THE INTERNATIONAL JOURNAL OF BLOCKCHAIN LAW

Volume 5

March 2023

GBBC
Global Blockchain
Business Council

Geneva | London | New York | Washington, D.C. | Austin | Seattle

TABLE OF CONTENTS

NOTE FROM THE EDITOR-IN-CHIEF

DR. MATTHIAS ARTZT
SENIOR LEGAL COUNSEL
DEUTSCHE BANK

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

Welcome to the 5th issue of the IJBL! I am extremely proud to share with you several excellent blockchain-related articles and other media from attorneys in the US, England and South Korea.

Starting with the U.S., Jai Massari considers the issues raised in Lewis Cohen´s scholarly article "Why Crypto Assets are not Securities," and provides a thoughtful overview of the key arguments. David Simonds, Edward McNeilly, and Kaitlyn Hittelman, all from Hogan Lovells in Los Angeles, offer insight into Guidance which was recently issued by the New York State Department of Financial Services on crypto custodial accounts and its impact on a bankruptcy estate.

Law Professors Kara Bruce (University of Oklahoma College of Law), Christopher K. Odinet (University of Iowa College of Law) and Andrea Tosato (University of Nottingham), have written a scholarly article that examines the legal terms of service associated with the issuance of the most popular stablecoins. We bring you the article's abstract and a helpful infographic that highlights the key points, along with a link to the article.

Attorney Jake Schneider from Holland and Knight's Boston office illustrates the danger of compromising our current encryption scheme which is integral to many technologies including DLT.

Moving on to England, attorney Laura Douglas from Clifford Chance's London office fleshes out the latest developments on the regulatory landscape for crypto assets in the EU and UK and suggests practical conclusions for each regime.

Attorneys Ben Hitchens and Oliver Roberts from CMS London office, explore the question of Decentralized Autonomous Organizations (DAOs), and dive into the murky legal question how DAOs should be treated under the laws, particularly where investors are seeking to sue a DAO.

South Korean contributors, attorneys Joon Young Kim & Mooni Kim from the Kim & Chang law firm in Seoul shed light on the recently released and long-awaited guidance of the Financial Services Commission of Korea on the treatment of security tokens.

Finally, we call your attention to two recent IJBL webinars (with links included):

- The first is a point-counterpoint discussion , "Competing Views: Are Fungible Crypto Assets Securities Under US law?" in which several blockchain lawyers (including the author) explore Lewis Cohen´s groundbreaking article, "*The Ineluctable Modality of Securities Law: Why Fungible Crypto Assts are Not Securities*".

- The second, "Hot Topics in Blockchain Law," features seven top blockchain lawyers delving into pressing legal blockchain-related issues of the day, including the SEC's proposed rule on safeguarding client assets, the recent Tulip Trading opinion from London, and the latest SEC enforcement actions.

Happy reading and viewing!

ABOUT THE CO-EDITORS

You can find the editors' full bios here.

LOCKNIE HSU

PROFESSOR
SINGAPORE MANAGEMENT UNIVERSITY

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.

STEPHEN D. PALLEY

PARTNER
BROWN RUDNICK

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

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.

ANDREA TINIANOW

CHIEF LEGAL OFFICER AND HEAD OF POLICY - AMERICAS
GBBC

Andrea Tinianow, a Delaware attorney, is the Chief Legal Officer and Head of Policy - Americas at GBBC. In 2015, Andrea started the Delaware Blockchain Initiative which gave rise to the "Blockchain Amendments" to Delaware's business entity statutes that authorize corporations (and other business entities) to maintain their corporate records, including stock ledgers, on a blockchain.

JAKE VAN DER LAAN

CHIEF INFORMATION OFFICER & DIRECTOR
FINANCIAL AND CONSUMER SERVICES COMMISSION, NEW BRUNSWICK, CANADA (FCNB)

Jake van der Laan is the Director, Information Technology and Regulatory Informatics and the Chief Information Officer with the New Brunswick Financial and Consumer Services Commission (FCNB) in New Brunswick, Canada. He was previously its Director of Enforcement, a position he held for 12½ years. 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

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. He is an Observing Member of the Global Blockchain Business Council. Before Joining Tufts, Gary served as Data Protection Officer for Notarize, and Senior Counsel at Rocket Mortgage.

HONOR ROLL

Previous contributors to the International Journal of Blockchain Law.

Commissioner Caroline Crenshaw
U.S. Securities and Exchange Commission

Ciarán McGonagle
International Swaps and Derivatives Association (ISDA)

Alexander Lipton
SILA

Lewis Cohen
DLX Law

Eric W. Hess
Hess Legal Counsel

Christopher D. Clack
University College of London (UCL)

Andrew Hinkes
K&L Gates

Ciara Cullen
RPC

Alessandro Cerri
RPC

Sophie Parkinson
RPC

David Adlerstein
Wachtell Lipton

Olta Andoni
Ava Labs

Collins Belton
Brookwood P.C.

Jason Gottlieb
Morrison Cohen LLP

Christine Parker
Coinbase

Lee Schneider
Ava Labs

Robert Schwinger
Norton Rose Fulbright

Harriet Jones-Fenleigh
Norton Rose Fulbright

Jonathan Hawkins
Norton Rose Fulbright

Samir Patel
Holland & Knight LLP

Barry Sookman
McCarthy Tétrault LLP

Dr. Michael Jünemann
Bird & Bird LLP

Udo Milkau
Digital Counselor

Raoul Renard
International Chamber of Commerce

Carmen María Ramírez Ortiz
Asian Development Bank

Oswald Kuyler
ICC Digital Standards Initiative

Steven Beck
Asian Development Bank

Tran Viet Dung
Ho Chi Minh City University of Law

Le Tran Quoc Cong
Ho Chi Minh City University of Law

Marvin Ammori
Uniswap Labs

Andrew Balthazor
Holland & Knight LLP

Sabina Beleuz Neagu
Wachtell Lipton

HONOR ROLL

Previous contributors to the International Journal of Blockchain Law.

Collins Belton
Brookwood P.C.

Max Dilendorf
Dilendorf Law Firm PLCC

David Kirk
Wachtell Lipton

Peter McBurney
Norton Rose Fullbright

Hannah Meakin
Norton Rose Fullbright

Kayvan Sadeghi
Jenner & Block

Kevin Schwartz
Wachtell Lipton

Sonal Tolman
Uniswap Labs

Albert Weatherill
Norton Rose Fullbright

Sujay S. Davé
The Brattle Group

Paul Yuen
Monetary Authority of Singapore (MAS)

Andrea Tinianow
Global Blockchain Business Council (GBBC)

Stephen Palley
Brown Rudnick

Sarah Brennan
Delphi Research & Delphi Ventures

Dr. Matthias Artzt
Deutsche Bank

Eric Hess
Hess Legal Counsel

WEBINARS

"COMPETING VIEWS: ARE FUNGIBLE CRYPTO ASSETS SECURITIES UNDER U.S. LAW?"

FEBRUARY 2023

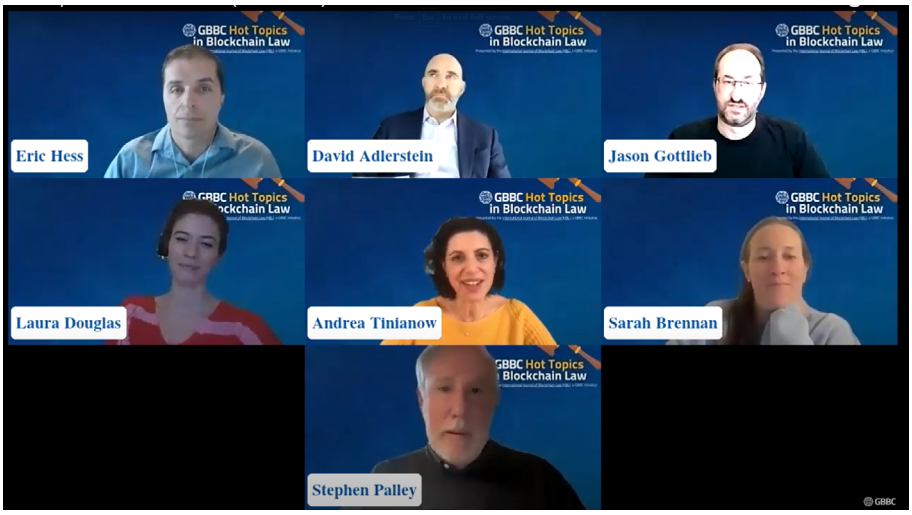
This IJBL webinar delves into the groundbreaking article, "The Ineluctable Modality of Securities Law: Why Fungible Crypto Assets are Not Securities," with the article's author, attorney Lewis Cohen, and blockchain lawyers Liz Boison, Alan Cohn, Stephen Palley, and Andrea Tinianow. The first part of the webinar is a fireside chat with Lewis and Liz, followed by a point-counter-point discussion with Stephen and Lewis moderated by Alan. Watch the sparks fly!

WATCH IT HERE

"HOT TOPICS IN BLOCKCHAIN LAW"

MARCH 2023

This team of top blockchain attorneys discuss the pressing issues of the day in blockchain law, including the SEC's recent enforcement actions, Operation Choke Point 2.0, The Tulip Trading opinion, and much more; with David Adlerstein, Sarah Brennan, Laura Dougas, Jason Gottlieb, Eric Hess, Stephen Palley, and Andrea Tinianow.



WATCH IT HERE

VIEW THE IJBL PLAYLIST ON GBBC's YOUTUBE

ARTICLE I

WHY CRYPTOASSETS ARE NOT SECURITIES*

JAI MASSARI
COFOUNDER AND CHIEF LEGAL OFFICER
LIGHTSPARK

FTX's collapse reiterates the need for comprehensive U.S. regulation of crypto markets. This regulation must have a solid legal foundation, a key pillar of which is a workable framework to distinguish cryptoassets[1] that are securities from those that are not. A new paper provides this framework, by showing why fungible cryptoassets are not themselves securities under existing U.S. federal securities laws. But also why ICOs and similar token sales should be regulated as securities offerings.

In 2014, the sponsors of the Ethereum Network sold 60 million ether tokens to fund the development of the network, which launched a year later. Because of similarities with a traditional common stock IPO, the ether "initial coin offering," or ICO, raised a fundamental question: are cryptoassets securities under U.S. federal securities laws? The answer to this question, which we have been debating ever since, determines not only whether and how cryptoassets can be sold to the public but also whether we must hold and trade them under the existing rules and market structure developed over the past 80 years for securities.

The Securities and Exchange Commission's primary theory on whether a cryptoasset is a security appears to be based upon whether the blockchain project associated with a cryptoasset is, at any point in time, "sufficiently decentralized."[2] If so, the cryptoasset is not a security.

This theory was first proposed by the SEC staff in 2018 to address ICOs, which were then all the rage, and was followed by more detailed staff guidance in 2019. But the theory has not aged well. It is impractical—if not impossible—to apply to today's real life blockchain projects. It is not supported by existing judicial precedent, including the now crypto-famous *Howey* Supreme Court case.[3] And it has resulted in market distortions that harm both market participants and long-term innovation in the crypto industry.

An intriguing new paper, *The Ineluctable Modality of Securities Law: Why Fungible Crypto Assets Are Not Securities*,[4] points us to the right path. The paper analyzes the relevant caselaw and concludes there is scant legal basis to treat fungible cryptoassets as securities, and it sets out analytical approach that is far more satisfying. The paper separates capital raising transactions by blockchain project sponsors or other insiders in which a cryptoasset may be sold—which are typically securities transactions—from the treatment of the cryptoasset, which is not a security. This analytical framework addresses the now apparent challenges created by the SEC staff's approach and appropriately focuses the SEC's regulatory jurisdiction on capital raising transactions.

* This article was first posted to the Harvard Law School Forum of Corporate Governance in December 2022 and is reposted here with permission from the author.

1 In this article, the term "cryptoasset" to means fungible digital assets that are natively created, recorded, and transferred through blockchain technology, but excludes cryptoassets that are specifically designed to be securities, such as tokenized versions of equity or debt securities.

2 William Hinman, "Digital Asset Transactions: When *Howey* Met Gary (Plastic)" Hinman speech available at https://www.sec.gov/news/speech/speech-hinman-061418.

3 *SEC v. W.J. Howey* Co., 328 U.S. 293 (1946). The factors set out by the court in this case for determining when a given contract, transaction or scheme would be an investment contract for purposes of federal securities law has become known as the "*Howey* test."

4 Cohen, Lewis R., Strong, Gregory, Lewin, Freeman & Chen, Sara, The Ineluctable Modality of Securities Law: Why Fungible Crypto Assets are Not Securities available at https://dlxlaw.com/wp-content/uploads/2022/11/The-Ineluctable-Modality-of-Securities-Law-%E2%80%93-DLx-Law-Discussion-Draft-Nov.-10-2022.pdf (discussion draft).

The paper's approach is the right one and should be taken on both by the US Congress as it considers legislation to regulate the crypto industry and by courts as they consider high-stakes cases that hinge on the securities law treatment cryptoassets. Doing so will avoid the flaws of the SEC's well-intended but flawed current approach. And, together with legislative initiatives to regulate crypto markets and intermediaries, it will better protect market participants and more responsibly support innovation.

THE SEC'S DECENTRALIZE-AND-MORPH APPROACH

In the wake of the 2014 ether ICO and the following ICO boom,[5] the SEC staff provided the crypto industry with an analytical framework meant to clarify when and whether a cryptoasset is a security. First set out in a 2018 speech by SEC Corporation Finance Division Director William Hinman, and then described in more detail in 2019 staff guidance,[6] the core idea is that where a blockchain project is sufficiently decentralized, the cryptoasset associated with the project will not be or represent an "investment contract" under the so-called *Howey* test, named after a 1946 Supreme Court case. And therefore the cryptoasset would not be a security.

Under the 2019 SEC staff guidance, the decentralization level of a project is to be determined based upon fifty or so factors that involve characteristics both intrinsic and extrinsic to the project. These factors range widely and include, for example, whether so-called "active participants," which can include a "promoter, sponsor, or other third party," from time to time have a role in developing, marketing, improving or operating the blockchain project; whether an active participant "owns or controls ownership of intellectual property rights of the network or digital asset, directly or indirectly;" and whether the cryptoasset "is transferable or traded on or through a secondary market or platform, or is expected to be in the future." [7]

These factors are meant to be evaluated at a particular point in time. Accordingly, the decentralization level of a blockchain project could, and indeed would be expected to, change over time.

As a result, a cryptoasset could start its life as a security—for example when it is first sold to investors by the project's sponsors—and then, at some point later, it could morph into a non-security as the project becomes sufficiently decentralized. This very morphing was, according to Mr. Hinman, what had happened in the case of ether and the Ethereum Network, which had achieved the Holy Grail of sufficient decentralization at some unspecified time sometime between the network's launch in 2015 and the time of his speech in 2018. (Mr. Hinman did not reveal when.)

Classifying cryptocurrencies based on project decentralization was a deft bureaucratic solution to a practical problem. It helpfully provided some reassurance that the two largest cryptocurrencies, bitcoin and ether, were not—or at least were no longer—securities. Under the opposite view, the initial sales of these assets to the public could have violated registration and disclosure requirements for public securities offerings. And intermediaries, such as cryptocurrency exchanges and dealers as well as early investors in the tokens, could have been engaged in illegal unregistered securities exchange, brokerage, dealing or underwriting activities. Given the billions of dollars of value transacted in these two tokens, the SEC staff's approach avoided catastrophic consequences for holders of these cryptoassets and for firms providing services and building on the related blockchains.

But in practice, outside of Bitcoin, Ethereum, and a few other blockchain projects, it has been almost impossible to apply the SEC staff guidance in a way that provides agreed-on and repeatable answers. Market participants are expected to analyze a cryptoasset and its underlying project under many vague factors, some of which are based upon information not publicly available.

5 See, e.g., Lyandres, Palazzo, Rabetti, initial Coin Offering (ICO) Success and Post-ICO Performance, available at https://pubsonline.informs.org/doi/abs/10.1287/mnsc.2022.4312.

6 Securities and Exchange Commission, Framework for "Investment Contract" Analysis of Digital Assets, available at https://www.sec.gov/files/dlt-framework.pdf.

7 Id.

The analysis is unwieldy at best and impossible at worst, particularly without guidance on which factors might outweigh others and with little clarification through rules or substantive litigation. Adding further complexity, market participants are expected to evaluate the relevant facts and circumstances about a cryptoassets on an ongoing basis, as a cryptoasset that achieved non-security status at one point could, nevertheless, revert to security status if the project's ecosystem becomes less decentralized.

For blockchain project sponsors,the expectations created by the SEC staff's guidance have distorted economic incentives in unhelpful ways. Blockchain projects often plan on token issuances in early stages of their development, both to jumpstart network effects and to meet investor expectations. Project sponsors then quickly find themselves in a race to decentralize—not based on the economic or practical characteristics of the project or its underlying technology, but instead based on the presumed need to address some number of the SEC's decentralization factors. The decentralization of a blockchain project often is a critically important goal. But the imperative to decentralize to achieve a particular regulatory outcome is a distraction that promotes short-term tactics—sometimes disparagingly been referred to as "decentralization theater"—at the expense of longer-term strategy. Ultimately, this incentive is detrimental to value creation and innovation in the crypto industry.

The decentralize-and-morph theory seems to confound even the regulator who coined it. The SEC has deployed the theory inconsistently and sometimes confusingly in the enforcement context. In some instances, the SEC describes the cryptoasset as a security.[8] In others, the SEC describes the cryptoasset as embodying or representing a security.[9]

And in yet others, the cryptoasset is described as being part of a securities transaction, whether or not the cryptoasset is itself a security.[10] This inconsistency suggests the need for a better approach.

SEPARATING THE INVESTMENT CONTRACT FROM THE CRYPTOASSET

With the benefit of a few years of experience, it is clear that SEC's decentralize-and-morph theory is flawed. But then how should we think about the fundamental question of whether fungible cryptoassets are securities?

The *Ineluctable Modality* paper shows us how, by starting with the basics and discussing key federal appellate decisions applying the *Howey* test. The paper persuasively shows why ICOs and other capital raising transactions—which may well involve securities offerings—are distinct from the subject cryptoassets themselves. This intuitive step makes room for an analytical approach grounded in existing law that yields better incentives for crypto market participants and a path to better investor protection.

A capital-raising transaction where a blockchain project sponsor (or other insider) sells a cryptoasset to finance development of the project likely involves an investment contract and thus a security. Investors purchasing from the project sponsor would be participating in an "investment scheme" with an understanding of how sale proceeds were going to be used by the sponsor to increase the value of the cryptoassets sold. This would be the case whether or not the project is decentralized at the time of the transaction.

But the cryptoasset sold under the investment contract is never a security—no more than were the citrus groves in *Howey*.

8 *SEC v Ripple*, https://www.sec.gov/litigation/complaints/2020/comp-pr2020-338.pdf at 1 ("From at least 2013 through the present, Defendants sold over 14.6 billion units of a digital asset security called 'XRP,'" ...)

9 *SEC vs Ripple*, https://www.crypto-law.us/wp-content/uploads/2021/05/SEC_Memorandum-of-Law_Opposing-Motion-to-Intervene-050321.pdf at 24 ("The XRP traded, even in the secondary market, is the embodiment of those facts, circumstances, promises, and expectations, and today represents that investment contract.")

10 SEC vs Ripple https://www.crypto-law.us/wp-content/uploads/2021/05/SEC_Memorandum-of-Law_Opposing-Motion-to-Intervene-050321.pdf at 25 (". . . most assets sold as part of an investment contract in fact do have some use (though the SEC disputes that XRP has any use) . . .."

Instead, the contract or arrangement under which the project sponsor or insider sold the cryptoasset, whether or not its terms are written in a single document, is the investment contract .

Of course, even after the initial sale, a cryptoasset can again be sold in an investment contract transaction—for example, as part of a distribution by an insider or large holder who received tokens under the initial investment contract. And other types of arrangements involving promises and commitments by a project sponsor or insider and token purchasers can constitute investment contracts under a traditional *Howey* analysis. But that does not mean the cryptoasset itself ever is, becomes, or later stops being a security, as "morphing" would imply. Accordingly, absent the promises, claims and inducements made by a project sponsor to a buyer that are the hallmark of an investment contract, third-party trading of cryptoassets anonymously on crypto exchanges would not be securities transactions.

Applying this approach to the ether ICO yields the correct result. A court would likely have found the initial sale of ether by project sponsors to the public in 2014 to be a securities transaction and subject to the registration and disclosure requirements of the Securities Act of 1933. But subsequent anonymous trading of ether, which is not a security, on cryptocurrency exchanges or in peer-to-peer transfers among third parties should not involve securities transactions. This is similar to the end result contemplated by Mr. Hinman in his 2018 speech, but without the need for market participants to constantly assess whether, when and how the Ethereum Network later became decentralized enough for ether to morph into a non-security.

The paper's approach does not require new and confusing legal theories. It avoids the impracticalities of an asset changing its status as a security over time based upon extrinsic or nonpublic events, which would require market participants to constantly reassess the regulatory status of a cryptoasset based upon factors they may not be able to ascertain. It would appropriately capture capital-raising activities by blockchain project insiders, even where a blockchain is arguably decentralized. It also appropriately allocates regulatory responsibility for those capital raising activities to the SEC while avoiding subjecting all dealings in cryptoassets to laws that were not designed to regulate commercial activities not involving securities.

This does not mean that marketplace transactions in cryptoassets cannot or should not be regulated. FTX's demise is yet another demonstration of why they should be. Instead, it means only that secondary market trading in cryptoassets should not be regulated by existing securities laws. Instead, regulatory gaps should be closed by new law. The authors of the paper call for Congress to these gaps through legislation Commodity Futures Trading C with authority to regulate cryp and intermediaries operating in them. Indeed, several bills contemplating this type of regulation have been introduced in Congress this past year.

In the meanwhile, courts and litigants working through the fundamental question of a cryptoasset's status under the securities laws should take note of this paper and the briefs arguing to apply the approach.[11] The appeal of demystifying the legal classification of cryptoassets without new and muddled theories is clear.

It provides a more elegant outcome for many of the pending cases that hinge on whether a cryptoasset transaction involved an investment contract by treating fundraising activities appropriately—as being subject to federal securities laws—without harming cryptoasset markets and investor value.

11 E.g., https://www.dropbox.com/s/ommsv9bt6rbar9o/Paradigm%20Operations%20Amicus%20Package.pdf?dl=0

ARTICLE II

NEW YORK'S GUIDANCE ON CRYPTO CUSTODIAL ACCOUNTS AND ITS IMPACT ON A BANKRUPTCY ESTATE

DAVID SIMONDS
PARTNER
HOGAN LOVELLS

EDWARD MCNEILLY
SENIOR ASSOCIATE
HOGAN LOVELLS

KAITLYN HITTELMAN
ASSOCIATE
HOGAN LOVELLS

The crypto winter has brought a flurry of bankruptcy filings into the digital asset space. As pioneering cryptocurrency platforms collide with the Bankruptcy Code, unprecedented questions of law have left customers asking a fundamental question: who owns my crypto?

This question—the answer to which is critical to customer recoveries in cryptocurrency platform bankruptcy cases—is especially prevalent in cases where the debtor company's platform offered custodial accounts to customers. Custodial accounts are not new to the financial world; however, digital asset custodial accounts have unusual attributes (such as limited regulatory oversight) that have revealed cracks in customer protection when custodians have filed for bankruptcy.

To address these concerns, the New York Department of Financial Services (the "NYDFS"), the agency that supervises and regulates New York's financial institutions (including, as of 2015, virtual currency companies conducting business in the state under a BitLicense), recently issued guidance that, if followed, could significantly impact customer recoveries in future bankruptcy cases of digital asset platforms.

WHAT IS A CUSTODY ACCOUNT?

Digital asset custody accounts operate differently from a typical custody account at a bank: digital asset custodians do not technically store any of the customer's assets. This is due to the nature of cryptocurrency—the assets themselves actually exist on the blockchain (a quasi-public ledger). Instead, a crypto custodian holds a user's "private key"—the part of a crypto wallet that grants access to the funds associated with it.

Crypto custody accounts became a popular method for customers to secure their assets from theft.

Unfortunately, many traits that attract investors to a groundbreaking and unregulated industry also attract individuals who are less scrupulous or conscientious, and cryptocurrency platforms have not all proven themselves to be hack-proof or otherwise vault-like. Moreover, unlike tangible assets secured by a traditional financial institution, once digital assets are stolen, it is difficult, and in some cases, impossible, to recover them. As customer concerns increased, platforms began offering custodial services to safeguard customers' digital assets. These accounts also benefitted platforms—they offered customers a comprehensive place to hold all their digital assets, increasing the likelihood of attracting and retaining customers. And, notably, custodial accounts also generated substantial revenue.

As customers learned, however, there can be drawbacks to entrusting digital assets to a third-party custodian. One risk is that a custodian who holds the private key controls the assets and can freeze accounts, block access, or limit withdrawals.[1] In more severe cases, cryptocurrency platforms essentially could be considered to have acted like unregulated banks, with few controls in place to ensure that custody account assets never were commingled with other types of assets.

Thus, when a company offering custodial services files for bankruptcy, customers can be left at the court's mercy to determine whether digital assets meant for a custody account, but commingled with other funds, belong to the customer or the bankruptcy estate.

In such circumstances, there is a risk that bankruptcy courts could hold that the assets within the custody account belong to the bankruptcy estate, leaving customers, who thought they had mitigated the risk of loss of their digital assets by entrusting them to the custodian, as unsecured creditors of a bankrupt company.

1 https://www.coindesk.com/learn/what-is-crypto-custody/

OVERVIEW OF THE NYDFS GUIDANCE

On January 23, 2023, the NYDFS issued recommendations on policies and controls for digital asset custodians to prevent future governance and operational issues: an industry letter entitled "Custodial Structures for Customer Protection in the Event of Insolvency."[2]

The NYDFS issued this guidance to emphasize "sound custody and disclosure practices to better protect customers in the event of an insolvency or similar proceeding," stressing the importance of equitable and beneficial interest always remaining with the customer.[3]

This letter sets forth best practices for digital asset custodians to follow. Not all the recommendations are in direct response to issues that have arisen during crypto-related bankruptcy cases; rather, the guidance also serves a preventative purpose. We provide a high-level summary overview of the guidance below:

Segregation of and Separate Accounting for Customers' Digital Assets. To maintain appropriate books and records, the NYDFS expects that the custodian will separately account for and segregate customers' digital assets from the corporate assets of the custodian and its affiliated entities, both on-chain and on the custodian's internal ledger accounts.[4]

Custodian's Limited Interest In and Use of Customers' Digital Assets. When a customer transfers possession of an asset to a custodian for safekeeping, the NYDFS expects that the custodian will take possession only for the limited purpose of carrying out custody and safekeeping services, and that it will not thereby establish a debtor-creditor relationship with the customer.[5]

2 https://www.dfs.ny.gov/industry_guidance/industry_letters/il20230123_guidance_custodial_structures
3 Id.
4 Id.
5 Id.

Sub-Custody Arrangements. A custodian may elect to arrange for the safe keeping of customers' digital assets through a sub-custody arrangement with a third party.[6] The NYDFS views a third-party arrangement as a material change to a custodian's business; as such, approval by the NYDFS is required before the implementation of any arrangement.

Customer Disclosure. A custodian is expected to (i) clearly disclose to each customer in writing the general terms and conditions associated with its products, services, and activities and (ii) obtain acknowledgment of receipt of such disclosure before entering into an initial transaction with the customer. Additionally, the guidance recommends that customer agreements clarify the parties' intentions to enter into a custodial relationship rather than a debtor-creditor relationship.[7]

Industry letters like these aim to clarify regulations and establish best practices for entities supervised by the regulator. Crypto companies are likely to follow this guidance if they want to stay in the regulator's good favor and avoid the NYDFS's enforcement powers—especially as the New York State Senate recently provided the regulator with an enhanced budget.[8] If the guidance is followed, it could impact which assets are determined to belong to the customer and which are determined to belong to the bankruptcy estate.

THE IMPACT ON A BANKRUPTCY ESTATE

A fundamental issue in any bankruptcy case is determining which assets are property of the estate. The commencement of a bankruptcy case creates a new entity called an "estate," which becomes the temporary legal owner of all of the debtor's interests in property.[9]

In a chapter 7 liquidation, a bankruptcy trustee is appointed to administer the estate.[10] In a chapter 11 case, unless a bankruptcy trustee is appointed for cause, the debtor's management in a business bankruptcy case remains in control, and the debtor becomes a "debtor in possession" with most of the same rights and responsibilities as a bankruptcy trustee.[11]

Determining whether an asset is property of the bankruptcy estate is critical for multiple reasons, including that estate property: (1) is subject to the automatic stay and thus not subject to creditor collection action absent leave of the bankruptcy court;[12] (2) may be sold or used by the debtor-in-possession or trustee, subject to court supervision;[13] and, perhaps most importantly, (3) is available for general distribution to creditors under a plan of reorganization. **If a custodial customer's digital assets are characterized as the property of the estate, that customer may never see those assets again or may receive mere cents on the dollar as an unsecured creditor under a plan of reorganization.**

The NYDFS guidance aims to preemptively address this property characterization problem by requiring an express custodian-customer agreement from the beginning of the commercial relationship. Absent an ambiguity in the contract requiring looking beyond the document, New York (and most states') law requires courts to look within the four corners of an agreement to determine the respective parties' rights—and, in general, bankruptcy courts look to state law for purposes of determining property interests.

By requiring both parties to the agreement to acknowledge that the customer, rather than the custodian, maintains an ownership interest over the assets at all times, the NYDFS aims to increase the certainty that a bankruptcy court would determine that a custody account belongs to the customer and is not part of the bankruptcy estate.

6 Id.
7 Id.
8 https://www.coindesk.com/policy/2022/04/09/new-york-senate-authorizes-nydfs-to-assess-crypto-companies/
9 11 U.S.C. § 541(a); Section 541 of the Bankruptcy Code defines the scope of the property of the estate, which generally includes all legal and equitable interests of the debtor in both tangible and intangible property as of the filing of the bankruptcy case.
10 11 U.S.C. § 704.
11 11 U.S.C. § 1101.
12 11 U.S.C. § 362(a)
13 11 U.S.C. § 363(b)

Relevant to issues uncovered during recent bankruptcies, having distinct processes in place so that custody account assets are not comingled with other assets would help to define ownership interests. In some recent crypto-related cases, digital assets meant only for custody accounts may have been comingled with digital assets intended for other types of accounts. This comingling led to uncertainty for customers and the bankruptcy court regarding which digital assets (if any) belonged to custody customers at the time of bankruptcy filing.

If a future platform were to follow the NYDFS guidance by maintaining separate accounts and implementing controls to disable comingling, digital assets within custody accounts would provide more specific protection to customers wishing to have their digital assets excluded from the bankruptcy estate.

CONCLUSION

This NYDFS guidance was published to encourage non-bankrupt custodians to implement strict controls and clarify the scope of their customer relationships. While it may be too little, too late for some customers, this guidance provides a path for custodians to firm-up their policies and prevent headaches and uncertainty in the event of a digital asset platform's future insolvency. Following this NYDFS guidance would likely increase the chances of custodial accounts being excluded from a bankrupt custodian's estate.

ARTICLE III

PRIVATE LAW OF STABLECOINS

KARA BRUCE
PROFESSOR OF LAW
UNIVERSITY OF OKLAHOMA
COLLEGE OF LAW

CHRISTOPHER ODINET
PROFESSOR OF LAW
UNIVERSITY OF IOWA
COLLEGE OF LAW

ANDREA TOSATO
ASSOCIATE PROFESSOR,
COMMERCIAL LAW
UNIVERSITY OF NOTTINGHAM
SCHOOL OF LAW

Presented on the next six pages are infographics highlighting the key points of the article, 'The Private Law of Stablecoins', written by law professors Kara Bruce (University of Oklahoma College of Law), Christopher K. Odinet (University of Iowa College of Law) and Andrea Tosato (University of Nottingham). Access the full article here

ABSTRACT

Stablecoins are one of the cornerstones of the crypto world. They've attracted significant attention over the past few years, ranging from Wall Street to kitchen table investors, and even the White House. Stablecoins are designed to offer a low-volatility alternative to crypto-assets like bitcoin. According to their proponents, stablecoins have the potential to transform payment systems, lay the foundations for sophisticated blockchain-based financial applications, and shift the economy towards the use of private money.

But how stable are these stablecoins, really? How much of the popular beliefs about these crypto-assets match their realities? Can they be relied upon in the way their many advocates claim?

This Article shows how unreliable and unstable this latest crypto innovation can be. It makes three important contributions to the legal literature in this nascent field. First, it introduces an innovative taxonomy that clarifies the various business models and issuer configurations across the stablecoin landscape. This taxonomy is not a mere upgrade to existing descriptive accounts of the stablecoin landscape. It offers a crucial tool to identify the flaws and dangers in the stablecoin market.

Second, through a comprehensive investigation of corporate records, audit reports, protocol white papers, and user terms of service, this Article reveals the yawning chasm between the narrative surrounding stablecoins and the reality of the underlying private law relationships. This is followed by a thorough analysis of the rights of stablecoin holders in the event of either a technological collapse or the bankruptcy of their issuers. This assessment reveals just how vulnerable stablecoin holders really are as they place their hopes (and sometimes their life savings) in this opaque and fragile market, rife with contradictory claims.

The final contribution of this Article is a menu of private ordering solutions that issuers can adopt as legal foundations for their stablecoins. The suggested transactional structures offer important insights regarding the bodies of private law—specifically, property law, contract law, and corporate law—required to forge a stablecoin that can be reliably traded and used as collateral and that bestow holders with strong proprietary rights which will not be lost in the event of the issuer's insolvency.

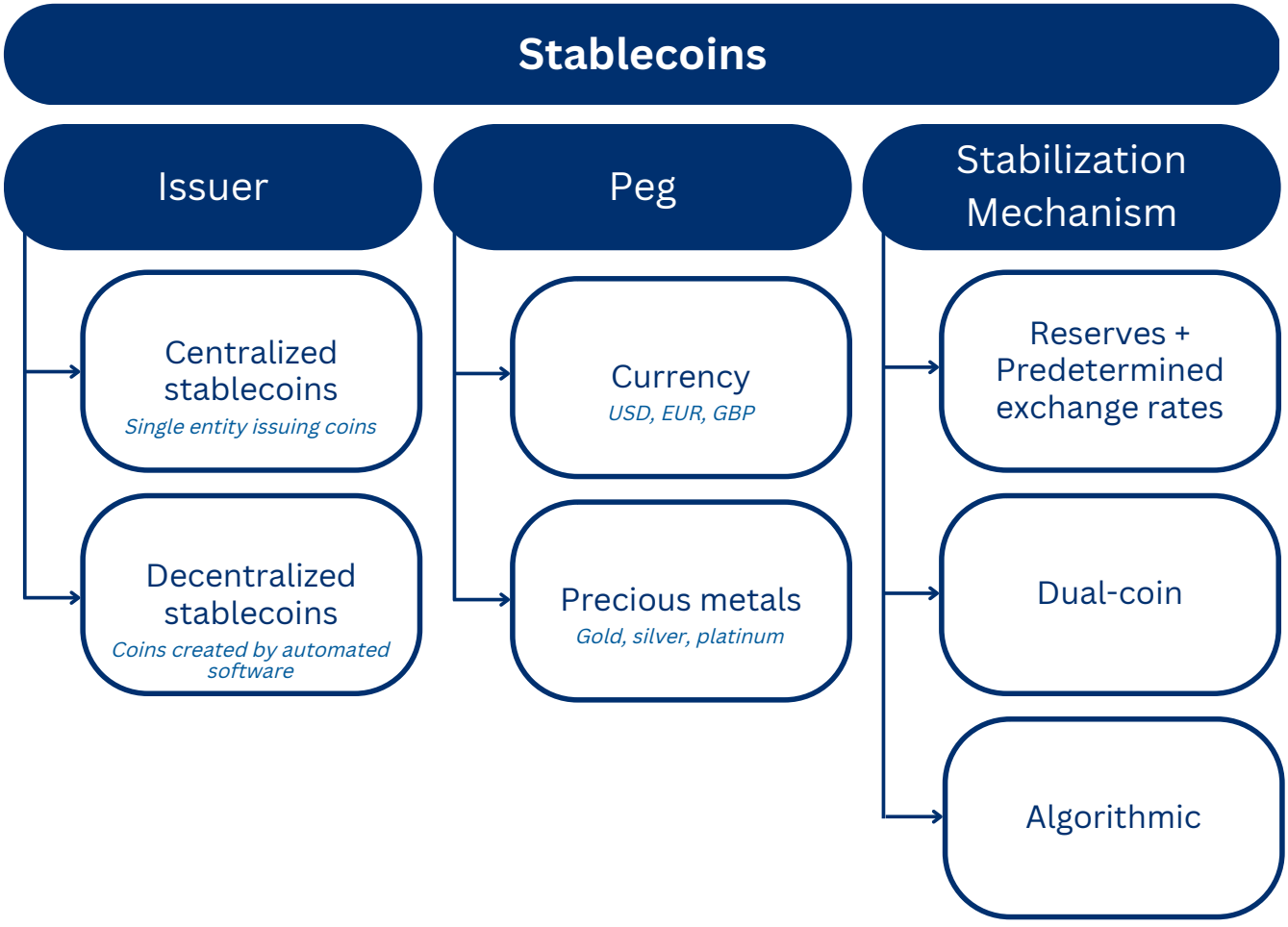
INFOGRAPHICS

I. STABLECOINS AND DECENTRALIZED FINANCE

Crypto-assets, especially payment coins (BTC, ETH), have very volatile prices. **Stablecoins are designed with the primary purpose of maintaining a stable price relative to a specified asset, or a basket of assets (referred to as the peg).**

There are three elements in a stablecoin: the issuer, the peg, and the stabilization mechanism.

- **ISSUER -** Can be decentralized (protocol) or centralized (organization)
- **PEG -** Most commonly pegged to a currency or precious metal
- **STABILIZATION MECHANISM -** The mechanism through which a stablecoin counteracts market volatility and maintains a stable price relative to its peg



Stablecoins are able to create opportunities for use cases that are not always available with cryptocurrency volatility.

USE CASES

Base Currency

- Base currency to trade other crypto assets
- Traders keep resources in DLT ecosystem, avoiding traditional financial institutions

---

- Forex – small and large scale
- Payment for goods and services in DLT ecosystem

Retail Transactions

DeFi

- Stablecoins are used as the currency of choice in yield farming

II. STUDY OF STABLECOIN TERMS OF SERVICE

The authors analyzed contracts used by seven stablecoin issuers and identified significant barriers to understanding what rights come with stablecoin ownership:

- Use of "sign-in wrap" contracts
- Terms of Service are often difficult to find on a website
- Each issuer uses different labels to refer to the terms, eg., “Legal Terms," “Legal & Privacy, ”User Agreements"
- Not always available in one location, sometimes the terms are chopped up and spread across multiple website pages

The chart below details each of the seven issuers' approaches to their legal agreements.

	USDT: Tether	USDC: Circle	USDP/BUSD: Paxos	TUSD: Techteryx	GUSD: Gemini	HUSD: Stable	DAI: MakerDAO
Unequivocal redemption?	Refusal/ delay in some circumstances and/or at discretion				Yes	Refusal at discretion	Yes - but not for fiat
Account required to redeem?	Yes						
Disclaimer of warranties?	Expressly Disclaim all reps & warranties						Disclaims that tech will be un-interrupted or error free
Exculpatory provision?	Yes						N/A – issuer not an entity
Unclaimed property surrendered to govt due to inactivity?	Not mentioned	Yes		Not Mentioned	Yes		No
FDIC pass-through insurance?	No		Opt-in, conditions apply	Not mentioned	Conditions apply	Unclear	No
Issuer discretion in use of reserve assets?	Yes	In interest-bearing accounts or yield-generating instruments	Unclear			Yes	No – except for auto-liquidation
Capacity in which assets are held?	Property of the Issuer	Property of the Issuer	Unclear; possibly property of the coinholder	Unclear	Unclear; possibly property of the coinholder	Unclear	Self-Custody

III. WHEN STABLECOINS FAIL

Stablecoins can raise many risks for coinholders.

Decentralized

- If the software protocol in control of the stablecoin fails, coinholders are unlikely to have any recourse
- There is likely no person against whom to claim, let alone limited or non-existent contractual rights
- Even if there are assets backing the stablecoin, recovery is likely to be technologically difficult if not impossible

Frax FRAX

Dai DAI

Dual-coin

- These stablecoins are not backed by reserves - they are dependent on market participants attributing value to the secondary coin that serves a volatility absorption buffer
- Coinholders implicitly accept the risk that their stablecoin will become worthless if the secondary coin falter

USDX [Kava] USDX

TerraClassicUSD USTC

Iron IRON

Asset-backed

- Holders of asset-backed stablecoins typically have a contractual counterparty
- Holders also have a right to redeem their coins from a large pool of reserve assets
- Whether holders can reach these assets if a coin issuer fails depends on the nature of the coinholders' rights in the reserves, which is often unclear

USD Coin USDC

Gemini Dollar GUSD

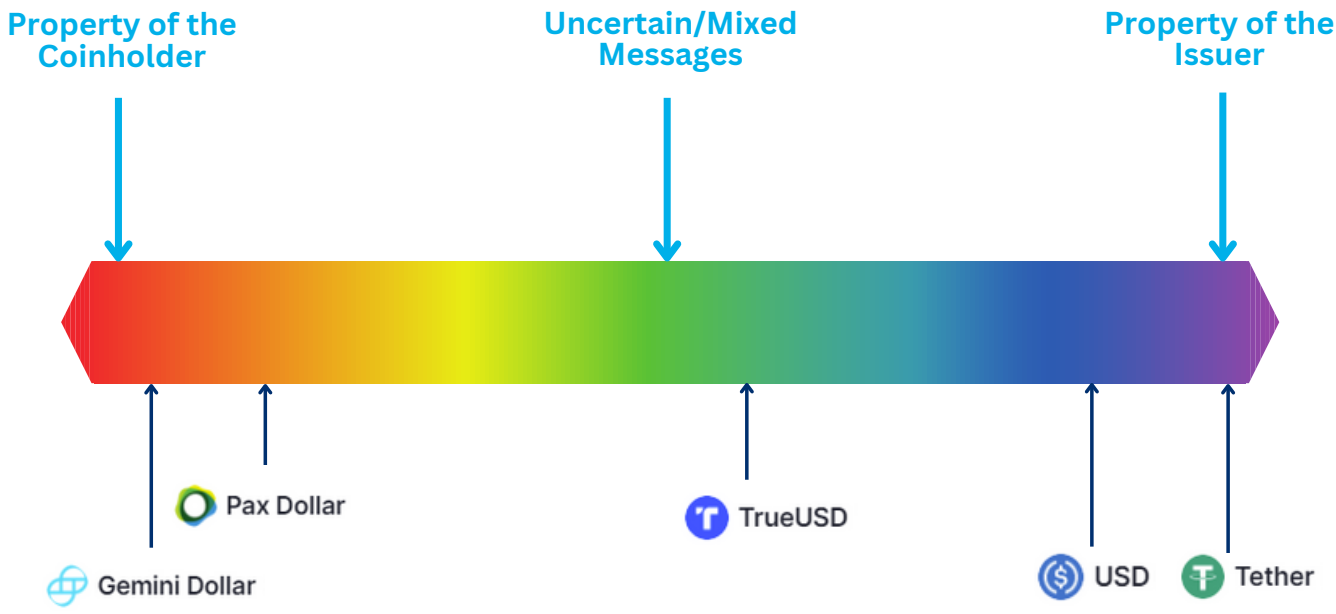
Tether USDT TrueUSD TUSD

Binance USD BUSD

Pax Dollar USDP

This illustration shows on a spectrum how stablecoin issuers approach reserve assets.

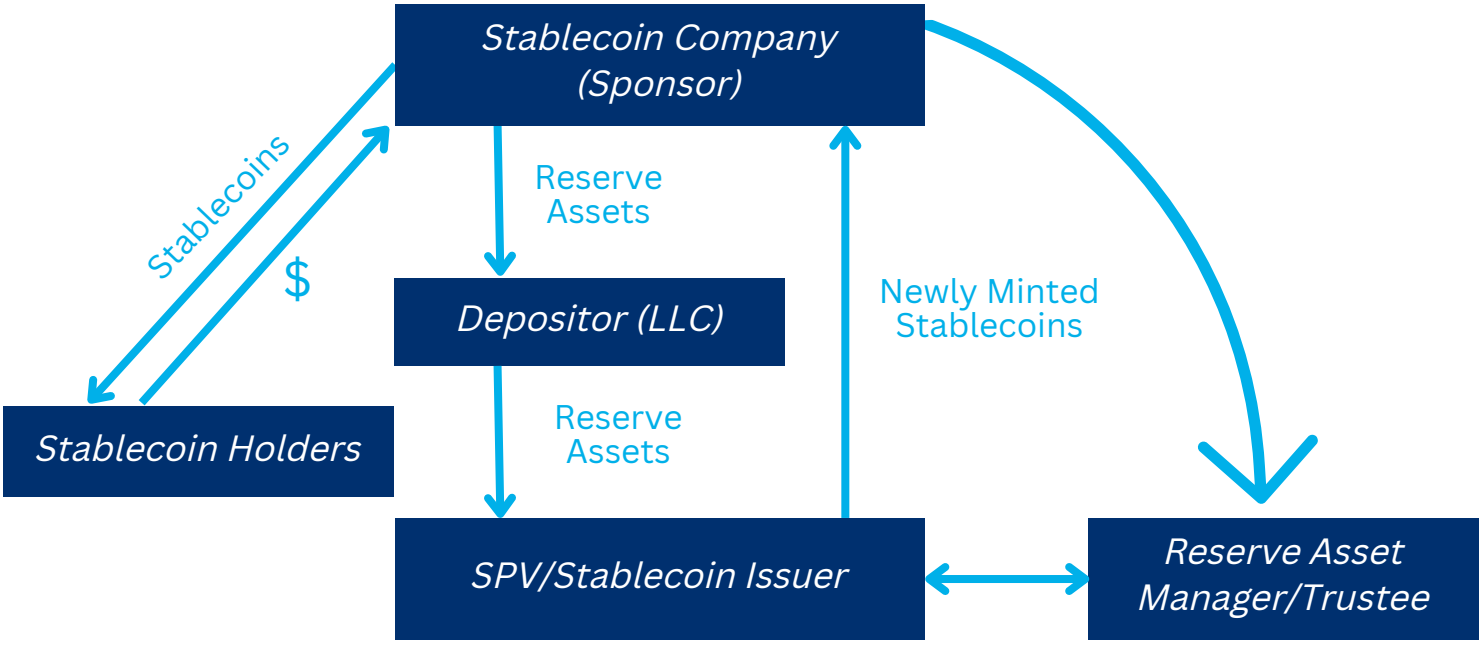
WHO OWNS THE RESERVE ASSETS?



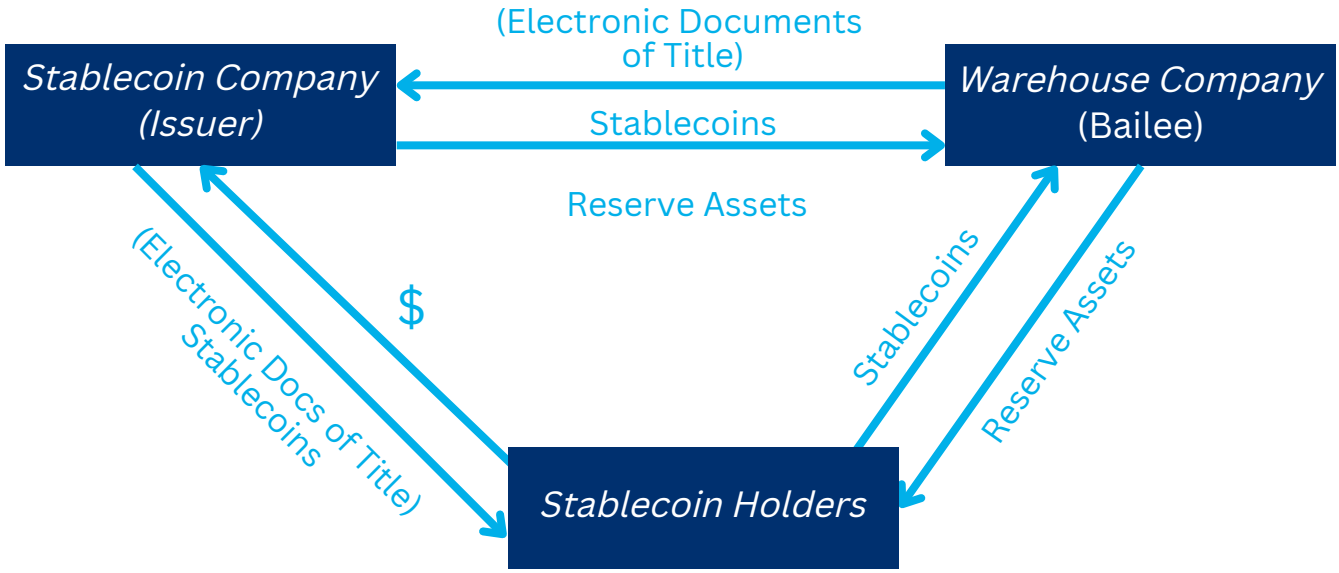
IV. POLICY IMPLICATIONS AND PRIVATE LAW SOLUTIONS

Below are proposed solutions for reserves and documents of title processes.

BANKRUPTCY REMOTE RESERVE STRUCTURE



UCC ARTICLE 7
ELECTRONIC DOCUMENTS OF TITLE



CONCLUSION

Key Takeaways

- Stablecoins are a central component to the crypto world.
- There is often a gap between the stablecoin narrative and the Issuer's Terms of Service.
- An exploration of the nature of stablecoin holders' rights in the bankruptcy process reveals important weaknesses in the stablecoin system, demonstrates the continued relevancy of private law in the digital age, and highlights the vulnerability of stablecoin tokenholders.
- A complete understanding of the private law dimension of stablecoins is necessary for balanced and sophisticated regulatory solutions.

ARTICLE IV

THE DEVELOPING REGULATORY LANDSCAPE FOR CRYPTOASSETS IN THE EU AND UK

LAURA DOUGLAS
SENIOR ASSOCIATE
CLIFFORD CHANCE

INTRODUCTION

The regulatory landscape for cryptoassets is set to change in both the EU and the UK, through the introduction of new, comprehensive regulatory frameworks for cryptoasset service providers. The EU Markets in Cryptoassets Regulation (MiCA) is expected to be published in the EU Official Journal by Summer 2023 and will introduce a pan-EU regulatory framework for the issuance of, intermediating and dealing in, cryptoassets. The shape of the UK framework is still under consultation, though the UK is coming under some pressure to provide clarity on the scope of the new regime quickly, to provide firms with certainty they need and details of both regimes are yet to be fleshed out by regulators starting later this year.

THE STORY SO FAR

At present, there is no specific UK or EU-wide[1] regulatory regime for cryptoassets beyond anti-money laundering (AML) related requirements that implement international Financial Action Task Force (FATF) recommendations.

In particular, both the UK and EU have introduced registration regimes for cryptoasset exchange providers and custodian wallet providers, who are subject to ongoing AML-related obligations, such as requirements to take steps to identify and manage the risks of money laundering and terrorist financing. These include establishing appropriate policies, controls and procedures, and carrying out the requisite customer due diligence.

The UK Financial Conduct Authority (FCA) has applied a particularly high bar in vetting cryptoasset firms seeking registration for AML purposes, approving only 15% of applications submitted as of January 2023.[2]

Beyond AML-related requirements, the UK's current approach to regulating cryptoassets is articulated in the Final Guidance on Cryptoassets[3] (the Final Guidance), published by the FCA in July 2019.

This approach requires a case-by-case analysis of the relevant cryptoasset's substantive characteristics to determine whether or not it falls within the perimeter of the existing regulatory framework.

1 Although some EU jurisdictions such as France have introduced national regimes for the regulation of cryptoasset service providers.

2 See FCA webpage "Cryptoasset AML/CTF regime: feedback on good and poor quality applications" at https://www.fca.org.uk/cryptoassets-aml-ctf-regime/feedback-good-poor-quality-applications

3 FCA, Guidance on Cryptoassets Feedback and Final Guidance to CP19/3 (Policy Statement, PS19/22) <https://www.fca.org.uk/publication/policy/ps19-22.pdf> Accessed December 2022.

For those types of cryptoassets that do fall within the regulatory perimeter, different regulatory rule sets may apply depending on whether the cryptoasset is characterised as a transferable security, a deposit, electronic money (e-money) or another type of regulated financial instrument.

Unregulated tokens include all other types of cryptoassets which are not treated as regulated financial instruments or products. In general, this means that firms carrying on activities relating to unregulated tokens fall outside the UK regulatory perimeter. In practice, many "*cryptocurrencies*" marketed to consumers currently fall within the category of unregulated tokens.

A similar approach is taken under existing EU-level regulation, to determine whether cryptoassets meet existing definitions of regulated financial instruments under the EU Markets in Financial Instruments Directive (MiFID2) or qualify as e-money under the E-Money Directive.

INTRODUCING MICA, A PAN-EU CRYPTOASSET REGULATORY FRAMEWORK

Just over two years after it was first proposed, the agreed text of MiCA was released in late 2022. MiCA aims to create an EU regulatory framework for the issuance of, intermediating and dealing in, cryptoassets. It will introduce licensing and conduct of business requirements as well as a market abuse regime with respect to cryptoassets.

MiCA applies with respect to "cryptoassets", which are defined very broadly as *"a digital representation of a value or a right that uses cryptography for security and is in the form of a coin or a token or any other digital medium which may be transferred and stored electronically, using distributed ledger technology or similar technology"*, with certain specific carve-outs.

For example, MiCA does not apply to security tokens which would quality as financial instruments for the purposes of MiFID2, deposits, securitisation positions, insurance or pension products. This means that firms engaging in cryptoasset activities will still need to consider whether they will fall under the MiCA definition of "cryptoassets" or whether they are subject to another regulation.

MiCA creates a broad regulatory framework for cryptoassets in the EU which:

- regulates the issuance of, and admission to trading of, cryptoassets, including transparency and disclosure requirements;
- introduces licensing requirements for cryptoasset service providers, issuers of asset-referenced tokens (ARTs) and issuers of electronic money tokens (EMTs);
- introduces regulatory obligations applicable to issuers of ARTs and EMTs and cryptoasset service providers, including consumer protection rules for the issuance, trading, exchange and custody of cryptoassets;
- creates a market abuse regime prohibiting market manipulation and insider dealing; and
- sets out enforcement powers available to national regulators.

Many requirements under MiCA are broadly similar to requirements under the existing EU financial services regimes, including requirements relating to disclosures, governance and licensing. For further detail on MiCA, please see the briefing "*Crypto Regulation: the Introduction of MiCA into the EU Regulatory Landscape*".[4]

MiCA is expected to be published in the EU Official Journal by Summer 2023. It will "enter into force" 20 days later, which will allow the European Securities and Markets Authority (ESMA) and the European Banking Authority (EBA) to develop the various technical standards and guidelines envisaged under MiCA, which will flesh out the details of the rules.

4 https://www.cliffordchance.com/briefings/2022/12/crypto-regulation--an-introduction-of-mica-into-the-eu-regulator.html

Provisions relating to ARTs and EMTs will formally start to apply from 12 months after entry into force (likely mid-2024) and remaining provisions will apply from 18 months after entry into force (likely towards the end of 2024). Firms are already starting to prepare for the implementation of MiCA, including in some cases positioning themselves to benefit from certain grandfathering and provisions that will give firms already carrying on cryptoasset activities in the EU more time to apply for authorisation under MiCA.

MiCA does not provide for a separate third country regime, so non-EU firms will have to obtain full authorisation to provide services within the EU (other than cross-border services provided on a strict reverse solicitation basis). **This means that non-EU firms will need to assess whether and how their activities will be caught by MiCA and what restrictions will apply. Depending on the outcome of that assessment, firms may consider whether seeking an authorisation in an appropriate member state ahead of MiCA taking effect would be worthwhile to benefit from the transitional arrangements and to avoid post-MiCA delays.** Firms that wish to do so must act swiftly as authorisations can take many months to secure.

UK'S PROPOSED COMPREHENSIVE REGULATORY REGIME FOR CRYPTOASSETS

The UK has so far lagged behind the EU in developing its cryptoasset regulatory framework. However, it is now seeking to catch up, as the Financial Services and Markets Bill (FSMB) , which is expected to become law in the Spring, will introduce new powers for HM Treasury (HMT) to bring cryptoassets within the scope of the UK financial services regulatory perimeter.

On 1 February 2023, HMT published its long-awaited consultation[5] on a comprehensive regulatory regime for cryptoassets other than fiat-referenced stablecoins. This latest consultation on regulation of wider (non-stablecoin) cryptoasset activities builds on previous discussion papers and consultations, including a January 2021 consultation[6] which focused on stablecoin regulation. It also complements other proposals in the FSMB to introduce a regime that will allow for the regulation of "digital settlement assets", which are defined as fiat-backed stablecoins which are used for payments.

In its latest consultation, HMT indicates that it intends to create various new regulated activities relating to cryptoassets. This means that firms would need to be authorised (or exempt) under the Financial Services and Markets Act 2000 (FSMA) in order to carry on those activities by way of business in (or into) the UK. Many of these proposed activities mirror, or closely resemble, regulated activities under the existing FSMA regime, though are also some novel cryptoasset activities proposed.

HMT also indicates it may use the new "designated activities regime" (DAR) that will be introduced under the FMSB to regulate certain activities relating to cryptoassets where it is not necessarily appropriate to impose licensing requirements. Similar to MiCA, HMT's proposals include a regime for the issuance, offering and admission to trading of in-scope cryptoassets and a cryptoassets market abuse regime, where certain rules may be introduced using the DAR.

The definition of "cryptoasset" for this purpose comes from the FSMB and is extremely broad. HMT indicates that it may introduce certain carve outs from the definition for the purpose of the new regulatory regime, but has not yet provided detail of any such carve outs.

5 HMT, "Future financial services regulatory regime for cryptoassets Consultation and call for evidence" https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1133404/TR_Privacy_edits_Future_financial_services_regulatory_regime_for_cryptoassets_vP.pdf

6 HMT, "UK regulatory approach to cryptoassets, stablecoins, and distributed ledger technology in financial markets: Response to the consultation and call for evidence" O-S_Stablecoins_consultation_response.pdf (publishing.service.gov.uk)

As such, the expected scope of the new UK cryptoasset regulatory regime remains hazy.

This latest consultation forms part of "Phase 2" of the UK's phased approach to cryptoasset regulation – with Phase 1 being implementation of the digital settlement assets regime for regulation of fiat-backed stablecoins. Once the FSMB gains Royal Assent (expected in Q2 2023) HMT will be able to make secondary legislation covering the detail of the regime. The Financial Conduct Authority (FCA) will then need to consult and make the wide range of relevant rules to bring the regulatory regime into operation.

These are expected to include minimum capital, liquidity and other prudential requirements for firms requiring authorisation under the new regime, as well as ongoing conduct of business rules for authorised firms and rules on admission and disclosure requirements where cryptoassets are traded in the UK. **Firms that are already authorised under FSMA would also need to apply for a variation of their permissions to include newly regulated cryptoasset activities.** However, details of how authorisation and variation of permission processes are expected to operate (and whether there would be any grandfathering for firms that have already registered under the MLRs) have not yet been published.

OTHER REGULATORY DEVELOPMENTS

UK financial promotions regime for cryptoassets

Marketing of unregulated cryptoassets in the UK is not currently subject to FCA regulation and is overseen only by the Advertising Standards Authority (ASA). However, HMT has published draft regulations that would bring certain qualifying cryptoassets[7] into the scope of UK financial promotions restrictions.

The effect of the rules would be that, unless they are exempt, businesses that intend to make financial promotions in relation to qualifying cryptoassets would need to have their promotions approved by an authorised person under FSMA. The regime will apply even where the person communicating the financial promotion is based overseas, and regardless of how it is communicated (including online or on social media).

Due to industry feedback, HMT has proposed introducing a temporary exemption to Section 21 FSMA, which will enable cryptoasset businesses that are registered with the FCA under the MLRs (but who are not otherwise FSMA-authorised persons) to communicate their own financial promotions in relation to qualifying cryptoassets.

The FCA has also consulted on rules for the promotion of cryptoassets and other high-risk investments that will apply to authorised firms making (or approving) cryptoasset promotions. The final rules for cryptoassets have not yet been published thought FCA has indicated that those rules will closely follow the final rules for high-risk investments, which were published in August 2022 and came into force on 1 February 2023.[8] It is not yet clear exactly when the new rules will be implemented, although the FCA warned firms to start preparing now for the new regime[9] in a statement published in February 2023.

Central bank digital currencies

Like most jurisdictions, both the UK and EU have been exploring whether and how to introduce a central bank digital currency (CBDC). Following preliminary consultations and exploratory work, the Central Bank launched an investigation in October 2021 into how a digital euro could be designed and distributed, as well as the impact it could have on the market. This investigation phase is expected to conclude in autumn 2023.

7 HMT has indicated that it will define qualifying cryptoassets as "any cryptographically secured digital representation of value or contractual rights which is fungible and transferable".

8 FCA, "Strengthening our financial promotion rules for high-risk investments and firms approving financial promotions" PS22/10: Strengthening our financial promotion rules for high-risk investments and firms approving financial promotions (fca.org.uk)

9 FCA, "Cryptoasset firms marketing to UK consumers must get ready for financial promotions regime" Cryptoasset firms marketing to UK consumers must get ready for financial promotions regime

In the UK, the Bank of England and HMT launched a CBDC Taskforce in April 2021 and most recently in February 2023 published a consultation on the design of a potential UK retail CBDC. This latest consultation paper sets out analysis conducted by HMT and the Bank of England to date on the potential case for a UK retail CBDC and seeks feedback on the key features of a potential retail CBDC model.

Neither the UK nor the EU have yet taken a firm decision on whether to actually go ahead and develop a CBDC. However, if they do go ahead these would be major infrastructure projects spanning several years. Therefore, it is expected that the earliest "go-live" date for a UK or EU CBDC would be towards the end of this decade. Further phases of work would also be needed to flesh out the role of intermediaries in providing CBDC wallets or other services, and any regulatory regime that would apply to them.

Travel rule

Both the UK and the EU have also published legislation implementing the "travel rule" set out in FATF Recommendation 16,[10] requiring that cryptoasset transfers must be accompanied by certain identifiable information on the transferor and transferee. The UK has already published its implementing legislation[11], which will apply from 1 September 2023. Registered cryptoasset service providers under the MLRs will need to prepare now for its implementation. The EU has also agreed the text of its implementation of the travel rule for cryptoasset transfers and it is expected to be published in the Official Journal alongside MiCA later this year, and apply from the same time as MiCA. Again, EU cryptoasset service providers will need to prepare to comply with these new requirements.

10 See the FATF Recommendations at https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html

11 The Money Laundering and Terrorist Financing (Amendment) (No. 2) Regulations 2022, which will insert a new Part 7A MLRs setting out these requirements.

ARTICLE V

FIRST STEP TOWARDS THE RIGHT DIRECTION: REGULATORY GUIDANCE ON SECURITY TOKENS IN KOREA

JOON YOUNG KIM
SENIOR ATTORNEY
KIM & CHANG*

MOONI KIM
FOREIGN ATTORNEY
KIM & CHANG**

INTRODUCTION

The potential treatment of digital assets as securities is not a new topic in Korea. The door for the regulators to apply the Financial Investment Services and Capital Markets Act (the "Capital Markets Act"), the securities law of Korea, to digital assets has been wide open, but the question of "how" has always followed with respect to the identification and treatment of such tokens.

On February 6, 2023, the Financial Services Commission of Korea (the "FSC") finally provided answers by releasing the overhaul plan for security tokens (the "Plan") with the regulatory goal of both fostering innovation and protecting investors. The Plan is the first and long-waited regulatory guidance on security tokens in Korea, illustrating how the regulators understand and intend to regulate security tokens.

The Plan defines a "security token" as a new form of security that is digitized using distributed ledger technology and announces that security tokens must be issued or otherwise distributed in accordance with the Capital Markets Act.

Accordingly, digital assets that are not security tokens are to be governed by the Act on Reporting and Using Specified Financial Transaction Information, currently in effect, and the Framework Act on Digital Assets, to be enacted later.

The details of the Plan are as follows.

HOW TO IDENTIFY SECURITY TOKENS

In the Plan, the FSC clarifies that the obligation to determine whether a digital asset constitutes a security falls on the market (and not the regulators). Such a determination must be made on a case-by-case basis and in the totality of circumstances, including terms and conditions of any underlying agreements, actual execution and details of any profit-sharing, whether explicit or implicit.

Out of the six types of securities under the Capital Markets Act, the investment contract securities-type is most relevant to security tokens. **The Capital Markets Act defines investment contract securities as "contractual rights in which a specific investor invests money, etc., in a joint business between such investor and a third party and any profits or losses are attributed mainly as a result of such joint business carried out by such third party" which is similar to the US *Howey* test.**

* Disclaimer: The view and opinions expressed in this article are those of the authors. They do not purport to reflect or imply the opinions or view of Kim & Chang.

** Id.

The Plan highlights that the element of "mainly as a result of such joint business carried out by such third party" would be satisfied with efforts of the third party (i.e., issuer) that are indispensably significant to determine the success or failure of the relevant business and/or material information asymmetry.

In addition, any promise to attribute profits from the performance of the relevant business would constitute "contractual rights to gain or lose profits as a result of joint business". The issuer's mere promise to implement certain smart contracts (to which the issuer is not party) with the investor's right embedded would satisfy this element. In other words, any explicit or implicit commitment to distribute profits, whether directly or indirectly, should be sufficient.

The Plan further illustrates that it would be highly likely to be a security token: (i) if the investor of such token gets any equity interest, dividend right based on the performance of the business or a right to claim distribution of residual assets; (ii) if the issuer attributes any profit generated from the business to the investor; or (iii) despite any appearance of paying consideration for certain activities, if such payment to the investor has the actual effect of distributing profits.

On the other hand, it would be highly unlikely to be a security token: (i) if there is no issuer with obligations correlated with any investor right; (ii) if there is no right, including any right to profit, embedded with the token ownership; (iii) if such token is issued and used for goods or services; (iv) if such token is issued as a payment or exchange means without any promise for redemption; or (v) where there is no information asymmetry with respect to the business in favor of the issuer.

The FSC added that while it is difficult to uniformly determine whether a digital asset would constitute a security, most digital assets that are currently traded on virtual asset exchanges appear unlikely to fall under the definition of "securities" under the Capital Markets Act.

We expect the Plan to mitigate the unpredictability around classification of security tokens.

HOW TO TREAT SECURITY TOKENS

Once security tokens are identified, the nexOnce security tokens are identified, the next question is how they should be treated under the Capital Markets Act and other relevant laws. The FSC has made several proposals.

According to the FSC, the proposals would undergo legislative review before the National Assembly and the Government in 2023. While there is no guarantee that the proposals will be enacted as proposed, the Plan is likely to be granted a certain level of deference.

First, the Electronic Securities Act will be amended to cover security tokens under the definition of electronic securities and thereby recognize the distributed ledger technology as a means of recording information on the creation, change, and extinguishment of securities rights in a public register. Additional verification requirements and fraud preventative measures will be implemented.

Accounting for the separate ecosystem around tokens, the FSC seeks to introduce an "issuer account management agent" for which any qualified person could register and issue security tokens on its own. Issuance of security tokens via securities firms like any other securities will remain available for those that do not qualify as issuer account management agents.

Moreover, issuance of security tokens will be deemed as a public offering unless all investors are accredited. The existing threshold for small public offerings will be raised from KRW 1 billion to KRW 3 billion (around USD 0.8 million to USD 2.3 million) while a new type of small public offerings with a cap of up to KRW 10 billion (around USD 7.6 million) but subject to more stringent investor protection measures will be made available.

Distribution of security tokens will generally follow the existing system under the Capital Markets Act except that a new license requirement for over-the-counter brokerage and a new listed-securities market for investment contract securities will be established.

CONCLUSION

The release of the Plan has at last clarified the lingering question of how to identify digital assets that are securities. The Plan also forecasts the likely treatment of security tokens under the Capital Markets Act and related laws.

Without the Plan, everyone had been cautious not to step over the invisible line for incidental violations of the Capital Markets Act. Now, the Plan affords predictability for both existing and new players to explore the market.

Going forward, some tokens may become delisted from exchanges and new tokens may invite scrutiny from related parties, ranging from the issuer, to the exchanges to the investors. Innovative types of investments around security tokens and new market players like issuer account management agents and over-the-counter brokers dealing with security tokens will likely emerge.

This is not to say that there is no more question remaining around security tokens. As the FSC acknowledged, everyone needs more precedents to accumulate in this industry and the Plan, while significant, is only the first step towards the right direction.

ARTICLE VI

DECENTRALISED AUTONOMOUS ORGANISATIONS (DAOS): WHAT ARE THEY? AND CAN THEY BE PARTIES TO A CLAIM?

BEN HITCHENS
PARTNER
CMS LAW

OLIVER ROBERTS
TRAINEE SOLICITOR
CMS LAW

INTRODUCTION

On 16 November 2022, the UK Law Commission announced that it will begin work on a scoping study into Decentralised Autonomous Organisations ("DAOs"). The review will shed light on how DAOs are to be treated under UK law, which is part of the UK's greater drive to become a global cryptoasset technology hub.

DAOs are a strange (relatively) new entity, whose legal status is currently something of a mystery. Their structure does not quite fit within any current model of legal entity. They are projects that operate almost exclusively over the internet, whose participants make decisions collectively without anyone directly in charge. DAOs have been used in an array of areas in the crypto-sphere, for instance as investment groups, to fundraise for new projects, and as software development and social clubs.

For those without a foothold in the crypto sphere, DAOs have sprung seemingly out of nowhere. **In the past year alone, DAO treasuries reported surging from $400 million of crypto funds at the start of 2021, to an estimated $12.5 billion in January 2023.** DAOs are a particularly popular model for new crypto and metaverse ventures and are seen by crypto enthusiasts as the tonic to the concentrated power of Big Tech for their democratic and decentralised structures. As such, they are deeply embedded in the culture and ethics underpinning web-3.

New types of organisations are rare, and it often takes a long time for the law to catch up. In the meantime, there will inevitably be uncertainty whenever disputes arise involving a DAO. In particular, it is difficult to determine who can bring a claim on the DAO's behalf or, in the event that the DAO itself has committed a wrongful act, serve as a Defendant. The huge market share gained by DAOs in the past year suggests we are destined to see many more disputes, which all begs the question: What are DAOs? And can they be parties to a claim?

WHAT EVEN IS A DAO?

That's a good question. **DAOs are the crypto sphere's version of a joint enterprise. The simplest definition is that they are a group making decisions towards a common goal without a centralised command structure.** Instead, decisions are made by a consensus of the members of the DAO. They are, in many ways, a company with voting buttons instead of a board of directors.

What a DAO looks like in reality can be a little more complicated. Most DAOs' decision-making is built into their structure through a complex web of smart contracts. Voting rights may be conferred by crypto-coin ownership: the more you own, the greater your say in the future direction of the DAO. All of the voting mechanisms are pre-determined by the smart contract, which acts as the DAO's version of a constitution. Most follow an open-source set of smart contracts on the Ethereum blockchain, which are then modified to fit with the specific needs of the DAO. In this respect, coin holders look somewhat like shareholders: they often own a proportional share of the DAO and have a corresponding voting power.

However, unlike a company, there is usually minimal or no delegation of decision-making to an executive board. Whilst some have committees to carry out various functions, these usually do not exercise high degrees of autonomy and usually only execute on the decisions of the majority. Voting can cover a vast array of areas, which will vary from DAO to DAO. Tokens can give voting rights over wide issues, such as the governance or economic trajectory of the DAO, or more narrow issues such as whether to hire a contractor for a specific task or to implement a new feature into their products.

This is not to say that every DAO is structured in the same way: some DAOs are much more like an online members' club whose decision-making is made through a specific forum or social media channel. However, DAOs of this type tend to have crude voting systems, which usually indicate they are less sophisticated and economically active than DAOs governed through smart contracts, thereby reducing the likelihood that they will become involved in disputes.

CAN A DAO BE PARTY TO A CLAIM?

First thing's first, a comment on why this is important. Disputes involving crypto and metaverse companies are becoming increasingly common, particularly in relation to intellectual property. **The culture and ethos behind Web3 is particularly recalcitrant to commercial monopolies and intellectual property is designed to protect just that.**

We have seen an explosion of parodies of famous trade marks, including the widely reported MetaBirkin case and even a parody of McDonald's involving metaverse Pigeon McNugget shoes. Irreverence and hype often translate into significant boosts in sales, which has significantly fuelled (often deliberate) trade mark infringement in a digital context.

Metaverse organisations, including DAOs, also have a significant interest in figuring out how to protect their intellectual property in a digital setting. The damage that can be caused by copycat products and fake coin scams in particular can be extremely damaging to a metaverse brand, particularly as trust and transparency are considered key in the industry.

With the growing interest and money being poured into the metaverse, particularly by tech giants such as Meta, Alphabet and Amazon, we expect many cases of patent, trade mark, copyright and design infringement to follow. If you are considering expanding your business into the crypto space, it is becoming increasingly inevitable that you will eventually have dealings with a DAO. As part of that process, your due diligence should include assessing how you might recover your losses if things go wrong. On the other side of the coin, the number of new start-ups electing to operate as DAOs is growing rapidly. Those enterprises will need to know exactly how they can bring legal proceedings should their valuable IP be misappropriated.

Bringing a claim on behalf of or against a DAO could be tricky. Understanding your DAO's structure and how you might bring a claim is important at the outset, otherwise you run the risk that service may not be valid. On the other hand, the main issue around pursuing a DAO is figuring out who to take action against. If voting rights are established by the ownership of a publicly traded coin, tracking down and serving on all of the owners is logistically difficult, if not impossible: the speed at which crypto transactions occur means that, between postage and receipt, the ownership may have changed hands numerous times.

However, if you serve on the DAO itself (presuming that you find a suitable postage address), you run the risk that the service is not valid and that your claim fails at the first hurdle. Recently, we have seen service by NFT arise as one solution to this problem. However, it nonetheless requires a proper understanding of how the DAO operates, to ensure that the correct token holders are served.

From a legal standpoint, figuring out exactly what a DAO is appears to be a tricky question and there currently is no clear answer. The characteristic part of a DAO is how it makes decisions, not what it does or how it is structured. This makes DAOs a broad church of ventures and activities and no single rule is likely to apply in all cases. Whilst the precise nature of DAOs will be a matter for the courts or Law Commission, there are a few questions which can be helpful to consider in practice:

Is the DAO actually a company? Generally speaking, no, a DAO is unlikely to be a company. The limited constitutions and decentralised structure mean they are not compliant with the UK's Companies Act and therefore they are unable to register in the UK. However, some states in the US allow certain DAOs to register as limited liability companies. Whilst take-up within the sector has been poor as it is seen as going against the grain of web-3's decentralised ethos, this is nonetheless worth investigating in the first instance.

Furthermore, a company may have some features or connections which operate as a DAO, whilst nonetheless being incorporated. For instance, the Bored Ape Yacht Club ("BAYC") has an associated DAO governed by ownership of ApeCoin, which makes decisions about the future direction of the NFT, ownership perks and other key points of economics and governance. However, BAYC's creator, Yuga Labs, is a company incorporated in Delaware. Whilst the DAO makes decisions to which Yuga Labs then usually complies, it is nonetheless a company which has elected that a portion of its decision-making should be made through a DAO.

Therefore, whilst the general rule is that DAOs are not companies, there may be a company associated behind a DAO which could be a valid party to proceedings.

Is the DAO a partnership? Under UK law, a partnership involves two or more people coming together with a view to making a profit. One current legal uncertainty is whether coin ownership can amount to an intention 'to make a profit'. This will in part be a matter of context, which will depend on the structure and purpose of the DAO.

For DAO investment clubs, the activity itself may make a strong case that they are acting as a partnership. Where DAOs confer voting rights without ownership rights, then those structures seem less likely to be partnerships: the decisions are being made by people who have no stake in any potential profit. However, even if collective ownership is conferred with voting rights, it is still necessary to show that there is an intention to make a profit.

Many DAO projects have broad social aims, such as developing new technologies, increasing access to decentralised banking or solving inflationary pressure. Whilst some coin owners will have bought their coins speculatively, hoping that they will appreciate in value, many others will be invested in the projects for non-financial purposes. Figuring out motive in an anonymous, decentralised system is particularly problematic and it is not clear how the courts would go about doing so. It will remain a point of uncertainty until someone is brave enough to test the issue in court or until the outcome of the Law Commission's study.

If a DAO is a partnership, then the individual partners are jointly and severally liable: in other words, the claimant can pursue any one of the participants for the entirety of their loss, and it is for that person to seek a contribution from the others. This is particularly helpful or concerning where there are members with deep pockets, such as founders or institutional investors, depending on which side of the table you are sitting on.

Is the DAO an unincorporated association? An unincorporated association is a fancy term for something we are all familiar with: a group of people brought together for an activity, such as a sports club. They are unincorporated, meaning that they do not have their own legal personality: they cannot own property, register for loans or have standing in court. This means that they cannot bring a claim against any party, but also that parties cannot bring claims against them. If a DAO is an unincorporated association, that could prove to be a major headache for any rightsholder seeking to enforce their intellectual property rights: there will be no legal entity encompassing the 'DAO', instead the individual members will be responsible for their own actions.

How this would work in the context of a dispute with a DAO is unclear. It may mean that all of those who participated in a vote which led to infringement are liable. It may be possible to claim that they are jointly and severally liable, as with a partnership, but this is a complex legal argument which will depend on demonstrating that the individual participants voted in a fashion that led to the infringement.

As discussed earlier, identifying who was involved in a vote and tracking them down could be logistically difficult where there are large numbers of participants. In fact, the complications surrounding the service of a DAO were a central issue in a recent case before a Californian court bought by a regulator against Ooki DAO. By implicating the DAO in regulatory action, the court considered whether the regulator would have to serve on all of the members in order to be valid under the laws of California. It held that it was sufficient to serve on the founders of the DAO as identifiable coin owners in the US, although it is unclear whether the reasoning behind the decision would also apply in the UK if the DAO was not a partnership.

Overall, from a litigation standpoint, treating DAOs as unincorporated associations is problematic and makes legal action difficult, whether the DAO is the subject or the instigator of a claim.

Does it have a 'wrapper'? Where a DAO has sought legal advice, they will often have a 'wrapper'. Wrappers are legal entities associated with a DAO, which act as tools for the DAO to carry out functions it would otherwise not be able to do. These functions include hiring employees, registering and paying tax and registering with regulators in key industries. One of the most important functions of a wrapper is to own property, including intellectual property.

For instance, Maker DAO operated through a wrapper called the Maker Foundation. Maker DAO is a highly successful crypto venture operating in fintech which created DAI, a stablecoin pegged to the dollar which currently has a market cap of nearly $6 billion dollars. Maker Foundation owned all trade marks for Maker DAO, allowing Maker DAO to protect and grow its brand. Wrappers can take many forms, but most DAO wrappers are companies or non-profits incorporated in the US or Switzerland. Wrappers are useful from a litigation standpoint: **if a DAO has a wrapper, then it is a good candidate to be a party to litigation. It will also hold most of the assets for the company, meaning that you know it should have the funds to meet your claim in the event you are bringing a claim against a DAO.**

COMMENT

Whilst the legal status of DAOs is uncertain, context is the key to any dispute involving a DAO. Members of DAOs should consider carefully how they wish to structure their organisations, as ease/speed of initiating proceedings can often be critical in instances of egregious and/or fraudulent infringement of intellectual property rights.

As to bringing a claim against a DAO, a thorough investigation into how the DAO operates, and whether it has relationships with companies or with a wrapper, should always be your first pre-action step. Thankfully, the transparent nature of web-3 means much of this information is readily available online. Knowing what to look for is therefore crucial, meaning it is particularly helpful to get legal advice early on in your dispute.

Another approach when contracting with a DAO is to leverage the smart contract in your favour: if your transaction will auto-execute with the DAO paying, you can insist on all of the payment being paid upfront, to avoid the risk of a payment dispute.

The uncertainty around the legal status of DAOs is likely to continue. It may be resolved by a brave party taking the issue of partnership to court. Alternatively, it may be established by the Law Commission's study or by future legislation giving them their own legal personality.

ARTICLE VII

QUANTUM COMPUTING: THE LOOMING THREAT OF QUANTUM DECRYPTION AND CURRENT EFFORTS TO MITIGATE FUTURE RISK*

JACOB W.S. SCHNEIDER**
PARTNER
HOLLAND & KNIGHT

Every portion of a home relies on a solid foundation. If that foundation fails, then everything above it could also be compromised. Many systems work this way: There are one or more critical elements that act as their foundations, and if those foundations fail, then the systems collapse. Much of modern life has one such foundation: data encryption. Should data encryption fail, the results would be disastrous to government, banking, e-commerce, cryptocurrencies and much more.

Although quantum computers[1] capable of compromising our current encryption may be many years (or indeed decades) away, the threat of quantum decryption looms in our future. This article explores quantum decryption in more detail as well as current efforts to mitigate this future risk.

I. ANYTHING THAT CAN BE ENCRYPTED CAN BE DECRYPTED

Encrypted data is everywhere because transmitting and storing sensitive data becomes less risky when it is in an encrypted form. If a digital eavesdropper intercepts a message in-transit or a hacker downloads a database, then the risk that the hacker can read anything meaningful is reduced when that data is encrypted.

Even without knowing the key or password, anything that can be encrypted can be decrypted - the question is only how difficult it is to decrypt the data. If the recipient of an encrypted message has the cryptographic key to read it, then the decryption is easy. If the eavesdropper does not have that key, then cryptography attempts to make the task of decryption as hard as possible so the eavesdropper will give up (and probably go look somewhere else).

To make decryption hard, researchers often turn to hard math problems. This approach makes sense: If a math problem takes a very long time to solve, then you can incorporate it into an encryption scheme so the decryption will likewise take a very long time to perform.

* Portions of this article were originally published on the Holland & Knight LLP IP/Decode Blog. http://www.ipdecode.com.

** Jacob W. S. Schneider is an Intellectual Property Partner in Holland & Knight's Boston, Massachusetts office. His practice focuses on patent, trademark, copyright and trade secret litigation and licensing transactions. https://www.hklaw.com/en/professionals/s/schneider-jacob-w-s.

1 Quantum computers leverage quantum mechanics - the physics of the very smallest particles in our universe - to compute data. See https://www.hklaw.com/en/insights/publications/2022/09/exploring-quantum-computing. Quantum computing is a rapidly developing field that represents a giant step forward in our computing capabilities. It is unlikely that quantum computers will appear on our desktop any time soon, however, because while they are very good at solving certain very hard problems, they are not well-built to run the applications with which we are most familiar (e.g., web browsers).

That approach only works so well, however, because computers happen to be very fast at solving math problems. As a result, as computers became faster and faster over time, the difficulty of these underlying math problems had to grow along with them. If you explore the history of encryption, you will find moments when "X-bit encryption" schemes fell to then-current computers. In 1997, a 40-bit encryption scheme was cracked in hours;[2] in 1998, a 56-bit DES encryption scheme was cracked in less than 3 days.[3] Today, web browsers typically use 128- or 256-bit encryption schemes to stay ahead of current computers' abilities.

II. ENCRYPTION USING PRIME NUMBER FACTORIZATION

One of the primary "very hard math problems" in modern cryptography is prime-number factorization. Prime numbers are those that can be divided evenly only by 1 and themselves (e.g., 2, 3, 5, 7, etc.). Prime numbers can be very large (e.g., 370,248,451 and 6,643,838,879), and while multiplying two very large prime numbers together is easy enough, figuring out *which two prime numbers* created the result is exceedingly difficult. For example,

370,248,451 * 6,643,838,879 = 2,459,871,053,643,326,429

Calculating this product is easy (at least for a computer). Determining which two prime numbers need to be multiplied together to make 2,459,871,053,643,326,429 is hard. And determining which two prime numbers need to be multiplied together to make an even larger product becomes substantially more difficult. Putting some shortcuts aside (e.g., do not waste time with low prime numbers, such as 2 and 3), a computer needs to try multiplying *all* pairs of prime numbers until it reaches the target product. Because there are a lot of prime numbers, it could take an even very fast computer centuries to complete the task. Hackers do not have centuries to wait, so they give up and move on.

The fact that prime-number factorization takes a very, very long time is foundational to modern encryption schemes. For example, the RSA algorithm[4] relies on prime-number factorization. And the RSA algorithm is widely used to protect banking, telecommunications and e-commerce.

Cryptocurrencies, also utilize the power of large numbers to perform their encryption.[5] For example, Bitcoin uses Secp256k1, a type of elliptic curve cryptography, to generate public keys from private ones. The goal for hackers is working backwards from the public key to derive the private key. If successful, bad actors could sign fraudulent transactions on the Bitcoin network. As with the prime-number factorization problem, it would take a tremendously long time for a classical computer to derive a private key from a public one, so Bitcoin remains secure. Theorists have, however, shown that a sufficiently powerful quantum computer would compromise Bitcoin's Secp256k1 encryption scheme.[6]

We are many years away from building a machine that could "break" Bitcoin and other cryptocurrencies, but measures could be taken ahead of that event to avoid the risk. As discussed below, there are several cryptographic algorithms that are considered "quantum-safe," and chains could fork to begin using these algorithms when the quantum threat appears imminent.[7]

III. THE PROBLEM OF QUANTUM DECRYPTION

Shor's Algorithm[8] demonstrates that theoretical quantum computers should be able to perform prime-number factorization at a much faster rate than today's best computers.

2 https://www.cnet.com/personal-finance/crypto/40-bit-crypto-proves-no-problem.

3 https://w2.eff.org/Privacy/Crypto/Crypto_misc/DESCracker.

4 https://people.csail.mit.edu/rivest/Rsapaper.pdf.

5 https://cointelegraph.com/news/why-quantum-computing-isn-t-a-threat-to-crypto-yet.

6 See https://eprint.iacr.org/2017/598.pdf (proposing a quantum algorithm to compromise Bitcoin's elliptic curve-based encryption scheme).

7 Particularly with an ungoverned cryptocurrency like Bitcoin, questions of governance and consensus necessarily arise. A coin could fork in two or more branches, each using a different quantum-safe encryption method.

8 https://quantum-computing.ibm.com/composer/docs/iqx/guide/shors-algorithm.

While employing Shor's Algorithm at scale is still perhaps many years (or even decades) away, it was experimentally shown to work in 2001.[9]

In that experiment, a quantum computer factored 15 into its constituent primes: 3 and 5.[10] As a result, sufficiently powerful quantum computers in the future may be able to decrypt current encryption schemes with much greater ease than today's computers. That is, while the hardware is not yet ready, the method to compromise certain modern encryption schemes is already known.

IV. THE UNITED STATES' RESPONSE TO THE THREAT OF QUANTUM DECRYPTION

In the waning days of 2022 and the 117th Congress, President Biden signed H.R.7535, the Quantum Computing Cybersecurity Preparedness Act, into law.[11] The law recognizes the future threat that quantum decryption poses to federal administrative agencies and orders an examination of the agencies' data cryptography to prepare for a time, perhaps many years from today, when quantum computing is capable of decrypting that data.[12]

A. Developing Post-Quantum Cryptography / Quantum-Safe Algorithms

Quantum computers are very good at a certain class of problems, but lousy at others. While a quantum computer would have a hard time doing something as basic as rendering a webpage, as discussed above with regard to Shor's Algorithm, certain types of quantum computers should excel at prime factorization. As cryptographers search for the next "very hard math problems" that secure encryption schemes, they are looking to a set of problems that quantum computers are no better at solving than classical computers. Encryption schemes that rely on those sets of problems should be more resilient to a quantum decryption attack.

In 2016, the National Institute of Standards and Technology (NIST)[13] began a lengthy public competition to develop these "post-quantum" cryptographic schemes, which are a subset of "quantum-safe algorithms."[14] NIST described the quantum decryption problem as its motivation for the project:

In recent years, there has been a substantial amount of research on quantum computers – machines that exploit quantum mechanical phenomena to solve mathematical problems that are difficult or intractable for conventional computers. If large-scale quantum computers are ever built, they will be able to break many of the public-key cryptosystems currently in use. This would seriously compromise the confidentiality and integrity of digital communications on the Internet and elsewhere.

NIST's stated goal was "to develop cryptographic systems that are secure against both quantum and classical computers, and can interoperate with existing communications protocols and networks."

In 2022, the ongoing project identified several promising candidate algorithms,[15] including CRYSTALS-Kyber[16] (for key establishment) and CRYSTALS-Dilithium[17] (for digital signatures). NIST is currently working to standardize these algorithms for wide-scale use.

B. The Quantum Computing Cybersecurity Preparedness Act

Quantum decryption could also compromise government secrets. So, with quantum decryption on the horizon, Congress passed, and the President signed into law, the Quantum Computing Cybersecurity Preparedness Act to mitigate the looming threat.[18]

9 https://research.ibm.com/blog/factor-15-shors-algorithm.
10 https://www.nature.com/articles/414883a.
11 https://www.congress.gov/bill/117th-congress/house-bill/7535/text.
12 https://www.hklaw.com/en/insights/publications/2023/01/quantum-computing-the-looming-threat-of-quantum-decryption.
13 https://www.nist.gov.
14 https://csrc.nist.gov/Projects/post-quantum-cryptography.
15 https://csrc.nist.gov/News/2022/pqc-candidates-to-be-standardized-and-round-4.
16 https://eprint.iacr.org/2017/634.pdf.
17 https://csrc.nist.gov/CSRC/media/Presentations/Crystals-Dilithium/images-media/CRYSTALS-Dilithium-April2018.pdf.
18 https://www.congress.gov/bill/117th-congress/house-bill/7535/text.

The Act acknowledges the threat that quantum computing raises for national security:

(1) Cryptography is essential for the national security of the United States and the functioning of the economy of the United States.

(2) The most widespread encryption protocols today rely on computational limits of classical computers to provide cybersecurity.

(3) Quantum computers might one day have the ability to push computational boundaries, allowing us to solve problems that have been intractable thus far, such as integer factorization, which is important for encryption.

(4) The rapid progress of quantum computing suggests the potential for adversaries of the United States to steal sensitive encrypted data today using classical computers, and wait until sufficiently powerful quantum systems are available to decrypt it.

Sections 2(a), 3(d)(9) (defining a "quantum computer" as "a computer that uses the collective properties of quantum states, such as superposition, interference, and entanglement, to perform calculations").

The Act requires that the Director of the Office and Management and Budget (OMB) develop and issue guidance for administrative agencies "on the migration of information technology to post-quantum cryptography." Section 4(a). This guidance must include "a requirement for each agency to establish and maintain a current inventory of information technology in use by the agency that is vulnerable to decryption by quantum computers." Section 4(a)(1).

Following that guidance, agencies will then report back to the OMB with their inventory of IT vulnerable to quantum decryption. Section 4(b). One year after NIST issues its post-quantum cryptography standards, OMB will issue further guidance to prepare agencies for the migration of their data to the new, quantum-resilient standards. Section 4(c). Throughout this period, and for the following five years, OMB will report back to Congress on the migration's progress. Section 4(e).

This lengthy period acknowledges the difficulty that agencies, many of which still rely on older, legacy systems, will have in overhauling their encryption schemes.

The Act exempts all national security systems. Section 5. Migrating these systems to post-quantum cryptography, however, is already underway.[19]

While the Act will go a long way toward strengthening agency data against a quantum attack, in some respects, the cat is already out of the bag. Today's hackers can obtain encrypted data and store it for years, knowing that a future quantum computer will be able to decrypt it. This technique is sometimes called "harvest now, decrypt later," and the Act cannot protect already compromised data from future decryption.

Still, the government's acknowledgement and mitigation of future threats is an important step toward protecting its data in the future. **Governments and commercial entities alike must acknowledge and plan for a future when quantum computing reaches a mature point and the encryption upon which we rely may be compromised.**

19 https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems.

HOW CAN I GET INVOLVED?

Interested in submitting new work or becoming an editor for the International Journal of Blockchain Law (IJBL)? Review the below submission guidelines and then email 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
Content is Key	The editors will take care of final product
What can I Submit?	Previously published work is welcome for submission to the IJBL