THE INTERNATIONAL JOURNAL OF BLOCKCHAIN LAW

Volume 6

July 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 sixth issue of the IJBL! We are thrilled to share with you five insightful articles covering blockchain-related topics from several jurisdictions, plus a link to a recording of the June 2023 episode of the IJBL/GBBC webinar, "Hot Topics In Blockchain Law."

First off, Martin Bartlam and Dan Jewell from DLA Piper LLP's London office delve into the *Tulip Trading* case which has been the subject of controversial rulings from the English High Court and Court of Appeal and which could have far reaching implications. Both courts considered whether there is an arguable case that bitcoin developers owe a duty of care to the holders of bitcoin. The trial court found that there was not, but the appellate court reversed. Many are watching this case, noting the significant impact it could have beyond the immediate facts of the case.

Next, Chief Legal Officer and Head of Policy, Americas, Andrea Tinianow, provides an overview of the sweeping legislation introduced by the New York Attorney General to regulate the crypto asset industry. The bill would largely stunt the current BitLicense and require those organizations that have received a license under that regulatory regime to break up their businesses or leave the State.

The U.S. Chairs of the House Committees on Financial Services and Agriculture jointly released an ambitious discussion draft of new legislation aimed at filling the persistent gap in regulation of spot cryptoasset markets and to resolve lingering uncertainty regarding federal securities laws' application in the cryptoasset arena. Attorneys Kevin S. Schwartz, David M. Adlerstein and Samantha M. Altschuler from Wachtell, Lipton, Rosen & Katz offer an overview of the 162-page bill, providing thoughtful insights on key aspects.

Holland & Knight attorneys Andrew Balthazor, Scott Mascianica and Allison Kernisky offer in-depth analysis of the SEC's recent dual enforcement actions against Binance and Coinbase, respectively.

John Bassilios and Max Ding from Hall & Wilcox's Melbourne office unpack Australia's financial services and anti-money laundering laws, as applied to crypto products in Australia. They also discuss the gaps in Australia's regulatory framework and how they might be addressed.

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 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

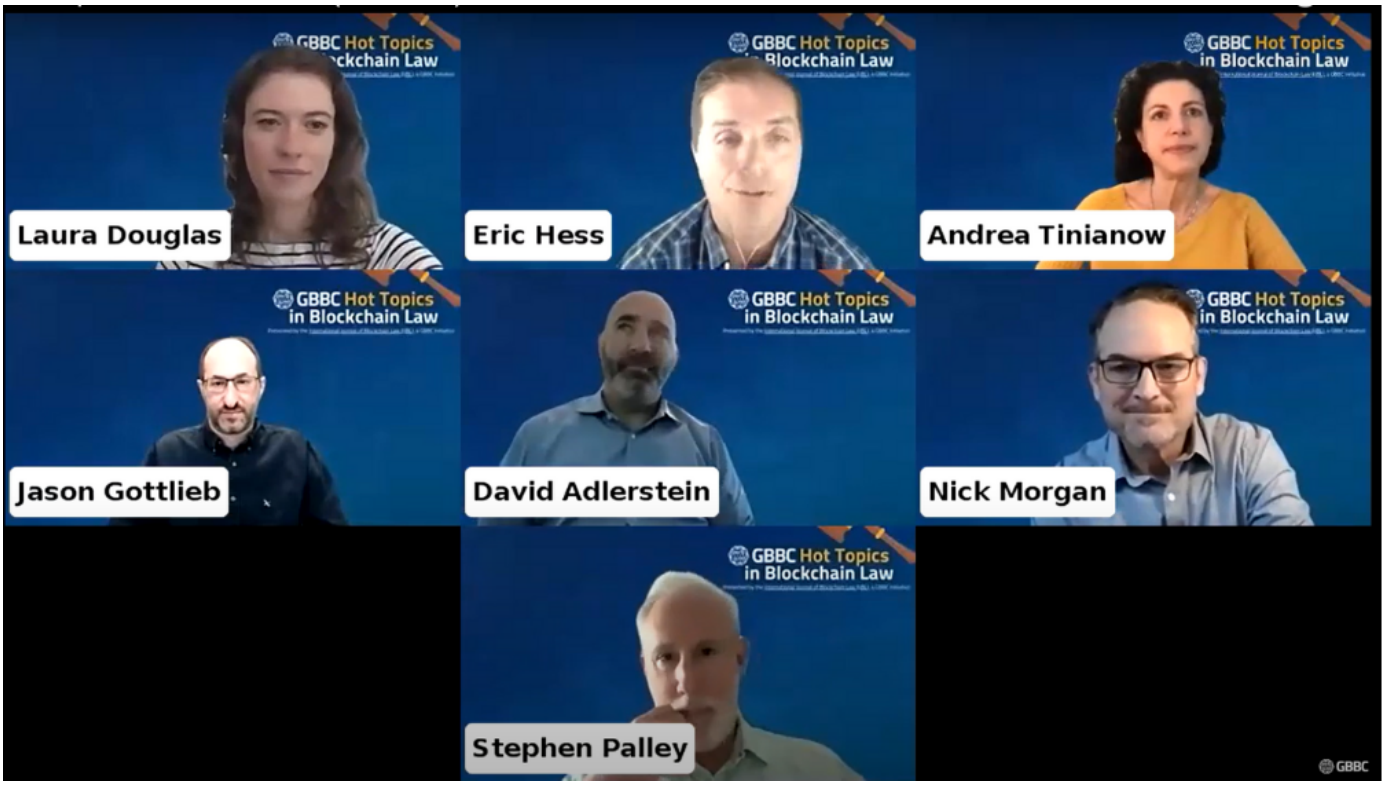
PRIVACY OFFICER AND DIRECTOR OF IT SECURITY COMPLIANCE
TUFTS UNIVERSITY

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.

WEBINAR

"HOT TOPICS IN BLOCKCHAIN LAW"

JUNE 2, 2023



"Hot Topics in Blockchain Law," a virtual roundtable presented by GBBC's International Journal of Blockchain Law (IJBL), explores the pressing legal and regulatory issues related to blockchain and digital assets.

In June, blockchain attorneys David Adlerstein, Laura Douglas, Jason Gottlieb, Eric Hess, Nick Morgan, Stephen Palley, and Andrea Tinianow unpacked topics including the UK Treasury Committee's recent cryptoassets report and the State of New York's proposed legislation.

Register for the next "Hot Topics in Blockchain Law" on September 22, 2023 here.

VIEW THE WEBINAR

ARTICLE I

TULIP TRADING: A DEVELOPING RISK, AND HOW TO LIMIT IT

MARTIN BARTLAM
PARTNER, AND GLOBAL CO-CHAIR, FINTECH
DLA PIPER

DAN JEWELL
LEGAL DIRECTOR
DLA PIPER

INTRODUCTION

Advances in technology are enabling a wider use of decentralised organisational structures, automated contract formation and generative decision-making capabilities, all of which pose new and interesting challenges for determining the boundaries of responsibility in commercial relationships. It is not surprising therefore that the courts are beginning to assess these boundaries and whether existing principles are sufficient or if it will be necessary to create or extend duties of care to address the new elements of these relationships.

In *Tulip Trading*, the English High Court[1] and, subsequently, Court of Appeal[2], considered whether there is an arguable case that software developers and controllers of digital asset networks owe a duty of care to the holders of cryptocurrencies reliant on their software. Whilst this addresses the issue in the context of cryptocurrencies, it may be particularly important in determining the approach to bottom-up design and product development in Web 3.0 applications and the increased use of decentralised organisations for a wide emerging range of new technology services and products.

Tulip Trading Limited ("Tulip") claimed that the Defendants owed a duty of care to assist it in regaining bitcoin allegedly lost during a hack[3] by implementing a software "patch". Although the High Court held that Tulip's argument had no realistic prospect of success, the Court of Appeal disagreed, deciding that there was at least a serious issue to be tried and allowing the case to proceed to trial.

In the event the case goes to full trial this provides an opportunity for the courts to assess the scope of the duties which developers and controllers of digital asset networks owe to users.

In this article, we look at the factors considered by the High Court and Court of Appeal in determining whether Tulip's case had a realistic prospect of success and set out some practical steps for software developers and network controllers to consider in order to limit their exposure to potential claims.

BACKGROUND

Tulip is a Seychelles incorporated holding company. Its CEO is Dr Craig Wright, who claims to be Satoshi Nakamoto, the author of the bitcoin White Paper and the creator of bitcoin.

1 *Tulip Trading Limited v bitcoin Association for BSV and ors* [2022] EWHC 667 (Ch).

2 *Tulip Trading Ltd v Van Der Laan and ors* [2023] EWCA Civ 83.

3 It is worth noting that several of the Defendants now dispute the facts averred by Tulip, alleging the claim is fraudulent.

Dr Wright claimed Tulip owned £3 billion of bitcoin, which he accessed and controlled from his private computer system in England, and that hackers accessed his computer in February 2020 and removed Dr Wright's secure private keys.[4] This resulted in Tulip being unable to access its bitcoin.

Tulip sought a declaration that it owned the lost bitcoin and an order requiring the Defendants, the core developers and/or controllers of four relevant digital asset networks, to take reasonable steps to ensure Tulip was provided access to and control of the bitcoin, or equitable compensation or damages.

THE HIGH COURT DECISION - NO SERIOUS ISSUE TO BE TRIED

The Defendants were all outside the jurisdiction. Therefore, Tulip was required to, and did, obtain permission from the English Court to serve the claim out of the jurisdiction.

Following service, the majority of the Defendants challenged the jurisdiction of the Court. The Court overturned the permission to serve out of the jurisdiction, on the basis that there was no serious issue to be tried on the merits of Tulips claim. The Defendants overcame a high threshold, with the Court concluding that Tulip had no realistic prospect in establishing that the facts pleaded demonstrated a breach of fiduciary and/or tortious duty owed by the Defendants.

On the issue of whether a fiduciary duty was owed, the Court ruled in favour of the Defendants on the basis that the developers were a "*fluctuating body of individuals*" and it "*could not realistically be argued that they owe continuing obligations*" to carry out software updates whenever owners of relevant digital assets require. The Court found no basis for imposing an obligation which would require developers to remain involved and make changes when required by asset owners in circumstances where they had not provided any commitment or assurance that they would do so.

The defining characteristic of a fiduciary relationship is the obligation of undivided loyalty; however, in taking steps in favour of benefitting Tulip alone, which Tulip's case required them to do, the Defendants could disadvantage other users of the networks. While such fiduciary relationships are subject to positive duties, what was being requested by Tulip was beyond the scope typically imposed on fiduciaries and would expose the developers to risks on their own account (for example, from a rival claimant to the relevant bitcoin).

In relation to the alleged tortious duties, the Court found that Defendants owed no duty of care to Tulip. Notably, Tulip's loss in this case was purely economic. Therefore, no duty could arise unless a special relationship existed between Tulip and the Defendants and in this case it was not arguable that one did.

The Court also considered the practical implications if it were to find in favour of Tulip. The potential class of persons to whom any such duty would be owed would be unknown and potentially unlimited, with the result that there would be no definitive restriction on the number of claims that could be advanced against the developers by persons alleging loss of cryptoassets or keys.

4 Private keys are used to create digital signatures that can easily be verified, without revealing the identity of the private key owner. They are also used in cryptocurrency transactions in order to show ownership of a blockchain address.

This would require the Defendants to investigate and take steps to address claims by any individuals professing to have lost their private keys. Due to the anonymity present in the system and function of cryptoassets, such investigation would be extremely time consuming, costly and difficult to conduct.

In contrast, bitcoin owners themselves have significantly more control over their digital assets and could take reasonable steps to protect themselves against the loss of their private keys, for example by storing the private keys on backup drives or protecting themselves with insurance.

The Court therefore decided that imposing such a duty of care would not be an equitable extension of the law, particularly given the loss was purely economic, and could not realistically be argued to be fair, just, and reasonable.

That said, while the Court did not find any duties had arisen between the software developers and Tulip, it did recognise that software developers may be under other, more limited, duties in certain circumstances. One such instance is where they must take reasonable care not to harm the interests of users when making software changes, for example by introducing a malicious bug or compromising the security of the network. Further, where developers have control over a network, it is conceivable that some duty might be imposed to address bugs or other defects that arise in the course of the operation of the system which threaten its operation.

COURT OF APPEAL DECISION – THERE *IS* A SERIOUS ISSUE TO BE TRIED

The Court of Appeal overturned the High Court's decision and held that Tulip's case on fiduciary duties gave rise to a serious issue to be tried. The Court of Appeal did not specifically consider whether the defendants owed tortious duties to Tulip.

However, it was considered that if the appeal in respect of a fiduciary duty succeeded, then it would follow that the appeal regarding tortious duty should also be allowed.

The central considerations in Court of Appeal's determination that there was at least a serious issue to be tried were:

- **Decision making:** the developers had a decision-making role, in effect making discretionary decisions and exercising power for and on behalf of all of the participants in the relevant bitcoin network, including miners and owners of bitcoin, in relation to property owned by those participants. That property has been entrusted into the care of the developers. These features of authority and discretionary decision making are common to fiduciaries.
- **A defined group:** it is arguable that the developers of a bitcoin network are a sufficiently well-defined group, rather than, as the High Court initially found, a fluctuating and unidentified body. The Court of Appeal highlighted that a state of trust existed between network participants and developers since developers could decide what software patches would be implemented, consequently making decisions on behalf of everyone on the network.
- **Existence of positive and negative duties:** it is conceivable that there exists a negative duty for developers not to act in their own self-interest, as well as a duty to act in positive ways, such as fixing code errors or rectifying abnormalities within the network. Although it may be a significant step to identify a fiduciary duty in that manner, there is at least an arguable premise in Tulip's case.

The essence of such duties would be single minded loyalty to the users of bitcoin software and would include a duty not to act in their own self-interest and a duty to act in positive ways in certain circumstances.

The Court of Appeal concluded that such duties may also include a duty to introduce code so that an owner's bitcoin can be transferred to safety in the circumstances alleged by Tulip.[5]

However, the Court of Appeal acknowledged that, for Tulip's case to succeed at trial, there would need to be a significant development of the common law on fiduciary duties. From a legal standpoint, while the established categories in which fiduciary relationships arise are not closed, it is exceptional for fiduciary duties to arise outside of them.

The case will now proceed towards trial. The proceedings are however, still at a relatively early stage, with considerable water still to pass under the bridge before the question of whether blockchain developers owe legal duties to their users will be decided.

HOW CAN DEVELOPERS MINIMISE THEIR RISKS?

If Tulip's case is successful at trial, the potential ramifications for the scope of developers' obligations under English law are huge and will affect developers more broadly than those involved in the Tulip case directly.

The consequences of having to police the activity of users and assist those who allege that they have been victims of fraud involving their cryptoassets or private keys would be costly and potentially very difficult. It could even expose developers to claims from other users adversely affected by any changes made to their network by the developers, particularly in circumstances where the original request for assistance turns out itself to be fraudulent (as is now alleged against Tulip).

It is therefore important for developers to consider, when developing and providing technology, whether there are any steps they can take to minimise their exposure.

The difficulty for developers is that, in a world of increasing decentralisation, in which software and networks are often developed and provided cross-border in a form accessible by all, many of the risk-limitation methods companies relied upon in the past can be more difficult to implement. Nevertheless, developers should consider if there are means to protect themselves from liability. Some possible considerations would be as follows:

1. **Use a limited liability company as a shield:** a common method of protecting participants from liability is to set up corporate entity, to stand between the product and the ultimate individuals or parent company. Under English law, the circumstances in which the courts will permit a claimant to look through the company that is directly liable to the individuals or parent company that stands behind it (which claimants often view as "the deep pockets at the end of the chain") is limited. The ability of the company to become insolvent if faced with a large claim, protects the ultimate parent company and often discourages claims altogether, as a victory against a limited liability company with few assets is often pyrrhic.

2. **Disclaimers / clear and standard terms:** the Court noted in the first instance decision that the owners of digital assets on the relevant networks were by definition an anonymous and fluctuating class, with whom the Defendants had no direct communication or contractual relationship. If Tulip's case is successful, that will have to change, as if they are found to owe duties to users, it will be crucial for developers to define the limits of such duties.

5 *Tulip Trading Ltd v Van Der Laan and ors* [2023] EWCA Civ 83 at [86].

Disclaimers and clear and standard terms provide a means to achieve this, with users being required to "click and consent" to terms of use before being granted access to the network or software. The difficulty is that users might be viewed as "consumers", who are typically afforded greater protection by law than commercial entities. Nevertheless, disclaimers and developer-friendly (albeit reasonable) terms can still be a crucial line of defence.

3. **Governing law / jurisdiction clauses:** if users can be required to "click and consent" to developers' terms before using their network or software, it is important to include in those terms provisions dealing with governing law and jurisdiction. Particularly in circumstances where users of the networks and software are likely to be located across the globe, specifying the applicable law and the forum for disputes (i.e. the relevant national courts or arbitral rules under which any dispute will be heard) is crucial to provide certainty, including in relation to the scope of any duties owed and the procedure for dealing with disputes. For example, in part due to the rise of class actions, companies across various sectors are increasingly incorporating arbitration clauses in their standard terms, to seek to make it more difficult for collective claims to be brought (albeit the validity of such clauses as against consumers is open to challenge).

The suggestions above might be said to be inconsistent with principles of consensus-based distributed ledger technologies, where "code is law". However, it is important to realise that new technology does not operate in a vacuum.

If disputes arise, users will inevitably petition the courts to intervene, particularly when large sums are in dispute, and in those circumstances, developers and controllers who have taken steps in advance to define their relationship with users and limit their exposure are considerably better placed than those who have not.

CONCLUSION

Although the Court of Appeal allowed Tulip's case to proceed towards trial, recognising that it has at least a realistic prospect of success, as noted above, the Court also acknowledged that there would need to be a substantial increase in the current scope of fiduciary duties for Tulip's case to succeed. Therefore the risk should not be overstated... yet.

That said, that risk, however small, is real. In that context, forewarned is forearmed, and developers and controllers should take steps to ensure their potential liability to users is limited to the extent possible.

ARTICLE II

NY ATTORNEY GENERAL POSES SWEEPING CRYPTO REGULATION

ANDREA TINIANOW
GBBC CHIEF LEGAL OFFICER AND HEAD OF POLICY, AMERICAS

On Friday, May 5, 2023, New York Attorney General Letitia James ("AG") announced sweeping legislation to regulate the cryptoasset industry. The bill's purported intent is to "protect customers and investors in digital assets from fraudulent practices, eliminate conflicts of interest and increase transparency." The Office of the New York Attorney General ("OAG") said in its press release that it will submit the bill to the State Senate and Assembly during the 2023 legislative session.

Per the press release, the impetus for the legislation is the "lac[k] of robust regulations" that have led to rampant fraud and dysfunction which are the "hallmarks of cryptocurrency."

The draft legislation is comprehensive and includes, among other things, provisions requiring stablecoin issuers to hold a highly constrained set of reserves (inadvertently, it appears, excluding bank deposits) at a 1:1 ratio. Persons acting as newly defined "digital asset brokers" and "digital asset investment advisors" are required to comply with state and federal KYC/AML rules (otherwise applicable only to "financial institutions"), and "digital asset issuers," and "digital asset marketplaces," as well as digital asset brokers and digital asset investment advisers, are required to make public quarterly financial statements and independent annual audits.

The bill also includes several rules to regulate a class of crypto enthusiasts which it refers to as "digital asset influencers," making it illegal, among other things, for them to merely "widely circulate" a posting the "encourages" investment in a digital asset they may own a modest amount of without first registering with the State and disclosing their ownership interest, compensation, or both, among many, many other things.

Significantly, the legislation would make it illegal for a person or affiliate to act as more than one of these service providers: digital asset issuer, digital asset broker, digital asset marketplace, and digital asset investment adviser. This is dramatically at odds with how both centralized and decentralized crypto exchanges operate today. The legislation also prohibits digital asset brokers and their affiliates from trading on their own account, unless an exception is made in the rules or regulations adopted under the legislation.

In addition, the legislation requires issuers of digital assets to publish and distribute a prospectus that contains prescribed information, including, all related material information about the issuer and the digital asset.

Moreover, the digital asset marketplace (crypto exchange) is required to verify that the digital asset's software code is consistent with the issuer's disclosure in the prospectus, among many other requirements and restrictions.

The draft legislation is the NYAG's latest effort to assert control over the crypto industry. In March 2023, the AG filed a lawsuit against the KuCoin crypto exchange for failing to register as a securities and commodities broker-dealer, among other things. That lawsuit drew (negative) attention due largely to its claim that the cryptoasset, "ether" is a security. (Notably, not even the Securities and Exchange Commission ("SEC") Chair Gary Gensler was willing to characterize ether as a security during a hearing before the House Financial Services Committee.)

The New York legislation is similarly heavy handed. Although the bill does not attempt to label cryptoassets as "securities," it would handle crypto-related activities in a manner that is even more exacting than how the law requires treatment of securities-related activities. Early feedback from participants in the cryptoasset community suggests that the bill is a dramatic overreach that seeks to indirectly create a regulatory framework that would throttle the crypto industry.

In crafting the bill, the OAG appears to subject the crypto industry to least favored nation status, borrowing requirements from disparate regulatory frameworks. For example, the bill grafts various federal securities regulations, such as capital requirements, onto the draft law. Moreover, any violation of the law would be deemed to constitute fraud.

One prominent New York attorney who asked that his name be withheld is concerned about the power that the bill vests in the NYAG who would have broad authority under the bill to adopt new rules and unilaterally implement listing standards for digital assets. He explains, "**the bill would effectively render the NYAG the czar of the digital economy insofar as it touches New York in any way. This may be appealing to the AG, but beyond that, not so much**."

According to some, these efforts could backfire. They say that the NYAG is methodically pushing the crypto industry out of New York. If the bill were to become law, crypto businesses would exit the State until Congress enacts preemptive federal legislation, and only return once a single set of sensible rules apply nationwide. The same attorney concurs, warning that "as drafted, the bill would have the effect of making New York a no-go zone for centralized and decentralized exchanges."

Political observers also see this as an encroachment on the authority of the New York State Department of Financial Services ("DFS"), the regulator in New York State responsible for the crypto sector under New York's "BitLicense" regime. **DFS gets short shrift in the bill, and it is unclear whether they were consulted in the bill's preparation**. (Despite the OAG's press release featuring quotes from 25 different policymakers and others in New York State, there is not one quote given to anyone currently in the DFS).

"New York is an effective global regulator with respect to the securities and banking industries when it acts interstitially, that is, when federal regulators fail to act and the New York AG or the DFS takes action pursuant to state law that has global impact because of New York's unique status a global financial center," says Daniel Alter, a partner at Abrams Fensterman LLP in New York who specializes in FinTech regulation. "It is one thing for a state attorney general to be a regulatory gadfly within a national regulatory structure. But currently, there is no national regulatory framework for cryptoassets," Alter stresses. "New York has no federal backstop in that financial sector against which to leverage its power."

There are some who believe that with this legislation, Attorney General James is trying to create a Martin Act for cryptocurrency. The Martin Act is a New York State law empowering the attorney general to investigate and prosecute securities fraud.

Under the law, the attorney general can issue subpoenas and otherwise investigate misconduct in securities without having to bring an enforcement action. This legislation incorporates by reference certain of these investigative tools, thus effectively expanding the Martin Act to cover cryptoassets.

But critics think that Attorney General James has it backwards. First you need the national framework for crypto regulation, and then you layer on top of that the types of powers that the Martin Act grants.

Frequent commenter on the regulation of the cryptoasset space, Lewis Cohen, co-founder of DLx Law, noted that "**this bill reads more like a holiday wish list cobbled together by outside consultants seeking simply to prevent otherwise law-abiding New York State businesses from utilizing cryptoassets, rather than a genuine attempt to provide a thoughtful regulatory framework that would enable innovation in New York State** while providing practical protections cryptoasset users are actually calling for. Similar to the "Red Scare" of the 1950s which used a few dramatic examples of seditious activity to whip up broad anxiety in order to achieve otherwise unacceptable political outcomes, this bill references genuine issues (the collapse of the Terra/Luna platform and the bankruptcies of FTX and Celsius) in an attempt to impose what would be a highly unpopular functional ban on crypto activity within the State."

Perhaps the best thing that can come of this is that it catalyzes Congress to act. "No act of Congress has yet to create a national framework," says Alter. New York should keep its powder dry until then."

Recent industry events, such as the failure of centralized cryptoasset lenders like Celsius, and the spectacular implosion of FTX, demonstrate that there are areas of weakness in the cryptoasset industry that are appropriate for regulators to respond to.

However, **top heavy regulation of the type proposed in the bill may cause more harm than good**, by penalizing compliant actors, such as the existing DFS-licensed cryptoasset exchanges by making their business models illegal, and making it more difficult for every-day New Yorkers to participate in the digital economy.

Author's Note: This article was originally published by Forbes.com and is reprinted with permission. The opinions herein are my own and do not reflect the opinions or position of the Global Blockchain Business Council.

ARTICLE III

CONGRESSIONAL BILL PROPOSES COMPREHENSIVE CRYPTOASSET LEGAL FRAMEWORK AMIDST SEC'S CONTINUED REGULATION-BY-ENFORCEMENT

KEVIN SCHWARTZ
PARTNER, LITIGATION
WACHTELL, LIPTON, ROSEN & KATZ

DAVID ADLERSTEIN
COUNSEL
WACHTELL, LIPTON, ROSEN & KATZ

SAMANTHA ALTSCHULER
ASSOCIATE, CORPORATE
WACHTELL, LIPTON, ROSEN & KATZ

On Friday, June 2nd, the Chairs of the House Committees on Financial Services and Agriculture jointly released an ambitious discussion draft of new legislation aimed at filling the persistent gap in regulation of spot cryptoasset markets and to resolve lingering uncertainty regarding federal securities laws' application in the cryptoasset arena.

While the 162-page draft is complex and invites many questions, it represents an intriguing potential springboard for advancing the regulatory discussion in the United States beyond backward-looking, one-off enforcement actions, which have long been the overwhelming focal point. In the most recent and high-profile examples, the SEC has unveiled a sweeping complaint against the world's largest cryptoasset exchange, its founder, and its U.S. arm, and separately a complaint against the largest cryptoasset exchange in the United States.

In what has become a pattern, the SEC has chosen to use its enforcement action tool to launch new assertions that specific cryptoassets (even a particular stablecoin) are securities — without bringing enforcement actions against the relevant developers or issuers of the purported securities.

The cryptoasset industry has witnessed some pronounced failures meriting vigorous enforcement. But the SEC's practice of issuing summary declarations about the status of widely traded digital assets through ad hoc civil litigation, while refusing to promulgate a tailored, navigable regime of appropriate disclosures and other rules, is not conducive to U.S. leadership in this industry or to the meaningful protection of investors.

In stark relief, regulatory clarity is increasing abroad (notably in the European Union, with its adoption in May of new rules on markets in cryptoassets).

In the limited circumstances that the SEC has engaged in focused cryptoasset-related rulemaking, it has largely sought to fit cryptoassets into the familiar rails that apply to traditional securities, such as in its April proposal to require decentralized software protocols to designate a specific entity with compliance responsibility, thereby calling into question the ability of these protocols to function in a decentralized manner.

The draft proposal (a more detailed summary of which can be found here) would resolve several fundamental regulatory questions about jurisdictional authority over cryptoasset markets—dividing authority between the CFTC and the SEC based on functional standards — and facilitate, through a tailored regime, compliant capital formation and trading activity. In particular, the bill would:

- provide the CFTC with jurisdiction to regulate spot markets in cryptoassets constituting commodities and establish requirements for registered digital commodity exchanges, including to prohibit market abuse and to meet cybersecurity requirements;
- create a framework for registration of digital commodity brokers and commodity dealers;
- set conditions for a cryptoasset to be deemed a commodity, including:
  - ◊ assets issued through an "end user distribution" (such as through mining, staking
  - ◊ or an "airdrop") other than to an issuer, a related person or an affiliate; or
  - ◊ assets held by a person other than an issuer where the applicable blockchain network is functional and is formally self-certified as decentralized; coverage to retail customers in the event of an insolvency.
- establish SEC jurisdiction over cryptoassets that are offered as part of an investment contract pending the cryptoassets meeting the definition of a commodity;
- exempt payment stablecoins from treatment as securities while reserving certain antifraud authority to the SEC;
- create a tailored disclosure regime for capital-raising transactions involving cryptoassets and periodic reporting for cryptoasset issuers (including filing of annual and semiannual reports, pending certification that the applicable network is decentralized);
- provide a mechanism for cryptoasset issuers (or other market participants) to certify to the SEC that the relevant network has become decentralized, providing a potential offramp from SEC reporting that remains subject to SEC rebuttal of such certification;
- establish an SEC registration exemption for an issuer's sales of cryptoassets not involving equity or debt, subject to certain conditions (e.g., total sales by the issuer over the prior 12 months not exceeding $75 million, non-accredited investor's purchases not exceeding a prescribed financial threshold and the purchaser not owning more than 10% of the posttransaction units);
- require that the SEC enable registration of cryptoasset trading platforms as ATSs;
- permit a path to secondary trading of commodity digital assets even after an initial offering by investment contract;
- allow broker-dealers to custody cryptoassets, subject to conditions; and establish a joint CFTC-SEC advisory committee on cryptoassets, including for the express purpose of jointly studying decentralized finance (DeFi).

The bill raises many questions, including as to when a blockchain network would be sufficiently decentralized (as even under the objective criteria set out in the bill, this remains a heavily fact-intensive inquiry, leaving open how the SEC would attempt to wield its discretion).

The bill also raises the specter of a particular cryptoasset simultaneously trading on a CFTC-registered exchange and an SEC-registered ATS (e.g., in the case of insiders' tokens), posing potential market complexity.

But at least as a starting point, the bill reflects a constructive approach to regulation by applying the substance of traditional rules designed to promote market integrity and protecting investors in a tailored manner that seeks to preserve the potential benefits of new technology.

This stands in contrast to an enforcement-centric approach, or more caustic legislative approaches exemplified by a recent New York bill that could make cryptoasset-related activities in that jurisdiction prohibitively difficult.

ARTICLE IV

THE SEC LANDS FIRST BLOWS AGAINST CRYPTO INDUSTRY TITANS*

ANDREW BALTHAZOR
ASSOCIATE
HOLLAND & KNIGHT

ALLISON KERNISKY
PARTNER
HOLLAND & KNIGHT

SCOTT MASCIANICA
PARTNER
HOLLAND & KNIGHT

INTRODUCTION

In a one-two punch earlier this month, the U.S. Securities and Exchange Commission (SEC) brought successive actions against two of the world's largest cryptocurrency exchanges – the first blows in what will likely be prolonged litigation against some of the biggest players in the digital asset industry. First, on June 5, 2023, the SEC filed a complaint against Binance and its owner Changpeng Zhao. The next day, on June 6, 2023, the SEC filed a complaint against another large exchange based in the United States.

Neither of these actions should come as a surprise to those monitoring the cryptocurrency industry. In March 2023, the Commodity Futures Trading Commission (CFTC) filed an enforcement action against Binance, and, around the same time, the other national exchange announced it had received a Wells notice from the SEC regarding a likely enforcement action. The only real surprise was the SEC's decision to file the two complaints within a day of one another.

A CLOSER LOOK

Both SEC complaints include some similar claims. Specifically:

- operating an unregistered exchange, in violation of Section 5 of the Securities Exchange Act of 1934 (Exchange Act)
- brokering the purchase or sale of securities without registration, in violation of Section 15(a) of the Exchange Act
- functioning as a clearing agency with respect to securities without registration, in violation of Section 17A(b) of the Exchange Act
- control person liability against parent companies of the entities for the above violations under Section 20(a) of the Exchange Act
- the offer and sale of unregistered securities in violation of Sections 5(a) and 5(c) of the Securities Act of 1933 (Securities Act)

* This article is reprinted here with permission from Holland & Knight SECond Opinions Blog Summer Series which can be found here. The authors are attorneys from Holland & Knight's Securities Enforcement Defense Team and/or Digital Assets and Blockchain Tech Team.

The similarities continue. Each complaint alleges that:

- numerous digital assets traded on the respective exchanges are securities – 10 or 13 tokens, respectively, with some token overlap between the complaints
- the exchanges' staking services are securities offered and sold without registration[1]; and
- civil monetary penalties, disgorgement and injunctions against future such violations of federal securities laws are warranted.

But the similarities between the two complaints end there.

In contrast to the Coinbase SEC complaint, the SEC's complaint against Binance alleges egregious conduct – significantly, that Zhao engaged in an active, deliberate effort to create an illusion of regulatory compliance by creating a U.S.-based shell entity, operating as binance.us, which would ostensibly serve U.S. customers and be separate from Binance's international arm – itself operating as binance.com.

The SEC alleges these entities were never truly separate, assets of the different entities' customers were commingled, binance.us violated the negligence-based antifraud provisions of the Securities Act, and Zhao maintained control of all entities – failing to observe corporate formalities that would have made the entities distinct and independent from other Binance affiliates.

Moreover, the SEC alleges that Zhao operated two market making entities, Sigma Chain and Merit Peak, to manipulate trade volumes and token prices and engage in wash trading. Also, unlike the complaint against the U.S.-based exchange, the SEC alleges Binance issued and sold its own digital asset securities – BNB and BUSD tokens.

The SEC also seeks a permanent officer and director bar against Zhao, prohibiting him from ever acting as an officer or director of a public company.

Notably, the Binance complaint includes detailed allegations indicating the SEC's apparent access to cooperating witnesses and receipt of internal communications and text messages. For example: "Binance's CCO bluntly admitted to another Binance compliance officer in December 2018, 'we are operating as a fking [sic] unlicensed securities exchange in the USA bro.'"

Also unique to the Binance action: on June 6, 2023, the SEC filed an emergency motion requesting the court issue a temporary restraining order (TRO) freezing certain of Binance's assets. The motion requested entry of an order, requiring, *inter alia*, the repatriation of certain assets belonging to or owed to customers of binance.us, prohibiting destruction of records, requiring sworn accountings and ordering expedited discovery.

According to the SEC, a TRO is necessary because there is evidence, as detailed in the SEC's memorandum of law and several declarations, showing that Zhao and Binance are not reliable asset custodians, refused to agree to satisfactory procedures to safeguard the status quo, and are capable of easily removing assets from the jurisdiction of the court.

1 Staking is a means of generating a return on digital assets by committing the digital assets for a certain period of time – analogous to a certificate of deposit.

Binance argued in response that a restraining order was unnecessary, stating it was willing to make numerous concessions to address the SEC's concerns.

At a June 13, 2023, motion hearing, District Judge Amy Berman Jackson agreed with Binance and ordered the parties to agree to terms for a consent order. A few days later, the parties stipulated to a consent order in which binance.us agreed to 1) limit access to U.S. customers' assets to binance.us employees, 2) repatriate to the United States and place under the control of binance.us any U.S. customer assets, 3) not provide access to U.S. customer assets to binance.com or Zhao, 4) provide a written accounting of binance.us accounts, 5) provide the SEC monthly operational expense reports and 6) expedite discovery, among other things.

It is not clear whether such sweeping concessions by Binance will move the needle in terms of its reputation with the SEC. Chair Gary Gensler, at a conference on June 8, 2023, lumped Binance and Zhao in with the likes of FTX, Terra/Luna, Do Kwon, Tron and Justin Sun:

> We've seen this story before. It's reminiscent of what we had in the 1920s before the federal securities laws were put in place. Hucksters. Fraudsters. Scam artists. Ponzi schemes. The public left in line at the bankruptcy court.

Binance, for its part, filed a motion on June 21, 2023, requesting the court order the SEC to not "make misleading extrajudicial statements that may materially impact court proceedings."[2] Without waiting for the SEC to respond, Judge Berman denied Binance's motion on June 26, 2023, stating:

> While all of the lawyers in this case should adhere to their ethical obligations at all times, it is not apparent that Court intervention to reiterate that point is needed at this time, or that it is necessary or appropriate for the Court to get involved in wordsmithing the parties' press releases. Nor is it clear that the agency's public relations efforts to date will materially affect proceedings in this case.

The SEC's actions earlier this month against two of the largest cryptocurrency exchanges in the world are the latest moves in a developing agency trend: shifting focus from individual digital asset issuers – which is akin to regulatory whack-a-mole – to scrutinizing major industry intermediaries on which digital assets are traded.

KEY TAKEAWAYS

In the U.S., digital asset intermediaries may wish to consider ways either to register their activities with the SEC or strictly adhere to appropriate exemptions.

Expect increased SEC scrutiny of:

- digital asset intermediaries that seek to avoid U.S. federal securities laws by avoiding serving U.S. customers
- internal token listing policies established to ostensibly prevent an intermediary from offering securities on their platform
- any intermediary which combines traditionally separate functions – e.g., issuing securities, custody, brokering, buyer/seller matching, settlement and clearing

2 Defs.' Mot. for an Order Directing Counsel for Pl. to Comply with Applicable Rules of Conduct, SEC v. Binance Holdings Ltd., No. 23-cv-01599 (D.D.C. June 21, 2023), ECF No. 74.

ARTICLE V

CRYPTO REGULATION IN AUSTRALIA: WHERE ARE WE NOW AND WHERE ARE WE HEADED?

JOHN BASSILIOS
PARTNER
HALL & WILCOX

MAX DING
PARTNER
HALL & WILCOX

INTRODUCTION

Across the world, many jurisdictions have begun to consider or implement frameworks for regulating the crypto ecosystem. Some jurisdictions have taken the approach of repurposing or modernising existing legislation, whereas others are proposing crypto-specific laws.

The Australian Government's policy toward crypto regulation falls toward the former camp. However, it also recognises that some of the unique challenges of crypto may call for bespoke laws.

This article outlines Australia's current approach to regulating crypto, as well as the Government's proposed approach to reforming the existing framework. In the first part, we discuss how Australia's current financial services and anti-money laundering laws are used to regulate crypto products. Next, we discuss where Australia's regulatory framework is headed.

AUSTRALIA'S REGULATORY REGIME FOR CRYPTO-RELATED ACTIVITIES

There are a range of laws in Australia which regulate crypto-related activities. Chief among them are Australia's financial services, and anti-money laundering and counter terrorism financing (AML/CTF) regimes, respectively. Australia's financial services regime regulates activities relating to financial products such as securities, derivatives, payment services and investment products. Whereas the AML/CTF regime aims to prevent money laundering and the financing of terrorism by imposing requirements on certain service providers (referred to as "designated services").

Australia's Financial Services Regime

A key concept in determining whether an activity falls within the ambit of financial services regulations, is whether the object of the activity is a 'financial product'. Under the Corporations Act 2001 (Cth), a 'financial product' is a 'facility' through which a person 'makes a financial investment', 'manages financial risk', or 'makes non-cash payments'. 'Facility' is a broad term which includes intangible property, a term of a contract, agreement, understanding, or arrangement through which a person performs a function.

Australia's financial services regulator, the Australian Securities and Investments Commission (ASIC), has published guidance on whether certain crypto-related activity involves a financial product and, therefore falls within ASIC's regulatory ambit.[1]

ASIC's guidance suggests that in determining whether a crypto product is a financial product, they will consider all the rights and features associated with the crypto product in question, which is a question of fact turning on the circumstances of each case. This consideration is one of substance over form, as it is less important to consider how the crypto product is labelled or marketed, and more important to consider the substantive rights and features the crypto product offers.

Despite ASIC's guidance, **there remains substantial uncertainty among stakeholders in the Australian crypto space as to how the regime would apply to certain other crypto products that are not tied to what would be considered traditional financial products**. This has led to greater calls for clarity and reform in Australia.

Even if a crypto token is not deemed a financial product, certain activities related to crypto activities may still be regulated under Australian's consumer protection laws. For example, ASIC has suggested the use of marketing and social media to inflate the true level of interest in a crypto product or wash selling (the practice of buying and selling crypto assets to artificially increase the price), are examples of activities that constitute misleading or deceptive conduct which contravene Australian law.[2]

Australia's AML/CTF Regime

Australia's AML/CTF crypto regime seeks to prevent money laundering and terrorist financing activities involving crypto tokens by imposing obligations on digital currency exchange businesses that provide fiat-crypto on/off ramping.

These obligations include registering with Australia's AML/CTF regulator, the Australian Transaction Reports and Analysis Centre (AUSTRAC), performing know your customer and due diligence procedures to verify a customer's identity, reporting to AUSTRAC on certain matters, keeping records, and having systems and controls in place to mitigate and manage money laundering and terrorist financing risks.

PROPOSED REFORMS TO CRYPTO REGULATION IN AUSTRALIA

Proposed crypto reforms to Australia's financial services regime

The Australian Treasury has engaged in an exercise called Token Mapping to provide greater clarity to stakeholders on how, and the extent to which, the current financial services regime applies to crypto products.[3]

As part of the exercise, the Treasury has proposed that the test for assessing whether crypto products are financial products should be the same as that which is used for traditional financial products.[4] This involves determining whether the crypto product is a facility through which certain financial functions can be performed such as, making financial investment, managing financial risk, or making non-cash payments, which is in line with ASIC's guidance.

Further, Treasury has proposed the following definitions:

- Tokens -- physical or digital units of information that have a role in a token system.
- Token system -- a collection of steps involved in performing, or anything designed to ensure or facilitate, a function.
- Function -- any benefit ensured or facilitated by the token system to the token holder.

1 https://asic.gov.au/regulatory-resources/digital-transformation/crypto-assets

2 https://asic.gov.au/regulatory-resources/digital-transformation/crypto-assets

3 https://treasury.gov.au/consultation/c2023-341659; https://asic.gov.au/regulatory-resources/digital-transformation/crypto-assets

4 https://treasury.gov.au/consultation/c2023-341659

Applying these definitions, the test to determine whether a crypto product is a financial product may be restated as follows:

- Is the token system a facility?
- If so, is the token system one through which a person does any of the general financial functions (i.e. makes a financial investment, manages financial risk, or makes non-cash payments)?

In addition, the Treasury identifies two types of token systems: intermediated token systems, and public token systems. Intermediated token systems involve intermediaries or agents that perform functions pursuant to certain promises or other arrangements. Whereas public token systems involve functions that are performed by decentralised crypto networks in the absence of promises, intermediaries, and agents.

An example of an intermediated token system is an exchange where a customer can transfer cryptocurrencies or fiat money to a service provider which credits the consumer's crypto wallet. Another is a crypto token which gives the token holder rights to access an event or subscriptions, intellectual property, or reward programs offered by a third party.

In contrast, public token systems encompass crypto tokens that are created as part of a consensus mechanism on public crypto networks, where the tokens are created by the network itself (as opposed to an intermediary or agent). It also includes smart contracts (code) that are created for the purpose of enabling parties unknown to other to enter into commercial transactions without an intermediary.

Although the Treasury has not proposed specific regulations for public token systems, it does recognise that t*he current financial services regime is inadequate* to address the unique challenges posed by these systems. Public token systems are therefore fertile ground for future regulatory reform in Australia.

The Australian Government will soon begin consultation to revise regulations pertaining to the licensing and custody of crypto assets, particularly for crypto products which fall outside the financial services regime. It is anticipated that the new regulations will take the form of bespoke obligations and operational standards for crypto service providers to ensure they adequately safe-keep assets for customers.[5] It is also expected that ASIC will enhance its focus on crypto products by bringing enforcement actions where appropriate, and increasing the size of its crypto team.

Proposed Crypto Reforms To Australia's AML/CTF Regime

The Government plans to bolster the AML/CFT regime in relation to digital currency service providers. In particular, the Australian Government may expand the designated activities that will be subject to AML/CTF obligations to include:

- exchanges between one or more forms of digital currency;
- transfers of digital currency on behalf of a customer;
- safekeeping or administration of digital currency; and
- provision of financial services related to an issuer's offer and/or sale of digital currency.

Moreover, **the Government may require digital currency exchanges registered in Australia to comply with the travel rule**, as prescribed by the Financial Action Task Force (FATF). Currently, the travel rule only applies to traditional financial institutions. Under the travel rule, entities are required to obtain and share payer and payee information alongside a transfer of value as it is transmitted from one entity to another. Under FATF's standards, the travel rule applies to fiat-crypto on/off ramping, the transfer of digital currency, and the exchange between one or more forms of digital currency.

5 https://ministers.treasury.gov.au/ministers/jim-chalmers-2022/media-releases/making-crypto-safer-consumers

CONCLUSION

The Australian Government has taken a shoehorned approach to crypto regulation, largely through its financial products and AML/CTF regimes. Significantly, **the Government appears to recognize that crypto systems which are deemed decentralised public token systems cannot be adequately regulated under current legislation, and are considering how to address this challenge**.

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
What can I Submit?	Previously published work is welcome for submission to the IJBL

GBBC