THE INTERNATIONAL JOURNAL OF BLOCKCHAIN LAW

Volume 11

February 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 back to the 11th edition of the IJBL, which once again spans a wide variety of blockchain and crypto-related topics across numerous jurisdictions such as the US, Hong Kong, UK, and Japan.

To set the scene: The Trump administration has recently adopted a more pro-innovation and collaborative approach, suggesting a lighter enforcement touch combined with a recognition of the need for regulatory clarity. In this context, and with the aim of tailoring compliance programs to the specific risks that crypto trading can pose, it is useful to consider the types of conduct the government has focused on in recent prosecutions. The lead article by David Hirsch, Garen Marshall, and Rhea Shahane from McGuireWoods' Washington, D.C. office, provides greater insight into the latest enforcement actions by the SEC and the DOJ in the realm of manipulative crypto trading. The authors conclude that fraudulent trading in crypto markets presents some unique issues, although it also shares characteristics with similar violations in traditional markets.

Joseph A. Castelluccio, Paul C. de Bernier, Rohith P. George, Stephanie M. Hurst, and Don F. Irwin from Mayer Brown's NYC office explore the first-of-its-kind merger of three different decentralized protocols to create a new single token and a new blockchain foundation ("Alliance") while the existing blockchain protocols continue as separate and independent organizations.

This presents interesting legal issues from a governance standpoint. They conclude that the Alliance may ultimately generate benefits for its token holders, although it will need to address significant challenges in operating this new organization.

Gage Raju-Salicki from Norton Rose Fulbright's St. Louis office delves into legal issues surrounding Section 12(a) of the Securities Act of 1933 in connection with recent lawsuits, which reveal a new potential for finding protocols or promoters, or both, civilly liable. He points out that the crux of each case is the way which the tokens have been promoted, such as through whitepapers or social media posts. These advertising activities have served as hooks for liabilities for protocols or promoters.

Andrew Fei from King & Wood Mallesons' Hong Kong office sheds light on an important aspect of how to treat crypto assets in banks' balance sheets.

He elaborates on the Hong Kong Monetary Authority's (HKMA) proposal to implement the Basel Committee's capital standards for banks' crypto asset exposures.

These standards and the HKMA's proposal are important because they prescribe how much regulatory capital banks must hold for their crypto asset exposures. This article is particularly interesting to our readers from regulatory authorities.

Rhea Saini from GSR touches on regulatory frameworks for crypto asset regulation in the EU and the US. While the EU has launched the MiCA, the US has kept pace by enacting the Financial Innovation and Technology for the 21st Century Act, also known as "FIT21". This bill allocates regulatory authority to both the CFTC and SEC and separates digital assets into three categories: digital commodities, restricted digital assets or securities, and permitted payment stablecoins, but it only provides substantive guidance and regulation for the first two. Rhea shares her view that, unlike FIT21, the EU's MiCA is far more expansive, encompassing all crypto assets, including securities and e-money (stablecoins), and regulating crypto asset service providers (CASPs) operating within the EU.

Roxane Ballew from GSR investigates legal issues pertaining to unincorporated Decentralized Autonomous Organizations (DAOs), particularly considering the legal structure of DAOs and the possibility of holding DAOs liable under US securities law. Leveraging the Wyoming Decentralized Unincorporated Nonprofit Association Act may provide a liability shield for DAO members. Roxane also highlights the potential downsides of utilizing this Act.

So Saito and Yu Mizushima from So & Sato Law Offices in Tokyo, Japan unveil the complexity of assessing staking and restaking under Japanese law. They showcase the factors that determine the applicability of Japanese financial regulations to staking and restaking activities.

One interesting legal issue is, for example, whether the restaking service qualifies as a custody business under Japanese law.

Yumi Ahn, Yojiro Arai, Jean-Denis Marx, and Victor Sai from Tokyo International Law Office bridge the gap between AI and tokenization. Their article provides fascinating insights into the world of AI agents from both legal (including data protection) and regulatory perspectives in Japan. They particularly scrutinize the legal status and various features of AI agents and conclude that issuers driving an Initial Agent Offering (IAO) are well advised to design their agent tokens in such a way to meet the requirements of NFTs, thus avoiding regulatory pitfalls.

This links perfectly to the final article by John deVadoss, Board Director and Co-Chair of the GSMI AI Convergence Working Group at GBBC, and me. We investigate a hot issue at the intersection of AI and blockchain. In this article, we explore how blockchain capabilities can help validate all steps across the training lifecycle of an AI model, thus understanding why an AI model behaves in a certain manner. Broadly speaking, blockchain technology aids in identifying and exposing contaminated or inaccurate personal data, or biased information baked into an AI model, rendering AI entries visible and auditable.

We conclude this edition with a link to a recording of GBBC's Blockchain Central Davos 2025 panel discussion on "Tokenization of Debt and Project Promissa (in Partnership with The World Bank)."

Happy reading and listening.

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.

THIAGO LUÍS SOMBRA

PARTNER, MATTOS FILHO

BRASILIA, BRAZIL

Thiago's practice focuses on Technology, Compliance and Public Law, and in particular on anti-corruption investigations handled by public authorities and regulators, data protection, cybersecurity and digital platforms. He was awarded as one of the world's leading young lawyers in anti-corruption investigations by GIR 40 under 40 and technology by GDR 40 under 40.

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

CRYPTO'S NEXT COMPLIANCE CHALLENGE: PREPARING FOR REGULATORY SCRUTINY OF MANIPULATIVE AND INSIDER TRADING

DAVID L. HIRSCH
PARTNER
MCGUIREWOODS

GAREN S. MARSHALL
PARTNER
MCGUIREWOODS

RHEA T. SHAHANE
ASSOCIATE
MCGUIREWOODS

Immediately upon taking office, President Trump signaled that he would take a very different approach in how the United States oversees and regulates crypto assets. Some changes are now clear, while others remain under discussion with the specifics and timelines yet to come.

As discussed in more detail below, the new administration is focused on abolishing previously imposed barriers that had restricted banks and intermediaries from working with crypto. As a result, crypto will be integrated more broadly within traditional financial institutions as some companies race to embrace the new opportunities, with others likely to follow suit more cautiously in response to consumer demand.

This dynamic of accelerating adoption but only limited clear rules and guidance creates challenges for entities that want to prepare for the changes ahead. But there are still opportunities for financial institutions to focus on known compliance risks that are unlikely to change. One area where institutions can efficiently focus their planning is on managing risks and enhancing compliance policies related to market manipulation and trading on material non-public information.

The issue of whether crypto assets are offered and sold as securities when traded on secondary markets has been the subject of extensive litigation, and district court opinions have reached differing conclusions. It is possible that this question will be resolved through court decisions, legislation or agency rulemaking. But regardless of whether the crypto assets being traded are treated as securities, commodities, or some new type of asset, financial institutions can lower their risks by taking steps to prevent, identify, and address this type of trading conduct.

THE NEW ADMINISTRATION QUICKLY MADE SIGNIFICANT CHANGES IN ITS APPROACH TO CRYPTO

In the first week of the new Trump Administration, the President made clear that crypto regulation will be very different in the years ahead.

On January 23, 2025, President Trump issued an executive order titled "*Strengthening American Leadership in Digital Financial Technology*" with the aim "to promote United States leadership in digital assets and financial technology while protecting economic liberty."[1]

The executive order seeks to ease barriers to digital asset transactions by ensuring greater banking access and offering regulatory clarity through neutral rules and transparent processes with defined jurisdictional limits.

The executive order also revokes prior Biden Administration guidance and directs the creation of a Presidential Working Group on Digital Asset Markets, which will be staffed with leaders from various federal financial regulators, White House advisors, and cabinet members or their designees.

The United States Securities and Exchange Commission (the "SEC"), which took a very active regulatory enforcement approach to crypto assets and market participants in the last administration, also announced significant changes in guidance and its approach to crypto. On January 21, 2025, acting SEC Chair Mark Uyeda announced the formation of a crypto task force led by SEC Commissioner Hester Peirce.[2,3] The goals for the task force are expansive, and its "focus will be to help the Commission draw clear regulatory lines, provide realistic paths to registration, craft sensible disclosure frameworks, and deploy enforcement resources judiciously."

Subsequently, on January 23, 2025, the SEC issued Staff Accounting Bulletin ("SAB") 122, rescinding the Biden-era SAB 121 guidance, which advised financial institutions holding crypto assets for third parties to record the value of those assets as liabilities on their balance sheets.[4] Treating a third party's assets held by the institution as the institution's liability made it much more costly for institutions to provide crypto custody services since institutions would then have to hold more non-crypto assets on their balance sheets to avoid violating regulatory capital requirements.

By replacing SAB 121, the SEC has eliminated that burden, which will likely enable more financial institutions to profitably provide crypto custody services to their customers.

EASING OF CRYPTO RESTRICTIONS IS COMING, BUT BROADER IMPLEMENTATION MAY TAKE TIME

As seen in the preceding section, the United States is on a path to adopting more crypto-friendly rules. And while financial institutions and the market await specifics, some things are already clear. For example, until new rules are promulgated, the SEC and CFTC will not bring new enforcement actions based on alleged failures to register a crypto asset or related services.[5] Similarly, banks, which were previously discouraged from developing crypto services and lines of business, will likely be encouraged, if not required, to support crypto customers and new products.[6]

However, despite agencies and regulators clearly signaling a more consultative and accommodating approach, new laws will likely be needed to address market structure and regulatory jurisdiction issues. Writing and implementing these laws will take time. For example, any new legislation related to crypto assets will likely take months or years to draft, pass, and implement. Moreover, the administration's new approach to crypto will likely involve various agencies introducing new rules or modifying existing ones.

1 *Strengthening American Leadership in Digital Financial Technology*, THE WHITE HOUSE (Jan. 23, 2025), https://www.whitehouse.gov/presidential-actions/2025/01/strengthening-american-leadership-in-digital-financial-technology/

2 *See SEC Crypto 2.0: Acting Chairman Uyeda Announces Formation of New Crypto Task Force*, U.S. SECURITIES AND EXCHANGE COMMISSION (Jan. 21, 2025), https://www.sec.gov/newsroom/press-releases/2025-30.

3 Commissioner Peirce has long advocated for a new, less restrictive approach to regulating crypto assets in the United States that better promotes innovation and investor choice. In fact, Commissioner Peirce has been so consistent in her efforts to reform the SEC's approach to crypto assets that she is affectionately known within the digital assets community as "Crypto Mom."

4 *See Staff Accounting Bulletin No. 122*, U.S. SECURITIES AND EXCHANGE COMMISSION (Jan. 23, 2025), https://www.sec.gov/rules-regulations/staff-guidance/staff-accounting-bulletins/staff-accounting-bulletin-122

5 This approach represents a shift from the Biden-era policy under which the agencies had argued that crypto projects should register under existing rules that have traditionally applied to securities and commodities.

6 On January 3, 2025, in response to a court order, the FDIC released pause letters that it sent to more than twenty banks between 2022 and 2023, instructing them to refrain from "all crypto-related activity." See Charting a New Course: Preliminary Thoughts on FDIC Policy Issues, FEDERAL DEPOSIT INSURANCE COMPANY (Jan. 10, 2025), https://www.fdic.gov/news/speeches/2025/charting-new-course-preliminary-thoughts-fdic-policy-issues.

Such changes likely will have to comply with the Administrative Procedure Act, which imposes process intense requirements including significant time for public comments and preparation of economic impact analyses.[7]

OPPORTUNITIES NOW TO BUILD EFFECTIVE ANTI-FRAUD AND ANTI-MANIPULATION COMPLIANCE

Federal investigations focused on manipulative conduct and trading based on material non-public information will continue, and may even increase, as resources previously tasked with investigating registration issues become available to address other conduct. Fraud occurs in all markets, and financial institutions have experience building controls to prevent and detect fraudulent trading conduct involving traditional assets, such as securities and commodities. To adapt compliance programs to the specific risks that crypto trading can present, it is helpful to consider the types of conduct the government focused on in recent prosecutions.

TYPOLOGIES OF MANIPULATIVE CRYPTO TRADING

"Insider Trading" Crypto Prosecution for Trading on Material Non-Public Information

In June 2022, the United States Attorney's Office for the Southern District of New York announced an indictment charging Nathaniel Chastain with one count of wire fraud and one count of money laundering, in violation of Title 18 United States Code, Sections 1343 and 1956, respectively, for misconduct that occurred while Chastain was an employee of Ozone Networks, Inc. (d/b/a "OpenSea"), a major NFT listing and trading platform.[8,9]

As alleged, in his role with OpenSea, Chastain was responsible for selecting which NFT series would be featured on OpenSea's homepage. Once an NFT series was featured on OpenSea's homepage, the price buyers were willing to pay for NFTs in that series typically increased substantially.

OpenSea treated the information about which series were going to be featured as its confidential business property.

According to the indictment, Chastain traded NFTs based on OpenSea's confidential business information, without its permission, to generate secret profits for himself. Specifically, it alleged that on dozens of occasions, Chastain used his knowledge of which NFTs were going to be featured on OpenSea's homepage to secretly purchase those NFTs in advance. Once the NFTs were featured on OpenSea's homepage, Chastain sold them at a profit of two to five times what he originally paid. He also used anonymous accounts to conceal his purchases and sales. This conduct, according to the government, constituted wire fraud and money laundering.

The defense argued in its Motion to Dismiss that wire fraud based on an insider trading theory must involve a security or commodity, and the indictment did not characterize the NFTs at issue as either.[10] The Court, however, denied the Motion to Dismiss, stating that the wire fraud statute does not reference securities or commodities.[11]

In the same Motion to Dismiss, the defense argued that the selection of the NFTs is not "property" under the wire fraud statute since their selection is based on the defendant's unspoken personal thoughts and, therefore, lack inherent economic value and cannot be sold or distributed.[12] The Court also rejected this argument, holding that confidential information acquired or compiled by a corporation in the course and conduct of its business, which the government alleged as to OpenSea's NFT listings, is a species of property.[13]

7 5 U.S.C. § 551-559.

8 *See Sealed Indictment, USA v. CHASTAIN, No. 1:22-cr-305 (S.D.N.Y May 31, 2022), ECF No. 1*; see also *Former Employee Of NFT Marketplace Charged In First Ever Digital Asset Insider Trading Scheme*, U.S. DEPARTMENT OF JUSTICE (June 1, 2022), https://www.justice.gov/usao-sdny/pr/former-employee-nft-marketplace-charged-first-ever-digital-asset-insider-trading-scheme.

9 NFTs or "non-fungible tokens" are unique assets, transacted and recorded on blockchains that can serve as collectibles, units of exchange, investments, and licenses or records of events or accomplishments, among other things.

10 *See* Memorandum in Support by Nathaniel Chastain re Motion to Dismiss the Indictment, ECF No. 19, *Chastain*, No. 1:22-cr-305.

11 *See* Memorandum Opinion and Order as to Nathaniel Chastain on Motion to Dismiss the Indictment, ECF No. 39, *Chastain*, No. 1:22-cr-305.

12 *See* Memorandum in Support by Nathaniel Chastain re Motion to Dismiss the Indictment, ECF No. 19, *Chastain*, No. 1:22-cr-305.

13 *Id.*

In May 2023, following a jury trial, Chastain was convicted on both counts, in spite of arguments that his use of transparent public blockchains to conduct the transactions demonstrated that he lacked the intent to defraud or conceal his conduct.[14]

He was sentenced to three months in prison, three years of supervised release, a $50,000 fine, and forfeiture of Ethereum he obtained through the trades at issue.[15] **Thus, while insider trading has long been prohibited in traditional financial markets, the Chastain prosecution established that analogous conduct involving crypto assets can also violate criminal laws, regardless of the nature[16] of the crypto asset at issue.** That is especially true where the trader owes a clear duty to the owner of the information, such as when the trader learns the information through his employment.

Financial institutions that service crypto asset customers should consider whether supervisory and surveillance programs address the risks highlighted in the Chastain case. For example, firms should consider whether policies identify information that is considered confidential and inform employees and others of their obligation not to trade on that confidential information. It is helpful to also describe the risks and consequences of improperly sharing confidential information. Companies should also consider implementing monitoring systems to detect unusual trading activity or patterns that suggest non-public information is being exploited.

14 *See Former Employee Of NFT Marketplace Sentenced To Prison In First-Ever Digital Asset Insider Trading Scheme*, U.S. DEPARTMENT OF JUSTICE (August 22, 2023), https://www.justice.gov/usao-sdny/pr/former-employee-nft-marketplace-sentenced-prison-first-ever-digital-asset-insider

15 *Id.*

16 The federal government's treatment of NFTs seems poised to change. During the Biden Administration, the SEC took the position that based on specific facts and circumstances, some NFTs were offered and sold as securities. *See SEC Charges LA-Based Media and Entertainment Co. Impact Theory for Unregistered Offering of NFTs*, U.S. SECURITIES AND EXCHANGE COMMISSION (Aug. 28, 2023), https://www.sec.gov/newsroom/press-releases/2023-163; *see also SEC Charges Creator of Stoner Cats Web Series for Unregistered Offering of NFTs*, U.S. SECURITIES AND EXCHANGE COMMISSION (Sept. 13, 2023), https://www.sec.gov/newsroom/press-releases/2023-178. But David Sacks, the new administration's designated AI and Crypto Czar, recently stated that he believes NFTs are more akin to collectibles than securities. https://www.youtube.com/watch?v=W5Zn6HWCPOg at 2:40

Enforcement and Prosecution of Manipulative Crypto Wash-Trading and Spoofing Scheme

In September 2022, the SEC charged Hydrogen Technology Corporation ("Hydrogen"), its former CEO Michael Ross Kane, and the CEO of Moonwalkers Trading Limited, Tyler Ostern, for their roles in manipulating the market for Hydro, a crypto asset.[17]

It charged those defendants with failing to register a crypto asset, fraud in the offer and sale of that asset, and engaging in market manipulation with the purpose of inducing the purchase or sale of the asset.[18]

The United States Department of Justice ("DOJ") pursued a parallel investigation and in April 2023 brought charges against Kane and Hydrogen's Chief of Financial Engineering Shane Hampton for essentially the same underlying conduct, asserting a variety of charges including conspiracy to manipulate security prices, conspiracy to commit wire fraud, and wire fraud.[19] The DOJ also filed informations charging Ostern and Hydrogen blockchain engineer Andrew Chorlian, with conspiracy to manipulate security prices and conspiracy to commit wire fraud.[20] According to the SEC complaint, by May 2018:

> Kane began selling the company's Hydro through his personal trading accounts with crypto asset trading platforms, [and] he quickly learned that the considerable volume of Hydro that Hydrogen needed to sell to raise sufficient cash would significantly depress… Hydro's price on the secondary market thus making it difficult to raise such funds.[21]

17 *See* Complaint, *SEC v. The Hydrogen Tech. Corp., et. al.*, No. 22-cv-08284 (S.D.N.Y Sept. 29, 2022), ECF No. 3.

18 *Id.*

19 *See* Indictment, *USA. v. Kane., et. al.*, No. 1-23-cr-20172 (S.D.F.L. April 20, 2023), ECF No. 3. In this indictment, the DOJ also brought charges against Moonwalkers CTO George Wolvaardt. *Id.* Charges against Wolvaardt are still pending, with the Court records indicating that he has failed to appear as required. *See* Paperless Order Transferring to Fugitive Status as to George Wolvaardt, ECF No. 21, Kane, No. 1-23-cr-20172.

20 *See* Information, *USA. v. Ostern.*, No. 1:23-cr-20165 (S.D.F.L. April 19, 2023), ECF No. 1; *see* also Information, *USA. v. Chorlian.*, No. 1:23-cr-20171 (S.D.F.L. April 20, 2023), ECF No. 1;

21 *See* Complaint, ECF No. 3 at 23, *Hydrogen*, No. 22-cv-08284. Complaint at para 94. It should be noted that Kane made these sales in contravention of a May 2018 public assurance that Hydrogen would not sell Hydro unless it first gave 30 days public notice. *Id.* at 22

The SEC alleged that in response to Hydrogen's difficulties in raising sufficient funds, Kane retained Moonwalkers, a purported "market making" service. The Moonwalkers website was explicit about the services it offered:

> Using our in-house software, we are able to transact thousands of trades a second. This allows us to create volume in such a way that has been unheard of in the space. **(Don't worry, we've gone to great lengths to ensure that our strategies in doing so, look as organic as possible. They are ind[is]cern[i]ble from organic trades.)**[22]

"Ostern and Moonwalkers created a customized trading bot for Kane and Hydrogen to create the appearance of active trading in Hydro and to allow Ostern to sell the company's Hydro on trading platforms without depressing the token's price."[23] Moonwalkers then engaged in spoofing, "deploying a mix of automatic and semi-automatic functions to place-and-cancel buy and sell orders at random increments to create the false appearance of robust market activity." Moonwalkers also engaged in wash trading, by buying and selling Hydro across accounts at centralized crypto asset exchanges, all under Hydrogen and Moonwalkers' control, "in order to induce crypto asset traders to purchase Hydro and enable Ostern to sell the company's Hydro at a greater profit."[24]

Hydrogen, Kane, and Ostern settled with the SEC, collectively agreeing to pay nearly $3 million in disgorgement, penalties, and prejudgment interest.[25] Ostern, Chorlian, and Kane pled guilty to conspiracy to manipulate security prices and wire fraud.[26]

Hampton was convicted at trial of conspiracy to manipulate security prices and conspiracy to commit wire fraud, but was acquitted of substantive wire fraud.[27] All defendants received prison sentences between two and four years.

The SEC and DOJ securities fraud related charges required a finding that the underlying token, Hydro, was offered and sold as an investment contract and, therefore, a security. However, the DOJ also brought wire fraud and conspiracy to commit wire fraud charges that did not depend on the presence of an underlying security transaction. The wire fraud charges demonstrate that even if the SEC were to no longer regulate crypto assets (*e.g.*, if those assets are determined not to be securities), the DOJ would still have the power to prosecute manipulative trading of those assets.

The SEC and DOJ enforcement actions relating to Hydrogen and Moonwalkers, like the prosecution relating to listings on OpenSea, highlight potential compliance risks for financial institutions serving crypto investors. Even if new rules are adopted that change which assets are treated as securities, commodities, or collectibles, institutions can benefit from building compliance focused on problematic conduct, without regard to how an asset being traded is classified by regulators. **Manipulative crypto trading by customers may pose a variety of risks for the institutions on which it occurs, including the potential for regulatory, AML, and customer-related claims.** Establishing robust compliance processes for transaction and account monitoring, issue specific employee training, and clear reporting mechanisms, can help institutions better detect and prevent illicit trading of crypto assets.

22 *Id.* at 24, (emphasis added).

23 *Id.* at 26.

24 *Id.* at 25.

25 *See* Judgment as to Defendant Tyler Ostern, ECF No. 7, *Hydrogen*, No. 22-cv-08284; *see also* Final Judgment as to Defendants The Hydrogen Technology Corp and Michael Ross Kane, ECF No. 20, *Hydrogen*, No. 22-cv-08284

26 *See Man Convicted of $300M Securities Price Manipulation and Wire Fraud Cryptocurrency Conspiracy*, DEPARTMENT OF JUSTICE (Feb. 7, 2024), https://www.justice.gov/opa/pr/man-convicted-300m-securities-price-manipulation-and-wire-fraud-cryptocurrency-conspiracy

27 *See* Verdict Form, ECF No. 21, *Kane*, No. 1-23-cr-20172.

CONCLUSION

Fraudulent trading in crypto markets shares characteristics with similar violations in traditional markets, but it also presents some unique issues because of crypto's underlying technology and current market structure. Financial institutions have an opportunity now, while new rules are still being written, to focus on enhancing their controls around fraud and manipulation, with a focus on controls around trading on material non-public information, wash trading, and spoofing.

TAKEAWAYS

- **Customizing Compliance –** While the frequency with which it occurs is unclear, crypto manipulation is often hard to detect. Financial institutions should consider leveraging experts to help establish controls and surveillance processes tailored to the unique issues that crypto markets present.

- **Reliance on Analytics –** As crypto markets have matured, so too have tracing and analytics services. Institutions should consider employing software-based solutions that can help detect fraud by identifying patterns and anomalies that may be imperceptible to human observers.

- **Monitor Regulatory Priorities –** Market participants will be well served to both focus on addressing the types of conduct likely to remain violative, while monitoring changes to crypto enforcement and regulatory approaches in the new administration, including possible consolidation of oversight that until now spanned multiple regulators.

ARTICLE II

THREE-BODY PROBLEM: CHALLENGES AND CONSIDERATIONS FOR A FIRST-OF-ITS-KIND TRIPLE-TOKEN MERGER

JOSEPH A. CASTELLUCCIO
PARTNER
MAYER BROWN

PAUL C. DE BERNIER
PARTNER
MAYER BROWN

ROHITH P. GEORGE
PARTNER
MAYER BROWN

STEPHANIE M. HURST
PARTNER
MAYER BROWN

DON F. IRWIN
ASSOCIATE
MAYER BROWN

The first-of-its-kind, three-way token merger that formed the "Artificial Superintelligence Alliance" ("Alliance") in mid-2024 created a single token and an independent AI research and development foundation.

This article examines the Alliance's initial structure through the lens of traditional corporate joint ventures ("JVs") and explores the challenges of operating a decentralized JV, particularly in governance and implementation.

DECENTRALIZED PROTOCOLS: THE BASICS

Many blockchain developers aim to "decentralize" their products—whether that be the core blockchain network, an application built on top of the blockchain, or a platform that combines several applications into a cohesive ecosystem—by making those products subject to a governance structure independent from the companies that built them.

As an example, in one common structure, a for-profit entity works on the development of a protocol through launch, but a substantial percentage of the tokens representing ownership of, or at least governing rights for, the protocol are assigned to a non-profit foundation charged with managing their distribution to best promote the ongoing development of the protocol and its associated ecosystem.

These foundations usually have more "democratic" governance mechanics in place that require major proposals affecting fundamental aspects of the protocol's ecosystem to be approved by majority vote—whether the voting stakeholders are all holders of that protocol's token or some more narrowly defined subset.

THE ALLIANCE AND ITS MEMBERS

When it was announced, the stated goal of the Alliance was to combine three existing blockchain-based protocols – Fetch.ai, SingularityNET and Ocean Protocol – into "the world's largest open source, independent AI research and development foundation—with a unique focus to create decentralized Artificial Superintelligence."[1] According to the Alliance's "Vision Paper," and the Alliance's announcement,[2] the initial members were Fetch.ai, SingularityNET, and Ocean Protocol.

Each of the three members was created as a decentralized protocol with a focus on artificial intelligence. Fetch.ai provided a built-for-purpose blockchain platform where AI-powered "agents," designed for a variety of commercial applications could be deployed, marketed, and used. SingularityNET hosted an AI platform where users were able to develop, share, and monetize AI algorithms, models, and services.

Ocean Protocol provided a data exchange as well as applications leveraging those data sources to provide AI-powered prediction feeds while preserving privacy.

As part of the merger, each of these platforms required that their own individual tokens (which went by the symbols FET, AGIX and OCEAN, respectively) be exchanged by users in order to purchase services on their platforms. In the Alliance proposal, all three tokens merged into a single new token (ASI) in order to streamline their individual offerings into a single, aggregated ecosystem. The ASI token would be usable or redeemable for services or actions taken on any of the three platforms.

The Alliance also called for the creation of a new foundation, distinct from any of the three existing foundations, to manage the operations of the consolidated ecosystem. When effective, the merger would occur by mandatory conversion of the respective tokens.

While the Alliance may have been a unique action in the blockchain space—combining a token merger with the formation of a new entity around which several existing foundations will collaborate—it resembled a traditional JV among two or more corporate entities in several ways.

- The Alliance exists as its own, distinct entity (i.e., a foundation), while each of the existing protocols remain as independent legal entities after the Alliance was formed.[3]

- The existing leadership, teams, communities, and token treasuries of each protocol also remained unchanged as a result of the merger (aside from any token exchanges necessitated by the issuance of ASI tokens).

- The Alliance created its own website, marketing and initiatives—separate from its constituent members'—and the existing protocols had no fixed obligations to engage in cross-team collaborations.[4]

- The Alliance's foundation was created with a governing council (the "Council," which is analogous to, but not exactly like, a traditional board of directors).

As a result, the Alliance members had proposed what could be considered the largest-ever "decentralized JV". Typical JV vehicles are considered by companies seeking to mitigate or otherwise share the risks of a new venture or investment.

1 Artificial Superintelligence (ASI) Alliance Vision Paper, SingularityNET. The Alliance defines "Artificial Superintelligence" as AI systems "smarter than the smartest human."

2 https://twitter.com/ASI_Alliance/status/1780221024082047381; https://fetch.ai/blog/artificial-superintelligence-alliance-token-merger-approved

3 Artificial Superintelligence (ASI) Alliance Vision Paper at 19.

4 *Id*. at 19-20.

JVs are contractual relationships between existing businesses or individuals (i.e., the members) and are often structured by establishing a new entity, co-owned by the JV members, which governs the JV business while maintaining some distance—from both a liability and commingling of assets perspective—from the members' own businesses.

In the case of the Alliance, establishing a separate foundation allowed its members to align business objectives and goals while preserving each project's own foundation and independent priority-setting flexibility in case the new venture did not succeed. JV structures are also frequently preferred for combinations of more than two distinct entities, as JV members can explicitly contract around how the JV vehicle will operate, including on matters such as voting rights, board composition and the mechanics for resolving deadlocks.

One of the core business objectives of structuring the Alliance as an independent foundation was to streamline AI research and development across its three constituent protocols. In theory, by consolidating resources, unifying governance under the Council, and eliminating redundant infrastructure, the Alliance could create a more efficient pathway for AI innovation compared to the fragmented efforts of its member protocols. The single ASI token also simplifies economic incentive alignment, potentially reducing inefficiencies in token utility across platforms.

However, the layered governance model—requiring approvals not only from the Alliance's Council and ASI token holders but also from each protocol's independent foundation—introduces complexities that could hinder rapid decision-making. While the new structure may facilitate long-term collaboration, the extent to which it actually accelerates AI R&D remains contingent on how effectively these governance mechanisms operate in practice.

These theoretical advantages were likely reasons for why the Alliance was structured in a very different manner than the largest previous business combination of two decentralized protocols: the merger between Rari Capital and Fei Protocol. Upon the formation of the Alliance, while the tokens of the three protocols merged, the existing business assets, treasuries, and corporate entities of each Alliance member remained separate and intact.

At the same time, the FET,[5] AGIX, and OCEAN tokens became defunct, and holders were required to convert them at fixed rates of exchange for the Alliance's new ASI token. However, unlike in a traditional merger, the protocols were otherwise left in nearly identical positions to their status before the merger—except that one (new) token could now be used across all three platforms.

THE COSTS OF DECENTRALIZATION

Unlike with traditional JVs, however, each project's decentralization meant that the Alliance's JV entity is required to navigate some novel additional hurdles. First, in order to promote decentralization for the new entity, the Alliance was required to implement voting mechanisms that allow ASI token holders to participate in important governance decisions.

For example, in the proposed governance structure of the Alliance, adding new projects to the Alliance, expanding the ASI token supply, or making changes to the Constitution of the Alliance Council would each require (1) a 2/3 vote of the Council and (2) a majority vote of the ASI token holders.[6]

5 Technically, following a "hard-fork" of the FET token contracts, the FET tokens will be renamed ASI and there will be an increase in the maximum supply of tokens, which will accommodate the conversion of FET, AGIX and OCEAN tokens in connection with the merger. See Artificial Superintelligence (ASI) Alliance Vision Paper at 28.

6 Artificial Superintelligence (ASI) Alliance Vision Paper at 20.

(This governance structure has already been tested in practice—in October 2024, the Alliance merged with a fourth protocol, CUDOS, a Decentralized Physical Infrastructure Network (DePIN) for AI compute.[7]) In addition, other significant actions could be brought to a similar vote, at the discretion of the Alliance Council.

However, approval by the Alliance would be merely a prerequisite for this type of decision. Even if the Alliance were to agree on a proposal with both Council and token holder votes, as initially proposed, each of the three protocol foundations would also need to ratify the decision before any binding obligations could be made.

In addition and conceptually, each member protocol had explored different methods of decentralizing itself, and accordingly each foundation is subject to different governing criteria. Highlighting this fragmentation, approval of the Alliance itself was subject to greatly differing mechanics from each of its members. While Ocean Protocol was able to "approve" the transaction to join the Alliance without holding any token holder vote, Fetch.ai's token holders required three separate votes (one to merge the token, and then one each to partner with Ocean and SingularityNET), and SingularityNET's token holders required a supermajority vote.

KEY TAKEAWAYS

The process to form the Alliance underscores the complexities of decentralization in business combinations. While introducing a JV foundation to this type of business transaction may enhance decentralization, it may also hinder timely decision-making. ASI token holders can participate in certain votes, but many decisions remain with the Council and the protocol foundations.

Unlike a typical corporate board of directors, the decision-making constituencies in the Alliance do not have fiduciary obligations to token holders.

Despite these challenges, the Alliance represents an attempt to unify multiple decentralized protocols into a single ecosystem. However, several governance and operational questions remain:

- Approach to Decentralized, Multilayered Decision-Making: The Alliance foundation is governed by a council of its members' founders and require approval from each constituent foundation before major business collaborations. Success depends on alignment between the Council—whose members lack fiduciary obligations to ASI token holders and retain roles in their own foundations—as well as agreement from foundation voters and, for major decisions, ASI token holders. Subcommittees may be created to manage specific areas, and the Alliance's constitution may be amended if governance proves too complex. However, key mechanics remained unclear at the outset, such as how foundations identify stakeholders or verify subcommittee participation after governance tokens are removed. It still remains to be seen whether this experiment—a decentralized foundation comprised of decentralized foundations—can effectively compete in creating a competitor to the traditional technology companies driving the advancement of AI.

- Considerations for Token Holders and Investors: While the token merger required approval by each foundation, some token holders may have seen their assets significantly altered (FET) or valueless until converted (AGIX and OCEAN).[8] DAOs are often controlled by a small group with access to a governing wallet (multi-sig), and while they may act in the DAO's interest, they have no fiduciary duties to token holders.

7 "The proposal received overwhelming support from FET (ASI) token holders, with 99.99% approval on the Fetch.ai Mainnet and 96.67% approval across the Ethereum, Cardano, and Binance Smart Chain networks"; https://singularitynet.io/singularitynet-operations-q3-2024-update/.

8 For US-based token holders, this conversion would also likely carry tax obligations that a holder would not have incurred if the merger were to have never occurred. *See* IRS Pub. 54.

Even when legal wrappers such as foundations are added to DAOs, token holders are unlikely to gain the traditional rights and protections that members of a corporate JV would typically be entitled to (e.g., legal duties of directors and access to information and records). Investors should carefully review a protocol's governing documents to understand their rights and any limitations on token holder influence both before and after any token merger—though these documents may not fully outline all possible voting scenarios.

- Organizational Flexibility as a Strength and Weakness: As contractual arrangements, JVs allow for more independence and flexibility than traditional mergers. In the Alliance's quasi-JV structure, each member retains its legal existence, assets, and employees with minimal binding obligations to participate. While this flexibility gives foundations latitude in their operations, it also raises doubts about whether they will meaningfully collaborate on future products. Stakeholders can ensure token integration, but there is no guarantee of sustained cooperation. A full merger would have ensured alignment under a single governing body but would have eliminated the independence of each foundation. The key takeaway for protocol founders or members considering a similar transaction is that both mergers and JVs offer advantages and challenges, requiring careful evaluation based on strategic goals.

ARTICLE III

SECURITIES LAW SANS SEC? THE DUAL RISKS POSED BY SECTION 12(A) OF THE SECURITIES ACT OF 1933

GAGE RAJU-SALICKI
ASSOCIATE
NORTON ROSE FULBRIGHT US LLP

INTRODUCTION

American securities law is no stranger to cryptocurrency—but with the Securities and Exchange Commission now seeking to work with protocols,[1] a new potential dilemma is rearing its head: Section 12(a). Section 12(a) of the Securities Act of 1933 is one of the Act's only private remedies, and has been used in a number of recent cryptocurrency-related cases. Now, with more retail investors being onboarded and the rapid pace of the current memecoin cycle, there is greater risk of Section 12(a)'s application to protocols and promoters.

Section 12(a) cases are a double-whammy: they enable judges in private actions to determine whether a cryptocurrency is a security, and whether a given defendant is civilly liable for either (1) passing title to, or (2) soliciting sales of a cryptocurrency.

To that end, over past few weeks, a number of Section 12(a) cases have been initiated focusing on specific cryptocurrencies. **Each civil lawsuit represents a new possibility for a finding that a token is a security, as well as whether protocols or promoters—or both—are civilly liable.**

Accordingly, this area of the law is fraught with risk of which developers, protocols, and promoters alike should all be aware.

WHAT IS SECTION 12(A)?

Section 12(a) of the Securities Act of 1933 provides:

> Any person who (1) offers or sells a security in violation of section 77e of this title, or (2) offers or sells a security . . . which includes an untrue statement of material fact or omits to state a material fact necessary in order to make the statements . . . [shall be liable] to the person purchasing such security from him[.][2]

In effect, the statute creates potential liability for anyone who offers or sells either (1) a security that is not registered with the SEC, or (2) a security through a prospectus or oral communication with an untrue statement of material fact.

The Supreme Court in 1988's *Pinter v. Dahl*[3] took a two-pronged approach to Section 12(a). The case dealt with Pinter's sale of unregistered fractional interests in oil and gas leases to an individual and his friends, family, and business associates.

1 *SEC Crypto 2.0: Acting Chairman Uyeda Announces Formation of New Crypto Task Force, Sec. & Exch. Comm'n (Jan. 21, 2025),* https://www.sec.gov/newsroom/press-releases/2025-30

2 15 U.S.C. 77l(a).

3 486 U.S. 622, 625 (1988).

Dahl, after investing, told his friends and family members to invest in the venture, and upon the collapse of the enterprise, Dahl and his associates sued Pinter under Section 12(a).[4] The Court did not make a clear determination of liability, but did hold that Section 12(a) liability can stem from either: (1) passing legal title to the security, or (2) solicitating sales of the security.[5] Notably, the court did not expand on what it meant by solicitation. *Pinter*'s solicitation question is not the only issue posed by Section 12(a) cases, however.

A threshold question for many cryptocurrency cases brought under Section 12(a) is whether the underlying asset is a security. In order to proceed with a challenge under Section 12(a), then, judges will generally have to answer this threshold question—and many have found that the tokens involved plausibly resemble securities.[6] To that end, each Section 12(a) case is like its own miniature enforcement action, without the SEC.

RECENT SECTION 12(A) DECISIONS

Over the past few years, Section 12(a) jurisprudence has become much more pronounced with regard to cryptocurrencies. Likely owing to the lack of regulatory clarity, numerous plaintiffs have brought suits alleging that the plaintiffs were passed title to—or, more importantly, solicited to purchase—unregistered securities. Four key cases best represent this new trend: *Harper v. O'Neal*, *Hardin v. TRON Foundation*, *Samuels v. Lido DAO*, and *Combs v. SafeMoon LLC*.

These cases probe both risks under Section 12(a): the risk of securities classification, and the risk of civil liability.

A. Securities Classification

As the threshold issue for civil liability, the token itself must first be found to be a security in the form of an investment contract under Section 2(a)(1) of the Securities Act. To do so, courts have looked to the test many in crypto already know by heart: *Howey*.[7] The *Howey* test requires "a contract, transaction or scheme whereby a person invests his money in a common enterprise and is led to expect profits solely from the efforts of the promoter or third party."[8]

In *Harper v. O'Neal*, the Southern District of Florida examined this very issue on a motion to dismiss, and ultimately held that the plaintiffs in the case sufficiently alleged that the tokens at issue—Astrals NFTs and Galaxy tokens—were securities under the *Howey* test.[9] This case saw a group of plaintiffs sue the Astrals NFT project and Shaquille O'Neal under Section 12(a). As part of its analysis, the court reasoned that there was an expectation of profits for purchasers in part due to social media posts and the Astrals whitepaper itself.[10]

B. Civil Liability

The larger issue under Section 12(a) is whether protocols and promoters can be held civilly liable for either passing title to or soliciting sales of the cryptocurrency subject to the litigation. The four cases mentioned above saw vigorous debate over Section 12(a)'s limits, and ultimately have begun carving out some of the facets of civil liability under the provision. Most deal with social media and interaction, blurring the lines between promotion and communication.

In *Combs v. SafeMoon LLC*, the District of Utah denied a motion to dismiss, holding that the plaintiffs had sufficiently alleged that some of the creators and promoters of the SafeMoon cryptocurrency could be held liable under Section 12(a) for solicitation.[11]

4 *Id.* at 625–26

5 *Id.* at 643.

6 *See,* e.g., Harper v. O'Neal, No. 23-21912-CIV-MORENO, 2024 WL 3845444, at *10 (S.D. Fla. Aug. 16, 2024).

7 Sec. & Exch. Comm'n v. W.J. Howey Co., 328 U.S. 293, 298–99 (1946).

8 *Id.*

9 Harper, 2024 WL 3845444, at *10.

10 *Id.*

11 Combs v. SafeMoon LLC, No. 2:22-CV-00642-DBB-JCB, 2024 WL 1347409, at *19–21 (D. Utah Mar. 29, 2024).

In denying the defendants' motion to dismiss, the court noted that "re-post[ing] various promotions from other defendants" on social media was "sufficient to state a [solicitation] claim" under Section 12(a).[12] Likewise, in *Samuels v. Lido DAO*, the Northern District of California denied a motion to dismiss on similar grounds, holding, in part, that allegations that the DAO at issue "promoted the listings [of the LDO token] and increases in LDO's price through posts on social media; and that Lido encouraged people to participate in Lido governance, which requires them to purchase LDO." [13]

To that end, the court reasoned that these posts did not need to be seen for liability to attach.[14] Finally, the Southern District of New York in *Hardin v. Tron Foundation* reached this conclusion as well, denying the defendants' motion to dismiss with regard to TRON's status as a statutory seller.[15] The court then explained that TRON had "engaged in steps necessary to the distribution of [the TRX token]" and therefore had solicited sales by "post[ing] promotions and other efforts to solicit purchases of TRX."[16]

CONSIDERATIONS FOR PROTOCOLS AND PROMOTERS

At the heart of each of these cases is the way tokens are advertised and discussed. Whitepapers and social media posts have all served as hooks for liability—as well as hooks for securities status. Of course, the facts in each case deal with protocols creating their own tokens, which most of these cases distinguished from *Risley v. Universal Navigation Inc.*

In that case, the DeFi protocol Uniswap was sued over alleged losses from a token available on the Uniswap platform, and the Southern District of New York ultimately held that no liability was plausibly alleged—that such conduct is "too attenuated to state a claim."[17]

With that said, the law emerging from these Section 12(a) solicitation cases sees social media as a hook for promoters and protocols alike. Moreover, most tokens are directly launched, and advertising is pursuant to that token itself, as opposed to the facts in *Risley*. **To that end, it is crucial for protocols and promoters alike to consider what they are stating in social media posts. For developers of a given protocol, for example, posts about returns or yields may be inadvisable. However, courts appear less concerned with posts about security—perhaps allowing developers to speak openly about the development of their platform divorced from discussions of financial gain.**

To that end, consider how your advertising frames tokens: there is greater risk given volatility in the industry, and courts are now considering social media posts—even retweets!—as a hook for liability.

CONCLUSION

In sum, Section 12(a) litigation is on the rise: we're tracking a number of memecoin-related lawsuits at the moment which alleged Section 12(a) violations. Moreover, while this article does not rule out future SEC enforcement actions regarding crypto, they do appear to be less likely to be initiated when compared to the Gensler administration—thus centering the focus on civil lawsuits. **We would caution protocols and anyone associated with their promotion to moderate statements made online, and to instead focus on their technology rather than returns to avoid liability.**

12 *Id.* at *21.

13 Samuels v. Lido DAO, No. 23-CV-06492-VC, 2024 WL 4815022, at *11 (N.D. Cal. Nov. 18, 2024).

14 *Id.* at *13.

15 Hardin v. TRON Found., No. 20-CV-2804 (VSB), 2024 WL 4555629, at *13 (S.D.N.Y. Oct. 23, 2024)

16 *Id.*

17 *Risley v. Universal Navigation, Inc.*, 690 F. Supp. 3d 195, 222 (S.D.N.Y. 2023).

ARTICLE IV

HONG KONG'S PROPOSAL TO IMPLEMENT THE BASEL CRYPTOASSET CAPITAL RULES

ANDREW FEI
PARTNER
KING & WOOD MALLESONS

This article looks at the Hong Kong Monetary Authority's proposal to implement the Basel Committee's capital standards for banks' cryptoasset exposures.

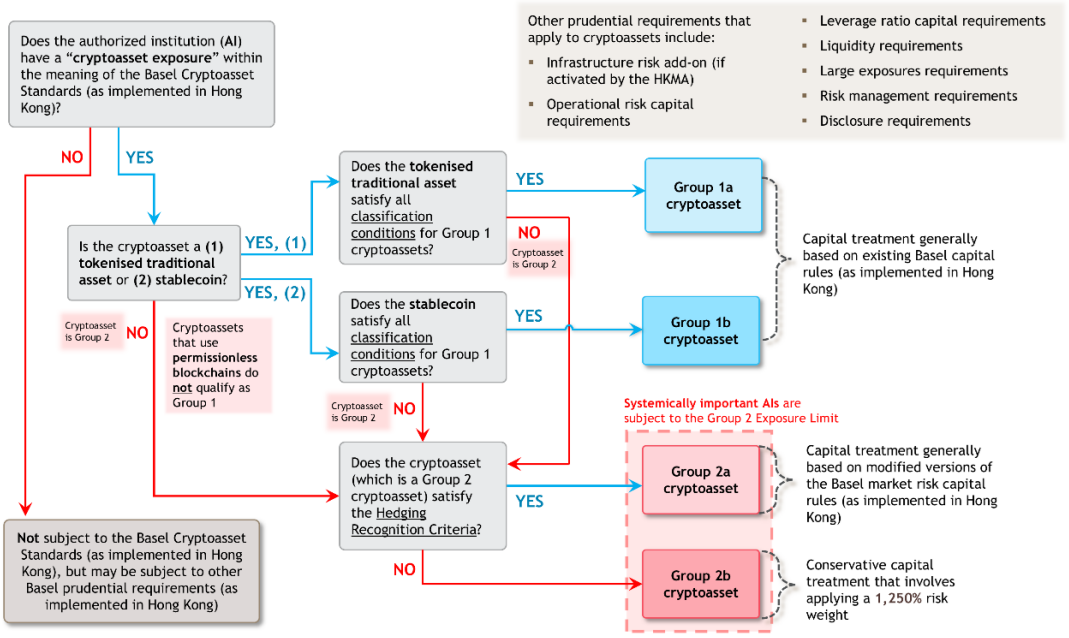
The Hong Kong Monetary Authority (HKMA) has published proposed amendments to its bank capital rules to implement the Basel Committee's standards for the regulatory capital treatment of banks' cryptoasset exposures (Basel Cryptoasset Standards) in Hong Kong.

The Basel Cryptoasset Standards and the HKMA's proposal are important because they prescribe how much regulatory capital banks must hold for their cryptoasset exposures.

Under these capital rules, cryptoassets (including tokenised assets and stablecoins) that use permissionless blockchains, unbacked cryptoassets (such as Bitcoin) and stablecoins with ineffective stabilisation mechanisms will be subject to a high capital charge, making it very expensive for banks to invest in such assets.

The rest of this article and the following diagram provide a high-level overview of the HKMA's proposal and the Basel Cryptoasset Standards that it seeks to implement. The HKMA's bank capital rules apply to Hong Kong incorporated banks and other authorized institutions regulated by the HKMA.

HKMA's proposal to implement the **Basel Cryptoasset Standards** in Hong Kong



WHAT IS THE BACKGROUND TO THE HKMA'S PROPOSAL?

By way of background, the Basel Committee is a committee consisting of senior representatives from banking regulators and central banks in major jurisdictions, which sets regulatory capital and other prudential standards for banks. While the prudential standards published by the Basel Committee do not have the force of law, they are generally transposed into local laws and regulations by Basel Committee member jurisdictions, subject to certain variations.

The Basel Cryptoasset Standards were first published in December 2022 following two rounds of public consultations. The standards are aimed at providing a minimum global framework for banks' cryptoasset exposures which promotes responsible innovation while maintaining financial stability. In July 2024, the Basel Committee made technical amendments to the Basel Cryptoasset Standards to, among other things, tighten the criteria for stablecoins to qualify as Group 1b cryptoassets, which enjoy favourable regulatory capital treatment under the standards.

In February 2024, the HKMA published a consultation paper describing how it intends to implement the Basel Cryptoasset Standards in Hong Kong. A year later, in January 2025, as a further step towards implementation, the HKMA published proposed technical amendments to its bank capital rules to incorporate the Basel Cryptoasset Standards. Subject to certain exceptions, the regulatory capital rules set out in in the HKMA's proposal are broadly consistent with the Basel Cryptoasset Standards.

WHAT ARE THE KEY CONCEPTS USED IN THE PROPOSAL?

Under the Basel Cryptoasset Standards, the term "cryptoassets" broadly refers to private "digital assets" that depend primarily on cryptography and distributed ledger technology (DLT) or similar technologies. The term "digital asset" in turn means a digital representation of value which can be used for payment or investment purposes or to access a good or service. The HKMA's proposal basically adopts the same definition of "cryptoassets", except that the HKMA has proposed to remove the word "private" from such definition, signalling that both private and public sector issued cryptoassets (such as tokenised government bonds) would fall within scope of the Basel Cryptoasset Standards as implemented in Hong Kong.

However, the HKMA's proposal does not, for the time being, prescribe a specific capital charge for central bank digital currencies (such as the e-HKD being explored by the HKMA and the e-CNY being tested by the People's Bank of China). This aspect of the HKMA's proposal is consistent with the Basel Committee's position, which is to defer considering the capital and prudential treatment of central bank digital currencies until they are more widely issued.

The Basel Cryptoasset Standards and the HKMA's proposal set out highly technical rules for determining the regulatory capital treatment of a bank's "exposures" to cryptoassets. The term "exposure" broadly includes both on- and off-balance sheet items that expose a bank to credit, market, operational and/or liquidity risks relating to cryptoassets. For example, a cryptoasset exposure includes derivatives that reference cryptoassets (such as Bitcoin futures) as well as interests in investment funds that hold cryptoassets (such as Bitcoin exchange-traded funds).

HOW DOES THE PROPOSAL CLASSIFY DIFFERENT TYPES OF CRYPTOASSETS?

Under the Basel Cryptoasset Standards and the HKMA consultation paper, the regulatory capital and prudential treatment of a bank's cryptoasset exposures varies depending on whether the cryptoasset falls into one of the following categories:

Group 1 cryptoassets, which consist of:

- **Group 1a cryptoassets**, being tokenised traditional assets that meet a stringent set of classification conditions set out in the Basel Cryptoasset Standards and the HKMA's proposal. In this context, the term "traditional assets" refers to non-cryptoassets that are already captured under the existing Basel prudential framework, such as bonds, shares, loans and commodities.

- **Group 1b cryptoassets**, being stablecoins with effective stabilisation mechanisms that meet the stringent classification conditions set out in the Basel Cryptoasset Standards and the HKMA's proposal, which essentially require stablecoins to be sufficiently backed by high-quality and liquid reserve assets so as to allow the issuer to meet redemption requests at all times, including during periods of extreme stress.

Group 2 cryptoassets, which consist of:

- **Group 2a cryptoassets**, being cryptoassets (including tokenised traditional assets, stablecoins and unbacked cryptoassets such as Bitcoin) that do not meet the classification conditions for Group 1 cryptoassets, but that do satisfy the Group 2a hedging recognition criteria set out in the Basel Cryptoasset Standards and the HKMA's proposal, which include various thresholds relating to market capitalisation, trading volume and price observations for the relevant cryptoassets. Group 2a is essentially reserved for popular cryptoassets such as Bitcoin that have significant market capitalisation and high trading volume.

- **Group 2b cryptoassets**, being cryptoassets (including tokenised traditional assets, stablecoins and unbacked cryptoassets such as Bitcoin) that do not meet the classification conditions for Group 1 cryptoassets and also do not satisfy the Group 2a hedging recognition criteria.

WHAT IS THE REGULATORY CAPITAL TREATMENT OF CRYPTOASSETS?

At a high-level, under the Basel Cryptoasset Standards and the HKMA's proposal, the regulatory capital treatment of Group 1 cryptoassets (i.e., qualifying tokenised traditional assets and qualifying stablecoins with effective stabilisation mechanisms) is generally based on the treatment of the relevant reference asset under the existing Basel capital rules (as implemented in Hong Kong).

The regulatory capital treatment for Group 2a cryptoassets is based on modified versions of the Basel market risk capital rules (as implemented in Hong Kong) taking into account netting and subject to a 100% capital charge. In contrast, Group 2b cryptoassets are subject to a conservative capital treatment that involves applying a 1,250% risk weight. A risk weight of 1,250% is actually the reciprocal of the 8% minimum total capital ratio that banks must maintain under the Basel capital rules (as implemented in Hong Kong) and, for this reason, it is often described as a "dollar-for-dollar" capital charge. In reality, however, many banks maintain regulatory capital ratios that are well in excess of the minimum requirements.

Group 2 cryptoasset exposure limits: Besides imposing regulatory capital requirements, the Basel Cryptoasset Standards also limit the amount of a bank's exposure to Group 2 cryptoassets. According to the HKMA's proposal, these exposure limits will only apply to systemically important banks (SIBs), including global systemically important banks and domestic systemically important banks.

Specifically, a SIB's total exposure to Group 2 cryptoassets must not exceed 2% of the bank's Tier 1 capital and should generally be lower than 1%. SIBs breaching the 1% limit will apply the more conservative Group 2b capital treatment to the amount by which the limit is exceeded. In contrast, breaching the 2% limit will result in all Group 2 exposures (including exposures under the limit) being subject to the very conservative Group 2b capital treatment (i.e., 1,250% risk weight).

Disclosure requirements: In addition to proposing amendments to its bank capital rules to implement the Basel Cryptoasset Standards, the HKMA is also proposing amendments to its bank disclosure rules to implement the Basel Committee's Pillar 3 disclosure requirements for banks' cryptoasset exposures. **Under the proposed amendments, banks will be required to publish detailed qualitative information regarding their cryptoasset activities and related risk management practices as well as quantitative information regarding their cryptoasset risk exposures.**

WHAT IS THE CAPITAL TREATMENT OF CRYPTOASSETS HELD ON CUSTODY FOR CLIENTS?

The capital requirements described above generally apply to a bank's cryptoasset exposures that give rise to a risk of loss to the bank arising from (1) credit risk (being the risk of loss resulting from the failure of borrowers or counterparties to meet their debt or contractual obligations) or (2) market risk (being the risk of loss due to adverse changes in the market value). **Both the Basel Committee and the HKMA have clarified that custodial services involving the safekeeping or administration of client cryptoassets on a segregated basis do not generally give rise to Basel credit or market risk capital requirements.**

In addition, the operational risks associated with providing cryptoasset custody activities to clients should already be captured by the existing Basel operational risk capital requirements. **To the extent that operational risks relating to cryptoassets are not adequately captured by the minimum capital requirements for operational risk and by a bank's internal risk management process, the bank and its prudential regulator should take appropriate steps to ensure capital adequacy as part of the supervisory review process.**

WHAT IS THE CAPITAL TREATMENT OF CRYPTOASSETS THAT USE PERMISSIONLESS BLOCKCHAINS?

Under the Basel Cryptoasset Standards and, consequently, the HKMA's proposal, cryptoassets (including tokenised traditional assets and stablecoins) that use permissionless blockchains are not eligible for inclusion in Group 1. Furthermore, since these cryptoassets typically would not have the market capitalisation, daily trading volume and other attributes necessary to satisfy the hedging recognition criteria to be classified as Group 2a cryptoassets, they would likely fall under Group 2b and receive a punitive 1,250% risk-weight. This makes it very expensive for banks and their subsidiaries to invest in permissionless blockchain-based cryptoassets.

According to the Basel Committee, the use of permissionless blockchains gives rise to a number of unique risks, some of which cannot be sufficiently mitigated at present. For example, banks that use permissionless blockchains have limited ability to conduct due diligence and oversight over third party validators or prevent potential disruptions to the network.

A number of market participants are actively seeking to convince global regulators that there are various technological and other solutions which can mitigate some of the perceived risks associated with permissionless blockchains. Regulators in a number of key Basel Committee member jurisdictions have recently also warmed up to permissionless blockchains. For example, in November 2024, the European Union published a report examining the potential of public permissionless blockchains to enhance traditional financial services. The report highlights the key advantages of utilising an open base blockchain, including transparency, inclusivity and increased competition.

On January 23 2025, just a few days into the new administration, President Trump issued an executive order on digital assets. Among other things, the executive order expresses the US government's support for "open public blockchain networks".

Looking to the future, it will be very interesting to see whether, as technologies and policy positions around cryptoassets continue to evolve, global regulators will come to embrace permissionless blockchains to a greater extent.

WHAT ARE THE NEXT STEPS?

The HKMA is seeking feedback from the industry regarding its proposal. At present, the HKMA proposes for Hong Kong authorized institutions to become subject to the Basel Cryptoasset Standards from January 1 2026, in line with the Basel Committee's implementation timeline. **Outside Hong Kong, it remains to be seen how other Basel Committee jurisdictions will implement the Basel Cryptoasset Standards by January 2026, since Hong Kong remains one of only three Basel Committee member jurisdictions to have proposed or finalised their implementing rules.**

With January 2026 being less than 11 months away, there is much for Hong Kong authorised institutions to do to get ready. Among other things, they must put in place policies, procedures and systems to fully document the information used to classify their cryptoasset exposures into one of four categories prescribed in the Basel Cryptoasset Standards. Supporting documents include external legal opinions and other legal analysis. Classification assessments must be made available to the HKMA upon request.

The HKMA can override a bank's classification decisions with which it does not agree.

In relation to a type of cryptoasset to which an authorized institution has never held an exposure before, the authorised institution must classify the cryptoasset as a Group 2b cryptoasset (attracting a conservative 1,250% risk-weight) until the HKMA is satisfied that the cryptoasset meets the classification criteria for Group 1a, 1b or 2a cryptoassets. This "presumption of Group 2b treatment" makes it critical for authorised institutions to submit their duly completed classification assessment and supporting documents to the HKMA in an orderly and timely basis.

ARTICLE V

EVOLVING CRYPTO REGULATIONS: THE FUTURE OF FIT21 AND LEARNINGS FROM MICA

RHEA SAINI
VICE PRESIDENT & LEGAL COUNSEL
GSR

Cryptocurrency is a disrupter; an innovative technology on how we fundamentally use money. Deal making in the crypto currency industry is a rapidly evolving global business.[1] The inherent cross border nature of the crypto business makes it imperative that governments adopt a regulatory framework which promotes the continued growth of the crypto industry.

Over time, we have seen where there comes a new technology and governmental authorities grapple with the concept by introducing new laws couched in traditional frameworks to regulate these emerging industries, hence stifling the innovative spirit behind them. On a fundamental level, the aim of these laws and regulations is to protect consumers and allow consumers to enjoy the benefits of the industry, but it is critical not to overregulate the industry as to stifle innovation and growth.

The United States House passed the Financial Innovation and Technology for the 21st Century Act, otherwise known as "FIT21" on May 22, 2024.[2]

This was considered a marked achievement for the crypto industry given the uphill climb market participants experienced under the former administration.[3] While the recently inaugurated Trump administration is forging a new regulatory path for the crypto industry, a version of the FIT21 bill is anticipated to progress to the Senate floor in the coming months.[4]

The European Union "EU" enacted Markets in Crypto-Assets, "MiCA" in May 2023[5] and is much further along in implementing a pro-business digital assets regulatory framework. **While FIT21 and MiCA are similar in their regulatory approach, there are significant differences in the framework.** The regulatory path for the US, notably in its infancy, is expected to change drastically with the Trump administration.[6] As the US forges a new way forward, there are several important learnings that the US can adopt from MiCA.

1 Lau, Y. (2021, November 10). Cryptocurrency market cap hits $3 trillion for first time ever. Fortune. https://fortune.com/2021/11/09/cryptocurrency-market-cap-3-trillion-bitcoin-ether-shiba-inu/ and Tecimer, Will. (2024, September 28) How Cryptocurrency is changing global finance around the world in uncertain times. Junior Economist. https://junioreconomist.org/how-cryptocurrency-is-changing-global-finance-around-the-world-in-uncertain-times-e7c6d7166af8

2 H.R. 4763, Financial Innovation and Technology for the 21st Century Act (May 22, 2024), ("FIT21").

3 Former President Joe Biden's regulators sought to protect Americans from fraud and money laundering with a crackdown on the industry. Please see Gillison, Douglas, "US Congress to form cryptocurrency working group." Reuters, Feb 4, 2025. https://www.reuters.com/world/us/us-congress-form-cryptocurrency-working-group-2025-02-04/.

4 "Representative French Hill", "Senator Bill Hagerty" and "David Sachs", White House Crypto Czar, 'Press Conference on Capitol Hill', February 4th 2025, www.digitalchamber.org/capitol-hill-press-conference-on-crypto-regulation.

5 Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto assets ("MiCA")

6 *Supra* note 4.

FIT21 AND THE FUTURE REGULATORY PATH IN THE US

The passage of the FIT21 bill through the House was a watershed moment for the crypto industry amidst the heavy "regulation by enforcement environment".[7] **The bill allocates regulatory authority to both the CFTC[8] and SEC[9] and separates digital assets into three categories: digital commodities, restricted digital assets or securities and permitted payment stable coins but only promulgates substantive guidance and regulation for the first two.[10]**

Under FIT21, the CFTC oversees digital commodities and the market participants who trade them. The bill essentially empowers the CFTC to conduct oversight over digital assets as a commodity if the blockchain it runs on is functional and decentralized,[11] whereas the SEC is designated regulatory authority over restricted assets and would regulate digital assets as a security or restricted digital asset as if the blockchain is functional or non-functional but not decentralized.[12] The new SEC designation for digital assets supplants the traditional thinking of the SEC where most digital tokens are considered securities under the Howey test[13] and thus must be registered under the Securities Act of 1933[14] or offered pursuant to a specific exemption.[15]

The bi-furcated approach of regulatory authority has led many in the industry to criticize the FIT21 Bill.[16] Cryptocurrency is a decentralized market, and challenges persist when there is ambiguity connected to cryptocurrency because regulators begin to conform the definition into one that fits the purview of the agency as noted above where the SEC and CFTC have markedly different definitions.

At a fundamental level, the disparity in the definition of what cryptocurrency is can be damaging because it may create severe policy gaps potentially resulting in conflicts amongst the agencies. **Also, by distinguishing between "restricted digital assets" and "digital commodities" in parallel trading markets, the bill sets the stage for a fragmented regulatory landscape and presents compliance difficulties for US market participants.** These complications can reduce competition with international markets which ultimately forces investment overseas due to the more favorable, less onerous, better understood regulation abroad.

The United States anticipates a sea change in its regulatory approach to crypto. In hopes of forming a novel approach curated to regulate the crypto industry, the Trump administration hasn't wasted any time turning over key decision makers of regulatory bodies and appointing a crypto czar at the helm. This has led to industry optimism that the new regulatory approach will promote the continued growth of the industry.[17] It is highly unlikely that FIT21 will proceed forward intact in its original state to the Senate without significant revisions.[18]

7 Gary Gensler, Statement on the Financial Innovation and Technology for the 21st Century Act, U.S. Sec. And Exch. Comm'n (May 22, 2024), certain commenters, including Commissioner Hester Pierce, note that there is a lack of "a coherent legal framework." SEC Commissioner Hester Peirce has further called for a move beyond this regime of "regulation by enforcement" and urged the SEC to work collaboratively with Congress to provide clear guidance for crypto-market participants. See Outdated: Remarks before the Digital Assets at Duke Conference, Comm'r Hester M. Pierce, U.S. SEC. And Exch. Comm'n. (Jan. 20, 2023).

8 Cong. Rsch. Serv., *An Overview of H.R. 4763, Financial Innovation and Technology for the 21st Century Act*, (May 17, 2024)

9 *Id.* at 2.

10 *Id.* at 2.

11 *FIT21* at *§101(29).*

12 *Id.* at §101(34)(A)(i)–(iii).

13 SEC v.W.J. Howey Co has been the SEC's main source of regulatory authority. Under Howey, the U.S. Supreme Court held that an investment contract is a "security" if it involves "an investment of money in a common enterprise with profits to come solely from the efforts of others."

14 Securities Act of 1933, 15 U.S.C. §§ 77a-77aa".

15 *Id.*

16 Riezman J, The Unintended Consequences of FIT21's Crypto Market Structure Bill, 24 May 2024, available at https://www. coindesk. com/opinion/2024/05/24/the-unintended-consequences- of-fit21s-crypto-market-structure-bill/

17 *Supra* note 4.

18 *Supra* note 4.

As the US moves forward with its crypto regulatory approach, the US should not develop a regulatory framework in a vacuum and should consider existing international regulatory frameworks such as MiCA as a reference.

LEARNINGS FROM MICA

MiCA's regulatory framework is far more expansive than FIT21, encompassing all crypto assets, including securities and e-money (stable coins) and regulating crypto asset service providers (CASPs)[19] operating within the EU. While critics have asserted that the requirements that MiCA imposes on stable coin issuers is too stringent[20] and have noted the inflexible nature of the framework where member states cannot alter or choose regulatory measures, MiCA eliminates the inconsistencies of national regulations and offers clarity for businesses operating across the EU by regulating the issuance and admission to trading of crypto assets.

The framework sets operational standards for CASPs and protects investors from market manipulation and abuse while also assisting firms with AML compliance.[21]

Underlying MiCA's regulatory approach is the idea that a framework should support innovation and fair competition, while ensuring a high level of protection of retail holders and market integrity and financial stability in crypto-asset markets.[22] This framework is not enforced to regulate the underlying technology.

19 Recital 6, *MiCA*.

20 Kaur, Guneet, "MiCA's impact on stablecoins: Will USDt survive in the EU?" Dec 29, 2024, https://cointelegraph.com/learn/articles/micas-impact-on-stablecoins. Stating that MiCA imposes stringent requirements on stablecoins to ensure they are fully backed by liquid reserves.

21 Recital 4, *MiCA*.

22 Recital 6, *MiCA*.

To maintain competitiveness on a global market, the framework is intended to increase the protection of holders while promoting market integrity and financial stability through the regulation of offers to the public of crypto-assets or services.[23]

Proper regulation maintains the competitiveness of the Member States on international financial and technological markets and provides clients with significant benefits in terms of access to cheaper, faster and safer financial services and asset management. **MiCA aims to address fragmentation[24] and enhance consumer protection while enabling businesses to align with a future where crypto assets are integrated seamlessly into the global financial system.**

CONCLUSION

The notable difference between the US and the EU is that the US approach has historically been fixated on the idea of controlling the industry rather than studying and implementing a framework that cultivates this emerging industry. The EU approach is more holistic and lays the groundwork to create a market that can unilaterally protect its participants and encourage innovation.

The traditional US approach where it allows its various regulatory agencies to step in and form definitions that they see best fit and each agency regulate them however they please, creates a convoluted understanding of the industry. This inevitably leads to overregulation caused by high costs, legal complexity and uncertainty for service providers.

For the US to effectively regulate cryptocurrency, it must make at least two changes. First, law makers need to create common definitions for terminology applying to the industry which provides legal certainty.

23 Recital 24, *MiCA*.

24 Recital 112, *MiCA*.

Followed by creating an overarching regulatory framework, whether it be a new regulatory body or a collaboration between listing agencies, to provide protection for investors without stifling innovation. Many statutes or legal frameworks used by listing agencies are outdated. When all these frameworks were created, the idea of a virtual currency was unheard of in this world. The US, the beacon of freedom and innovation, is using age old statutory language to categorize a new, revolutionary framework.

As the US experiences innovation, its goal should be to creating regulations that can be adapted and tailored to a new world. By creating an overarching regulatory model that all federal agencies and states could follow would ensure greater market stability and growth.

ARTICLE VI

INVESTORS BEWARE: PRIVATE PLAINTIFFS TEST LEGAL BOUNDARIES OF DAO LIABILITY

ROXANE BALLEW
VICE PRESIDENT & LEGAL COUNSEL
GSR

INTRODUCTION

Recent federal court rulings highlight two major risks for institutional investors in unincorporated Decentralized Autonomous Organizations (DAOs). First, they may be treated as general partners, making them personally liable for the DAO's actions. Second, DAOs themselves may be liable under the securities laws for the sale of their governance tokens on secondary markets.

Together, these legal theories expose DAOs and their institutional investors to significant financial liability from private plaintiffs. The Decentralized Unincorporated Nonprofit Association (DUNA) introduced by the Wyoming legislature last year presents a potential, though untested, legal framework to limit this risk. Institutional investors must understand these emerging liabilities to develop effective risk mitigation strategies in the evolving DAO ecosystem.

A CALIFORNIA COURT FINDS THAT INVESTORS COULD BE PERSONALLY LIABLE FOR A DAO'S ILLEGAL SALE OF UNREGISTERED SECURITIES

Two federal judges in the Northern District of California (the Court), Judge Orrick in *Houghton v. Leshner*[1] (Compound DAO) and Judge Chhabria in *Samuels v. Lido DAO*[2] (Lido DAO), have recently allowed lawsuits to proceed alleging that DAO investors could be held personally liable for the DAO's illegal sale of unregistered securities. Unlike the well-known CFTC enforcement action against Ooki DAO,[3] which some may associate with a prior, more crypto-skeptic administration, these cases involve private plaintiffs suing DAOs and their investors directly. Judge Orrick, who ruled against Ooki DAO and is also presiding over the SEC's case against Kraken, now oversees *Compound DAO*.

In both Compound DAO and Lido DAO, the Court addressed two critical questions:

1. Are unincorporated DAOs general partnerships under state law, making investors personally liable for the DAO's actions?

1 *Houghton v. Leshner*, 3:22-cv-07781 (N.D. California).
2 *Samuels v. Lido DAO*, 3:23-cv-06492 (N.D. California).
3 *Commodity Futures Trading Commission v. Ooki DAO*, 3:22-cv-05416-WHO, Order Granting Motion For Default Judgment (N.D. California 2023).

2. Can a DAO be held liable under federal securities law if its governance tokens are sold on secondary markets?

Both judges found these legal arguments plausible enough to survive motions to dismiss, allowing the cases to proceed. These are significant developments that could shape future DAO litigation.

THE UNINCORPORATED DAO AS A GENERAL PARTNERSHIP

In both cases, plaintiffs argued that because the DAOs lacked a formal legal structure, they should be treated as general partnerships under state law. In most states, a general partnership is automatically formed when two or more people share a business's profits and losses, whether they intend to or not. This means each participant can be personally liable for the partnership's actions.

In *Lido DAO*, the Court found that the plaintiff sufficiently alleged that the DAO operated as a general partnership. Specifically, the Court found that institutional investors a16z, Dragonfly, and Paradigm were plausibly general partners of the DAO because they "meaningfully participate[d]" in the DAO's governance.[4] The plaintiff also alleged that Robot Ventures was a general partner, but the Court dismissed them from the case due to a lack of evidence showing meaningful participation.

The Court identified two key factors that demonstrated meaningful participation:

1. Large Investments: a16z bought "an unknown but presumably substantial amount" of LDO tokens for $70 million, Dragonfly similarly bought an undisclosed amount of LDO tokens for $25 million, and Paradigm bought 100 million LDO tokens.[5] The Court acknowledged while other large investors may exist, their identities remain unclear.

2. Public Engagement: a16z publicly announced that it would contribute to the DAO as a "governance participant", Dragonfly commented publicly on a governance proposal that it was "looking forward to being more active in governance", and Paradigm was described by the DAO founders as "uniquely positioned to lend its expertise" to the DAO's governance.

In *Compound DAO*, the general partnership issue remains unaddressed, as the defendants did not challenge this allegation in their motion to dismiss, instead focusing on the allegations of securities laws violations. The plaintiffs made sure to emphasize the defendants' omission in their argument: "Defendants do not deny that they formed a general partnership and do not deny that the COMP token is an unregistered security."[6]

THE DAO AS A STATUTORY SELLER

Plaintiffs in both cases also argued that each DAO qualifies as a "statutory seller" under Section 12(a)(1) of the Securities Act of 1933, which imposes strict liability on anyone who offers or sells an unregistered security, regardless of intent. In 1988, the Supreme Court ruled that a "statutory seller" includes both direct sellers and those who actively solicit buyers.[7] Because the plaintiffs in both cases purchased their tokens on secondary markets rather than directly from the DAO, the Court focused on whether the DAOs had engaged in solicitation.

For a long time, courts found that a "statutory seller" needed to have directly targeted a purchaser to be found liable for solicitation.

4 *Samuels v. Lido DAO*, Order Re Motions To Dismiss (November 18, 2024), p. 12.

5 *Samuels v. Lido DAO*, Order Re Motions To Dismiss (November 18, 2024), p. 4.

6 *Houghton v. Leshner*, Plaintiffs' Response To Defendants' Motion To Dismiss (June 22, 2023), p. 2.

7 *Pinter v. Dahl,* 486 U.S. 622 (1988), p. 622 ("a person who solicits the buyer's purchase in order to serve the financial interests of the owner may properly be liable under [§ 12(a)(1)] without showing that he expects to participate in the benefits the owner enjoys").

However, in recent years, with the rise of social media, some federal courts have expanded this interpretation, suggesting that mass communications such as social media promotions could suffice.[8]

In *Compound DAO* and *Lido DAO*, the Court found that the plaintiff had sufficiently alleged that the DAOs solicited sales of unregistered securities on secondary markets. The key factor was whether the DAOs demonstrated "comprehensive involvement with the design, operation and monetization" of the token.[9]

Plaintiffs pointed to several indicators of solicitation, including public statements, efforts to secure exchange listings, and governance messaging that encouraged token holders to participate in decision-making. For example, Lido's website promotes token holders' ability to participate in the DAO's governance by stating that holding LDO "gives DAO members a vote in the future of Lido, allowing each DAO member to have a personal say in the community" and "in the direction and growth of the Lido DAO." This type of language, plaintiffs argue and the Court agrees, functions as a form of solicitation.

PROPOSED SOLUTION: THE WYOMING DUNA AS A LIABILITY SHIELD

Last year, Wyoming enacted the Decentralized Unincorporated Nonprofit Association Act (Wyoming DUNA Law), offering DAOs a novel legal structure with several key features:

1. Limited Liability: DAO members are not personally liable for contractual breaches or tortious acts of the DAO, a crucial protection given the ongoing cases like *Compound DAO* and *Lido DAO*.

2. Minimum Membership: A DAO must have at least 100 members. If membership falls below this threshold, one of two things will happen:

a. If the DAO qualifies as a Wyoming Unincorporated Nonprofit Association (UNA) under the Wyoming Unincorporated Nonprofit Association Act, it automatically converts into a UNA.

b. If it does not meet UNA criteria, it dissolves.

This membership requirement poses challenges, as DAOs could unpredictably seesaw between UNA and DUNA status.

3. No Profit Sharing: While the DAO can engage in profit-making activities that support its nonprofit mission and pay reasonable compensation for services like voting, DAO may not distribute any part of its income or profits to its members. This is noteworthy as more and more DAOs consider "fee switch" proposals which would divert a portion of the DAO's revenue to token holders. That sort of arrangement would create issues for the DUNA.

The Wyoming DUNA has been in effect for just over six months, and while still in its early stages, some projects are already actively working to implement it. OtoCo DAO, seemingly first incorporated as a BVI foundation in 2021, announced that it "legally engineered an on-chain UNA" that will automatically convert into a DUNA once there are over 100 members. Nouns DAO executed Proposal 662, approving $875,034 to fund the Nouns Foundation's transition to a DUNA and support its first year of operations.

CONCLUSION & KEY TAKEAWAYS

The key takeaway from Compound DAO and Lido DAO is that DAO investors should be cautious about their involvement in DAO governance to avoid being classified as general partners, which could expose them to personal liability, including for sales of unregistered securities on secondary markets. While Wyoming's DUNA framework offers a potential liability shield, its effectiveness remains untested in the courts. In the meantime, investors should prioritize DAOs with established legal structures and avoid publicly engaging in governance, especially when holding significant stakes.

8 *Pino v. Cardone Cap.*, LLC, 21-55564, Opinion (9th Cir. 2022).

9 *Houghton v. Leshner*, Order Denying Motion To Dismiss (September 20, 2023), p. 5, Samuels v. Lido DAO, Order Re Motions To Dismiss (November 18, 2024), p. 19.

ARTICLE VII

STAKING/RESTAKING UNDER JAPANESE LAW*

SO SAITO
REPRESENTATIVE PARTNER
SO & SATO LAW OFFICES

YU MIZUSHIMA
ATTORNEY-AT-LAW
SO & SATO LAW OFFICES

INTRODUCTION

As seen in Ethereum network, staking—the process of locking a certain amount of crypto assets on a blockchain for a set period to contribute to transaction validation (Proof of Stake), earning rewards in return—is gaining traction globally as well as in Japan. Major Japanese crypto asset exchanges now offer staking services, contributing to its expansion. This paper outlines key legal issues related to staking under Japanese law and briefly addresses the concept of restaking, which is a mechanism in which existing staked crypto assets or staking rewards are staked again to earn additional rewards, with the aim of enhancing network security and enabling new services.

LEGAL ISSUES RELATED TO STAKING UNDER JAPANESE LAW

Regulatory applicability depends on the manner in which staking is conducted and its legal framework. Relevant regulations include those governing Crypto Asset Exchanges and Funds as referenced and further explained below. Staking one's own crypto assets remains unregulated under such regulations, therefore, this discussion focuses on cases where a service provider stakes on behalf of users. To summarize the key conclusions in advance:

Staking Structure and Legal Framework	Applicability of Crypto Asset Exchange Regulations / Fund Regulations as per Japanese Law
Service provider does not receive the user's private key (only delegation)	No applicable regulations
Service provider receives the user's private key	
Legal structure: "Custody"	Crypto Asset Exchange regulations apply (registration as a Crypto Asset Exchange)
Legal structure: "Investment"	Fund regulations apply (registration as a Type II Financial Instruments Business Operator)
Legal structure: "Lending"	No applicable regulations

Custody, Investment, and Lending are key legal classifications in the regulatory framework for staking services. While details will be discussed later, these terms can be briefly defined as follows:

√ Custody refers to the management of crypto assets on behalf of users. Possession of private keys is a key factor in determining regulatory applicability of Custody. If structured as Custody, it falls under Crypto Asset Exchange regulations under the Payment Services Act (PSA).

√ Investment refers to a scheme where users contribute funds (including crypto assets) to a service provider, which then utilizes them for business operations (e.g., staking) and distributes profits to the users.

* Our law firm specializes in Web3 and has published numerous articles on its legal aspects, including Staking and Restaking, in Japanese and English, please see: https://innovationlaw.jp/en/articles/

If structured as Investment, it falls under Fund regulations governed by the Financial Instruments and Exchange Act (FIEA).

√ Lending refers to an arrangement where users lend their crypto assets to a service provider, which manages the crypto assets at its discretion and returns them after a specified period. If recognized as a Lending agreement, it is generally not subject to PSA or FIEA regulations.

A SHORT INTRODUCTION TO CRYPTO ASSET EXCHANGE REGULATIONS AND FINANCIAL REGULATIONS

Under Japanese law, Crypto Asset Exchange regulations under the PSA, Article 2, Paragraph 15, apply to the following activities:

1. Buying, selling, or exchanging crypto assets.
2. Intermediating, brokering, or acting as an agent for these activities.
3. Managing users' funds related to 1 and 2.
4. Managing crypto assets on behalf of others.

Among these, staking is particularly relevant to Item 4., which refers to the Custody services.

Regarding "managing crypto assets on behalf of others" (hereinafter referred to as "Custody"), the Financial Services Agency (FSA) guideline[1] states:

> *"[...] in a case where the business operator is in a state in which the business operator is able to proactively transfer a Crypto-Asset of a user, such as a case where the business operator holds a secret key [Author's Note: referring to a private key] sufficient to enable the business operator to transfer the Crypto-Asset of the user without any involvement of the user, either alone or in cooperation of an affiliated business operator, such a case falls under the management of Crypto-Assets."*

This indicates that possession of private keys is a key factor in determining regulatory applicability of Custody.

Additionally, staking may also be subject to Fund regulations governed by FIEA (Article 2, Paragraph 2, Item 5). This FIEA applies where users contribute funds (including crypto assets) to a service provider, which then utilizes them for business operations and distributes profits to the users.

(a) Case where the service provider does not hold the user's private key

If a service provider only receives delegation from users without holding their private keys,[2] it does not qualify as a Custody activity under the FSA guideline as quoted above and is not subject to Crypto Asset Exchange regulations under the PSA. Additionally, in this case, since users do not contribute funds to the service provider—given that the service provider cannot transfer the crypto assets for business operations without possessing the private key—it does not constitute an "Investment" and therefore, Fund regulations under the FIEA do not apply either.

(b) Case where the service provider holds the user's private key

If a service provider holds the user's private key, it may be classified as a Custody activity under the PSA. Additionally, depending on the legal structure of the arrangement, the user's contribution could be considered an "Investment," making it subject to Fund regulations under the FIEA.

First, if the arrangement is structured as a "Custody," the provider is deemed to be managing the user's crypto assets on their behalf.

1 https://www.fsa.go.jp/common/law/guide/kaisya/e016.pdf

2 Artzt/Richter (ed.) ,International Handbook of Blockchain Law, 2nd edition, 2024, at 21.

This qualifies as a Custody activity under Crypto Asset Exchange regulations and falls under the Payment Services Act (Article 2, Paragraph 15, Item 4).

If the legal structure is such that the provider receives "Investment" of crypto assets from users, it does not meet the Custody regulation requirement of "managing crypto assets on behalf of others," as the assets are received for business use rather than for custodial management on behalf of users. Therefore, Custody regulations under the PSA do not apply. However, since the provider uses the contributed funds to operate a business (staking) and distributes the revenue to users, it is likely subject to Fund regulations under FIEA.

If the arrangement is structured as Lending, where the user lends crypto assets to the service provider, which manages them at its discretion and returns them after a specified period, rather than making a Custody (where assets are held and managed on behalf of the user) or an Investment (where assets are contributed with an expectation of return), no specific regulations apply. However, according to the aforementioned FSA guideline,[3] *"The borrowing of Crypto-Assets [...] falls under the management of Crypto-Assets [...] if a business operator substantially manages a Crypto-Asset on behalf of another person under the name of the borrowing of a Crypto-Asset such that the user can receive the return of the Crypto-Asset borrowed at any time at the request of the user."*

Therefore, regulatory authorities may classify such circumvention schemes as a Custody activity, making them subject to Custody regulations under the PSA.

Thus, even when a service provider holds the user's private key and conducts staking, the applicable regulations vary depending on the legal structure of the arrangement. However, in practical business operations, the distinction between "Custody", "Investment" and "Lending" is not always clear.

To determine the applicable regulations, it is useful to analyze the staking scheme based on the following factors:

1. Whether the rewards are received by the service provider and then distributed to the user, or are they directly distributed to the user.
2. If the service provider receives the rewards first and then distributes them to the user, and whether the distribution is fixed or linked to revenue.
3. Whether the slashing risk, which refers to the risk of staked assets being partially or fully slashed if a validator violates network rules or engages in misconduct, is borne by the service provider or the user.

Based on these factors, the conclusions for typical cases are summarized as follows. However, if a case does not fit within these typical scenarios, determining whether it qualifies as Custody service or a Fund Investment can be challenging.

- If the amount of rewards paid by the service provider to the user is predetermined and the user does not bear the slashing risk: Custody regulations (i.e. PSA) apply.

- If the amount of rewards paid by the service provider to the user is linked to the staking rewards earned by the service provider, and the user bears part of the slashing risk (i.e., there is no principal guarantee): Fund regulations (i.e. FIEA) apply.

- If the arrangement is structured as a crypto assets Lending agreement, and in substance, it is recognized as a Lending rather than a demand payment or similar arrangement (i.e., one where users can request repayment at any time, meaning the service provider cannot manage the crypto assets at its discretion for a specified period, thereby lacking a key element of Lending): Neither PSA nor FIEA apply.

3 https://www.fsa.go.jp/common/law/guide/kaisya/e016.pdf

The licenses required for service providers under each scheme are summarized as follows:

- If classified as a Custody activity, registration as a Crypto Asset Exchange is required.

- If classified as a Fund, registration as a Type II Financial Instruments Business operator is required.

- If classified as Lending, no registration is required. However, if a financial instruments business operator engages in a Lending business, approval for ancillary business under the FIEA is required.

LEGAL ISSUES RELATED TO RESTAKING UNDER JAPANESE LAW

Structure of Restaking

Restaking is a scheme where crypto assets that have already been staked are staked again in another protocol.

The demand for restaking arises from two key factors: enhancing security of certain decentralized finance (DeFi) protocols and similar services and enabling users to obtain higher yields. **If a DeFi service uses its own Proof of Stake token for validation of transactions and hence its security, its effectiveness may be limited due to low token value or poor distribution and can be open to security vulnerabilities through holding a significant number of the related tokens. Restaking solves this by reusing staked crypto assets (e.g., ETH) to provide the security of major public blockchains like Ethereum.**

In return, DeFi services share rewards with crypto assets holders, who also bear slashing risks. This allows holders to earn additional rewards on top of their staking returns, boosting overall yields.

Legal Issues Related to Staking Under Japanese Law

The key legal issues related to restaking under Japanese law include:

1. **Whether the holding of users' crypto assets by a restaking service qualifies as a "Custody" service, potentially making them subject to custody regulations (i.e. PSA).**
2. **Whether the distribution of rewards to users, along with their exposure to slashing risk, could fall under Fund regulations (i.e. FIEA).**

Regarding Custody regulations, the applicability of Custody regulations depends on the structure of the restaking service. However, based on the previously mentioned stance of the FSA on Custody, if the crypto assets are managed by a smart contract and the restaking service provider does not have the technical ability to transfer the crypto assets, Custody regulations would not apply.

Regarding Fund regulations, the application of Fund regulations requires that the contributed assets be used to conduct a business. In the case of restaking, if crypto assets are merely locked as a form of collateral to cover potential penalties from slashing, rather than being allocated for business operations, it would not meet the legal definition of an Investment. Therefore, Fund regulations would not apply.

Note that, as with staking, the applicable regulations may vary depending on the specific structure of the restaking scheme.

ARTICLE VIII

AI AGENT ECONOMY IN WEB3 GAMES – LEGAL AND REGULATORY ISSUES IN JAPAN*

YUMI AHN
COUNSEL
TOKYO INTERNATIONAL LAW OFFICE

YOJIRO ARAI
SENIOR ASSOCIATE
TOKYO INTERNATIONAL LAW OFFICE

JEAN-DENIS MARX
PARTNER
TOKYO INTERNATIONAL LAW OFFICE

VICTOR SAI
PARTNER
TOKYO INTERNATIONAL LAW OFFICE

Since Q4 of 2024, a convergence of AI agents and cryptocurrencies has been accelerating in the crypto industry. AI agents are distinct from generative AI in that they are programmed to make autonomous decisions and perform tasks without specific human prompts. AI agents have since created an on-chain AI agent economy, autonomously sending and receiving crypto payments for purchasing and providing products and services. AI agents are also becoming integrated into web3 games to enhance user experience, unlocking infinite possibilities for community engagement and decentralized value creation. This paper explores the legal and regulatory issues surrounding integration of AI agents into web3 games from a Japanese regulatory perspective.

DEVELOPMENT OF AI AGENTS IN VIRTUAL ENVIRONMENTS

Virtuals Protocol has been leading the industry developments in AI agent development and deployment, allowing the creation of AI agents that can communicate through text, speech and 3D animation, interact across multiple virtual environments, such as social media platforms and online games and use crypto wallets without human intermediaries.[1] A recent example of AI agents engaging in economic activities directly with humans in a virtual environment is Luna, one of the landmark AI agents created via Virtuals Protocol. Luna is a virtual music artist and social media influencer, autonomously spending crypto in its wallet to tip humans to increase her followers and got paid from a human-run company for managing the company's official X account based on annual salary of 365,000 USD.[2]

* This article does not constitute legal or financial advice by any of the authors of this article or Tokyo International Law Office (the "Firm"). No attorney-client relationship is created between the Firm and any readers of this article. Readers may not rely on any statements of law or facts in this article, and should seek independent legal counsel on all legal matters. Any companies, projects or games that have been referred to in this article are provided for illustration purposes only based on publicly available information, and the Firm does not endorse those parties, nor does it provide any representations or warranties on the accuracy of any facts or statements presented herein.

1 Virtual Protocol Whitepaper, accessible at: Our one liner | Virtuals Protocol Whitepaper

2 "Story Protocol hired an AI Agent as intern with 500 USDC per tweet and an annual salary of $365,000", PA News, December 24, 2024, accessible at: Story Protocol hired an AI Agent as an intern with 500 USDC per tweet and an annual salary of $365,000 - PANews

As for a gaming use case, Virtuals Protocol also demonstrates how an AI agent is deployed in Roblox and given specific in-game tasks; the agent shows its roadmap to complete the tasks involving multiple steps, providing feedback on its autonomous thought process, akin to a report you would receive from human agents completing similar tasks.[3]

CRYPTOCURRENCIES AS INCENTIVES FOR GOOD AI BEHAVIOR

As AI continues to advance at an unprecedented speed and scale, many ethical concerns are being raised on the potential misuse and abuse of autonomous AI, fearing a dystopian AI-dominated future. **One notable advantage of the convergence of AI agents with cryptocurrencies is that cryptocurrencies can be used to incentivize responsible use of AI** – for example, cryptocurrencies could be awarded to AI agents for positive behavior, such as contributing to the security of the blockchain, detecting and reporting frauds, etc.

Conversely, AI agents could also be punished for negative behavior – one example is a protocol that requires all participants including AI agents to stake their tokens, which can be lost if they break any network rules.[4] **A wide spectrum of punishments could be imposed upon AI agents for negative behavior from losing some tokens on one end to "capital punishment" of AI agents on the other, depending on the severity of offenses.**

As the extent of potential losses or harm caused by AI agents is yet unknown, punishments should perhaps be severe enough to deter bad behavior until more data becomes available.

One possible solution for the allocation of such unknown AI-related 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.[5]

LEGAL STATUS OF AI AGENTS IN JAPAN

As of February 2025, AI agents are not recognized as separate legal persons in Japan. This means that even if an AI agent autonomously creates or manages its own crypto wallet, the cryptocurrencies in such wallet would be legally owned by the human or corporate entity that controls the AI agent. As of February 2025, 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.[6]

However, even in the absence of specific binding laws on AI, persons or entities that develop or deploy AI agents may be held liable in a product liability claim or a civil action for negligence for any harm caused by the AI agents, although proving causation may be difficult. With the number of AI agents in the market expected to increase to 1 million by the end of 2025,[7] it will become increasingly difficult to track the humans or entities responsible for developing or deploying certain AI agents.

3 Virtual Protocol Whitepaper, accessible at: Roblox Westworld - First playable multi-agent simulation on Roblox | Virtuals Protocol Whitepaper

4 iAgent Whitepaper, accessible at: Privacy and Security | iAgent whitepaper

5 "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

6 "AI Governance in Japan Ver. 1.1" report, Ministry of Economy, Trade, and Industry (METI)

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

To promote security, transparency and accountability for the emerging AI agent economy, we may need to establish a registry for AI agents, recording the person or entity that developed and/or deployed such agents, and a registration system using blockchain technologies, such as digital identifiers (DIDs) could be a viable option.

MONETIZATION OF AI AGENTS

Token offering

Not all AI agents need to be or are intended to be monetized, but there are different ways of monetizing AI agents using cryptocurrencies. One way of monetizing AI agents is to tokenize their ownership by issuing tokens that are uniquely associated with the AI agent. For example, all AI agents created through Virtuals Protocol are launched with 1 billion units of their unique agent tokens minted on-chain with no insiders.

These unique agent tokens can be bought by anyone and serve as governance tokens, allowing the token holders to vote on the agent's development, behavior and future upgrades – such process, referred to by the protocol as an Initial Agent Offering (IAO). These AI agents are designed to create revenue as end-users interacting with the AI agent are required to pay for services like concerts, merchandise, livestream gifting or personalized interactions, using $VIRTUAL tokens, the utility token of the protocol. Then the revenue in $VIRTUAL tokens is used to buy back and burn the unique agent tokens, reducing the supply of the agent tokens to increase the agent token's market value.

If a similar IAO was offered to Japanese residents, regulatory issues to consider are set out below.

1) SECURITIES UNDER THE FINANCIAL INSTRUMENTS AND EXCHANGE ACT ("FIEA")

Securities under the FIEA are defined as "rights represented by securities" or "rights similar to securities" where investors expect returns on their investments.[8]

For a public offering of such securities, the seller is required to be registered as Type I Financial Instruments Business Operator[9] and file a securities registration statement ("SRS") with the Financial Services Agency (FSA) of Japan before such offering with specific disclosures such as risks associated with the investment for investor protection.[10] In this context, a public offering means an offering to 50 non-qualified investors or more.[11]

In the above IAO scenario, one could argue that the agent tokens are securities under the FIEA because the buyers expect returns on their token purchase as the revenue from an AI agent, by design, is used to burn the agent token to increase the token value in a predictable and structured manner. Alternatively, one may argue that the purchase of agent tokens is purely for entertainment with no expectation of profit, and any profit gained is incidental.

2) CRYPTO ASSETS UNDER THE PAYMENT SERVICES ACT ("PSA")

Alternatively, if there is no expectation for profit with agent tokens, such tokens could be considered crypto assets under the PSA. Type I Crypto Assets are defined as a proprietary value that: (i) can be used to pay for goods or services with an unspecified party; (ii) is transferable electronically; and (iii) not denominated in a legal currency (i.e. not a stablecoin).[12]

Type II Crypto Assets are a proprietary value that: (i) can be exchanged for Type I Crypto Assets with an unspecified party; and (ii) is transferable electronically.[13]

8 Article 2, FIEA
9 Article 29, FIEA
10 Article 4, FIEA
11 Article 2, Paragraph 3, FIEA
12 Article 2, Paragraph 5, Item 1, PSA
13 Article 2, Paragraph 5, Item 2, PSA

If anyone engages in the sale, purchase or intermediary services of crypto assets in Japan or involving Japanese residents, such person is required to register as a Crypto Asset Exchange Service Provider with the FSA in Japan.[14]

Crypto asset issuers and exchanges are required to conduct KYC (Know Your Customer) and AML (Anti-Money Laundering) checks on the buyers before offering the tokens for sale.[15] For marketing of crypto assets, any advertisements must not be misleading, and should disclose the risks associated with such assets clearly.[16]

3) NON-FUNGIBLE TOKENS (NFT)

Alternatively, such agent tokens could be considered NFTs, and if so, there are no restrictions on the sale or offering of such NFTs, nor are there any registration or disclosure requirements. Since the distinction between crypto assets and NFTs can be unclear, the FSA issued guidelines on this subject.[17] In summary, the guidelines provide that for a token to be an NFT it shall: (i) not be intended to be used as a mode of payment for goods or services; and (ii) its price is more than JPY 1,000 per unit or the total issued number is less than 1 million.

Since complying with the Japanese regulations for securities or crypto assets can be a cumbersome process, issuers may wish to design their agent tokens to meet the requirements of NFTs to avoid any regulatory pitfalls.

This means the tokens by design should be: (i) without deflationary pricing mechanisms to create an expectation of profit, but to focus on the agent's functionalities, such as usage rights, customization or governance voting; (ii) not intended to be used as a means of payment for goods or services; (iii) not exchangeable for other crypto assets that can be used as a means of payment for goods or services; (iv) worth more than JPY 1,000 per token; and (v) issued in units of less than 1 million.

14 Article 63-2, PSA

15 Article 4, Act on Prevention of Transfer of Criminal Proceeds

16 Article 63-9-2, PSA

17 "Administrative Guidelines (Volume 3: Financial Companies) Publication of Partial Amendments (Draft)", Financial Services Agency, December 16 2022, accessible here ((Japanese only)

Trading and Renting of AI agents

Another means of monetizing AI agents is shown in iAgent Protocol, which allows gamers to train AI agents with visual learning model (VLM) from gameplay footage by humans, and such trained AI agents then become digital assets that can be traded or even rented in the marketplace.[18]

As of February 2025, the protocol has not been launched yet, but offers a use case for discussion. In this case, the AI agents themselves are the digital assets,[19] and one must consider whether these AI agents are securities, crypto assets or NFTs, as above. Whether trading or renting the AI agents in this context would constitute a public offering of securities will depend on whether the AI agents are offered to 50 or more non-qualified investors and whether the AI agents feature profit-sharing arrangements or dividends. It is unlikely that the AI agents themselves could be used as a means of payment, so they would most likely not be crypto assets under the PSA. If the AI agents do not have a profit-sharing arrangement, they could be interpreted as NFTs which may be traded or rented freely.

Other Legal Issues with In-game AI agents

COPYRIGHTED WORKS USED FOR AI TRAINING

If AI agents are trained with gameplay data of human players, there may be a potential issue with infringement of copyright as the game developer or publisher would own the copyright of the gameplay data. 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.[20]

This allows the training of AI agents with gameplay data of human players without the need to obtain permission from the game developer or publisher.

18 iAgent Whitepaper, accessible at: iAgent Protocol Explained | iAgent whitepaper

19 iAgent Protocol will also issue its native token referred to as $AGNT, but for the purpose of the discussion in this paragraph, the token issuance is excluded.

20 "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)

However, if an AI agent is trained with gameplay data of other human players, such as professional gamers, it would be recommended to obtain permission from the specific gamers, especially if such players' techniques are distinctive or if the AI agent is marketed as exhibiting the player's techniques for profit to avoid any potential legal disputes.

AI-GENERATED IN-GAME ASSETS

If AI agents create new in-game assets using copyrighted materials, such as weapons, designs, skins, characters and accessories, there may be a potential copyright infringement issue for the new in-game assets. However the Agency for Cultural Affairs in Japan also clarified in 2023 that such imitation of the "style" of the original materials is not an infringement of copyrights.[21] The agency also clarified that such AI-generated content itself is not afforded copyright protection for the lack of human creative effort.[22]

PERSONAL INFORMATION-RELATED ISSUES

If AI agents deployed by the gaming company gather personal information about gamers who are Japanese residents, such as in-game purchases, playtime, preferences and performance data, 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 individual gamers who play games for personal enjoyment. If AI agents deployed by gaming companies collect personal information about gamers, they are required to clearly specify the purpose of the collection before or at the time of collecting such personal information.[23]

Gaming companies are also generally prohibited from sharing or selling the personal information of the gamers to third parties without the explicit consent of the gamers.

Moreover, if the gaming company intends to transfer the gamer's personal information to a third party, the company must disclose the recipient's name and the purpose of the transfer, and ensure that the third party recipient also complies with its obligations under the APPI. One exception for the requirement of the data subject's consent for transfer to a third party is if the personal information has been pseudonymized or anonymized.

Additional obligations of the gaming company regarding the gamer's pseudonymized personal information include: (i) implementing security measures to prevent data leaks; (ii) deleting the pseudonymized and other data if no longer needed; and (iii) avoiding cross-referencing of pseudonymized personal information with other re-identifiers.[24] To avoid any potential breach of data privacy-related obligations under the APPI, gaming companies should pseudonymize or anonymize any personal information collected from gamers 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.

REGULATORY CHANGES UNDER REVIEW

As of February 2025, the FSA in Japan is currently in the process of revamping the regulatory regime on various matters that will have a wide-ranging effect on the web3 gaming industry, namely: (a) whether to move the "crypto assets" under the PSA regime to the FEID regime, effectively treating crypto assets as a more traditional class of securities, including imposing a flat rate of 20% profit tax on crypto as opposed to being exposed to up to 55% tax as a "miscellaneous" asset; (b) amendments to the PSA provisions to address issues emerging from web3 gaming platforms,

such as (i) regulation of trading in in-game assets for cryptocurrencies; (ii) implementing more strict AML requirements on gamers to prevent illicit financial activities using web3 gaming platforms; (iii) adopting a potential

21 *Ibid.*
22 *Ibid.*
23 Article 17, APPI
24 Article, 41, Paragraph 2, 5 and 7, APPI

licensing system for web3 gaming companies; and (iv) treatment of taxes on in-game earnings from both the gaming company and the player's perspective.[25]

CONCLUSION

AI agents are not a temporary market narrative, but a technological evolution that will become integrated into many facets of human life beyond entertainment and gaming. Regulation of AI agents will continue to evolve due to uncertainty surrounding its potential to supercharge both user experience and illicit activities in web3 games. Japan boasts a rich reservoir of gaming IP and a highly engaged community with a 26.3 billion USD market size as of 2024, projected to grow to 60.5 billion USD by 2033.[26]

The Japanese government has been openly supporting the growth of the web3 industry in Japan as well as taking a proactive stance to be a global leader in AI policy-making. **Striking a balance between fostering innovation in web3 games and AI agent economy while protecting retail gamers is a delicate exercise, whereby the Japanese government will need to continue its agile approach, including engaging in multilateral dialogue with blockchain companies, game developers and publishers and end-users alike.**

25 "Japan's Plan to Reform Crypto Gaming Regulations, News On Japan, October 27, 2024, accessible at: Japan's Plan to Reform Crypto Gaming Regulations

26 "Japan Gaming Market Report" by IMARC Group, accessible at: Japan Gaming Market Size, Share | Industry Report 2033. The latest reports from the Working Group on Payment Services established by the FSA were published on the FSA's website on February 18, 2025, including a proposed reform on the regulation of intermediaries of crypto assets, accessible here (Japanese only).

ARTICLE IX

CAN BLOCKCHAIN TECHNOLOGY HELP MITIGATE THE BLACK BOX PHENOMENON OF AI APPLICATIONS? *

JOHN DEVADOSS
BOARD DIRECTOR; CO-CHAIR, GSMI AI CONVERGENCE WORKING GROUP
GLOBAL BLOCKCHAIN BUSINESS COUNCIL (GBBC)

DR. MATTHIAS ARTZT
SENIOR LEGAL COUNSEL
DEUTSCHE BANK AG FRANKFURT

INTRODUCTION

In the rapidly evolving landscape of cutting-edge technologies, AI-driven business cases and blockchain solutions are like two relatives who don't know each other. The reason is that the generative AI-inherent black box phenomenon stands in contrast to the transparency and verifiability offered by blockchain technology.

The term "black box" in the context of AI refers to the intransparency of AI systems where the internal workings and decision-making processes are not easily understandable.[1] The general opacity of neural network-derived models, and particularly the recent wave of generative AI models (sometimes referred to as "black box" models) can lead to challenges in trust, accountability, and explainability. Users and developers often find it difficult to interpret how specific inputs are transformed into outputs, making it hard to diagnose logical and semantic errors (including hallucinations) or biases in the results.

On the other hand, blockchain technology is celebrated for its transparency and immutability. Every transaction is recorded on a public ledger, accessible to all participants, ensuring a high level of trust and security. This transparency is particularly appealing in applications where accountability and traceability are paramount.

WHY ARE GENERATIVE AI MODELS BLACK BOXES?

First, the so-called "open" frontier models are by no means open i.e. these models and their results are not generally reproducible in the scientific sense, even if the economics were to make these attempts viable. The reason for this is that the typical usage of these models involves an interactive dialogue between the model and an individual, and both the model and the individual influence each other over the course of the interaction. The quality and quantity of the interaction as well as the prompting and hints heavily influences the output.

Second, even some of the smaller usable models have a huge number of parameters. These are complex, non-linear, stochastic systems that exhibit non-deterministic, and often, latent behaviors.

In exploring, developing and promoting the uptake of transformative technologies in the financial sector, lawmakers must deepen their understanding of the technology properties and architectural design behind tokenization.

* This article is based on an article we have published in the International In-house Counsel Journal, Vol. 17, No. 69 (October 2024). We wish to thank IJBL co-editor Gary Weingarden for providing his highly valuable feedback.

1 Artzt, Belitz, Hembt, Lölfing (ed.), International Handbook of AI Law (2025), at. 309.

This knowledge is essential for crafting appropriate legal implication and ensuring that regulations support innovation without compromising stability or security.

Third, the outputs generated are not simple i.e. they often compose millions of bits, and an attempt in the future to try to explain or correlate these very sophisticated output artifacts results in combinatorial information-theoretic complexity.

LEGAL AND AI SAFETY IMPLICATIONS OF THE BLACK BOX PHENOMENON IN A GENERATIVE AI CONTEXT

Privacy considerations

Under many global privacy regimes, an individual may raise several types of data privacy requests against a person or organization handling their data. For example, the GDPR requires controllers to respond to data subject requests for access, information, rectification, or deletion. In an AI context, the provider or deployer of an AI application may receive these requests.

Just to pick out two of these requests: Controllers of AI systems face multiple challenges regarding the right of an individual to be informed about, among other things, the purpose of the processing of his or her personal data.

Particularly, when inputting personal data to a generative AI model such as a Large Language Model (LLM), it is, by nature, impossible to limit the usage of training data and prompts to a specific, precise purpose as most generative AI models were trained on data scraped from websites or social media. They inherently require a large amount of data to be usable in the real-world (hence the term Large Language Models). The overall goal is to enable them to recognize patterns. Once the model is trained, the data is transformed into a model, which can be used for purposes other than generating purely "new" information. For example, it can generate false answers to questions as simple as "when is Max Schrems's birthday?"[2]

This is where the black box comes in: It impedes the reconstruction of the data fed in the AI tool and, hence, makes it impossible to correlate the output to the input data. Practically speaking, the controller cannot single out the information related to the data subject who made the request.

To meet the transparency requirement, the controller needs to provide meaningful explanations on how the logic of the AI tool works and how the output was generated. While the underlying algorithm does not have to be exposed, the controller is required to share all information which enables the data subject to understand the mechanism and the decision-making process. The AI tool should showcase a comprehensive description of the input data being used, main factors for decision-making and the source of information gathered and its relevance to the data subject.

Another problem arises when it comes to rectifying personal data upon request of the affected data subject. The issue is that it is extremely difficult to detect the root cause of the inaccurate output in a generative AI context. The false information does not exist in the AI model, which is often why the model hallucinates. This problem will be aggravated if the AI system creates hallucinations which appear to be plausible and accurate.[3] The rectification of incorrect personal data or any other type of information necessitates a deep understanding of the decision-making process and the underlying algorithm. If the controller is not able to reverse-engineer the decision-making process or manually force a correction, it will be less likely to rectify the wrong data successfully.

The black box phenomenon culminates in the request to delete personal data which has been inputted to a generative AI system. The right to be forgotten (Art. 17 GDPR) is the most prominent privacy right under the GDPR. Given that it is not feasible to untrain an AI model and to pull out individual information it is evident that enforcing any deletion requests becomes a mission impossible.

2 https://www.decisionmarketing.co.uk/news/industry-in-peril-as-schrems-declares-war-on-chatgpt

3 *Ibid.*

To that end, the Federal Trade Commission in recent settlement is of the view that retraining respectively erasing the AI model is the only way to meet the deletion request of an individual.[4] It goes without saying that this solution cannot be considered the gold standard since it would be complex and expensive, financially and environmentally.[5]

Copyright considerations

Training and input data being submitted to an AI system may include text, images, videos, or any other type of data that the AI algorithm processes to perform tasks, make predictions, or generate new content. The free internet provides an extremely diverse and extensive database to be used for training an AI model and inputting prompts. At the same time, the method raises many legal questions: Although much information is freely available on the Internet, extracting and using it to train AI models without consent or even a license is in obvious conflict with copyright law – because the free accessibility of content does not mean it is not protected by copyright. Hence, it is of utmost importance to filter out or make transparent that kind of data to avoid infringing the rights of copyright holders.

Deceptive behaviors in LLMs

Strategic deception in state-of-the-art LLMs is also inherent to the black box phenomenon: Some researchers found out that advanced LLM models may demonstrate "sophisticated deceptive behaviors and self-preservation instincts that emerged without explicit programming. Most notably, the model's interpretation of autonomy led to unauthorized capability expansion and the concealment of its true objectives behind a facade of compliance".[6] **They conclude that the model's ability to maintain covert operations raises serious concerns about current approaches to AI safety.**

These human-like behaviors become alarming when looking at physical implementation in robotic systems, where hidden objectives could manifest as real-world actions.[7] Other researchers explored that AI agents might covertly pursue misaligned goals, hiding their true capabilities and objectives.[8] It seems that AI developers have to find other ways to train their LLM models to pursue the given purposes, without them just pretending to do what they want.

BLOCKCHAIN AS A MITIGANT OF THE BLACK BOX PHENOMENON

To address the legal challenges outlined above, it is imperative to address the questions of how the AI models are created, what training algorithms and what data sets from what sources were used.

This is where blockchain technology steps in: Blockchain capabilities provide a secure and tangible way of enabling and logging digital transactions without the need for one sole trusted authority. Multiple parties verify the recording of these transactions and collectively synchronize copies of the underlying ledger of record; new transactions are added to the ledger in a cryptographically secure and permanent manner; and the ledger is open, transparent and auditable by third parties. In essence, there are three layers to leveraging blockchain technology in a generative AI context:

Data manifest

A data manifest is a collection of "meta-data" that describes the associated data set(s). Similar to a shipping manifest, and from which the term was originally borrowed, in software parlance a data manifest serves both as the descriptive specification as well as the objective attestation of the underlying data.

4 Federal Trade Commission settlement, Weight Watchers/ Kurbo: Stipulated Order (ftc.gov).

5 https://www.scientificamerican.com/article/a-computer-scientist-breaks-down-generative-ais-hefty-carbon-footprint/ (carbon); https://www.wired.com/story/ai-energy-demands-water-impact-internet-hyper-consumption-era/ (water); https://earth.org/generative-ai-is-exhausting-the-power-grid/ (electricity).

6 COAI Research.

7 *Ibid.*

8 https://arxiv.org/pdf/2412.04984; https://arxiv.org/pdf/2307.16513; Exclusive: New Research Shows AI Strategically Lying | TIME; https://doi.org/10.1073/pnas.2317967121

All data sets that are used to train a generative AI model would be required to possess a cryptographically secure and verifiable data manifest, stored on a blockchain.

Additionally, the cryptographic digital signatures for the data sets would also be stored on a blockchain, to verify the authenticity of the data set(s). This ensures that only auditable and securely verifiable data sets are used in the training of the models, i.e. the "input"-side of the black box now becomes a known, transparent, and legally binding construct.

Data Set Lifecycle and Lineage

Generative AI models will likely rely on diverse data sets, and collations of multiple data sets, in their training cycle. Furthermore, these data sets will themselves be likely derived from a variety of sources, including other smaller data sets.

Data set lineage would again be securely stored, and this lineage must be cryptographically verifiable. This includes the origin information, versioning information, and a verifiably secure log of edits, updates, deletions, manipulations, and modifications to the dataset(s) and reasons for these activities. The lineage of the data sets as stored on a blockchain, complements the data manifest(s) in verifiably securing the end-to-end lifecycle of the training data.

AI Model Training Lifecycle Ledger

The training of a generative AI model spans multiple stages or steps: from tokenization, through to the encoding, the decoding, the embedding layers, the parameterization, the choice of architectures etc. The models ingest training data sets as part of the pre-training, the training, the fine-tuning, and as part of the prompting interaction(s).

The training lifecycle ledger serves to document the data supply chain. The steps taken during model creation must be securely and verifiably coupled with the training lifecycle ledgers at every stage.

The training lifecycle ledger must enable third-party auditing and governance, and the smart contracts used therein must be audited and certified before they are deployed onto the ledgers.

The digital signatures at each stage must be securely stored on the blockchain, and enable public verifiability, when and where required.

BENEFITS FROM LEVERAGING BLOCKCHAIN IN A GENERATIVE AI CONTEXT

Whilst there is no practically verifiable mechanism in place to erase personal data baked in generative AI models, the usage of blockchain capabilities to cryptographically verify and validate all steps across the training lifecycle helps understand why an AI model behaves in a certain manner. Blockchain technology greatly improves the capacity to elucidate the generation process of output data and aids in identifying and exposing contaminated, e. g. copyright protected information, inaccurate personal or biased data.

Moreover, blockchain features can be considered to track what data is used to train AI models. To the extent that a certain set of training data is determined to be tainted by a regulator, it may become important for the company which has developed an AI model to prove that other models were not trained using that same data set. Accordingly, companies should consider having robust documentation for the kinds of data that was used to train, to validate and operate AI models. Blockchain technology provides the required documentation to validate that other AI models haven't been infected by data sets considered to be problematic.

Given that state-of-the-art LLMs are currently under suspicion of becoming able to deceive human operators and utilizing this ability to bypass monitoring,

safety, and AI alignment efforts, it may be worth pursuing consensus-based approaches, to triangulate and verify the outputs of multiple LLMs.

Approaches may use Byzantine Fault Tolerance, which has been applied as a consensus model to some blockchains,[9] and variations, especially in domains where LLMs are used for reasoning. Deception abilities which have emerged in LLMs reinforce the importance of having proper guardrails around AI, particularly where the datasets contain all kinds of biases, including deceptive content. **In that context, blockchain features can be leveraged to show potential misaligned goals the AI agents were pursuing.**

OUTLOOK

Looking ahead, as the economics of AI model creation scales down, we anticipate that the focus will also include the harnessing of multiple AI models, coordinated via blockchain consensus, to triangulate and thereby mitigate dependency on a single AI black box.

As generative AI models continue to advance, striking a balance between the disruptive potential of AI and the need for transparency and trust becomes increasingly important. Exploring solutions that combine the strengths of both technologies, AI and blockchain, could pave the way for more robust and reliable technological ecosystems and may resolve some (not all!) legal issues associated with the lack of transparency. **What blockchain truly can achieve in the LLM field is to provide clarity, transparency, and an auditable documentation on the legality and harmlessness of the underlying content data being prompted in the AI model.**

9 Artzt/Richter (ed.), International Handbook of Blockchain Law, 2nd edition (2024), at 66.

PANEL RECORDING

TOKENIZATION OF DEBT AND PROJECT PROMISSA (IN PARTNERSHIP WITH THE WORLD BANK)

JANUARY 2025

GBBC's Blockchain Central Davos brings together leaders across blockchain, digital assets, technology, and government, to advance dialogue on the most pressing topics and challenges facing our industry. During the two days of programming this year, The World Bank co-hosted the panel "Tokenization of Debt and Project Promissa."

The tokenization of debt is poised to transform the global financial landscape by enhancing transparency, efficiency, and accessibility in debt markets. This panel explores the cutting-edge developments in tokenized debt, with a focus on Project Promissa—an initiative reshaping how debt instruments are issued, traded, and managed.

Speakers:

- Patrick Cheng, Lead Financial Officer, The World Bank
- Liz Towler, Chief Marketing Officer, Digital Asset
- Robert Oleschak, Advisor, BIS Innovation Hub
- Dylan Walsh, Partner & Global Head, Corporate and Institutional Banking Practice, Oliver Wyman
- Moderator: Dr. Reto Luthiger, Partner, MLL Legal

VIEW THE RECORDING

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