployer liability under the EU AI Act.[2]

AI legal framework in Japan

In contrast to the EU's prescriptive approach, there are no binding laws in Japan on the use of AI other than general non-binding guidelines on responsible development and deployment of AI - an agile approach taken by the Japanese government to foster innovation.[3]

1 The territorial scope of the EU AI Act is designed to ensure that all AI systems affecting individuals within the EU are comprehensively regulated, irrespective of where the operator is based. The applicability of the EU AI Act is very broad, please see: Artzt, Belitz, Hembt, Lölfing (ed.), *International Handbook of AI Law* (2025), at 110.

2 Artzt, Belitz, Hembt, Lölfing (ed.), *supra* n. 1, at 109.

3 "AI Governance for Business Ver. 1.1", Ministry of Economy, Trade, and Industry (METI) and Ministry of Internal Affairs and Communications (MIC) of Japan, accessible at: https://www.soumu.go.jp/main_content/001003028.pdf

In March 2025 the Ministry of Economy, Trade and Industry (METI) of Japan published non-binding guidelines titled "AI Business for Business Ver. 1.1"[4] (the "AI Guidelines") to provide guiding principles for AI governance in Japan to promote safe and secure use of AI, detailing the scope of responsibilities and concrete action points for AI business actors. The AI Guidelines stress the importance of "agile" governance, whereby multiple stakeholders continuously and repeatedly conduct environment and risk analysis, goal setting, system design, operation with evaluation in various governance systems, thus the guidelines being a "living document" framework with a continuous, multi-stakeholder review mechanism. The AI Guidelines are also intended to ensure consistency with the latest trends and contents of the international AI governance principles and standards. The AI Guidelines do not generally apply to the use of AI for non-business activities, but for the purpose of stakeholder engagement, non-business AI users are included as stakeholders, such as academic and research institutions, civil societies and general consumers.[5]

The AI Guidelines recommend that developers, deployers and users of AI comply with the following principles: (i) human-centric; (ii) safety; (iii) fairness; (iv) privacy protection; (v) ensuring security; (vi) transparency; (vii) accountability; (viii) education; literacy; (ix) ensuring fair competition; and (x) innovation.

In addition, the AI Guidelines recommend additional principles to be followed for AI business actors involved in "advanced AI systems", defined as "the most advanced AI systems including the cutting-edge foundation models and generative AI systems".

Although it is not clear whether AI agents would be considered "advanced AI systems" under this definition, but it is more likely than not that AI agents would be considered to be advanced AI systems as AI agents carry more legal risk than generative AI by its autonomous nature.

The additional principles or requirements that apply to advanced AI systems under the AI Guidelines, amongst others, include: (i) taking appropriate measures throughout the development of advanced AI systems, including prior to and throughout their deployment and placement on the market, to identify, evaluate, and mitigate risks across the AI lifecycle, including employing diverse internal and independent external testing measures, such as red-teaming; (ii) identifying and mitigating vulnerabilities, and, where appropriate, incidents and patterns of misuse, after deployment including placement on the market; (iii) publicly reporting advanced AI systems' capabilities, limitations and domains of appropriate and inappropriate use; (iv) working towards responsible information sharing and reporting of incidents among organizations developing advanced AI systems including with industry, governments, civil society, and academia; (v) developing, implementing and disclosing AI governance and risk management policies grounded in a risk-based approach – including privacy policies, and mitigation measures, in particular for organizations developing advanced AI systems; (vi) investing in and implementing robust security management, including physical security, cyber security and security measures against internal threats, throughout the AI lifecycle; and (vii) developing and deploying reliable content authentication and provenance mechanisms, where technically feasible, such as watermarking or other techniques to enable users to identify AI-generated content. These evidently represent a high bar for compliance, and developers and deployers of AI agents could be expected to comply with them in Japan.

4 *Ibid*. See also "Guidelines for Government Agencies on the Procurement and Utilization of Generative AI for Administrative Innovation and Evolution," issued by Japan's Digital Agency in May 2025, establishing normative end-to-end lifecycle frameworks, from planning and procurement to development, operation, and monitoring, to ensure the safe and effective integration of generative AI into government information systems while balancing innovation with risk management, accessible at: https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/80419aea/20250527_resources_standard_guidelines_guideline_01.pdf

5 *See supra* n. 3 at 4.

HOW DO LEGAL CHALLENGES OF AGENTIC AI TRANSLATE INTO LIABILITY CONCERNS?

Developer or deployer liability from the EU regulatory perspective

AI systems using algorithms and models to make predictions and decisions, are prone to any flaws or algorithmic biases which may result in financial losses, discriminatory outcomes, or harmful advice, leading to potential lawsuits.[6] This particularly applies to agentic AI. **Since the EU AI Act is a product safety regulation, it is pivotal to identify a natural or legal person which is subject to enforcement actions for launching AI agents in the EU market in case of any incompliance with the EU AI Act.** As mentioned above, the performance of an AI agent is under the authority of the deployer pursuant to Article 3 of the EU AI Act. The deployer can be held liable for all damages caused by AI agents which fall under its authority, irrespective of whether he has knowledge about the related performance of the AI agent. Authority as a legal term should be interpreted broadly aimed at enabling the affected individuals to enforce their legal rights against the deployer of AI agents.

The EU AI Liability Directive (AILD), alongside the revised EU Product Liability Directive ("PLD"), was one vehicle to address the challenges posed by tort liability of AI developers and deployers under national laws of the member states, which govern the enforcement procedures raised by the affected individuals. The AILD proposed significant alleviations for individuals seeking a compensation for AI-related harms by allowing them to access information about high-risk AI systems such as AI agents, and, more importantly, by providing a rebuttable burden of proof on the defendants for liability claims.[7]

However, the EU Commission decided to abandon the AILD based on its 2025 work program to reduce administrative burdens within the EU.[8]

This implies that individuals now need to prove the developer or the deployer's fault for the harm they have suffered because of any wrongdoings rendered by an AI agent. The burden of proof now resides with the affected individuals who will have to overcome more hurdles to sue developers or deployers of AI tools, including AI agents.

There is, for the time being, no EU law or regulation available which might help individuals enforce claims for damages caused by AI flaws. Even the revised PLD is not applicable to defective AI systems, let alone to AI agents. According to the PLD there must be a defect in the product which caused the damages. The PLD applies to a wide range of physical products, as well as software and AI systems. The scope of the PLD, as amended, has thus been extended to new technologies, and confirms that software-based products or services empowered by AI are subject to the revised regulation.[9]

It is irrelevant whether the software or the AI system is stored on a device or accessed via cloud technologies.[10] However, under the PLD, the AI system needs to be linked to or connected with a product or service as long as they are under the control of the manufacturer.[11] One example provided in the EU AI Act is an AI-enabled home security system where the AI component forms part of the product being placed on the EU market. In contrast, the PLD does not apply to AI agents if they are not connected to specific products or services.

Developer or deployer liability from the Japanese regulatory perspective

As of the date of this article, AI agents are not recognized as separate legal persons in Japan. This means that even if an AI agent autonomously makes transactions or performs a task, the agent cannot hold a legal title to any assets, nor could it be held liable for its actions in Japan.

6 Artzt, Belitz, Hembt, Lölfing (ed.), *supra* n. 1, at 211.

7 *Ibid*, at 233.

8 Caitlin Andrews, "European Commission withdraws AI Liability Directive from consideration", IAPP, 12 February 2025, accessible at European Commission withdraws AI Liability Directive from consideration | IAPP

9 Artzt, Belitz, Hembt, Lölfing (ed.), *supra* n. 1, at 220.

10 Revised PLD Compromise Text Recital 12.

11 Artzt, Belitz, Hembt, Lölfing (ed.), *supra* n. 1, at 220, 221; revised PLD Compromise Text Recital 15.

It would thus be desirable to have a system where the information about the developer and/or the deployer of an AI agent is disclosed. **Furthermore, developers or deployers of AI agents may be held liable in a product liability claim or a civil action for negligence in Japan for any harm caused by AI agents, although proving causation may be difficult.**

If AI agents are trained with copyrighted materials, there may be a potential issue with infringement of copyright under Japanese laws. In 2023, the Agency for Cultural Affairs in Japan clarified the interpretation of Article 30-4 of the Copyright Act, such that using copyrighted materials to train AI is permitted without obtaining permission from the copyright owner, regardless of whether such AI training was intended for commercial use.[12]

This allows the training of AI agents with copyrighted materials without the need to obtain permission from the copyright owners. However, this is limited to training AI systems, and if AI agents interact with humans or other AI agents and autonomously distribute and manipulate valuable IP without authority or a license from the owners, developers or deployers of AI agents could be held liable for the infringement of IP rights. Without such developer or deployer liability, rampant infringing acts by AI agents could threaten the integrity of IP regulatory regimes worldwide.

If AI agents gather personal information about Japanese residents, compliance with obligations under the Act on the Protection of Personal Information (APPI) should be considered. These obligations under the APPI apply to business operators, and do not extend to individuals who may collect personal information of other Japanese residents for personal use. If AI agents collect personal information about Japanese residents, they are required to clearly specify the purpose of the collection before or at the time of collecting such personal information.[13]

Developers or deployers of AI agents are also generally prohibited from sharing or selling the personal information of Japanese residents to third parties without the explicit consent of the related individuals.[14] Moreover, if the developer or the deployer intends to transfer any personal information collected to a third party, the developer or the deployer must disclose the recipient's name and the purpose of the transfer to the data subject and ensure that the third-party recipient also complies with its obligations under the APPI.[15]

To avoid any potential breach of data privacy-related obligations under the APPI, developers or deployers of AI agents should pseudonymize or anonymize any personal information collected from individuals as much as possible, prevent data leaks, and avoid re-identifying pseudonymized data, and regularly review the stored data to erase any that is no longer required.[16]

PRACTICAL RECOMMENDATIONS FOR MITIGATING LIABILITY RISKS

There are a couple of tangible measures developers and deployers of AI should consider aimed at reducing their liability exposure vis-à-vis individuals, irrespective of which AI regulation governs their activities.

AI safety by design

When developing and deploying an AI agent, it is critical to consider AI safety from the outset at the technology design stage.[17] AI safety by design is a great mechanism to manage down the liability exposure of both developers and deployers in cases where AI agents exhibit unpredictable failures or even arbitrary (Byzantine) behaviour, or deceptive behaviour as often evidenced in various case studies.

12 "General Understanding on AI and Copyright in Japan", the Legal Subcommittee under the Copyright Subdivision of the Cultural Council, May 2024, accessible at: 94055801_01.pdf (SECURED)

13 Article 17, APPI.

14 Ahn, Arai, Marx & Sai, *AI Agent Economy in Web3 Games – Legal and Regulatory Issues in Japan,* International Journal of Blockchain Law, Volume XI, February 2025, 35-40, at 39.

15 *Ibid.*

16 *Ibid.*

17 Artzt, deVadoss, *A Byzantine Fault Tolerance Approach towards AI Safety*, arXiv (April 2025), accessible at: https://arxiv.org/abs/2504.14668; Artzt, deVadoss, *Can blockchain technology help mitigate the black box phenomenon of AI applications?* Solicitors Journal (April 2025), at 21.

An example of such AI safety by design is the Byzantine Fault Tolerance (BFT) system. At a high level, it treats an AI system as a collection of redundant, cooperating modules rather than a single monolithic AI tool. Each critical decision, prediction or action is produced not by one component alone, but by multiple parallel components (potentially diverse in design) that collectively decide the output by running a consensus algorithm which allows multiple AI modules to agree on one output, reducing the risk of hallucinations.[18] There are various use cases for BFT such as autonomous vehicle decision-making or industrial control systems.[19]

Considerations for good AI agent governance

It is pivotal to implement ethical guardrails and clear pre-defined perimeters AI agents must adhere to from the outset. Such programming requirements based on ethical principles[20] before deployment should form part of an AI agent governance program, which deployers are required to adopt within their organizations. AI governance is not about mere compliance with black letter laws, but a more holistic approach is required to ensure that AI agents remain safe and ethical, increasing trust in the technology and mitigate any risks and reputational harm.[21] In the interest of transparency and accountability, the guardrails embedded in a proper AI governance program must be clearly defined, documented and made available to the users with the purpose of preventing the AI agent from exceeding the risk perimeters initially assigned to it.

Database for good governance practices

One possible measure to mitigate liability risks in AI development and /or deployment is to establish a database, which could be an industry or government-led initiative to systematically collect, analyse, and publish good practices among AI business actors.

By establishing a centralized repository of proven governance frameworks, risk management techniques, and operational protocols, such database can be used to equip business actors with concrete, field-tested examples that reduce the likelihood of non-compliance or liability risks.

Particularly, collecting sector-specific best practices provides organizations with templates that address their field's unique legal and ethical challenges, helping them to implement proven controls, avoid common pitfalls and stay compliant. Such system would encourage transparency within the nascent industry, foster accountability and enable smaller or less experienced entities to learn from industry pioneers, avoiding large front loaded compliance costs and accelerating maturity in safe and ethical development of the AI agent commerce. Furthermore, government agencies can further leverage aggregated data to identify emerging risk patterns, update regulatory guidance in real time, and design targeted capacity-building programs.

Through proactive stewardship of good practice dissemination, policymakers can empower AI business actors to make informed decisions aligned with societal expectations and legal and ethical obligations, thereby minimizing exposure to litigation, regulatory sanctions, and reputational harm.

Mandatory risk assessment and management

An AI governance program should also include restrictions such as limitations on data scraping, sharing or using sensitive personal information in an unauthorized manner.

18 *Ibid.*

19 *Ibid.*

20 Examples of ethical principles are provided in the AI Guidelines in Japan (see infra Section II. 2): (i) human-centric; (ii) safety; (iii) fairness; (iv) privacy protection; (v) ensuring security; (vi) transparency; (vii) accountability; (viii) education; literacy; (ix) ensuring fair competition; and (x) innovation.

21 Bird & Bird, Insights, 18 February 2025, accessible at: AI Governance Essential Insights for Organisations Part I Understanding Meaning Challenges Trends a - Bird & Bird

Developers or deployers of AI agents should understand and control the data set the AI agents will be working with and make clear disclosures to the end users, including publishing privacy policies and other mitigation measures.[22] Developers or deployers of AI agents are advised to assess with a critical eye what data the AI agent may have access to, and continue to monitor its performance – e.g. red-teaming to check if the agent draws any wrong conclusions from the information or giving harmful advice, including running safety impact assessments and documenting the training data, algorithms and decisions of the AI agents. This step would reduce the liability risk of agentic AI as it necessitates human supervision and control within the governance framework. And as with human employees, it would be good practice to give AI agents lower risk tasks only first and scale up the risk profile as trust around the agent performance builds.

Requirement of internal and regular third-party audits

Related to the implementation of various governance mechanisms proposed above, deployers of AI agents will also need to put in place internal controls within their organizations and audit such controls and measures, so that such governance mechanisms have been implemented correctly and there are no operational pitfalls. Regular audits on AI agents' outputs and functions by competent human personnel are crucial. Deployers of AI agents should also ensure that such internal human controls do not become the weakest link in the control mechanism as data or cybersecurity incidents often result from human errors, incompetence or illicit behaviour. To prevent such internal human pitfalls, regular third-party audits by independent and competent auditors regarding the internal governance controls would also help building more robust governance.

22 This is in line with one of the additional requirements under the AI Guidelines for advanced AI systems in Japan, see *infra*, Section. II. 2.

Creation of AI Agent Registry

As iterated above, at the core of liability concerns surrounding AI agents is the issue of not being able to identify or track whether we are interacting with AI agents in a virtual environment. With the number of AI agents in the market expected to increase to 1 million by the end of 2025,[23] it will become increasingly difficult to track the humans or entities responsible for developing or deploying certain AI agents.

Creation of an AI agent registry by self-governing industry-led organizations could serve as a public record that identifies deployed AI agents, their functions, and the organizations responsible for them. This type of an open and transparent system would enable regulators, deployers, users and other stakeholders to track and audit the actions and behaviour of AI agents to monitor and enforce upon any misuse or unforeseen behaviours.

Depending on the severity of misuse or performance failures, sanctions, such as warnings, suspension or decommissioning could be imposed upon AI agents by the self-governing industry organization.

Creation of such registry is undoubtedly mammoth of a task, with the need for standardizing across different sectors and jurisdictions. Without clear standards, a registry could become a bureaucratic tool with inconsistent data, making it less effective as an oversight mechanism. One possible solution for such authentication of data issue would be to create an AI agent registry using blockchain technologies, such as digital identifiers (DIDs), so that each AI agent is given a unique identification on the blockchain that cannot be tempered with.[24]

23 "New agent launches on Virtuals plummet amid AI token drawdown", Coin Telegraph, 8 February 2025, accessible at: New agent launches on Virtuals plummet amid AI token drawdown — TradingView News

24 Ahn, Arai, Marx & Sai, *supra* n. 14 at 37.

Insurance solutions

As the full extent of potential losses or harm caused by AI agents is yet unknown, one possible solution for the allocation of such unknown risks is insurance – there are some ongoing innovations in the insurance industry to develop insurance products to cover AI-related risks, including losses arising from AI's hallucination, false information or harmful content.[25] In May 2025, Lloyds of London announced a new insurance product that triggers payouts if an AI system's performance falls below an expected level – for example, if a chatbot causes an error, the error in itself is not sufficient for a payout, but the insurer would only provide coverage if the AI system's accuracy rate falls to 85% from the expected level of 95%, for example.[26]

As the scope of AI agents' use cases grow there could be further risks of litigation for errors committed by AI including AI agents, as the recent lawsuit brought by a consumer against Air Canada has set a clear precedent that deployers of AI systems are liable for errors made by AI systems that cause losses to a third party, even if such errors are not directly caused or intended by the deployer, and businesses cannot shift the blame on faulty AI systems.[27]

CONCLUSION

AI agents are still in early days of development, undergoing a constant influx innovation, and their liability issues are still evolving and largely unknown. Such liability issues of AI agents are not confined to a single jurisdiction but will continue to have an overarching impact on the developers, deployers and users of AI agents worldwide, thus open dialogue and collaboration between industry stakeholders, corporate and retail users and policymakers are pivotal for the technology's development based on principles of safety, fairness, transparency and accountability.

25 "Insuring Generative AI: Risks and Mitigation Strategies; Balancing creativity and responsibility to enable adoption", Munich Re (2024), accessible at: MR_AI-Whitepaper-Insuring-Generative-AI.pdf

26 Insurers launch cover for losses caused by AI chatbot errors

27 "Air Canada ordered to pay customer who was misled by airline's chatbot", The Guardian, 156 February 2024, accessible at: Air Canada ordered to pay customer who was misled by airline's chatbot | Canada | The Guardian

CONFIRMING A NEGATIVE: CFTC STAFF ISSUE AN ADVISORY CLARIFYING WHEN FOREIGN-ORGANIZED ENTITIES ARE TRADING AND BROKERING DIGITAL ASSET DERIVATIVES OUTSIDE OF THE COMMISSION'S CROSS-BORDER JURISDICTION

DANIEL J. DAVIS
PARTNER AND CO-CHAIR, FINANCIAL MARKETS AND REGULATION
KATTEN MUCHIN ROSENMAN LLP

CARL E. KENNEDY
PARTNER AND CO-CHAIR, FINANCIAL MARKETS AND REGULATION
KATTEN MUCHIN ROSENMAN LLP

ALEXANDER C. KIM
ASSOCIATE
KATTEN MUCHIN ROSENMAN LLP

Derivatives market participants and exchanges can breathe a little easier now that Staff of the Market Participants Division and the Division of Market Oversight of the Commodity Futures Trading Commission (CFTC or Commission) have jointly issued an advisory letter (the Advisory Letter) on May 21 clarifying Staff's interpretation of whether a person trading digital asset derivatives, which is organized and operating outside of the United States, is:

- A "non-U.S. person" as defined under the CFTC's cross-border regulations;
- Not a "U.S. person" as defined by the CFTC's 2013 Final Swaps Cross Border Interpretive Guidance;
- A "foreign located person" as defined for the purposes of determining whether such person is exempt from registration as a futures commission merchant (FCM) or introducing broker (under CFTC Regulation 3.10(c)(1)(ii));
- Not a "person located in the United States" for the purposes of determining whether a foreign intermediary must register as an FCM; and
- Not a "participant located in the United States" for the purposes of determining whether a foreign exchange must register with the Commission as a foreign board of trade.

If you are asking why CFTC Staff would have to issue such an interpretation, given that there is decades of CFTC precedent addressing many of these cross-border jurisdiction issues, you might be forgetting about the evolution of the previous Commission's approach to cross-border jurisdiction in digital asset enforcement actions. The CFTC first espoused this novel interpretive theory when it brought an enforcement action against a major offshore crypto exchange in early 2023.[1] In that case, the previous Commission advanced an expansive interpretation of "principal place of business" that went beyond the traditional "nerve center" test, focusing on where senior management makes strategic decisions,[2] instead looking to factors such as the location of ultimate beneficial owners, key personnel involved in trading operations, and other operational touchpoints with the United States. In response to that complaint and the previous Commission's expansive theories of US person status, a number of offshore crypto exchanges implemented aggressive onboarding questionnaires that went well beyond the statutory definition of US persons in an attempt to avoid potential CFTC jurisdiction.

THE FALCON LABS ENFORCEMENT ACTION: CEMENTING AN EXPANSIVE JURISDICTIONAL TEST

The previous Commission cemented its expansive view of what constitutes a US person with its enforcement action in May 2024 against Seychelles-organized Falcon Labs, Ltd. (Falcon Labs) for failing to register as an FCM with the CFTC.[3]

In essence, the CFTC's enforcement action against Falcon Labs established a new test for the extraterritorial application of the Commodity Exchange Act (CEA) by asserting that Falcon Labs was brokering digital asset futures and swaps transactions with "persons located in the United States."

Acting Chairman Caroline Pham—while a commissioner — noted in her concurring statement that the Commission's new test in the Falcon Labs case "could have the effect of requiring any non-U.S. legal entity that transacts in futures, options, or swaps that has a U.S. parent entity or beneficial owner, or has personnel located in the U.S. that 'control' . . . a non-U.S. prime broker sub-account, to be deemed 'located in the United States' even if its location of corporate organization is outside the United States and duly complies with the legal or regulatory obligations of the non-U.S. jurisdiction."[4]

Indeed, the CFTC's expansive interpretation of "U.S. person" had implications that extended far beyond the digital asset space, potentially affecting traditional derivatives market participants with any meaningful US operational nexus. The Advisory Letter was intended to reverse this novel interpretation espoused by the Commission in the Falcon Labs enforcement action, which some industry participants widely criticized for establishing "new regulation through enforcement."

CFTC'S EXTRATERRITORIAL JURISDICTION OVER FUTURES AND SWAPS

The CFTC's extraterritorial jurisdiction regarding futures and swaps is different and based on two separate sections of the CEA.

With respect to futures, Section 4(b) of the CEA grants the CFTC authority to regulate foreign futures activity of persons "located in the United States."[5] To explain the scope of its foreign futures authority, the CFTC promulgated Part 30 of its regulations to address when foreign brokers provide US customers with access to foreign futures, and Part 48 of its regulations to address when foreign exchanges provide direct access to US customers.

1 *See CFTC v. Changpeng Zhao et al.*, No. 1:23-cv-01887 (N.D. Ill. Mar. 27, 2023).

2 *Cross-Border Application of the Registration Thresholds and Certain Requirements Applicable to Swap Dealers and Major Swap Participants,* 85 Fed. Reg. 56,924, 56,936-937 (Sept. 14, 2020) (quoting *Hertz Corp. v Friend*, 559 U.S. 77, 80 (2010)).

3 The CFTC alleged that Falcon Labs facilitated access to digital asset exchanges to U.S.-located customers to trade spot crypto as well as crypto derivatives, including futures and swaps. Falcon Labs' CFTC settlement included a cease and desist from acting as an unregistered FCM, disgorgement of $1,179,008 in fees earned from its activities and a civil monetary penalty of $589,504. In short, the Commission found as the basis for Falcon's alleged violation of the FCM registration requirement that Falcon had customers "located in the United States," "such as non-U.S. incorporated entities operated and controlled by U.S.-based trading firms."

The Commission determined that Falcon Labs was offering FCM services to entities, which were "located in the United States" as a result of: (1) the location of entities' ultimate beneficial owners; (2) the location of entities' places of organization; (3) the principal place of business of each entity; and (4) the location of personnel controlling a non-US prime broker sub-account. None of these criteria, however, are set forth in the CEA's statutory language, and the CFTC has not issued an interpretation or adopted a regulation expanding its exterritorial jurisdiction over futures or swaps to capture such activity.

4 Caroline D. Pham, Concurring Statement of Commissioner Caroline D. Pham on Novel U.S. Location Test and FCM Registration, CFTC (May 13, 2024), https://www.cftc.gov/PressRoom/SpeechesTestimony/phamstatement051424.

5 7 U.S.C. § 6(b).

The key criteria used to determine when a customer is considered in scope for these purposes focuses on the customer's physical location (i.e., is the person "located in the United States, its territories or possessions who trades in foreign futures and options").[6]

Concerning swaps, Congress established the CFTC's extraterritorial jurisdiction under Section 2(i) of the CEA as part of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act). The Dodd-Frank Act establishes the CFTC's swap jurisdictional authority, which hinges on whether swaps activity occurring outside of the United States has "a direct and significant connection with activities in, or effect on, commerce of the United States."[7]

In explaining the scope of its swap jurisdiction, the CFTC first issued its *Interpretive Guidance and Policy Statement Regarding Compliance With Certain Swap Regulations in 2013* (2013 Guidance), which defined a "U.S. person" to include, among others, entities "organized or incorporated under the laws of a state or other jurisdiction in the United States or having its principal place of business in the United States."[8] Principal place of business was defined to included entities that are organized outside of the United States but have the "center of direction, control, and coordination" (i.e., the "nerve center") of their business activities in the United States.[9]

In 2020, the CFTC adopted final rules in CFTC Regulation 23.23 to supersede, in part, the 2013 Guidance with respect to the extraterritorial application of the swap dealer *de minimis* threshold calculation. The CFTC adopted a similar US person definition, which for entities also focuses on whether such entity was "organized, incorporated, or established under the laws of the United States or having its principal place of business in the United States."[10] CFTC Regulation 23.23 similarly defines "principal place of business" to mean the location of the legal person's nerve center.

Notwithstanding the above, the CFTC in the Falcon Labs enforcement action found Falcon Labs to have violated FCM registration requirements when dealing with non-US organized entities with principal places of business outside of the United States, but with beneficial owners located in the United States.

THE REQUESTOR'S SPECIFIC FACTS

The Advisory Letter addressed a request from a digital assets proprietary trading firm organized in the Bahamas. The Requestor's main office and headquarters are located in the Bahamas, where its high-level officers (including its chief executive officer, chief operating officer, and chief compliance officer) primarily direct, control, and coordinate the firm's activities. However, the Requestor is indirectly owned by a small number of closely associated natural persons who are residents of the United States, and these persons are also co-owners and co-managers of a separate, US-based proprietary trading firm.

The Requestor sought to expand its activities into the United States through several means: (1) engaging US-based traders, quantitative researchers and software developers (all of whom would be employed by a Bahamas-organized affiliate); (2) licensing trading technology from its related US firm; and (3) hosting trading technology on US-located servers. The Requestor requested a determination that it would nevertheless qualify as "located outside the United States" for purposes of the Commission's futures regulations and as a "non-U.S. person" for purposes of the Commission's swap regulations.

6 *See* the definition of "foreign futures or foreign options customer" in CFTC Regulation 30.1(c).

7 7 U.S.C. § 2(i).

8 2013 Guidance, 78 Fed. Reg. 45,292, 45,302 (July 26, 2013).

9 *Id*. at 45,309.

10 17 C.F.R. § 23.23(23)(i)(B).

CFTC STAFF'S ANALYSIS AND CONCLUSIONS

Based on the facts presented in the request for interpretation, specifically that the Requestor's "place of organization and the location where its high-level officers primarily direct, control, and coordinate" the Requestor's activities are outside the United States, the Advisory Letter concluded that the Requestor is (1) not "a person located in the United States" for the foreign futures or options analysis;[11] (2) not "a participant located in the United States" for CFTC Regulation 48.2(c); (3) a "foreign located person" for the foreign intermediary exemption in CFTC Regulation 3.10(c)(1)(ii); and (4) a non-US person for the CFTC's swap cross border jurisdiction.

Significantly, CFTC Staff clarified that the Requestor's proposed expansion activities—including engaging US-based personnel, licensing technology from a US firm, and hosting technology on US servers — would not impact the Requestor's status. Notwithstanding this expansion, the Requestor would continue to ***not*** be "a participant located in the United States" for Commission Regulation 48.2(c), remain a "foreign located person" for the foreign intermediary exemption in CFTC Regulation 3.10(c)(1)(ii), and continue to be a non-US person for the CFTC's swap cross border jurisdiction.

IMPLICATIONS FOR THE DIGITAL ASSET INDUSTRY AND BEYOND

The Advisory Letter represents a significant course correction for the CFTC's approach to cross-border jurisdiction, with implications that extend well beyond the digital asset space. By returning to the traditional "nerve center" test for determining principal place of business and rejecting the more expansive factors used in the Falcon Labs case, the Commission has provided much-needed clarity for market participants operating across jurisdictions.

The Advisory Letter's key takeaways for market participants include:

- **Offshore digital asset firms can now maintain non-US status while engaging meaningfully with the US market.** The letter's express approval of the Requestor's ability to employ US-based personnel, license technology from US firms, and host technology on US servers demonstrates that operational touchpoints with the United States do not automatically trigger CFTC jurisdiction.

- **Traditional derivatives market participants receive reassurance that routine US.** operational connections will not automatically trigger registration requirements.

  The expansive interpretation rejected by Staff would have potentially captured any foreign entity with meaningful US operational connections — including foreign banks, asset managers, and commodity trading firms — but the Advisory Letter reaffirms the traditional jurisdictional tests that focus on place of organization and management control rather than broader operational touchpoints.

- **Market participants can return to relying on decades of established precedent rather than navigating novel enforcement theories.** This should reduce compliance costs and encourage legitimate market participation by removing the specter of unexpected jurisdictional exposure that had emerged from recent enforcement cases.

However, the Advisory Letter comes with important limitations that market participants should carefully consider:

- **The guidance addresses only the specific factual situation presented by the Requestor.**

11 Note that for futures analysis, the test is location-based (i.e., whether a person is "located in the United States") rather than the "principal place of business" test used for swaps analysis.

Firms with different fact patterns — particularly those with US-based senior management or where strategic decision-making occurs in the United States — may still face jurisdictional exposure under traditional tests.

- **Staff guidance, while generally respected, could theoretically be superseded by future enforcement actions or formal rulemaking.** The Advisory Letter represents Staff guidance rather than a formal Commission interpretation or binding regulation.

- **The Commission has not completely retreated from aggressive enforcement theories.** Market participants should not assume that all jurisdictional concerns have been resolved, particularly for firms with more extensive US connections than the Requestor.

Looking forward, the Advisory Letter suggests that the Commission may be stepping back from the more aggressive jurisdictional theories advanced in recent enforcement cases, potentially signaling a more measured approach to cross-border regulation. For an industry that has faced significant regulatory uncertainty, this return to established precedent and traditional jurisdictional tests should provide a more stable foundation for compliance planning and business development across international markets.

ARTICLE VI

UK CRYPTOASSET REGULATION: WHAT IS THE IMPACT OF THE PROPOSED REGIME?

DIEGO BALLON OSSIO
PARTNER
CLIFFORD CHANCE

DR. MONICA SAH
PARTNER
CLIFFORD CHANCE

SARA EVANS
SENIOR ASSOCIATE
KNOWLEDGE LAWYER
CLIFFORD CHANCE

MADELEINE YATES
SENIOR REGULATORY ADVISOR
CLIFFORD CHANCE

LAURA NIXON
KNOWLEDGE DIRECTOR - FINTECH
CLIFFORD CHANCE

On 29 April 2025, HM Treasury (HMT) published a draft statutory instrument which will create a new UK regulatory regime for cryptoassets, including stablecoins, with the legislation due to be finalised by the end of the year.

In this briefing, we consider what cryptoassets and activities will be caught by the new regime. We highlight some issues that may need clarification and outline what firms might do now to prepare.

HMT originally consulted on its developing cryptoassets policy in 2022 and confirmed its approach in 2023. Some further clarifications followed from the new UK Government in November 2024.

The long-awaited draft Financial Services and Markets Act 2000 (Regulated Activities and Miscellaneous Provisions) (Cryptoassets) Order 2025 (Draft Order) will primarily extend the UK regulatory perimeter by amending the Financial Services and Markets Act 2000 (Regulated Activities) Order 2001 (RAO) to include a range of cryptoasset activities and makes a series of consequential amendments to the wider regulatory framework.

WHAT DOES THE DRAFT ORDER DO?

Fundamentally, the Draft Order does three things: (i) it includes certain cryptoassets (and stablecoins) in the list of "specified investments" in the UK, (ii) it designates certain activities in respect of such investments as "regulated activities" so that carrying them on in the UK by

way of business triggers a licensing requirement; and (iii) it makes some consequential changes to legislation, bringing in a revised territorial scope, new exclusions to regulated activities and new exemptions to avoid other frameworks inadvertently overlapping.

DOES THIS MEAN THAT CRYPTOASSETS ARE EFFECTIVELY TREATED AS 'SECURITIES' IN THE UK?

No, the current list of specified investments in the UK includes abroad range of investments such as deposits, consumer loans, electronic money (e-money), emission allowances and insurance contracts, as well as things that qualify as securities such as shares or bonds. The effect of adding qualifying cryptoassets into the list of specified investments simply means that qualifying cryptoassets are investments in respect of which certain regulated activities are licensable.

The specific rules that apply as a result are currently being discussed and consulted upon by the UK Financial Conduct Authority (FCA).

WHAT ACTIVITIES ARE IN SCOPE OF THE DRAFT ORDER?

The Draft Order will introduce new cryptoasset-specific activities, as well as apply existing activities to cryptoassets. The new cryptoasset activities introduced under the Draft Order are:

- issuing a qualifying stablecoin in the UK;
- operating a qualifying cryptoasset trading platform;
- safeguarding of qualifying cryptoassets and relevant specified investment cryptoassets;
- dealing in qualifying cryptoassets as principal;
- dealing in qualifying cryptoassets as agent;
- arranging deals in qualifying cryptoassets; and
- qualifying cryptoasset staking.

While some of these activities have parallels with activities in relation to existing specified investments, the requirements are not necessarily aligned with the equivalent existing activities for such specified investments and so require careful analysis.

WHAT CRYPTOASSETS ARE IN SCOPE OF THE NEW REGIME?

The Draft Order builds on the existing definition of 'cryptoasset' in the Financial Services and Markets Act 2000 (FSMA) which means: "any cryptographically secured digital representation of value or contractual rights that: (a) can be transferred, stored or traded electronically, and (b) that uses technology supporting the recording or storage of data (which may include distributed ledger technology)".

The new terminology is important in delineating the scope of the new regulated activities, particularly the new definitions of "qualifying cryptoasset" and "qualifying stablecoin".

- **"qualifying cryptoasset"** – a FSMA-defined "cryptoasset" which is fungible and transferable but specifically excluding specified investment cryptoassets, e-money, fiat currency, central bank digital currency and utility or closed loop tokens that cannot be transferred or sold and allow the holder to acquire goods or services from the issuer or within a limited network of service providers which have direct commercial agreements with the issuer. This definition is specifically stated to include "qualifying stablecoins" (unless within an exclusion) but would not include tokenised versions of other specified investments, for example.

  This definition is similar to, but amends (and replaces) the definition of "qualifying cryptoassets" in the Financial Services and Markets Act 2000 (Financial Promotion) Order 2005 (SI 2005/1529), Schedule 1, para 26F.

The terms "fungible" and "transferable" used here both require further consideration

Although used in wider financial services regulation, English law has no general definition of "fungible", and it would be worth HMT clarifying the meaning here. For example, in this context should "fungible assets" be limited to assets which are legally or operationally indistinguishable, or should they include assets considered to be functionally equivalent (even if not actually identical)? Whether a cryptoasset is genuinely fungible, or is simply treated by the parties as such, will generally vary, depending on the terms and mechanism for the creation of the relevant cryptoassets.

In contrast, the Draft Order gives some explanation of the term "transferable", stating that the circumstances where a cryptoasset is "treated" as transferable "include" where a cryptoasset confers transferable rights, or a communication is made in relation to the cryptoasset which describes it as being transferable or as conferring such rights. While this is not an exhaustive definition of "transferable" it does leave open questions, in particular it is unclear what is intended to be covered with the specification of transferrable rights. Arguably these are circumstances where the asset is not transferred but merely the resulting rights. However, neither the Draft Order nor the Policy Note that was published in parallel clarify this point.

More generally, the reference to a "communication" also leaves unanswered questions.

For example, where an asset relies on the communication to qualify as transferable, who does this have to be issued or communicated by? Is it enough that any person issues the communication? What if the issuer specifically says that a cryptoasset is not transferable but a market for secondary transfers develops and communications from sellers or others say the contrary?

- **"qualifying stablecoin"** – a qualifying cryptoasset that (a) references a fiat currency; and (b) seeks or purports to maintain a stable value in relation to that referenced fiat currency by the issuer holding, or arranging for the holding of: (i) fiat currency; or fiat currency and other assets, irrespective of whether the holding of a fiat currency other than the one referred to in (a) or other asset contributes to the maintenance of that stable value. The Draft Order amends the RAO with the effect that qualifying stablecoins will not be considered deposits. The Draft Order also amends the Electronic Money Regulations 2011 (EMRs) to provide that "stored monetary value" for the purposes of the definition of e-money (Reg 2, EMRs) will not include qualifying stablecoins, money or assets held as a qualifying stablecoin's backing assets or the stabilisation mechanism for a qualifying stablecoin.

As drafted, the interplay of the definitions of cryptoasset (which includes e-money) and qualifying cryptoasset (which includes qualifying stablecoins but excludes e-money) and the amendment in respect of "stored monetary value" is likely to cause practical difficulty in distinguishing between qualifying stablecoins and e-money.

Additionally, the Draft Order creates two subcategories of specified investments:

- **"specified investment cryptoasset"** – a type of cryptoasset that meets both the definition of "cryptoasset" and the FSMA definition of "specified investment", for example a token on a blockchain representing an interest or right to an equity. It could be argued that a truly technology-neutral approach would apply the relevant existing regime to tokenised versions of existing specified investments. HMT has not clarified in its Policy Note accompanying the Draft Order why this new definition has been introduced, although it may be for the purposes of allowing the FCA to make rules specific to this type of cryptoasset.
- **"relevant specified investment cryptoasset"** - means a specified investment cryptoasset that is a security or a contractually based investment. The proposed definition is unclear as currently drafted, as it may not allow a legal analysis to confirm that traditional dematerialised securities are not caught by the definition of relevant specified investment cryptoassets.

WHAT STABLECOIN-RELATED ACTIVITIES WILL BE REGULATED UNDER THE DRAFT ORDER?

The Draft Order will introduce a new regulated activity of "issuing qualifying stablecoin in the United Kingdom". A person ('A') established in the UK will be conducting the activity where they:

- offer (or arrange for another to offer) a qualifying stablecoin created by or on behalf of A for sale or subscription (including where A accepts an invitation from another person ('B') for B's purchase of a qualifying stablecoin);
- undertake, or arrange for another to undertake, to redeem a qualifying stablecoin created by or on behalf of A (including where A assumes an undertaking by or on behalf of another, for example under a contract, to redeem a qualifying stablecoin created by, or on behalf of another); or
- carry on, or arrange for another to carry on, activities designed to maintain the value of the qualifying stablecoin created by or on behalf of A.

For the purposes of the definition, 'creating' a qualifying stablecoin includes the design of that stablecoin. Where the person that created the qualifying stablecoin is a group member of A, then that qualifying stablecoin is treated as having been created by or on behalf of A.

Maintaining a stable value is achieved by the issuer holding, or arranging for the holding, of either fiat currency or fiat currency and other assets.

A stablecoin that references other assets but does not reference a fiat currency will not fall within the definition of "a qualifying stablecoin".

ARE THERE ANY EXCLUSIONS TO THE REGULATED ACTIVITY OF ISSUING QUALIFYING STABLECOINS?

Yes, the Draft Order confirms that the regulated activity scope does not include the creation (including the design) or the minting of a qualifying stablecoin, provided that it first exists as an identifiable asset on the blockchain and is in a transferable form.

HOW WILL THE DRAFT ORDER APPLY TO STABLECOINS ISSUED OUTSIDE THE UK?

Notably, the new regulated activity of issuing qualifying stablecoins specifically applies to the issuance of stablecoins within the UK.

The Draft Order does not restrict stablecoins issued from outside the UK from being traded, or dealt in, within the UK.

While it is not clear that this is the intended policy outcome, the current drafting to set the territorial scope of the regime under the Draft Order has the consequence that foreign stablecoin issuers or others trying to sell in the UK might be regarded as carrying on another regulated activity introduced by the Draft Order. For example, unless one of the limited exclusions applies, this could potentially be caught by the activities of dealing in qualifying cryptoassets as principal (or agent) or arranging deals in qualifying cryptoassets (which both include qualifying stablecoins). As outlined in further detail below (see "What is the territorial scope of the Draft Order?" on page 37), with limited exceptions, the new regulated activities (other than qualifying stablecoin issuance) are intended to capture any firm that deals directly (without an intermediary) or indirectly (through an intermediary) with UK consumers with the result that those impacted are required to obtain UK authorisation, wherever the firm is based. As the need for clarity of the precise scope of the regulatory perimeter has been a focus of industry feedback on the Draft Order, this may be addressed by HMT when the Draft Order is finalised.

HOW DOES THE DRAFT ORDER REGULATE CRYPTOASSET TRADING PLATFORMS?

The Draft Order introduces the regulated activity of "operating a qualifying cryptoasset trading platform".

Closely following the existing "multilateral trading platform" definition under the RAO, a "qualifying cryptoasset trading platform" (CATP) is a system which facilitates the buying and selling of qualifying cryptoassets by bringing together (or facilitating the bringing together of) multiple third parties in a manner that results in a contract for the exchange of qualifying cryptoassets.

The scope of the regulated activity extends to exchange of qualifying cryptoassets for either other qualifying cryptoassets or money (including e-money) and accordingly clearly differentiates between the trading of qualifying cryptoassets and of traditional securities, including tokenised forms of traditional securities (which fall within the definition of "specified investment cryptoasset"). The regulated activity does not extend to clearing of trades by a CATP.

WHAT SAFEGUARDING PROVISIONS DOES THE DRAFT ORDER INTRODUCE?

The new regulated activity of "safeguarding" of qualifying cryptoassets and relevant specified investment cryptoassets has been adapted from the existing RAO definition of "safeguarding and administration of investments" (Article 40 of the RAO) to cover only "safeguarding", but not administration, in contrast to the position for a securities custodian. The regulated activity consists of:

- Safeguarding of qualifying cryptoassets or relevant specified investment cryptoassets on behalf of another; or
- Arranging for one or more persons to carry on that activity.

The activity is broad: "safeguarding" encompasses any situation where a firm has control of a relevant cryptoasset in a manner that allows it to transfer the benefit of the cryptoasset to another person (including itself).

The concept of "on behalf of another" includes scenarios where the person to whom the firm provides the service holds both legal and beneficial title to the relevant cryptoasset, holds only the beneficial title, or has a right against the firm for the return of the cryptoasset.

As currently drafted, this expansive definition could potentially bring agency services, lending activities, custodial staking, and some decentralised finance or DeFi activities into the new framework.

More importantly, the order may have significant consequences for the custody of relevant specified investment cryptoassets, on the basis that collateral arrangements with relevant specified investment cryptoassets may be brought into scope. For example, arguably repos and other securities financing transactions in respect of relevant specified investment cryptoassets may therefore require an additional licence.

The Draft Order sets out some relatively narrow exclusions to the activity. For example, qualifying cryptoassets held on behalf of another entity "temporarily to facilitate the settlement of transactions" are exempt from safeguarding requirements. As acknowledged by HMT, this exemption is necessary to provide UK customers with access to global markets. Additionally, a sub-custodian of a UK authorised cryptoasset custodian will be able to hold relevant cryptoassets without such sub-custodian being regarded as performing the regulated activity of safeguarding cryptoassets, provided that the sub-custodian is in the same group as the UK authorised custodian, and the UK authorised custodian accepts to the person for whom the cryptoassets are safeguarded a responsibility no less onerous than if the UK authorised custodian were safeguarding the cryptoassets itself.

HOW WILL THE DRAFT ORDER REGULATE DEALERS?

The Draft Order inserts new Articles 9U to 9Z of the RAO to introduce regulated activities and exclusions relating to dealing in qualifying cryptoassets (but not specified investment cryptoassets) as principal or agent and arranging transactions in qualifying cryptoassets (but not specified investment cryptoassets).

These new regulated activities have been adapted from existing regulated activities and drafted so as to be wide enough to include cryptoasset lending and borrowing services. The scope of the regulated activities does not include the new regulated activities of issuing qualifying stablecoin in the UK, operating a cryptoasset trading platform, or cryptoasset staking.

- Dealing in qualifying cryptoassets as principal encompasses buying, selling, subscribing for or underwriting qualifying cryptoassets as principal.
- Dealing in qualifying cryptoassets as agent encompasses buying, selling, or subscribing for or underwriting qualifying cryptoassets as agent.
- Arranging deals in qualifying cryptoassets comprises (i) making arrangements for another person (whether as principal or agent) to buy, sell, subscribe for or underwrite qualifying cryptoassets, and (ii) making arrangements with a view to a person who participates in the arrangements buying, selling, subscribing for or underwriting qualifying cryptoassets falling within (i), whether as principal or agent.

A range of exclusions apply to these activities, including:

- Creation including the design of a qualifying stablecoin, or the minting of a qualifying stablecoin such that it first exists as an identifiable asset on a blockchain and in a transferable form, are excluded from the scope of all three activities.

- A person ('P') will not be carrying out the activity of dealing as principal unless P holds himself out as willing, as principal, to buy, sell, subscribe for or underwrite qualifying cryptoassets at prices generally and continuously determined by P, or as engaging in the business of buying qualifying

cryptoassets of the kind to which the transaction relates with a view to selling them, or as engaging in the business of underwriting qualifying cryptoassets of the kind to which the transaction relates. This exclusion also applies unless P regularly solicits members of the public with the purpose of inducing them, as principals or agents, to enter into transactions constituting the activity of dealing as principal, and the transaction is entered into as a result of P having solicited members of the public in that manner.

- The activity of dealing as principal excludes any transaction a person ('A') enters as principal with another person ('P') if P is also acting as principal within the scope of the regulated activity of dealing, and (a) A and P are members of the same group; or (b) A and P are, or propose to become, participators in a joint enterprise, and the transaction is entered into for the purposes of or in connection with that enterprise. A similar exclusion applies to exclude transactions for which a person is engaged in arranging.

- A person will not be dealing as principal or agent where: (i) the qualifying cryptoasset is bought, sold, or subscribed for no consideration; (ii) there is a distribution of a qualifying cryptoasset that was automatically created as a reward for the maintenance of the distributed ledger or the validation of transactions; (iii) the qualifying cryptoasset is issued by and sold to or subscribed for by an employee or partner of the person carrying on the activity; or (iv) there is a non-public sale or transfer by a person ('A') of a qualifying cryptoasset created and minted by, or on behalf of, A and having as its sole purpose the raising of capital by A.

- The activity of arranging deals in qualifying cryptoassets excludes arrangements where they are solely arrangements under which persons will be introduced to a person authorised to carry on one of the regulated activities newly introduced by the Draft Order.

HOW WILL THE DRAFT ORDER REGULATE STAKING?

The activity of "qualifying cryptoasset staking" is defined as the use of a qualifying cryptoasset in blockchain validation, and "blockchain validation" means the validation of transactions on (a) a blockchain; or (b) a network that uses distributed ledger technology ("DLT") or other similar technology, and includes proof of stake DLT consensus mechanisms.

The activity includes making arrangements for qualifying cryptoasset staking.

There are only two exclusions for this activity, introducing and enabling parties to communicate. On its face no other exclusions apply. As such, arguably all proof of stake network operators may be caught on the basis that "arranging" has typically been regarded as being a very broad definition.

WHAT IS THE TERRITORIAL SCOPE OF THE DRAFT ORDER?

Given that many cryptoasset services are offered online and cross-border without the need for physical presence, a notable feature of the Draft Order is that it will apply not only to UK-based firms engaged in in-scope cryptoasset activities but also to overseas firms that actively solicit UK clients or market cryptoasset services within the UK. The policy intent is that any cryptoasset firm that deals directly (without an intermediary) or indirectly (through an intermediary) with UK consumers will be required to obtain UK authorisation, wherever the firm is based.

Various exemptions will operate to enable some firms to avoid the new regulatory burdens. The Policy Note says that the intention is for overseas firms that serve only UK institutional customers to not require UK authorisation, provided those clients are not intermediaries to UK consumers. If a firm deals with a UK consumer through intermediaries authorised to operate a qualifying cryptoasset trading platform or deal in qualifying cryptoassets as principal, authorisation will not be required. There is no corresponding exclusion where a firm is dealing with UK consumers through intermediaries who are instead authorised to deal in qualifying cryptoassets as agent, or to arrange deals in qualifying cryptoassets. Given that there is no overarching clear exclusion in the Draft Order that exempts overseas firms that serve only UK institutional customers, HMT's stated policy intention may not have been fully achieved.

With respect to in-scope safeguarding and staking activities, authorisation will be required if the firm carries on the activities in the UK or on behalf of a UK consumer. However, if a firm carries out safeguarding activities at the direction of a person that is authorised to perform the safeguarding activity, then the policy intention is that a firm should be able to conduct the activity from overseas without UK authorisation. This concession does not extend to staking.

As noted above, if a firm issues qualifying stablecoins, it will require authorisation if the issuance occurs from a UK establishment.

Based on the current drafting to set the territorial scope of the regime under the Draft Order, there is a risk that foreign stablecoin issuers or others trying to sell qualifying stablecoins in the UK may (depending on their arrangements) be regarded as dealing in qualifying cryptoassets as principal (or agent) or arranging transactions in qualifying cryptoassets in the UK if they seek to sell to UK persons, which would then trigger a separate authorisation requirement unless one of the limited exclusions applies. It is not clear that this is HMT's intended policy outcome and many industry responses to HMT on the Draft Order have flagged the concern.

While it is therefore hoped that some amendments will be made to the Draft Order by HMT following technical responses from industry to bring clarity on this (as well as other concerns), firms should consider reviewing their existing or planned arrangements to establish whether and to what extent cross-border marketing or service provision may bring them within UK regulatory scope.

WHAT DOES THE DRAFT ORDER MEAN FOR FINANCIAL PROMOTIONS?

Since October 2023, it has been a criminal offence under the Financial Promotions Order (FPO) to communicate a financial promotion in relation to qualifying cryptoassets in the UK unless it has been made or approved by a firm authorised under FSMA or it qualifies for an exemption. Currently, cryptoasset businesses registered with the FCA under the Money Laundering Regulations 2017 (MLRs) benefit from an exemption that permits them to approve their own financial promotions relating to cryptoassets. The Draft Order amends the FPO to remove this exemption, although given the scope of the new authorisation requirements under the proposed new framework, such firms will in practice require FCA authorisation to continue to operate their cryptoasset businesses in any event.

The Draft Order makes further amendments to the FPO to ensure that the new regulated activities are all included within the financial promotions regime.

ARE THERE ANY TRANSITIONAL ARRANGEMENTS UNDER THE DRAFT ORDER?

The Draft Order includes transitional arrangements to provide firms with sufficient time to apply for authorisation. The Draft Order requires the FCA to specify an application window period, no later than one year before the full implementation of the regime, during which firms can submit their application for authorisation or variation of permission (as the case may be). Under the current drafting, the FCA is free to set the duration of that application window, subject to the requirements that the minimum duration must be 28 days, and the window must have closed at least 28 days before the new regime goes live.

Presently, there are no firm dates for the new regime to enter into force or the application window to start and end. The date on which the regime will enter fully into force will be set out in the Draft Order once finalised, and it will then be for the FCA to decide on the start date and appropriate duration of the application window. We expect that the duration of the application window would be longer than the minimum 28 days. By way of example, when the FCA introduced an approval requirement for firms wishing to approve financial promotions, the FCA set an application window from 6 November 2023 to 6 February 2024.

A transitional period of two years from the full implementation date of the regime will apply for firms that submitted applications during the application window and whose applications have not yet been resolved by the FCA. A separate two-year transitional period will also apply for firms whose applications are denied or withdrawn, for the purpose of allowing firms to wind down their operations in an orderly manner.

Firms that are already registered with the FCA under the MLRs will not be subject to any automatic or priority authorisation procedure. All firms will be permitted to continue their operations for a period of time while they apply for full authorisation under the new regime. As noted above, the Draft Order provides that there will be a minimum of 12 months between the FCA's specification of the application window and the new regime becoming effective.

The Draft Order also provides that applications for authorisation or variation of permission can be made outside of the application window, but that this would impact the application of the transitional arrangements.

HOW WILL THE DRAFT ORDER ADDRESS DECENTRALISED FINANCE (DEFI)?

The Draft Order makes no provision for DeFi. DeFi activities will not fall within the scope of the Draft Order where the activities are undertaken on a truly decentralised basis with no sufficient controlling party. It will be for the FCA to assess if any party's control is sufficient to prevent the activities from being truly decentralised and to determine whether and for what activities any "sufficiently controlling party or parties" should be authorised.

WHAT HAPPENS NEXT?

Technical comments on the Draft Order were invited by 23 May 2025. **HMT intends to publish the final statutory instrument "at the earliest opportunity" after that date, which is hoped will take account of some of the industry feedback received.** HMT also plans to publish statutory provisions relating to the new market abuse and admissions and disclosures regimes for cryptoassets in due course.

The Draft Order forms an important part of the evolving UK cryptoasset regulatory regime. However, the day-to-day rules that cryptoasset firms will need to comply with are the remit of the FCA. The FCA is working to develop these rules through a sequence of discussion papers and consultation papers as outlined in its Crypto Roadmap. These include DP25/1: Regulating cryptoasset activities which requests feedback on the proposed regulatory regime for cryptoasset trading platforms, cryptoasset intermediaries and cryptoasset lending and borrowing, staking and DeFi, and consultation papers CP25/14: Stablecoin Issuance and Cryptoasset Custody and CP25/15: A prudential regime for cryptoasset firms, each published in May 2025.

All firms involved in cryptoasset-related activities in the UK should be engaged in reviewing their own regulatory permissions, structure, marketing and custody and trading models to establish how the new framework may apply to them, what available exclusions they may benefit from and what authorisations or variations of permission they may need to make. This should include considering how the outstanding concerns with the Draft Order may impact their business and how this may change when the final rules are published, as well as engaging with the separate draft legislation to be published on the admissions and disclosures and markets abuse regime. Firms should also engage with FCA consultations to help set the parameters of their regulated status.

GBBC AND NORTON ROSE FULBRIGHT'S FUTURE OF FINANCE CONFERENCE 2025

MATTHEW GREGORY
PARTNER, FINANCIAL SERVICES REGULATION (LONDON)
NORTON ROSE FULBRIGHT

SÉBASTIEN PRAICHEUX
PARTNER , FINANCIAL SERVICES REGULATION (PARIS)
NORTON ROSE FULBRIGHT

HANNAH MEAKIN
PARTNER, FINANCIAL SERVICES REGULATION (LONDON)
NORTON ROSE FULBRIGHT

DAVID SHEARER
PARTNER, CAPITAL MARKETS (LONDON)
NORTON ROSE FULBRIGHT

THE FUTURE OF DIGITAL PAYMENTS

Moderator: Matthew Gregory, Partner, Norton Rose Fulbright

Speakers: Angie Walker, Global Head of Banking and Capital Markets, Chainlink; Basak Toprak, EMEA Head of Kinexys Digital Payments, J.P. Morgan; Matthew Osborne, Europe Policy Director, Ripple; Nilixa Devlukia, EMEA Policy Advisor, GBBC

In a panel moderated by Matthew Gregory, Partner at Norton Rose Fulbright, experts explored the trajectory of digital payments in the UK, focusing on the next inflection point and what a world-class payment ecosystem might look like in the UK. Nilixa Devlukia, EMEA Policy Advisor at GBBC, opened by highlighting the UK's fragmented infrastructure and the absence of a collective PLC taking forward a new payments infrastructure; and the need for participants to coalesce around the growth agenda.

In her view, as the National Payments Vision takes shape, it should engage with the possibilities of Distributed Ledger Technology (DLT) to ensure the UK can deliver a secure, inclusive, and future-ready payment system.

Considering the significant change in attitude towards stablecoins, Matthew Osborne, Europe Policy Director at Ripple, pointed to their explosive growth; they now have a market capitalisation exceeding $250 billion and facilitate $4 trillion in monthly transactions—nearly matching the UK's GDP. This figure reflects real-world utility, with stablecoins increasingly used in lending, borrowing, collateral, and cross-border payments.

Osborne noted that regulatory support from MiCA and the Trump administration is a sign of how stablecoins could transform digital payments by offering a low-cost, fast alternative to current payment systems.

Angie Walker, the Global Head of Banking and Capital Markets at Chainlink Labs, added that proof of reserve is critical for stablecoin credibility and highlighted the work which Chainlink had been undertaking in this regard. She also highlighted the importance of secure minting and distribution, supported by data oracles, and referenced the UAE's recent regulatory developments and Brazil's Drex programme's second phase, with its emphasis on trade finance use cases for stablecoins.

Basak Toprak, EMEA Head of Kinexys Digital Payments at J.P. Morgan, discussed the growing use of blockchain and stablecoins in international remittances. She emphasised that while on-chain solutions are promising, the ecosystem must be connected to traditional systems. In her view, not everything will be on-chain immediately, and so strong links between on- and off-chain environments are essential. If enough utility within on-chain markets is created then off-ramping may not be necessary for a long time, though the ability to move between both will still be required.

The panel also considered the potential for a UK retail Central Bank Digital Currency (CBDC), noting that while the Bank of England is still exploring the digital pound, the European Central Bank is already in phase two of developing a digital euro, and Thailand is preparing to release a 'stablecoin'. The consensus was that central and commercial banks must collaborate rather than operate in silos. This cooperation would allow for organic growth, broader adoption, and increased use cases.

Angie Walker pointed out that interoperability is key and that there is likely to be less relevance for single DLT use cases which do not have clear practical application.

A seamless cash chain between public and private domains is seen as essential, and for growth to occur, a functioning cash leg must be in place, which is now beginning to emerge.

Regulation was another major theme. Matthew Gregory raised the question of whether we are heading toward regulatory convergence or divergence. In the crypto space, divergence seems more likely, and the panel considered the contrasting approaches in the EU and the UK – for example, highlighting MiCA's location-based requirements for stablecoin issuance. This presents a challenge, as stablecoins are designed to facilitate cross-border payments, which becomes difficult if they are tied to specific jurisdictions. However, the UK appears more open to overseas stablecoins, and the U.S. has introduced reciprocity arrangements to allow their use across borders. Despite these hurdles, the panel agreed that the market is moving away from experimentation and into real-world application. The regulatory landscape is evolving rapidly, and achieving a world-class payment ecosystem will require not only technological innovation but also degrees of regulatory alignment and cross-sector collaboration.

In summary, the UK's future in digital payments depends on infrastructure reform, regulatory clarity, and the integration of technologies like DLT and stablecoins. With the right strategy, the UK can position itself as a global leader in digital finance.

Summary provided by Matthew Gregory.

FIRESIDE CHAT

Moderator: Emma Joyce, Chief Revenue Officer, GBBC

Speaker: Superintendent Adrienne A. Harris, New York State Department of Financial Services (NYDFS)

In a wide-ranging fireside chat, Emma Joyce, Chief Revenue Officer at GBBC, sat down with Adrienne A. Harris, Superintendent of the New York State Department of Financial Services (NYDFS), to discuss the evolving regulatory landscape in the U.S. and its transatlantic implications.

Harris began by outlining the NYDFS's decade-long role in regulating over 3,000 financial institutions, including state-chartered banks, credit unions, and 120 foreign banking entities. Notably, it remains one of the few prudential regulators of cryptocurrency at both the state and federal levels. To operate in New York, virtual currency businesses must obtain either a BitLicense or a limited-purpose trust charter. While the process is intentionally rigorous, Harris defended its necessity, especially in light of the crypto winter. The NYDFS did not license firms like FTX, Voyager, or Celsius, a decision that, in hindsight, has proven prudent. During her tenure, the NYDFS issued nine new pieces of regulatory guidance, covering areas such as blockchain analytics, stablecoins, coin listings, and market manipulation, ensuring the framework evolves alongside the industry.

Harris emphasised that crypto companies in New York are held to the same standards as traditional financial institutions. This includes compliance with the Bank Secrecy Act (BSA) and stringent cybersecurity requirements. The NYDFS applies a bespoke supervisory model to each company, requiring a tailored risk framework and governance policy to determine which coins can be offered to customers. With over 60 full-time staff dedicated to crypto oversight, the NYDFS operates with the same depth as full-scope banking supervision. This robust model has earned the NYDFS a seat at the table as Congress drafts new legislation, often seeking its feedback. Harris also stressed the importance of preserving state authority in the face of federal legislative efforts, advocating for comprehensive legislation. **Despite concerns that strict regulation might stifle innovation, Harris pointed out that New York continues to compete with Silicon Valley when it comes to U.S. crypto investment, proving that a strong regulatory framework can coexist with a thriving fintech ecosystem.**

The conversation also touched on the broader political and legislative context. Harris noted that the Trump administration's deregulatory stance has led to significant shifts in the regulatory environment.

The GENIUS Act, which recently cleared a procedural hurdle in the Senate, and the House's STABLE Act are both key pieces of legislation to watch. While there is still a long road ahead for federal regulation of stablecoins and crypto, Harris expressed optimism about future collaboration with federal partners. She predicted that within a year, the U.S. would see finalised legislation on stablecoins and the emergence of more national trust frameworks for issuers.

Looking ahead, she anticipates a return to familiar themes from traditional banking such as tokenising reserves and creating derivatives but in a technological context. Harris also highlighted the importance of international cooperation, citing the NYDFS's Transatlantic Regulatory Exchange with the Bank of England as a vital step toward regulatory harmonisation. As more jurisdictions require stablecoin reserves to be held domestically, such collaboration becomes essential. In summary, the NYDFS's proactive and rigorous approach has positioned New York as a leader in crypto regulation, balancing innovation with consumer protection and setting a model for others to follow.

Summary provided by Hannah Meakin.

CAN TRADFI & DEFI COEXIST?

Moderator: Sébastien Praicheux, Partner, Norton Rose Fulbright

Speakers: Eva Wong, Director of Legal Affairs, Parity Technologies; Ian Taylor, Board Advisor, CryptoUK & COO, HT Digital; Ryan Hayward, Head of Digital Assets and Strategic Investments, Barclays; Dr. Vic Arulchandran, Head of Digital Product and Market Design, Deutsche Börse

Until recently, traditional finance (TradFi) and decentralised finance (DeFi) operated with distinct architectures and ideologies, but as moderator Sebastian Praicheux, Partner at Norton Rose Fulbright, noted, this is beginning to change.

The panel explored how these two systems might coexist and how DeFi protocols are adapting to regulatory constraints. Eva Wong, Director of Legal Affairs at Parity Technologies, addressed the governance challenges in DeFi, particularly around transparency and compliance on permissionless blockchains.

Despite concerns raised by the Bank for International Settlements about the lack of compliance checks on such infrastructures, Wong argued that innovation can still thrive in a decentralised setting. She explained how Parity's Polkadot network allows developers to build bespoke rollups using modular components, enabling them to choose the level of decentralisation and permissions appropriate for their use case. This flexibility allows builders to integrate compliance features – such as identity controls or access restrictions – without undermining the decentralised nature of the system.

Praicheux asked whether everything can be on-chain or if off-chain solutions are still necessary. Wong responded by highlighting the importance of tools like zero-knowledge proofs, which allow one party to prove the truth of a statement without revealing sensitive information. This cryptographic method enhances both security and privacy, making DeFi more trustworthy. She also introduced the concept of "proof of personhood," which could help verify a user's humanity without disclosing their identity a promising avenue to prevent malicious activity on blockchain networks. Ian Taylor, Board Advisor at Crypto UK, added that regulation often targets DeFi due to a lack of understanding.

He argued that misuse of code doesn't imply poor design or bad intentions. Instead, developers should implement safeguards like kill switches to recover compromised protocols, much like stablecoins. Taylor likened it to leaving a key in a safe: if someone accesses it, the issue lies in the handling, not the technology.

He stressed the need for greater education and awareness to bridge the gap between DeFi and TradFi, especially given the complex cryptography and security involved.

The discussion then turned to the use of Distributed Ledger Technology (DLT) in payments and settlements, and how this could reshape the future of banking. Dr. Vic Arulchandran, Head of Digital Product and Market Design at Deutsche Börse, spoke about central securities depositories (CSDs) and their role in managing securities electronically. While private adoption of DLT by CSDs is growing, public chain integration remains limited due to significant regulatory responsibilities, institutional caution and a preference for stability. However, in order for the DeFi and TradFi spaces to converge, there may be key roles for CSDs to play in a future where capital markets instruments, commercial and central bank money, are largely transacted and governed on private and/or public DLTs.

Ryan Hayward, Head of Digital Assets and Strategic Investments at Barclays, noted that permissionless systems are evolving, but widespread institutional adoption will take time. He suggested that tokenised deposits could become the endgame for banks in their transition toward digital finance, though they differ fundamentally from stablecoins in terms of issuance model, regulatory oversight and liability structure. Hayward emphasised that banks must engage with these technologies to remain competitive, particularly in foreign exchange and liquidity management.

The transparency and programmability of blockchain could offer significant advantages in meeting capital requirements and managing liquidity. In conclusion, while TradFi and DeFi can coexist, the journey will require time, education, and regulatory clarity. The chasm between the two remains wide, but with continued innovation and collaboration, it is possible to build a more integrated financial future.

Summary provided by Sébastien Praicheux.

FIRESIDE CHAT: EXPLORING DIGITAL ASSETS AND THE IMPACT AI HAS ON THEM

Moderator: Marcus Evans, Head of Information Governance, Privacy and Cybersecurity, EMEA, Norton Rose Fulbright

Speaker: Tanvi Singh, Founding Partner, Nirmata-ai Ventures & GBBC Board Director

In this session, Marcus Evans spoke with Tanvi Singh about the dynamic relationship between blockchain and artificial intelligence (AI). Their discussion emphasised the evolving intersections of new technologies and the opportunities and challenges that lie ahead.

Singh described how AI is driving advancements in blockchain-based systems, particularly in financial compliance and transaction monitoring. Traditional compliance processes mostly rely on expensive, rules-based engines that often produce a large number of false positives. This is where AI comes in, as it offers more precise and effective substitutes that are particularly effective for monitoring blockchain transactions where certain elements of transaction histories can be reviewed from end-to-end. The implementation of AI has helped reduce costs and complexity in moving projects from proof-of-concept to production and in the development time for producing smart contracts.

Singh also pointed to an increase in funding for projects combining blockchain and AI, which has reportedly reached over $10 billion in recent years.

Projects are shifting towards a shared innovation space and away from compartmentalised development.

One expected development of AI agents on blockchain is intelligence systems being able to carry out tasks autonomously across decentralised platforms. Although widespread trust and acceptance are still work in progress, these agents have the potential to simplify complex DeFi (decentralised finance) operations such as staking or token trading.

On the flip side, she touched on how the blockchain might be used to address AI challenges. **For example, it is difficult to trust and verify the training data that an AI model has been trained on: using a blockchain might present a way of re-assuring third parties of the provenance of the training data set.**

NAVIGATING THE REGULATORY LANDSCAPE

Moderator: Hannah Meakin, Partner, Norton Rose Fulbright

Speakers: Delphine Forma, Head of Policy, Europe & UK, Solidus Labs; Jordan Wain, UK Public Policy Lead, Chainalysis; Tiana Whitehouse, Co-Founder, Equisscore; Reagan Cook, GTM Lead, Taxbit

This panel explored how the global regulatory landscape for digital assets is evolving, and what this means for firms, regulators, and innovation. The panellists offered an incredibly grounded and candid discussion that covered the complexity of compliance and the future of proactive regulatory engagement.

One of the key themes was the fragmented nature of global crypto regulation. Forma pointed out that different jurisdictions have each taken varied approaches to regulating digital assets, with some employing a single regime, and others integrating crypto into existing frameworks, with the result being a patchwork of legal requirements that businesses must navigate carefully.

Whitehouse noted that, in the midst of this complexity, predictability and certainty in any area is valuable and praised Singapore for its transparent and consistent process.

Wain explained that the development of stablecoin regimes on a jurisdictional basis is a very fragmented approach to an asset that is intended to be used globally and that this fragments liquidity. All in all, the panellists discussed the difficulties of designing comprehensive and effective regimes because while many nations have rules in place, few have achieved both clarity and market confidence.

The panellists also discussed whether global harmonisation is realistic, let alone possible. Some pointed to signs of convergence in areas like reporting. Cook, for instance, discussed how more than 50 jurisdictions are starting to adopt new regulations that require cryptoasset service providers to combine and submit transaction and user identity data to tax authorities. This is an example of regulators modifying current reporting requirements to apply to the cryptocurrency industry. However, others voiced doubts that financial regulation would ever fully converge, especially in areas like stablecoins, referencing the stark disparities in legal systems, political priorities, and enforcement cultures.

The panel closed with a discussion of how firms are handling regulatory ambiguity and divergence. Speakers emphasised that success depends more on strong internal governance, particularly when it comes to risk appetite and decision making. Firms must be able to record how they handle compliance issues across jurisdictions, even when rules and regulations change or contradict each other. Despite the fact that many firms today juggle multiple overlapping compliance systems, technology was seen as both a potential enabler, but also a source of further complexity. Ultimately, the panellists agreed that while complete compliance comes at a significant cost, the cost of failure brings an even greater penalty.

To close the discussion, the audience was invited to share their thoughts via an interactive menti link on the question, "What do you think are some of the best crypto regulatory initiatives worldwide?".

Responses showed a wide range of global efforts, including Hong Kong's stablecoin regime, Singapore's Digital Payment Token framework, the UK's Digital Securities Sandbox and FCA crypto roadmap, as well as Switzerland's Crypto Valley initiative.

Summary provided by Hannah Meakin.

TOKENISATION AT SCALE: ARE WE FINALLY READY FOR INSTITUTIONAL ADOPTION?

Moderator: David Shearer, Partner, Norton Rose Fulbright

Speakers: Breige Tinnelly, Head of Market Development, Archax; James Pollock, EMEA Sales Director, Digital Asset

This panel paid key attention to one of the most commercially anticipated applications of blockchain technology—tokenisation at scale. This discussion explored whether the sector is finally ready for true institutional adoption, and what hurdles remain on the road to widespread adoption.

The panellists emphasised that tokenisation is more than just theoretical innovation. Tinnelly gave some examples of real projects that are being developed and implemented, such as the tokenisation of uranium, US Treasuries, and money market funds. Pollock discussed a multi-layered project involving a stablecoin, a medium-term note, and utility across a single blockchain network, in order to demonstrate early signs of system interoperability. Even though these use cases are still relatively small-scale compared to traditional financial markets, their movement into real-world settings signals maturity and utility.

The panel recognised that despite momentum, the path to widespread adoption is still full of obstacles associated with regulatory fragmentation, infrastructure limitations, and unresolved legal enforceability. Tinnelly mentioned, for example, that on-chain transfers of fund units are legally recognised in jurisdictions like Luxembourg, however, this is not the case in the UK.

Such legal inconsistency makes scaling difficult. Major problems still exist in areas like privacy, compliance with securities law, and standardisation across jurisdictions.

It is important to emphasise that the sector must prioritise privacy, control, and trust because regulation alone may not address these issues.

Another particularly insightful moment was when Pollock referenced Geoffery Moore's *Crossing the Chasm*, implying that the industry is now transitioning from bleeding-edge innovation into early adoption. **While full-scale transformation is yet to arrive, there is clear momentum as projects are moving forward, coalitions are forming, and asset managers are beginning to ask how to develop their digital strategies.** He and Tinnelly agreed that this moment is a crucial turning point.

Summary provided by David Shearer.

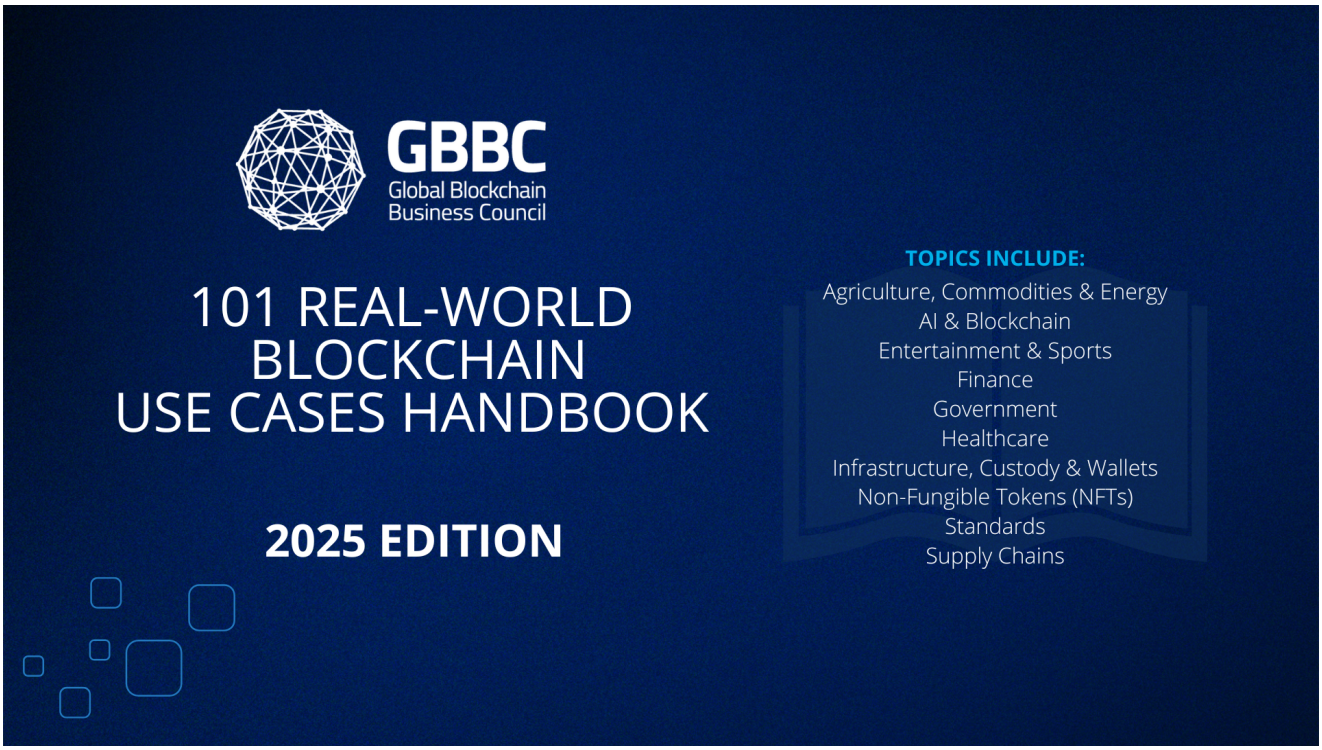
GBBC COMMUNITY'S 101 REAL-WORLD BLOCKCHAIN USE CASES HANDBOOK, 2025 EDITION

GBBC and our community have recently released the 101 Real-World Blockchain Use Cases Handbook, 2025 Edition.

This Handbook is a valuable reference guide for government agencies, regulators, and central banks worldwide, providing an educational resource to deepen their understanding of blockchain and digital assets. It highlights practical solutions, moving beyond the hype to showcase real-world use cases that are driving meaningful impact across industries, jurisdictions, and organizations.

A huge thank you to our community for the incredible work you have been doing and for taking the time to share your use cases with the industry. Your contributions make this resource possible.

GBBC's 101 Real-World Blockchain Use Cases Handbook is certified using SureMark Digital's blockchain-based registry to authenticate content. SureMark Digital is an authentication and content verification platform, leveraging the pioneering work of Stuart Haber and W. Scott Stornetta, co-inventors of early blockchain technology, to combat misinformation, certify digital documents, and protect against deepfakes.



ACCESS THE HANDBOOK

HOW CAN I GET INVOLVED?

Interested in submitting new work to or becoming an editor for the International Journal of Blockchain Law (IJBL)? Review the submission guidelines below and write to us at IJBL@gbbcouncil.org.

Length	3-4 print pages including footnotes
Target Audience for Submission	Broader business community aiming to better understand the technology and the legal issues associated with it
Content	All legal areas related to blockchain technology and digital assets
Structure	Introduction - Description of legal matter - Proposed solution - Conclusion/key takeaways
Writing Style	Not too academic; lucid and clear-cut language
What can I Submit?	Previously published work is welcome for submission to the IJBL