THE INTERNATIONAL JOURNAL OF BLOCKCHAIN LAW

Volume 3

July 2022

GBBC
Global Blockchain
Business Council

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 third issue of the IJBL! I am proud to present a great set of articles covering cutting edge legal topics related to blockchain technology, digital assets and much more, including stablecoins, DeFi, the metaverse, and proposed legislation in the U.S.

We received overwhelming positive feedback on the virtual round table on DeFi in the last edition of the IJBL. So, we asked attorneys Andrea Tinianow and Stephen Palley to curate another virtual round table discussion, this time focusing on stablecoins. The round table is driven by lawyers who offer thoughtful and provocative insights about the current state of this nascent digital asset, and how stablecoins will evolve in the near and long term. A special shout out to Andrea and Stephen for orchestrating the discussion and bringing us a unique compilation of leading voices on this topic. (You won't find this type of discourse anywhere else!)

Next, we explore certain features of decentralized autonomous organization (DAO) governance that present distinct challenges for counterparties seeking to invest or engage in commercial transactions with DAOs. Wachtell Lipton attorneys Kevin S. Schwartz, David M. Adlerstein, David E. Kirk and Sabina M. Beleuz Neagu scrutinize the pitfalls of setting up DAOs and make tangible recommendations for both DAO organizers and DAO investors.

Many believe that DeFi has the potential to disrupt traditional finance. We continue the DeFi theme from the last issue, with an article from Norton Rose Fulbright LLP attorneys Hannah Meakin, Professor Peter McBurney and Albert Weatherill who consider the regulatory aspects (and challenges) of DeFi.

Another related hot topic is the metaverse, the seamless convergence of our physical and digital lives. The metaverse creates a unified, virtual community which gives rise to a wealth of legal issues. Gary Weingarden and I consider these legal issues as they relate to privacy policy and offer our thoughts about how they should be addressed.

With several million users, the Uniswap platform, a leading decentralized crypto trading protocol, has not escaped its share of controversy. We present two articles on the question of Uniswap's state of decentralization, the first by attorney Max Dilendorf who challenges Uniswap's state of decentralization, and the second, a rebuttal by Uniswap lawyers Marvin Ammori (Chief Legal Officer) and Sonal Tolman (Associate General Counsel). We encourage you to read both and decide for yourself!

Finally, we bring you Andrea Tinianow's article on Title III of the recently introduced Lummis-Gillibrand Responsible Financial Innovation Act. This innovative piece of legislation brings digital assets fully within the regulatory perimeter and is, as of today, one of the most significant U.S. regulatory developments in the digit asset space.

Happy reading!

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
ANDERSON KILL

Stephen Palley is a partner in the Washington, D.C. office of Anderson Kill. He is the founder and chair of Anderson Kill's Technology, Media and Distributed Systems Group, a cross-disciplinary team of lawyers, with experience across a wide range of legal practice areas, who specialize in advising software, internet, and FinTech companies.

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
IOV LABS

Andrea Tinianow, a Delaware attorney, is the chief legal officer for IOV Labs, the brand behind the Rootstock and RIF protocols. 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.

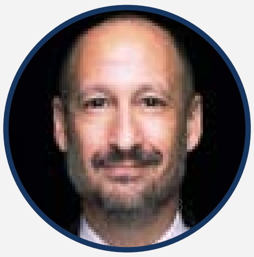
JAKE VAN DER LAAN

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

ASSISTANT VICE PRESIDENT, DATA PROTECTION OFFICER
NOTARIZE, INC

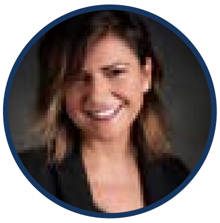


Gary Weingarden is AVP and Data Protection Officer at Notarize, Inc. He is responsible for their information security, privacy, IT, and fraud prevention programs. Gary has over 15 years of experience in the mortgage industry having served as Chief Privacy Officer and General Counsel at Birmingham Bancorp Mortgage Corp.

ARTICLE I

A ROUND TABLE DISCUSSION ON STABLECOINS: TAKING THE WORLD BY STORM OR STORMING THE WORLD?

DAVID ADLERSTEIN
COUNSEL
WACHTELL, LIPTON



OLTA ANDONI
DEPUTY GENERAL COUNSEL
AVA LABS

ANDREW BALTHAZOR
LITIGATION ASSOCIATE
HOLLAND & KNIGHT LLP

COLLINS BELTON
MANAGING PARTNER
BROOKWOOD P.C.

LEWIS COHEN
CO-FOUNDER
DLX LAW

JASON GOTTLIEB
PARTNER, CHAIR
MORRISON COHEN LLP

STEPHEN D. PALLEY

PARTNER
ANDERSON KILL

KAYVAN SADEGHI
PARTNER, BLOCKCHAIN
PRACTICE LEAD
JENNER & BLOCK

LEE SCHNEIDER
GENERAL COUNSEL
AVA LABS

ANDREA TINIANOW
CHIEF LEGAL OFFICER
IOV LABS

This roundtable discussion was curated and edited by Andrea Tinianow and Stephen Palley, Editors of the IJBL.

INTRODUCTION

Stablecoin is the latest category of digital asset to take the world by storm. **Stablecoins helped drive the growth of decentralized automated organizations (DAOs) and Decentralized Finance (DeFI). And, with a total market value of $163 billion, they have become a pillar in the blockchain ecosystem**. Following the Terra/Luna debacle, stablecoins have attracted increased scrutiny, and this scrutiny is not going to go away soon. In fact, it will probably increase until there is a proper regulatory solution. That may be easier said than done.

Stablecoins are not monolithic. Some are issued on a centralized basis and others are not. And those that are decentralized come in all sorts of varieties. At the present time, stablecoins are a bit of a free for all. And their future is not clear. They could be eclipsed by the advent of digital currency issued by Central Banks (referred to as CBDCs). They could fall victim to an overly oppressive crypto regulatory regime or something else, such as an extended crypto winter. In this virtual round table, we share with you current thinking about stablecoins from blockchain attorneys who don't hold back. But since nearly everything in crypto is fluid, many of these comments may be out of date by the time this article is published (and there's nothing we can do about that!)

A special thank you to all of the contributors who shared their insights to make this virtual conversation possible.

ROUND TABLE DISCUSSION

Are stablecoins an innovation or is it new wine in old bottles? Is there technical innovation here that warrants or necessitates new legal/regulatory innovation?

LEE SCHNEIDER: Let's first stipulate that we are talking about fiat-linked stablecoins, rather than stablecoins that might seek to be stable against a different asset or basket. Second, let's acknowledge that old wine often tastes better than young wine and there might be good reasons to put it in a new bottle. To directly respond to the question, in my view the best "innovation" here is blockchain.

People are so focused on the cryptoassets that they forget what blockchains do and why they are important. For stablecoins and lots of other tokens, the best things about them is the blockchain technology and the experimentation it is encouraging. That includes catastrophic failures like UST and Luna, which attempted an interesting concept that is normally the province of nation-sized economies and central banks and perhaps still best done at that level.

On the question of whether new regulation is needed, I think that depends on how you feel about things like Starbucks, Amazon, Apple and other gift cards as well as prepaid cards more generally. It also depends on how you feel about fractional reserve banking and FDIC insurance. Both the bank account and the prepaid card examples are ones in which consumers place their trust in an organization to return their money or equivalent value; one is highly regulated, while the other is not really regulated in the US (Europe, for example, has e-money laws that impose regulation on prepaid and gift cards).

OLTA ANDONI: I really like this question because Lee and I approach it from different perspectives. Since I have been ingrained in the NFT industry, stablecoins represent innovation. **Even though we have yet to see the widespread adoption of stablecoins, we can see some benefits that come with them, the main ones being a store of value (potentially…) and enabling novel forms of exchange in a digital economy**. With each innovation comes regulatory issues triggering the need for regulation to address the risks associated with that particular technology/innovation. Particularly as it relates to stablecoins, the regulation should be around consumer protection, fraud and security issues.

DAVID ADLERSTEIN: Although with the exception of physical cash, our money today exists in the form of ledger entries, the innovation offered by functionally having money on a blockchain (as long as the stablecoin in question does in fact maintain a stable fiat-based value) is very significant.

First, it enables money to be recorded in a ledger without a trusted third party intermediary doing the recording (but without the price instability of some other cryptoassets, such as bitcoin). While that feature poses the risk of abuse such as money laundering, there are also potential significant efficiency gains, including the functional ability to bank the unbanked, to complete rapid remittances and otherwise avoid the friction associated with moving money between financial institutions and environments.

And second, it enables all manner of transactional activity to happen via smart contracts, which offers exciting potential with potentially transformative business effects (with innumerable possible examples including the ability to make a micropayment to read an article or listen to a song, or the ability to pay an employee literally by the hour rather than biweekly).

To the extent regulators may require stablecoins to be 100% backed by highly liquid assets and to be redeemable for fiat money, it can be said that stablecoins will still necessitate the involvement of a trusted third party intermediary, but not as a **transactional** intermediary. While there are scaling challenges, e.g., for ERC-20 stablecoins, friction in the form of gas, the **innovation here is real**.

ANDREA TINIANOW: For the first time, individuals in every part of the world can go online to purchase and hold digital money, and not just any digital money, digital dollars. For people in emerging markets, this is a big deal, particularly in those countries where the inflation rate is high or where governments are not stable. In these instances, holding stablecoins (even those that carry with them a modicum of risk) can provide a great source of value.

Responding to Lee's comment earlier about whether new regulations are needed for stablecoins, the answer is "yes." **Stablecoins issued by a third party like Circle may be similar to a Starbucks or Target gift card because they are issued by a corporate entity, but that is where the similarities end**.

The regulators think so too. The New York State Department of Finance Services ("DFS") recently introduced guidance regarding stablecoins that are issued under DFS oversight. Stablecoins also figure prominently in the draft legislation introduced by Lummis-Gillibrand. There is good reason to have a regulatory regime for stablecoins.

Significantly, with stablecoins, you are not getting dollars. You are getting a claim on a dollar reserve that is held in dollars and other liquid assets (if you're lucky). Unless the stablecoin is backed by fiat, there is risk to the issuer. Without regulations, there is no mandate that the reserves include quality assets or even that the reserves are backed one:one with the stable coins issued.

What are your thoughts about the UST/Luna collapse and algorithmic stables in general. Do you expect the UST collapse to be a setback to or have an impact on the development/use of stables? Does your opinion change when considering stablecoins issued by a centralized organization, such as Circle and USDC?

LEE SCHNEIDER: We should start this answer by noting that footnote 5 of the President's Working Group Report on stablecoins specifically said it was not discussing algorithmic stablecoins because they are a "smaller subset of stablecoin arrangements." I do not expect a significant setback for algorithmic stablecoins from the UST catastrophe. The experimentation will continue and although a bunch of the other algorithmic stablecoins saw short blips in their pegs, most of them have recovered.

I do think there will be some shift to an even greater number of "backed" stablecoins, whether just more money flowing to the existing ones or the creation of new backed ones. **The centralization or decentralization of a stablecoin is not, in my view, a significant factor one way or other for adoption, but it will be a significant factor for regulation, as we already see with Europe's proposed Markets in Crypto Assets ("MiCA") regulation**.

DAVID ADLERSTEIN: The UST collapse is already providing more fuel for regulators to push stablecoins in the direction of the regulated banking perimeter (as per the Lummis-Gillibrand bill and newly issued New York Department of Financial Services guidance).

While it should not be illegal per se to create an asset that is designed to maintain a stable value, the stakes associated with a stablecoin's failure are extremely high, and for all the harm wrought by the UST collapse, the crypto ecosystem is fortunate that it transpired before UST became "too big to fail." **One lesson of the UST experience is that for any algorithmic stablecoin, if there is a scenario where an actor in the market can exploit a design flaw to their pecuniary advantage, they should be expected to do that**.

For complex algorithmic products, stress-testing and crisis planning exercises should become de rigueur, albeit likely administered by developers (perhaps analogous to banking regulators as in the case of financial institutions after Dodd-Frank).

ANDREW BALTHAZOR:

Under U.S. law, fiat-backed and algorithmic stablecoins are two completely different animals. Fiat-backed stablecoins are more akin to a tokenized negotiable instrument, like a bearer bond or an endorsed check. In this sense, issuers should be required to comply with financial regulations similar to banks, such as mandating a certain reserve level and requiring insurance coverage.

Algorithmic stablecoins, however, are likely to be considered securities—because their entire value depends on others' market activity driving the algorithm's engine. If the Securities and Exchange Commission takes this view and treats algorithmic stablecoins as securities, this could severely impact how and to whom such tokens are offered. I would expect the SEC to be closely examining this issue given the spectacular collapse of UST/Luna.

What type of existing asset are stablecoins most similar to? What useful historical analogies are there? And what guidance can they provide?

LEWIS COHEN: To me, algorithmic stablecoins are closer to alchemy than chemistry. We can wish for a way to turn base metal into gold but doing that under lab conditions ain't going to happen.

I understand the support for censorship resistance in a monetary asset but, for those seeking that goal, I believe there will be more success with a unique asset like bitcoin rather than trying to "peg" a digital asset synthetically to the dollar or another fiat currency. I distinguish here assets like DAI that are backed by assets with value, but just not dollars themselves. Depending on the level of overcollateralization, I see no reason why assets like these cannot be successful in the long term.

LEE SCHNEIDER: This question is a bit tough to answer without the specifics of a particular stablecoin's structure. **I see analogues in gift cards and other prepaid cards, bank accounts, money market mutual funds, locally-issued or company-issued scrip, fiat currencies without government backing and others**. These questions about the structure or nature of an asset, that is to say its functions and features or characteristics, are really the big questions right now not just for stablecoins but for all cryptoassets.

The rush to treat cryptoassets as a homogenous asset class (e.g., "all tokens are securities") seems to have subsided a bit, but there is still much work to do on this front. It is hard work because it requires scrutinizing each token individually and understanding it. We do this hard work all the time in other contexts, but in cryptoassets it seems that the temptation to treat everything as being of like kind is too strong. Getting policy makers and regulators to focus on the nature of each cryptoasset remains the biggest issue, in my view, which is why this question is so important but also suffers from being too broadly inclusive when it does not ask about a particular cryptoasset.

Who should have regulatory oversight over stablecoins? Should there be one or multiple regulatory regimes? Do we need new laws/regs or do regulators have the tools that they need? What about the role/relationship between state and federal regulation – should there be one national regulator? Co-equal regulation?

LEE SCHNEIDER: The regulation questions are difficult ones without parsing the different stability mechanisms and the presence of a central authority. Although I do not necessarily agree with all aspects of the way Europe proposes to regulate stablecoins ("asset-referenced tokens" and "e-money tokens", in MiCA's parlance), there is much to recommend a single regulator approach.

A single regulator would, for example, develop expertise, benefit from deep study, data collection and observation, and otherwise consider the market in ways that dispersed regulation likely will handle with less efficiency. Whether it should be a banking regulator, a commodities regulator, a securities regulator or a consumer protection regulator remains an open question in my mind. And I would like to make sure equivalent products that do not utilize blockchain technology are subject to the same level and type of regulation. There is merit to the idea that regulation should be technology neutral.

KAYVAN SADEGHI: I agree that there is a lot to be said for a single regulator approach, and one that is technology agnostic, when speaking about similar products. That said, not all products labeled as stablecoins are similar to each other; each presents different risks and may need different regulatory solutions. It would be helpful to evolve the terminology to better differentiate between stablecoins backed one-to-one by fiat reserves, over-collateralized stablecoins, or other algorithmic models.

For fiat-backed stablecoins, banking regulation seems a better fit than securities regulation. Securities laws are a disclosure-based regime and work well for investments, where even high risks of failure may be acceptable so long as the risks are adequately disclosed and investors can make an informed choice. For fiat-backed stablecoins, **the goal should be to minimize, not just disclose, the risks of failure. Banking regulation concepts (capital requirements and the like) appear better suited to addressing these concerns than a disclosure-based regime**. Banking laws may need to be amended to accomplish this, but trying to use securities laws to fill the void is an imperfect solution.

LEWIS COHEN: I agree with Lee and Kayvan that, at least when it comes to fiat-backed stablecoins, financial regulators are much better positioned to oversee the product. Fiat-backed stablecoins are payment instruments, not "investments" in any meaningful sense, thus treating them as if they were securities blurs that regulatory framework and only contributes to misunderstandings of what securities regulation should be covering.

Stablecoins fueled the surge in DeFi. But, will they go mainstream? For example, a recent headline reported, "FinTech giant Stripe jumps into crypto with a feature that lets Twitter users get paid in stablecoin"

LEWIS COHEN: The idea of "programmable money" is an exciting one, with plenty of opportunities to go mainstream. One can imagine freelancers instantaneously getting paid for work delivered, easier and economically practicable micropayments to content creators, and even uses in machine-to-machine transactions (such as a "smart grid" where a homeowner can program a device to "negotiate" among electricity providers based on pre-programmed rule sets). These uses and many more have the potential to rapidly drive mainstream adoption of stablecoins in everyday settings.

ANDREA TINIANOW: I agree with Lewis, the potential for stablecoins is boundless. However, stablecoins likely won't realize their potential until everyday people believe that they are safe and can be trusted like cash. This probably won't happen until we have smart and effective regulation at the federal level.

What about the interplay between stable coins and DAOs? Will stable coins provide the financial foundation for the growth of DAOs?

DAVID ADLERSTEIN: If DAOs are to conduct business at scale, they need to be able to pay consideration for the goods and/or services that they receive, to receive consideration for the goods and/or services that they provide, and to share economic benefits with their owners.

While it is possible that DAOs could do some of this with fiat money (for example, by setting up an entity as a legal wrapper) or with a cryptoasset with a fluctuating value, **there would appear to be a natural efficiency for a DAO to transact with stablecoins**.

Without stablecoins in the picture, DAOs either have to accept value instability (not a desirable feature of money) or the friction associated with fiat money. Many things are needed for DAOs to grow and scale, but stablecoins can constitute part of their life blood.

ANDREA TINIANOW: And not just DAOs, but also co-ops dealing in digital information. In the future, co-ops will transact in anonymized information that is shared securely, instantly and peer-to-peer. Co-op participants will make payments (and micro-payments) with stablecoins (or some other crypto asset) in real time via blockchain networks.

I want to shout out to blockchain attorney, Eric Hess on this because his podcast, The Encrypted Economy provides excellent insight into co-ops and how they could be used in the blockchain space. One recent episode focuses on farming co-ops, and it was fascinating!

Current payment laws require employees in the U.S. to be paid in U.S. currency. Is this a relic from an earlier time or is it relevant today? Should the law be changed to allow for payment in stablecoins? Why or why not?

OLTA ANDONI: This is mostly an issue for employers that earn revenue in cryptocurrencies. Chances are that they would be more interested in paying their employees in cryptocurrencies. But under both federal law (Fair Labor Standard Act) and many state laws there are several restrictions regarding cryptocurrencies that employers need to consider. Having said that, I think that **employers should have the right to pay employees in stablecoins so long as the stablecoin issuers provide sufficient disclosures** and ensure that the stablecoin is fully backed.

ANDREW BALTHAZOR: **There should be safeguards, though, to prevent employers from creating their own "stablecoin" and then forcing it on employees**. Let's not return to times of company scrip only usable in company towns (virtual or otherwise).

Are fully backed stables a threat to fiat currency? Can central bank digital currencies (CBDCs) be a viable alternative?

LEE SCHNEIDER: Neither is a threat to the other, mostly because they are/will be designed for different use cases. **Stablecoins will be designed for people who want to make cross-border payments, want programmable money and want interoperability of money between different rails**. CBDCs are not likely to have any of those characteristics or, if they do, the government issuers will severely circumscribe them. But this argument comes from an intensely pragmatic view of what the future of CBDCs will be.

JASON GOTTLIEB: Fully backed stables are unlikely to ever be a threat to fiat as a whole, because there just isn't enough liquid backing for that. There are about US$2.2 trillion dollars in active circulation right now. (As always, FRED is a great data source.)

Other markets are a bit smaller, but still sizeable – about US$1.5 trillion worth of euro, about a trillion dollars' worth of yen, etc. That's a lot of cash to try to "replace" with a stablecoin that needs to be backed with something.

Obviously, the asset markets that would be required for potential backing are far larger – the total market cap of the S&P 500 alone is around $40 trillion, and the Dow Jones companies around $10 trillion, for example. Other potential backing assets – gold, oil, real estate, etc. etc., add trillions more. (Give or take; what's a trillion dollars or two between friends?)

But backed stables aren't likely to be able to use even a tiny fraction of those assets. First, doing so would impact the valuations for those assets pretty significantly. Right now, the top three asset-backed stablecoins are collectively valued at around $150 billion, and the size drops off pretty significantly after that. So the overall impact on the markets for the assets backing them is small.

Second, using illiquid assets for backing – like real estate or structured assets – would be riskier. If redemptions were demanded, handing out cash or liquidating treasury bills or commercial paper is easier; I can't imagine backing stablecoins with high percentages of, say, long-term real estate investments.

Third, using backing assets that are more than just cash or treasury bills makes it more likely that a company would be regulated as an investment company, which might change their nature significantly. (Whether registration would be required is an open question, one of crypto's many "square peg, round hole" problems.)

So backed stables need to back with liquid assets, and the more stablecoins were used – requiring liquid backing – the less non-stablecoin liquidity there would be in the markets. Hard to see the United States government (or the EU, Japan, etc.) even allowing that.

But what about a smaller country? Well, maybe, and we've seen some feints in that direction from El Salvador and others. Time will tell how that experimentation will play out.

Which leads us to the CBDC – a way for a country to move to a blockchain standard, without allowing a private stablecoin to usurp its financial control. A CBDC could be a viable alternative from a governmental point of view – it's not too far off from the digitized dollar anyway (which, let's face it, is most dollars these days). And **it would give the government unparalleled control and surveillance over the lifeblood of our society**. That's arguably a positive factor for a government trying to monitor and squelch bad financial (and other) behavior, but, for the same reason, it's pretty disastrous for financial privacy, and in my opinion, the reason most of the technical community hates the idea.

So frankly, I am pessimistic about the future of CBDCs (outside the People's Republic of China, perhaps). Nobody who thinks about the privacy implications really wants it, and I don't see it happening without the support of the technical community.

COLLINS BELTON: If cryptocurrency is going to supplant fiat in some way, it is unlikely to be in the form of an asset fully backed by real world assets - especially one pegged to an existing fiat currency - unless or until a substantial transformation occurs across society.

This transformation would need to be one that entailed either (i) intangible, digital assets ballooning many multiples in value or (ii) an effective digital title and licensing scheme being developed that enabled the digitization and transfer of a significant swathe of tangible and valuable productive real world assets, which are both unlikely to occur at scale in the near future to a point that would enable a stablecoin not backed by fiat currencies to contend with fiat.

The reason I feel this way is that **one of the key reasons stablecoins have exploded is because they effectively serve as something like a bridge between crypto native systems and participants and "meatspace."** People are using stablecoins to do everything from making venture capital investments, to compensating service providers, to buying standard goods and services in ways that may not be feasible or desirable with other cryptocurrencies that are subject to material value fluctuations.

The rapid adoption of "fiat backed stablecoins," even by crypto natives, suggests that a key component to their success has been the easy narrative of 1:1 backing, regardless of the veracity of those claims. Introducing complex mechanisms and exotic pegs to assets such as gold or real world assets undermines this simple narrative and muddies layman's understanding.

Historically, attempts at making these types of alt-currencies have failed and I suspect that stables treading this path while attempting to be a bridge to the real world will fail (although those contained to digital spaces may find limited success in niche communities).

A CBDC can be a viable alternative to existing fiat in my opinion because there's nothing that makes a CBDC and fiat currency status mutually exclusive. In fact, to the extent that CBDCs are introduced, there's really only two broad models that will work, and only one is likely to win out long term. That is, either a CBDC is wholly controlled from the top down by a national government, or some private public partnership wherein the government allows private parties to leverage central banking rails which is likely to be the "winning" CBDC model.

In the former model, there won't be much distinction between fiat currency as it exists today and a CBDC, except for the loss of privacy inherent to cash (but this is already under attack with the various forms of digital fiat currency accounts that exist today).

In the latter, we could call that an alternative, but if anything, it would be better to reference that as an "evolution" of the fiat model, just as modern day central banking was an evolution of the fiat model at the time.

What is the bull case for stables? The bear case? Do stablecoins in their current form present systemic risk or are risks misunderstood/exaggerated?

LEE SCHNEIDER: Hopefully, there is neither bull nor bear case on stablecoins because they should not fluctuate much at all in value. I refer to my answer to item 1: it's the underlying technology that allows for the transfer of value over the internet anywhere in the world. As more and more people recognize this capability and the speed and ease it brings, stablecoins should see wider adoption. **The winning stablecoins will be the ones people trust**. How that trust takes hold, how it remains strong, and whether it ever fades are questions beyond my limits.

DAVID ADLERSTEIN: From an investor lens, I emphatically agree with Lee that there should be neither a bull nor a bear case, but from a categorical standpoint, I think there is both a bull case and bear case.

The bull case is that one or more stablecoins see wide adoption and start to be used in a manner that transcends participation in DeFi to encompass every day financial activity such as paying for goods and services, and institutional usage, as well as being used in the context of smart contracts as the promise of blockchain technology is increasingly realized.

And in this bull case, there is no systemic failure and regulators and users achieve a comfort level with stablecoins both in terms of their design (including liquidity and bankruptcy remoteness) and the rails that they run on being truly robust.

In the bear case, there is another significant stablecoin failure, stablecoins remain a relative backwater of the financial system, and/or stablecoins are overregulated or fall prey to rent-seeking to a point that the efficiency gains are lost. **Regulation is necessary, and institutions need incentives to issue and transact in stablecoins, but there is a balance to be struck**.

Another bear case for stablecoins is that a CBDC is adopted that supplants their use although there would of course be benefits from a well designed CBDC.

Do stablecoins present unique issues/ challenges for anti-money laundering (AML) and financial crime surveillance?

JASON GOTTLIEB: Interestingly, I think stablecoins make life easier for AML and financial crime surveillance. It's true that stablecoins make it easier to move large sums of money across borders without permission or the knowledge of an intermediary, such as a bank, who might be required to report that transfer.

But, as I have said repeatedly in the past, trying to launder money with crypto (stablecoins or otherwise) is just dumb. If someone is trying to commit financial crime, I would not recommend doing it in a way that leaves a publicly available, immutable trace of the crime. (This is not legal advice! The legal advice is, don't commit crime at all!)

The dirty little not-so-secret secret of AML and crypto is that many law enforcement officials (FBI, FinCEN, DOJ prosecutors, etc.) love crypto, because it's more easily traceable than cash, or other laundering techniques. Companies like TRM Labs and Chainalysis have incredibly sophisticated techniques to trace movements across blockchains. Sure, there are ways for criminals to muddy the waters – mixers, privacy coins, "peel chains," and veils of anonymity – but similar methods exist in the "real" world as well, and frankly, they're a lot easier and more effective outside crypto than within the digital walled garden.

The most pressing challenge for AML/surveillance is the intersection of anonymity, internationality, and time. Because stablecoins can be used to send money nearly instantly, all over the world, with low friction, and through anonymous wallets, bad actors will leave a trail, but they can make that trail very long and cumbersome. It can take significant time and law enforcement personnel and resources to trace a chain, and then unveil the real people at the ends of the chain. It's hard work; lots of digital shoe leather. And that hunt can detract from other work the enforcers could be doing.

Tracing and surveillance are particularly problematic when the bad actors are in countries that are not cooperative. Laundering stablecoins within the United States is difficult – woe be to the American wannabe criminal who keeps his financial bad acts entirely onshore. But a North Korean hacking group doesn't have to bother much with veiling itself, or fancy tricks for concealment. Once the money is in North Korea, it's pretty much impossible to recover.

These arguments hold for all of crypto, not just stablecoins. But to the extent that people might choose stablecoins as a substitute for fiat, instead of other crypto, the rise of stablecoins as an "intuitive" substitute for fiat will make life easier for law enforcement and surveillance.

COLLINS BELTON: While stablecoins do introduce new issues and challenges for AML and financial crime surveillance, I'm inclined to agree with Jason that stablecoins are more of a boon for financial regulators than a drawback in their current form.

In fact, in some ways, I think the inverse of this question is more interesting. That is, **do stablecoins and/or CBDCs present unique issues/challenges for financial and individual privacy to the point that we should be more careful in encouraging widespread adoption?**

What's most interesting is that the answer to addressing some of the privacy concerns inherent to most stablecoins also "creates" some of the perceived issues for AML and financial regulators. Specifically, tools like Tornado Cash, privacy preserving techniques, and natively anonymous blockchains all provide limited means of ensuring individual privacy, but these things are frequently the same items highlighted by regulators and law enforcement as problematic from a crime or national security perspective.

This debate within crypto is a microcosm of the broader societal debate that has been occurring since the Snowden revelations (and really, since the dawn of encryption and *Bernstein*) that pits national security interests against individual privacy rights.

Perhaps controversially, I'd argue that the unique issues/challenges for AML and financial crime surveillance created by using privacy preserving tools and techniques may be the only way that this technology can be adopted "safely" on a wide scale.

If stablecoins and cryptocurrencies more broadly are adopted at scale, the breadth of transactions and personal information that will be inherently transparent to anyone in the world will be breathtaking. While this level of transparency is arguably a boon in areas like politics or banking where obfuscation has notoriously created societal woes, it's unacceptable for an average person in their daily life and creates situations where governments and criminals may have unprecedented insight and improper leverage over the average person's private affairs.

For this reason, the focus on whether there are novel challenges to AML and financial surveillance is sometimes overstated relative to the concerns we should have on individual privacy rights when considering widespread stablecoin adoption.

ANDREW BALTHAZOR: I agree with Jason and Collins—stablecoins have the potential to help, not hinder, anti-money laundering and financial crime surveillance. Recently, a cryptocurrency exchange client approached my law firm about freezing and recovering the proceeds of a hack from the exchange.

Ordinarily, asset freezes and recovery is only possible when the wallet address holding the assets is in the custody of a third party, like another exchange. In this case, the client had traced the funds to a specific wallet address but we did not identify any third-party that had custody of the address itself. But the suspected hacker had purchased a significant quantity of the USDC stablecoin.

USDC includes the capability to deny access to an address, preventing the person controlling the address from transacting the USDC. **We requested–and the Court granted–a temporary restraining order directing Centre Consortium, the entity controlling the USDC protocol, to freeze the USDC at the address of the digital wallet**. The Centre Consortium implemented the freeze immediately.

Moreover, we were able to accomplish all this within 48 hours of being contacted by the client; this would be impossible with conventional fiat currencies (and most other cryptocurrencies).

I disagree that mass adoption of privacy preserving tools—tools like Tornado Cash which can be abused to enable money laundering—is the answer to the transparency provided by the blockchain. Instead, on- and off-ramps to the financial system should develop a travel rule that transmits know-your-customer information along with blockchain transactions, but in a way that is encrypted and only readable by the on- and off-ramps serving as gateways between on-chain and off-chain transactions. Some private companies are doing just that via the Travel Rule Information Sharing Alliance (TRISA).

ARTICLE II

RECENT DEVELOPMENTS HIGHLIGHT FUNDAMENTAL LEGAL CONSIDERATIONS FOR DAOS*

DAVID ADLERSTEIN
WACHTELL LIPTON

SABINA BELEUZ NEAGU
WACHTELL LIPTON

DAVID KIRK
WACHTELL LIPTON

KEVIN SCHWARTZ
WACHTELL LIPTON

INTRODUCTION

We recently wrote about the emergence of a new breed of business organizations — decentralized autonomous organizations (DAOs) — to contend that the governance design for these blockchain-based organizations should heed some of the hard-fought lessons that have helped to form the pillars of modern corporate governance.

It is also important to confront certain features of DAO governance that present distinct challenges for counterparties seeking to invest or engage in commercial transactions with DAOs. A few recent DAO controversies highlight the need for greater clarity in the legal status of DAOs, more robust governance, and a reckoning with the distinct legal and commercial risks that may accompany transacting with a DAO.

Potential investor liability

A recent putative class action filed against one DAO raises the specter of potential liability for DAO investors, potentially even for mere purchasers of DAO governance tokens. In this case, after a theft of cryptoassets from a blockchain protocol controlled by the bZx DAO, the users whose assets were stolen sued various parties that included the DAO itself for failing to maintain adequate security measures. The suit alleges, among other things, that because the DAO was not established as a legally recognized entity, it should be treated as a general partnership, such that each DAO member — potentially including every holder of a bZx DAO governance token — should be jointly and severally liable for the DAO's alleged negligence.

This unusual general partnership theory is not a central aspect of

*This article was created as a client memo by attorneys at Wachtell Lipton. They have provided us permission to print it here.

the lawsuit and has not yet been addressed by the court.

Nevertheless, the theory bears close attention as investors who participate actively in a DAO's governance may face greater risk of unlimited liability as constructive general partners.

Consequently, DAO organizers should consider forming traditional business entities (so-called "legal wrappers") for DAO activities where liability concerns are heightened. Prospective DAO investors, for their part, should be mindful of the risk of investing in organizations that lack a traditional legal entity's liability shield and consider self-help measures, such as forming limited liability entities to hold DAO tokens.

Breach of commercial agreements

A recent dispute between Merit Circle DAO and one of its earliest investors highlights the uncertainties facing counterparties that enter into commercial arrangements with a DAO. Here, a seed investor entered into an investment contract with a legal entity affiliated with Merit Circle DAO that entitled the investor to a large allocation of the DAO's governance tokens.

After the tokens grew substantially in value, an individual member of the DAO community proposed that the investment be unwound on the basis that the investor had not been sufficiently active in supporting the DAO. Management of the DAO's affiliated legal entity (that had entered into the investment contract with the investor) objected to the proposal, noting that the investor had fulfilled its contractual obligations and that negative community sentiment cannot justify a breach. The DAO nonetheless approved the proposal by majority vote. The parties eventually reached a negotiated resolution that avoided litigation.

This dispute highlights important considerations for DAOs and their counterparties when entering into agreements. Clear and intentional breaches that may be unusual in a typical commercial environment could arise more frequently in settings where a DAO's members, through express governance rights or community pressure, could cause the contracting entity to breach an agreement. The prospect of such conduct could hinder DAOs' ability to enter into commercial agreements on desirable terms.

Counterparties should be prepared to litigate to enforce contracts with DAO-affiliated entities, although pursuing contractual remedies may be complicated by open questions about the legal status of DAOs, the pseudonymity of their participants, and jurisdictional issues. Careful drafting is essential to ensure clarity as to the remedies for a breach and to delineate what effect, if any, a vote by DAO members can have on contractual obligations.

Altering the functionality of a blockchain protocol

Another recent proposal approved by a DAO underscores the risk that a majority vote could disparately treat users of DAO-controlled blockchain protocols — potentially including the expropriation of assets. The largest user of the Solend DAO's decentralized finance (DeFi) protocol had deposited into the protocol a significant amount of cryptoassets as collateral to borrow stablecoins. Under the mechanics of the protocol, if the market value of the deposited cryptoassets fell such that the loan became under-collateralized, the protocol would automatically liquidate the deposited cryptoassets.

The proposal — made by the Solend code development team — requested emergency power to take over the user's account and complete an over-the-counter liquidation in the face of perceived risk of the loan position unwinding in a disorderly manner. The DAO overwhelmingly approved the proposal, although later voted to reverse the decision in the face of criticism. And this situation was not a unique occurrence. As another example, the development team behind Bancor (another DeFi protocol) also recently determined — unilaterally — to modify an important feature of its protocol and then sought ratification of this action by Bancor DAO after the fact.

The ability of a centralized body to modify a blockchain protocol calls into question the degree of some DAOs' actual decentralization in certain circumstances.

Counterparties should evaluate the extent to which a DAO (or its development team) can alter the functionality of the protocol to modify an idiosyncratic commercial arrangement and potentially damage the counterparty's economic position. Counterparties should also assess the DAO's governance framework — for instance, whether the development team has actual or effective voting control.

Up-front risk assessment is prudent when transacting directly with DAO-affiliated blockchain protocols, as there will typically be no written agreement between the user and the protocol other than the source code itself. As a result, aggrieved users may be left with no clear legally responsible counterparty, and instead bear only nuanced, untested arguments regarding implied agreements or theories such as unjust enrichment or conversion.

* * * * *

Setting aside the merits of the parties' respective positions in the controversies above, **we believe these situations underscore the need for greater clarity regarding the legal status of DAOs and their members, the urgency of developing and enhancing DAO governance best practices, and the importance of a DAO's counterparties to carefully consider the legal and commercial risks that may be attendant to transactions with this novel form of business organization.**

ARTICLE III

DECODING DEFI REGULATION: CHALLENGES AND OPPORTUNITIES

HANNAH MEAKIN
PARTNER, LONDON
NORTON ROSE FULBRIGHT

PROFESSOR PETER MCBURNEY
CO-HEAD OF TECHNOLOGY
CONSULTING, LONDON
NORTON ROSE FULBRIGHT

ALBERT WEATHERILL
COUNSEL, LONDON
NORTON ROSE FULBRIGHT

INTRODUCTION

Technological innovation has continued unabated over the course of the past few years, and financial services has fared no differently. Replicating the core Web3 principle of shifting control and ownership away from a centralised operator, decentralised finance (DeFi) has created a new model for financial services that threatens to disrupt the existing order. In this article, we will explore the core characteristics of DeFi: how it works; what the key use cases are; and what regulatory challenges it creates.

WHAT IS DEFI?

DeFi is a collection of financial applications and services involving cryptocurrencies, tokens or other digital assets implemented by means of smart contracts (automated programs) running on blockchains. Many of these services are decentralized apps (D-Apps), with no central person or financial organization in control. The applications are generally permissionless (ie, open to anyone to participate), rely on open-source code, and are operated by the community of participants. D-Apps are typically interoperable, using smart contracts on blockchains to exchange assets or to transfer data between one another.

These features lead to several potential benefits for market participants. DeFi provides transparency based on a permissionless ledger. It provides transparency and predictability based on the open source code. It enhances competition because of the transparency that can contribute towards the avoidance of monopolies, as it should be relatively easy for new market contestants and disruptors to challenge traditional players. The use of blockchain cryptography provides confidence to users regarding the security and immutability of transactions.

Arguably, DeFi prevents single actors from manipulating the DeFi ecosystem. Even if they do manage to manipulate the DeFi cosystem, manipulation should be relatively easily identifiable by other market participants. DeFi reduces transaction costs and market friction and thereby increases transaction velocity in clearing and settlement of trades, which can result to an increase in certainty of ownership and further transparency, which in turn, can be beneficial for the larger DeFi ecosystem.

THE RELATIONSHIP BETWEEN WEB3 AND DEFI

Web3 refers to the latest iteration of the World Wide Web's (WWW) evolution and is centred on using decentralised blockchain technology to create a more equitable WWW. While Web3 refers to a larger technological ecosystem, DeFi is a segment of this ecosystem. Whereas Web3 is imagined as a decentralised version of the WWW, DeFi leverages the fundamental principles of Web3 to facilitate a decentralised financial system that is no longer reliant on centralised operators.

While the full vision for Web3 is yet to be realised, a key feature of Web3 is that shared ownership with respect to protocols and propositions creates opportunities for capital appreciation through cryptoassets, NFTs and other forms of digital assets. Many Web3 projects have a native token (ie, a cryptocurrency that runs on someone else's blockchain platform), and that token may grant certain governance rights or facilitate transactions occurring within the ecosystem of that project.

By playing an active role in the community of a particular Web3 project, participants may receive a portion of that project's tokens, which may also have economic benefits. A similar philosophy is inherent in DeFi, whereby users of a particular protocol can be empowered to shape the future of that project as an active member of the community that takes decisions with respect to that protocol, often through holding the tokens of that protocol.

USE CASES OF DEFI

Whilst DeFi provides an arguably limitless base of use cases, there are certain areas of the financial services ecosystem where its adoption has been more advanced, and we set out examples below.

Exchanges

Traditionally, an exchange is run by a centralised organisation, commonly known as an operator. The operator is responsible for determining, among other things, which assets can be traded and in what specific form, and deciding which criteria participants should satisfy before they are permitted access to the exchange. Operators are also responsible for setting the rules that determine how bids and offers are matched, maintaining liquidity by developing market making frameworks, and overseeing orderly and fair trading on the exchange.

To date, exchanges for crypto assets have tended to have a centralised operating model like those deployed by Binance, FTX, Coinbase, Kraken and others. However, decentralised exchanges (otherwise known as DEXs) allow users to exchange assets on a peer-to-peer basis without the need for an intermediary or operator. Popular DEXs include Uniswap, PancakeSwap and dYdX. These DEXs rely on automated smart contracts to execute trades instead.

The terms of the transactions are built into smart contracts and they can involve assets that are relatively illiquid or traded in volumes that are too small for larger exchanges.

The basis on which one asset is swapped for another is also built into the smart contract along with the pricing mechanism. Participants may even be able to develop the smart contracts to create and trade bespoke contracts in terms of asset class, size, maturity and price. The smart contracts can be used by participants to hold their assets to facilitate settlement. Many DEXs are open to participation by a wider range of users than traditional exchanges.

Lending and yield generation strategies

Lending is an area of huge growth when it comes to DeFi. One of the core problems with the cryptoassets ecosystem is that assets are typically held in wallets for long periods without any ability to generate income on those assets. This differs to more traditional structures like savings accounts or cash ISAs, where a return is generated on invested assets.

DeFi has evolved to provide a solution which is to some degree akin to a more traditional securities lending type arrangement, whereby the ownership of the relevant cryptoassets that are stored in the wallets is effectively transferred or contributed to the protocol and the smart contract governing that protocol then lends those assets to third-parties, generating a yield or fee for the original lender. The smart contract determines the nature of the loans and will undertake the relevant underwriting of the borrower. Returns on the loans are then usually paid in cryptoassets and automatically credited to the wallet address of the original lender.

Beyond lending, other yield generation strategies have evolved. In these arrangements, cryptoasset holders contribute their assets into a particular protocol and the protocol then automatically determines how to allocate those assets into different strategies. The strategies could include lending, but also automated market making (contributing the assets for liquidity on centralised exchanges and DEXs) and staking. For companies like Compound and Aave, the overall strategy is, therefore, to generate a yield on the use of cryptoassets which would otherwise sit dormant in a wallet.

DAOS

Decentralised autonomous organisations (DAOs) are platforms operating in accordance with rules and smart contracts coded on a blockchain and enable users to interact with the platform without (as the name suggests) a point of centralised control or intervention.

A typical DAO structure is run through a smart contract, with its own native token usually held by its users. The native token can then be used to interact with the platform by using the platform's products and services or by being involved in governance processes of the platform. The DAO might have a real world committee or board type concept, which might be deigned to act as a circuit breaker to white list certain proposals or restrict certain governance decisions. For example, the real-world committee may consider and endorse proposals for new versions of the protocol and its operating software, including proposals for forks.

A significant obstacle facing DAOs is the uncertainty surrounding their legal and regulatory status since most legal systems do not yet recognise them as forms of legal personality. This presupposes it is possible to identify the applicable law in the first place but that is inherently difficult when there is no centralised operator that would otherwise create a jurisdictional nexus and persons from many countries may hold tokens or otherwise participate.

From an English law perspective, the concept of a DAO has similarities to a general partnership between some or all of the token holders. If a court were to come to this conclusion, that would create a number of risks, including the rights, duties and possible regulatory obligations that may be imposed on the members of the partnership. Assuming there is no formal partnership agreement in place stating the contrary, courts could attach unlimited liability to the members for the debts and obligations of the general partnership.

From an English regulatory perspective, a DAO may also resemble certain features of a collective investment scheme, particularly where those who participate benefit from the development of some underlying project. While the ability for token holders to participate in decision making should undermine the concept, the courts have made clear that participants must have real day to day control in order to avoid being a collective investment scheme and not all DAO structures may pass this test.

THE CHALLENGES OF REGULATING DEFI

Many regulators take a technology-neutral approach to regulation, such that market participants fall to be regulated based on the activities that they perform, irrespective of how technological the performance of those activities may be. **However, proclaiming a technology neutral approach to regulation and applying existing legislation and regulation to technological innovation in practice is easier said than done**.

By its very nature, **DeFi creates complex legal and regulatory considerations and whether and how it should be regulated is open to debate**. In this section of the article, we provide certain examples of the challenges that arise when approaching DeFi from a legal and regulatory standpoint and seek to offer some thoughts on how these challenges could be addressed.

Who to regulate

A major challenge of DeFi is identifying the relevant person to regulate. This question is normally fairly obvious in centralised arrangements, but when a protocol or arrangement is decentralised, it becomes increasingly difficult to point to a particular person or group of persons and state that it is those persons to whom regulatory obligations should apply.

Many DeFi structures involve a software development firm that builds the original protocol and smart contracts before the community assumes control for its ongoing deployment and maintenance.

Should those persons be regulated because they developed the original code? That approach is not commonly taken within financial services when considering the role played by technology providers who do not themselves perform regulated activities.

Should the founding team by regulated? Again, this depends on their level of control – if they do not control a decentralised protocol, it is hard to see why, by virtue of founding it, a person or group of persons should be held entirely responsible for regulatory compliance.

Given community-based decision-making, how might a regulator view the involvement of multiple parties in the decision-making process? Should all of those community members be held to be performing regulated activities by virtue of their role in the governance process?

These questions stretch far beyond the mere academic, rather their answers could go a long way to determining whether DeFi has a truly viable and scalable future, or whether it is simply a gimmick that has no real ability to align with our existing financial services regimes.

Regulatory leakage and geographical nexus

Even if a viable candidate for regulation can be identified, an additional challenge that arises is the concept of regulatory leakage in the application of regulatory obligations to that person. Some decentralised structures may be perceived to be general partnerships, which under English law create joint and several liability for the partners. There is a risk, therefore, that various other actors inadvertently assume responsibility for regulatory compliance, many of whom may not have the resources or knowledge to comply with the relevant obligations.

In addition, DeFi projects are geographically diverse and touch a number of jurisdictions, and many have no "host" jurisdiction or place of establishment. Consequently, it is unclear which jurisdiction's laws would apply.

For example, if somebody loses money in a particular country due to the use of the protocol, or if the protocol becomes insolvent and there is a shortfall or total loss of assets, local regulators might conclude that they have jurisdiction in that particular case and seek to apply consumer protection rules or local regulatory requirements.

But without a habitual resident or permanent establishment, it remains to be seen how regulators might practically enforce their supervisory powers in such circumstances.

Does regulating DeFi mean regulating technology?

How regulators should approach regulation for DeFi is a nuanced question. Existing financial services regimes were not designed with something like DeFi in mind, rather their application relies heavily on centralised operators and physical presence. Without those two key features, it becomes an open question as to whether existing regimes are capable of working with such a radical departure from that for which they were designed.

An alternative is to create a new regime to address DeFi, building out specific rules that apply specifically for DeFi. One possibility is to regulate the technology itself but it is difficult to see how this would work when technology has no legal personality. Notwithstanding the obvious complexities, some consider this approach to be the primary mechanism for developing tailored regulation.

An arguably less extreme approach would be to identify aspects of centralisation within the apparent decentralisation and in fact some regulators have questioned how decentralised most DeFi arrangements actually are.

For example, a majority of governance tokens might actually be owned by a particular person, who can in reality control the protocol through the governance rights even though there are many participants in the community. It might even be possible to identify persons who play a pivotal role in different elements of the protocol and seek to regulate them in relation to their activity only, such that those who design a particular protocol can take responsibility for what they have done but do not take responsibility for how others may develop or use their work in ways they did not envisage or have control over.

This may be a question of designing a series of more appropriate regulated activities for such purposes.

There is also the possibility of regulating the persons who use a protocol for investment purposes, rather than the persons who are providing it. In some ways this seems like a change in emphasis to the current regulatory approach but it is not so different to the way some regulated activities operate today, particularly in the OTC space. That said, it might be difficult to enforce and could exponentially expand the number of persons who are in scope of the regulatory framework, which might itself lead to additional challenges.

As indicated, the potential solutions all have their complications and none of them seems likely to work in all potential manifestations of DeFi.

CONCLUSION

DeFi represents a segment of Web3 and promises to revolutionise the world of traditional finance by offering more control and transparency to its users. The rapid expansion of DeFi use cases has given rise to an active dialogue on the legal and regulatory framework surrounding DeFi.

Inevitably, there is always a time lapse in the development of regulation because regulation is responding to adaptive changes and practices in the market.

Particularly for DeFi, regulators are seeking to understand the use cases, systemic risks and the possibility of consumer harm because they recognise that it is important to assess the landscape in order to reach the right conclusions as to 'whether', 'when' and 'how' DeFi should be regulated, whether it is appropriate to apply existing law or whether they should adopt the route of creating new laws to reflect the nuances of this particular technology.

ARTICLE IV

METAVERSE AND PRIVACY

DR. MATTHIAS ARTZT

SENIOR LEGAL
COUNSEL
DEUTSCHE BANK

GARY WEINGARDEN

ASSISTANT VICE PRESIDENT,
DATA PROTECTION OFFICER
NOTARIZE, INC

INTRODUCTION

From Facebook's recent decision to rename itself "Meta" to Epic Games' billion-dollar investment in metaverse technologies, the metaverse has dominated the news and will likely continue to do so over the next several years. To date, there is no universally accepted definition for the term, "metaverse" and, for many, it suggests a new, but still undeveloped future of the internet.

According to J.P. Morgan, the metaverse is a seamless convergence of our physical and digital lives, creating a unified, virtual community where we can work, play, relax, transact and socialize.[1] That said, most conceptualizations of the metaverse include the use of virtual reality (VR), augmented reality (AR) and avatars,[2] connected by a massive network.

Another key feature is that there is actually no one virtual world, but many worlds which are taking shape to enable people to deepen and extend social interactions digitally.[3] This is done by adding an immersive, three-dimensional layer to the web, creating more authentic and natural experiences.

As a result, a likely feature of the metaverse will be interoperability.[4] An interoperable metaverse would allow users to transport their avatars and other data, including digital assets, between metaverse applications, regardless of whether those metaverses are under common ownership or operation. Retention of a user's metaverse identity and ownership over their digital assets could be accomplished, among other ways, through blockchain technologies.

As with any innovative technological development, the metaverse will raise novel and complex legal issues related to intellectual property rights, digital security, privacy and identity (and self sovereignty).

HOW DOES DATA PRIVACY POLICY APPLY IN THE METAVERSE?

Applying privacy rules to virtual identities

Consumers typically participate in the metaverse by using one or more

[1] J.P. Morgan/Onyx, Opportunities in the metaverse (2022), available at: https://www.jpmorgan.com/content/dam/jpm/treasury-services/documents/opportunities-in-the-metaverse.pdf?mc_cid=0b22b34707&mc_eid=55476ebd9d.

[2] An avatar is a computer user´s representation of himself/herself, usually in the form of a three-dimensional model, through which that person interacts in a virtual world.

[3] In that article referred to as "the metaverse".

[4] Clifford Chance, The metaverse: what are the legal implications? (Feb. 2022), available at: https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2022/02/the-metaverse-what-are-the-legal-implications.pdf.

avatars or virtual life identities. The question arises whether virtual life activities and identities can be traced back to real individuals.

Most systems permit users to create avatars without providing personal information when they create their avatars' profile data.[5] Significantly, that doesn't mean that the consumers are anonymous.

On the one hand, metaverse platform owners know which account and user created the avatar, so to them the avatar is not anonymous.

However, avatars can, at best, be pseudonymous. And the avatars's in-metaverse actions and statements will be attributed to the avatar, which weakens any protection pseudonymization offers for two reasons: First, the avatar itself develops a sub-identity, which identifies the avatar in-metaverse. Second, the sub-identity is likely to leak information about the real-world identity, either through behavioral or knowledge-based clues.

Another issue is whether or not the avatar has its own privacy or it is just a pseudonymous, animated version of the individual behind it. Provided that privacy rights can be attributed to avatars, the follow-up question must be taken into consideration whether they or their "owners" have in-game (or, less likely, real world) rights and remedies against other avatars or their related users/individuals for the violation of their rights.

How do privacy rules apply?

Protecting data transferred across the metaverse

Personal data of users will be at particular risk of exploitation given the vulnerabilities involved when data is ported from one metaverse to another one (e. g., data breaches, scams, etc.).

Further, platform operators and owners will need extensive agreements to govern data transfers, information security standards, and responsibility for compliance (as well as data breaches, which could cause even more chaos than they do today).

Further, the metaverse typically includes virtual advertising (e.g., if brands are using NFTs and virtual items to directly promote their products and services to metaverse users). Chances are that brands will employ avatar-based influencers, participate in sponsored events or engage in other metaverse activities.

All of these activities can create opportunities to collect personal data of metaverse users for advertising or communication purposes. **There will be a desire for implementing strict and transparent privacy standards aiming to protect the rights of consumers capitalizing on metaverse offers**.

Metaverse as melting pot of many privacy regimes

It is apparent that the metaverse cannot be limited to one or a few data privacy regimes since it has a global reach and offers its features to users irrespective of where they are located.

In many cases, multiple privacy regimes will apply to the same data and even the same individual. For example, the European data protection

[5] https://yourstory.com/the-decrypting-story/decoding-identity-metaverse/amp

regime, GDPR, allows for any business located anywhere in the world to fall under its terms if a business offers goods or services in the European Union or monitors the behavior of EU citizens, even though it has no physical presence in Europe (article 3 sec. 2 GDPR). European users of a metaverse operated by an US-company may thus exercise their rights under the GDPR.

In the metaverse, that EU data subject may be in a virtual nightclub with a Japanese citizen and a California resident. Physically, all can still be in their homes, each subject to a different privacy regime. Privacy law has not quite caught up to state and international boundaries yet, and we are years away from reaching consensus on choice of privacy law in the metaverse.

This is likely to generate complex conflicts between the requirements of the regulations from differing jurisdictions, i.e. data breach notification requirements. Therefore, it's tempting to include a "privacy law selection clause" in the Terms of Service (ToS) of the particular metaverse. There's probably no penalty for including such a clause, but privacy laws tend to grant little validity to this approach.

For example, the California Consumer Protection Act (CCPA), applies to natural persons who are Californian residents, as defined in Section 17014 of Title 18 of the California Code of Regulations. That's how the statute defines Consumer, and that's who is protected. There is no provision that allows Consumers to opt-out of coverage, and no way for others to opt-in. Instead, Section 1798.192 says that attempts to waive CCPA rights are against public policy and declares them "void and unenforceable."

Whether this kind of language is included in terms of service or not, it's not a surefire success. At least, forum selection and dispute resolution clauses provide some certainty about where any litigation will be resolved and who will resolve it. Other clauses may provide guidance as to which law applies to interpreting the metaverse ToS. None of these approaches is likely to work if a regulator seeks to conduct an investigation. And this kind of clause isn't universally enforced around the world, so one may still face litigation in several forums.

In summary, it will be crucial for companies to understand which privacy rules will apply to what parties and to which data.

Enforcing data subject rights in the metaverse

Who is the addressee for enforcing data subject rights?

Irrespective of which data protection rules apply, the question arises against whom the individuals may exercise their rights. That is not apparent since the metaverse is a virtual world and the operators who are typically acting as controllers will often not be inclined to disclose their identity voluntarily and to comply with any data subject right requests. They may hide them behind email aliases or other proxies. This challenge can be magnified if the user's privacy has been invaded by another user (here pseudonymity is a cost instead of a benefit), an advertiser, or other commercial entity.

Divergent data subject rights across different privacy regimes

There are diverging rights and obligations depending on which privacy regime comes into play. Under the GDPR, the controller must disclose the information mentioned in article 13 sec. 1 GDPR.[6] Further, the individual can request access to all data collected (article 15 GDPR), its rectification (article 16 GDPR) or erasure (article 17 GDPR) under certain circumstances.

Whenever an individual is consuming services or, for instance, buying NFTs in a metaverse, its personal data is collected and stored.

For example, a business which offers goods and services should take into account that it can be the addressee of various data subject right requests it has to comply with. If a well-known international brand has established a virtual store in a metaverse operated in the U.S., and the user is domiciled in Europe, the GDPR will apply pursuant to article 3 sec. 2 GDPR and any non-compliance could spark major fines or lawsuits. Many other global privacy laws could apply based on similar factors.

While the specific legal requirements may differ, most modern privacy laws require providing disclosure at collection (types of data, some kinds of processing activities alike, “sale” of data or “sharing”) and many also distinguish between “ordinary” data and “sensitive” data.

As noted above, determining all the potential privacy law requirements applicable to metaverse users will be complex, and while there are many similarities, the devil is in the details.

For example, applicable privacy laws will likely include different triggers for breach notice and different notification requirements, different definitions of data types and categories, and variations of access rights. There will be no right way to comply. Most disclosure requirements require them to be clear, conspicuous, and understandable.

In addition to the usual disclosures, which will likely expand given the new types and higher volume of data involved, one may need a disclosure to explain who should read each part of each disclosure.

Profiling in the metaverse

Profiling is certainly a beneficial feature for those who are operating a metaverse. What does this mean in a metaverse context? Operators of a particular metaverse can track and monitor the behavior of the avatars and the individuals/users associated with them. This can be considered profiling pursuant to article 4 sec. 4 GDPR and many US-based privacy laws.

Under the GDPR, the individual shall have the right not to be subject to a decision based solely on automated processing, including profiling, and which produces legal effects concerning him or her (article 22 sec. 1 GDPR). This doesn´t apply if the decision is made with the data subject´s explicit consent.

In other words: Operators are entitled to implement profiling measures provided the data subjects concerned have explicitly consented to do so. But how will they gather that consent, and how will the experience differ for those who refuse or revoke consent?

Importance of data protection by design and default

Pitfalls of forgetting data privacy when designing new technologies

Failing to consider data privacy aspects is one of the common potential legal pitfalls when designing

[6] For example: the identity and the contact details of the controller, the purposes of the processing, the legal basis for the processing, the recipients of the personal data.

new technologies. Virtual or augmented reality interfaces allow for online collection and use of extensive sets of personal data including sensitive data.

Further, public blockchains can record personal data immutably to a distributed ledger accessible to virtually anyone with an internet connection. **Creators of virtual worlds who leverage these technologies should design their services from the outset in ways that address applicable data privacy, security and government access laws**. They may be able to track and record a user's behaviors, actions and communications in a virtual environment, and they may have legitimate reasons to do so such as to protect against objectionable content and conduct.

But, how can a metaverse creator devise systems to avoid privacy violations? How can the creator ensure that it can respond to users who exercise their rights under applicable privacy laws to obtain copies of their personal data, port that data to an alternative metaverse, or delete the users' personal data from the virtual world? What notice and consent mechanisms should the creator implement to ensure that users understand and can control how their personal data is being processed in a metaverse? What assistance can and must the creator provide to law enforcement authorities which request or order it to produce personal data relevant to an investigation? All these issues must be considered and ironed out from the outset.

Principles of data protection by design and default for the metaverse

Adherence to the principles of data protection by design and default, which are codified under article 25 GDPR and ISO 27701, entails asking these types of questions and proactively designing features to protect users' privacy rights, and, by default, only processing personal data that is necessary, and only to the extent necessary, to fulfill the purposes of the service being offered to the users.

Article 25 GDPR more specifically requires controllers to establish appropriate technical and organizational measures from the outset to implement data protection principles and to safeguard the rights of data subjects.

As a result, the metaverse creator has to implement measures which ensure that only that amount of data necessary to meet the purpose of the data processing operation is collected and processed, and that such data is optimally protected, for example through state-of-the art encryption, particularly by using blockchain technology.[7]

Data privacy by design from the US perspective

The U.S. has been slower to explicitly require privacy by design, but recent laws include risk assessment requirements, and it remains to be seen how closely these risk assessments resemble Data Protection by Design.

That said, enforcers such as regulatory authorities, are likely to consider whether a business's Software Development Life Cycle includes privacy by design in their enforcement decisions. Not following a privacy by design approach leaves a business blind to any possible privacy issues and increases the risk of litigation and regulatory interferences.

[7] For blockchain technology: Matthias Artzt, Thomas Richter (ed.), Handbook of Blockchain Law 222/223 (2020).

Data security in the metaverse is fundamental

Data security is the priority

Data security is the most important thing in the data ocean embedded in the metaverse. Risks associated with data security may materialize particularly when transmitting personal data from one metaverse to another one. Not only is personal data exposed to risk, but also transactional details of items (e.g., NFTs) which have been purchased in the metaverse are similarly exposed.

It is worth noting that regulators are aware of the metaverse and the related security issues. Some regulators are concerned about illegal financial activities conducted in the name of developing the metaverse.

On February 20, 2022, the China Banking and Insurance Regulatory Commission made a statement regarding such risks. The statement warned against the risks of illegal fundraising and fraud in the guise of metaverse investment projects, metaverse/blockchain games, and speculation in virtual real estate and virtual currencies.[8]

While virtual realities have always been prone to fraud,[9] chances are that online fraud will increase dramatically with many more metaverses being set up. This is because cybercriminals continue to exploit vulnerabilities in new technologies. They may find new opportunities for identity theft or creating synthetic identities. Metaverse designers will be facing challenges for protecting individuals against these new modalities of identity exploitation. For some time, the metaverse is likely to need virtual bouncers and virtual cops—seen or unseen.[10]

Ensuring secure transmission of personal data: data portability and interoperability

Under article 20 sec.1 of the GDPR, data subjects have the right to receive their personal data in a structured, commonly used and machine-readable format and have the right to transmit that data to another controller.

Accordingly, metaverse operators are required to allow portability and interoperability of data gathered in the metaverse. This should enable users to switch between platforms, which could lead to a loss of value between operators as interoperability erodes the value of processed data. Portability is a major risk in this context since a huge amount of data will be transferred in the metaverse.

Who is accountable when there's a data breach

It is crucial to determine who is responsible for data security, how data breach incidents may be prevented, and what happens in the event of such an incident.

The responsibilities of data controllers and data processors vary from one jurisdiction to another. However, in general, the concept of "data controller" is defined as a person, company, or other body that determines the purpose and means of personal data processing.

[8] Goodwin, Metaverse in China (May 2022), available at: https://www.goodwinlaw.com/publications/2022/05/05_11-metaverse-in-china

[9] Jake van der Laan, Dealing with Internet Mediated Securities Fraud (December 2008), available at: https://drive.google.com/file/d/13nB9FQmE8toO0fuV2yDRnTL3dd-lvAGu/view?usp=sharing

[10] https://slate.com/technology/2022/05/metaverse-content-moderation-virtual-reality-bouncers.html

In the metaverse, who is responsible depends on whether the metaverse is decentralized or centralized. There may be one main administrator acting in a centralized metaverse to process all personal data and determine how personal data will be processed, or there could be multiple entities (decentralized metaverse) that process personal data through a metaverse.

CONCLUSION

Since the metaverse embodies a virtual world akin to the real world, the application of data privacy policy is taking on new dimensions and raising novel questions.

The security of data in the metaverse is a significant concern. Users may see an increase of cyber risks correlated to the increase of exposure in the metaverse. However, that is not an argument to challenge the evolution of the metaverse. Even blockchain technology is relatively new, and there are countless new stories of people losing money through compromises in the components of blockchain ecosystems.[11] That issue has never been a "showstopper" for blockchain users to capitalize on that new technology.

The same will apply to the metaverse, particularly with a view to the enormous investments made by Meta and various platforms making up the metaverse network. Since it is a growing network there is scope for many more to join. It is therefore of utmost importance to strengthen the security and the protection of personal data of those who participate in the metaverse.

[11] Nils Amiet, Blockchain Vulnerabilities in Practice (March 2021) 2:2 Digital Threats Research and Practice, available at: https://dl.acm.org/doi/10.1145/3407230. To put it in a broader scope, see Barry Sookman, Blockchain Vulnerabilities and civil remedies to recover stolen assets International Journal of Blockchain Law (March 2022), available at: https://gbbcouncil.org/wp-content/uploads/2022/03/IJBL-Volume-II.pdf?mc_cid=e19f9dec02&mc_eid=55476ebd9d

ARTICLE V

UNISWAP: LEGAL POINT AND COUNTERPOINT

The Uniswap platform, a leading decentralized crypto trading protocol, has not escaped its share of controversy. We present two articles on the question of Uniswap's state of decentralization. The first is by attorney Max Dilendorf who describes flaws in the Uniswap platform that he asserts undermine Uniswap's claim of decentralization. The second article by Uniswap attorneys Marvin Ammori, Chief Legal Officer, and Sonal Tolman, Associate General Counsel, is written in response.

UNISWAP - AN ILLUSION OF DECENTRALIZATION?

MAX DILENDORF
PARTNER
DILENDORF LAW FIRM, PLCC

INTRODUCTION

Decentralized Finance (DeFi) has made great strides over the last year. In fact, the Total Value Locked (TVL–a statistic representing the number of assets staked in a particular protocol and one of the most important indicators to assess the overall growth rate of DeFi) across all DeFi platforms has grown from a relatively paltry $1 billion in June of last year to over $60 billion today (peaking at over $86 billion in mid-May).

Proponents of the movement see it as an opportunity to democratize finance, bringing the system out from under the control of central authorities like the US government and big banks and putting it into the hands of the community.

But whether these "decentralized" platforms are actually what they claim to be–that is, trustless and without a central controlling authority–remains an open-ended question subject to much debate.

Uniswap, a pioneer of the DeFi movement, is one of the largest DeFi platforms operating on the Ethereum blockchain and portrays itself as a champion of decentralization.

The Uniswap platform operates as a decentralized exchange that incentivizes users of the protocol to maintain liquidity in its liquidity pools by providing portions of the transaction fees and newly minted UNI tokens to those who participate. Since its inception, three iterations of the platform have been released by Uniswap Labs, the team responsible for the protocol.

According to Cryptofees, the third version of Uniswap, Uniswap v3, generates an average of $3 million in transaction fees on a daily basis–the second most of all crypto projects running on the Ethereum blockchain today. Uniswap v2, the second iteration of the decentralized exchange which continues to operate, is not far behind, generating an average of approximately $1 million daily in transaction fees.

In February of 2021, Uniswap became the first DeFi platform to process over $100 billion in volume. And in April of 2021, Uniswap surpassed $10 billion in weekly trading volume, which would amount to over half a trillion dollars per year.

It is safe to say that Uniswap processes an immense number of transactions amounting to hundreds of billions of dollars. But the platform and its team, Uniswap Labs, have been left to operate without regulatory scrutiny.

Uniswap Labs describes the Uniswap protocol as a "trustless and highly decentralized financial infrastructure." But is Uniswap as decentralized and trustless as the Uniswap Labs team make it seem? For one, Uniswap Labs not only developed the code for Uniswap v3 but also promoted the launch of the platform to the public. What is more, Uniswap Labs operates a centralized User Interface and consistently promotes Uniswap and new developments or changes to the protocol and interface. Not to mention the fact that Uniswap Labs airdropped 150 million UNI tokens–Uniswap's native governance token–to historical users and liquidity providers of the protocol in September of 2020.

And while Uniswap's "Governance Protocol" is depicted as a way to transfer governance to the community, in reality, it is an inefficient system that ultimately begs the question: how effective is this governance mechanism? And does it truly achieve the level of decentralization that Uniswap so proudly touts?

In the context of crypto currencies and federal and state securities, whether the Uniswap platform is truly decentralized will turn on the Howey Test. The Howey Test established a test for determining if an investment contract, which is a security, exists. Under the Howey Test an investment contract exists where there is (1) an investment of money (2) in a common enterprise (3) with the expectation of profit (4) to be derived solely or primarily from the efforts of others.

Why is this important? Because if Uniswap is not sufficiently decentralized and passes the Howey Test, then the platform and its team will be participating in the unregistered sale of securities and will be subject to federal and state securities laws and regulatory scrutiny.

UNISWAP GOVERNANCE PROTOCOL

Uniswap Labs released Uniswap's Governance Protocol in September 2020, when the team announced the launch of the UNI token. The UNI token is a governance token that enables holders of it to vote on changes to the Uniswap protocol and on how to allocate the funds in the governance treasury.

To participate in voting in Uniswap Governance you will need (1) UNI tokens; (2) ETH for transaction costs; and (3) a browser with Metamask installed.

The process begins in the "Governance Forum," where one can find proposals under current consideration, gather information about community sentiment, and engage with the Uniswap community. Once the proposal has passed through the proposal process and is ready for voting, the proposal will appear on the Uniswap voting dashboard.

There you can view all current and former Uniswap proposals. When a proposal reaches the voting stage, it represents real, executable code that will alter the functionality of Uniswap Governance or anything under its jurisdiction–if voted in favor of, of course.

UNI tokens are used as a voting mechanism. For UNI to be used as a vote, the owner must first delegate their votes to a particular address, which binds the voting power of the tokens to that address. This address can be the owner of the token themselves or a trusted party who they believe will vote in the best interest of the platform.

A democratic consensus, referred to as a "quorum," is determined by the percentage of UNI tokens in favor of, or against, a proposal. 1% of all UNI tokens must be cast in favor of a given proposal for the proposal to be submitted for a vote. And a quorum of 4% of all UNI must be cast in favor for that proposal to pass.

To date, it appears that only one governance proposal has been passed, as the only other two proposals to make it to the voting stage failed to meet the 4% quorum needed to pass a vote. The passed proposal established a Uniswap Grants Program (UGP), a program aimed at strengthening the development of the Uniswap ecosystem.

AN ILLUSION OF DECENTRALIZATION?

A deeper analysis of Uniswap and its Governance Protocol yields a multitude of questions that suggest the platform may not be as decentralized as advertised. As an initial matter, the Uniswap team provided the community with 60% of the genesis supply of UNI tokens (1 billion) while giving themselves, investors, and advisers the remaining 40%.

Although the Uniswap team pledged not to participate in Governance decision-making for the "foreseeable future," there is no doubt that the team has a disproportionate amount of power in the early stages of governance.

Skepticism surrounding Uniswap's decentralized governance protocol is certainly warranted. Despite Uniswap Lab's vow not to participate in governance, the team could in theory use their UNI tokens to unilaterally make changes to the protocol.

Just as troubling, the team has claimed that the tokens allocated to them and Uniswap investors will be vested over a four-year period, yet the exact schedule has not been announced.

And, as opposed to the treasury tokens, which are locked up in smart contracts and will be released on a scheduled basis, it appears that the tokens allocated to the team and investors are fully liquid, as they are held at regular Ethereum addresses and have no restrictions on transfers. In addition to the vesting schedule being kept under wraps and the tokens being liquid, no one knows who controls the keys to these addresses.

It is clear Uniswap Labs has not been transparent with their UNI tokens, despite transparency being a key characteristic of DeFi and blockchain generally. So, is the Uniswap governance truly decentralized?

Moreover, as previously mentioned, Uniswap Labs has now released 3 versions of the Uniswap platform–the latest in May of 2021. The updated platform allows liquidity providers to set minimum and maximum prices on their portion of any given liquidity pool, otherwise known as "concentrated liquidity," and allows different pools to be created with different fees.

In essence, the Uniswap team made changes to the Uniswap platform unilaterally, without submitting these changes to the same governance process as any other proposal. The team simply kept the previous version of Uniswap running and dressed up Uniswap v3 as a brand-new platform.

How is this any different from a central party having authority and control over a network so as to dictate the future value of that network's native token? And what is to stop Uniswap community members from believing Uniswap Labs will continue to release updated versions of the platform, regardless of how the community votes to change the current protocol?

Another issue early on in the Uniswap Governance Protocol was the level of difficulty associated with achieving quorum. Uniswap's Governance Protocol requires 1% of the total UNI supply (10 million UNI) to vote in favor of a proposal simply to submit the proposal for a vote. Once the proposal is submitted for a vote, it requires a 4% quorum (40 million UNI) to vote in favor of it for that proposal to pass.

Reaching these totals is no easy task. And as more votes are spread across more delegates, the goal of achieving the required quorum becomes increasingly diffcult. What is more, the issue of low voter turnout only adds to this diffculty. What results is a largely inefficient system where governance proposals seldom make it to the proposal stage; and, when they do get past the 1% threshold, rarely make it past the 4% quorum required to pass them.

On the other hand, several Ethereum addresses have accumulated a significant amount of UNI tokens by way of delegation. These addresses, also known as "whales," act as proxies for UNI holders who do not want to vote themselves but trust the given address to vote in the best interest of the protocol and Uniswap community.

These whales include several major platforms such as Compound, Gauntlet, and Dharma, and many prestigious Universities, including Harvard Law, UC Berkley, Stanford, and MIT. Each of these addresses holds more than 2.5 million UNI tokens, with the largest holding up to 15 million. Can the governance protocol be described as decentralized when only a few addresses can team up and unilaterally change the protocol or governance treasury?

Additionally, Uniswap Labs announced on Twitter that they have started restricting access to a number of tokens at app.uniswap.org, stating "[t]hese changes pertain to the interface at app.uniswap.org – the Protocol remains entirely autonomous, immutable, and permissionless."
It is quite ironic that the Uniswap Labs team asserts that the Protocol remains autonomous, immutable, and permissionless in the same tweet they announced they will be restricting access to tokens.

How can the Uniswap team have control over the User Interface (UI) and access to tokens but claim that the platform is "entirely" decentralized? Is it even possible to have a decentralized network when the UI is controlled by a central authority?

Aside from the Governance Protocol, an argument could be made that Uniswap is not decentralized based on the infamous "DAO Report" released by the SEC in 2017. In that case, the SEC argued that holders of the DAO token had to rely on the managerial efforts of the founding team because the team led investors to reasonably expect they would provide such efforts through their conduct and marketing materials.

The same reasoning can be applied here. UNI token holders may reasonably expect that the Uniswap

Labs team, led by founder Hayden Adams, will undertake the managerial efforts to drive the value of the token.

Through Uniswap Labs' and Hayden Adams' tweets, vision, and public engagements, it is not a stretch to say the Uniswap community reasonably expects Uniswap Labs and Hayden Adams to continue their managerial efforts.

One example is Mr. Adams' recent announcement that he is in talks with PayPal to roll out a joint venture together. Mr. Adams has made himself the face of the company, and community members could reasonably expect his managerial e!orts to continue driving the success of the platform and the UNI token.

CONCLUSION

Whatever our concerns may be, it is clear that Uniswap Labs and its legal team do not share the same sentiment.

Indeed, centralized exchanges require platforms to provide written legal opinions that they are sufficiently decentralized to faily he before any particular token can be traded on their exchange.

Who exactly concluded that the Uniswap platform is sufficiently decentralized? And what is their reasoning behind that conclusion?

An argument could be made either way. Further, if Uniswap constitutes an investment contract, then the platform is engaging in the unregistered sale of securities and will be subject to federal and state securities laws.

The only thing that is clear is that the answer is unclear.

REBUTTAL OF MAX DILENDORF'S ARTICLE

MARVIN AMMORI
CHIEF LEGAL OFFICER
UNISWAP LABS

SONAL TOLMAN
ASSISTANT GENERAL COUNSEL
UNISWAP LABS

INTRODUCTION

Just as Bitcoin functions autonomously without Satoshi Nakamoto approving or blocking transactions, the Uniswap protocol functions autonomously without Uniswap Labs–or anyone else–approving any transaction, trade, or withdrawal. While Uniswap Labs may have contributed to the original protocol code, the company cannot stop anyone from accessing the Uniswap protocol, integrating it into another application, or using it to provide liquidity, remove liquidity, or trade one token for another.

There are some limited features of the Uniswap protocol code that may be modified, including adding new fee tiers for trading pairs.

REBUTTAL

As the Dilendorf article acknowledges, Uniswap Labs passed control over those parameters to Uniswap governance when it "airdropped 150 million UNI tokens–Uniswap's native governance token–to historical users and liquidity providers of the platform." If Uniswap Labs disappeared tomorrow, the protocol would remain available to all users and changes to the protocol would remain in the hands of UNI holders.

The Dilendorf article ignores or misunderstands these and most other basic facts about the Uniswap protocol. Instead, **the Dilendorf article relies on a series of factual errors and rhetorical questions to insinuate that the decentralized protocol, which is largely immutable and otherwise managed by a widely distributed governance token, is somehow in a centralized grasp**. Here are the things it gets wrong:

It attempts to call into question the decentralization of the Uniswap protocol by implying that the Uniswap Labs interface offered at app.uniswap.org is the only way to access the protocol.

In reality, the Uniswap Labs interface is only one of hundreds of user interfaces and integrations that users can use to connect to the Uniswap protocol. Arguing that the Uniswap protocol is centralized because Labs developed one user interface for it is like arguing that Ethereum is centralized because Consensys developed Metamask (one of numerous Ethereum wallets).

In light of the many other interfaces and integrations, what Uniswap Labs does with its own interface has no bearing on the decentralization of the protocol itself:

- The article gets the basic facts about Uniswap governance wrong.

  The authors inexplicably claim there have been only three proposals and only one has passed when in fact fifteen proposals have been made as of May 1, 2022, and a full two-thirds have passed or been implemented, while the others have not. See here: https://app.uniswap.org/#/vote?chain=mainnet.

  Contrary to the article's suggestions, the proposal history shows Uniswap governance is robust and active, and that governance is no mere rubber stamp. The authors then attempt to sidestep the obvious success of Uniswap governance by suggesting it is not sufficiently democratic.

  First, they assert that a 1% quorum required to move a governance proposal to a vote is too high. They are unaware of or simply ignore that the Uniswap community voted to reduce the quorum from 1% to .25% almost one year ago–through a successful governance proposal.

  Second, they imply that the existence of governance delegates means the protocol is centralized, but virtually all modern governance systems rely on representation to get the work done. That does not render those systems centralized. Delegates are a feature of governance and nothing about the free and uncoerced delegation of UNI from token holders to delegates suggests that the Uniswap protocol is centrally managed.

- The authors speculate that Labs employees could "in theory" make unilateral changes to the protocol because of the initial allocation of UNI tokens to employees.

The article misleadingly omits that only about 20% of the total UNI was allocated to company employees and advisors– nowhere near a majority of the total supply.

More importantly, it ignores that a Uniswap Labs employee cannot simply “make changes to the protocol” and would still have to go through the governance process, where other UNI token holders could vote for or against the proposals the employee would have to put forward.

Likewise, the authors’ assertion that the allocation of UNI to Labs employees is not locked in a smart contract and instead held at regular Ethereum addresses is irrelevant. They claim that no one knows how employees’ UNI may have been used in governance but this ignores several obvious facts.

First, websites including sybil.org and withtally.xyz list the top delegates and voters in Uniswap governance that have validated their identity. None of the top validated voters are Uniswap Labs employees, and no combination of the unvalidated top voters could sway a governance vote without significant votes from validated voters (who are not Uniswap Labs employees).

Second, the Ethereum blockchain is transparent and evidence of a handful of employees controlling governance would be easily traceable on the blockchain.

Finally, the Uniswap protocol itself is largely immutable and automated—no governance vote would empower anyone to change the key features of the Uniswap protocol. No governance vote could block or reverse transactions, stop or hinder someone from adding or removing liquidity, or deny or revoke third-party integrations.

- The authors assert that Labs “subverted” the governance process by releasing a new version, v3, of Uniswap protocol.

  This characterization reflects a lack of understanding about the Uniswap protocol and autonomous software. It is not possible to upgrade or change v2 to incorporate the new features of v3. In light of that, anyone wanting to build substantial new features could only do so by releasing a new protocol.

  The real and relevant point is that although Labs built v3, it released it to the control of Uniswap governance. Moreover, users had the choice to opt into v3, rather than having to go through a mandatory upgrade from v2, which is in fact consistent with decentralization. Centralized companies can change their users’ experience without notice or opt-in, but members of the Uniswap community could choose to continue using v2 if they preferred.

- Beyond that, the article claims that Labs “promoted” Uniswap v3 to the public and “consistently promotes … new developments or changes to the protocol.”

> The authors provide exactly zero support for these assertions, so it is difficult to respond to the generality. Uniswap Labs did announce the release of v3 on company channels, but that does not suggest centralization. Indeed, Ethereum is considered decentralized despite consistent communication from the Ethereum Foundation about its roadmap and plans. Bitcoin is considered decentralized despite communication from its core developers about their roadmap and plans.

While the Dilendorf law article may potentially reflect the reality of other crypto projects, it really misses the mark for the Uniswap protocol. **While other companies may traffic in hype, copy-and-paste code, and flawed mechanism design and risk management, Uniswap Labs spent the past half-decade as a true pioneer of automated market maker technology and decentralized technologies**.

Labs continues to deliver products with high standards for security, safety, and decentralization. Also, due to the facts set out above, the Uniswap Protocol remains, deservedly, among the most widely used, well-respected, and decentralized projects in the entire digital asset space.

ARTICLE VI

USING THE WISDOM OF SOLOMON, SENATORS LUMMIS AND GILLIBRAND INTRODUCE INVENTIVE LEGISLATION

ANDREA TINIANOW
CHIEF LEGAL OFFICER
IOV LABS

On June 7, Senator Cynthia Lummis of Wyoming, and Senator Kirsten Gillibrand of New York introduced the highly anticipated Lummis-Gillibrand Responsible Financial Innovation Act (the "Act"). It was referred to the Finance Committee for their consideration.

The sweeping piece of legislation seeks to fix rough spots, fill gaps and address open issues across a spectrum of laws that regulate digital assets, including the Securities Exchange Act of 1934, the Commodity Exchange Act, and Internal Revenue Code, among others. Significantly, the Act brings digital assets fully within the regulatory perimeter, clarifying the regulatory rules for innovators and offering newfound protections for investors.

Among other things, **Title III of the Act offers benefits for innovators and investors that are designed to both spur innovation and protect investors from fraud and manipulation**.

For innovators, the Act provides the first clear framework for fungible digital assets distributed as part of a fundraising scheme that is treated as a "securities offering" under current law (which are referred to as "ancillary assets" under the Act), resolving long-simmering concerns about whether market transactions in these commodity assets implicate securities regulation.

In addition, those using, trading, or investing with these assets benefit from the Act's new disclosure provisions that provide critical information so long as the founding team has an active role in the success of the project (sometimes referred to the project not yet being "sufficiently decentralized").

In addition, **the Act harmonizes the regulatory authority of both the Securities and Exchange Commission ("SEC") and the Commodity Futures Trading Commission ("CFTC"), to create an efficient and streamlined process for regulating these ancillary assets and the markets in which they trade**.

To better understand the issues addressed by the Act, we turn to the seminal 1946 Supreme Court case, *Securities and Exchange Commission v. W. J. Howey Co*. There, tourists visiting Florida were solicited by the Howey company to purchase small tracts of land being used to grow oranges.

However, most tourists didn't just buy the land being offered. Rather, through a series of agreements, the Howey company agreed to do all of the work, including picking, processing, and selling the oranges, and the investors simply received profits from the business. Accordingly, the Supreme Court found that the scheme constituted an "investment contract" and, as such, the transactions fell within the Securities Act of 1933. Because the Howey company failed to register the transactions with the SEC, it was found to violate federal law.

The case (and its progeny) remain good law all these years later. It is particularly relevant in the context of digital assets because the same analysis used in the *Howey* case (which is known as the *Howey* test), is used for determining when any apparently standard commercial transaction should be treated as an investment contract (and benefit from the protections provided by our securities laws).

According to *Howey*, an investment contract exists where there is "contract, transaction or scheme" that involves:

- an investment of money
- in a common enterprise
- where those contributing the funds have a reasonable expectation of profits
- to be derived primarily from the efforts of others.

In this light, we see that, as was the case in *Howey*, many fundraisings conducted through the sale of digital assets may well constitute "investment contracts" (and therefore securities offerings, making the entity raising the funds a securities "issuer").

Unlike traditional securities, most digital assets, created through computer code called a "smart contract," are deployed to a blockchain network and will continue to exist indefinitely, even if the entity that originally sold the assets is dissolved or no longer in existence. In addition, most digital assets do not attempt to create legal rights, like an ownership interest in a company or a company's debt obligation. (Clearly, those types of digital assets would likely be considered "securities"). The Act recognizes them as "commodities" and gives jurisdiction of the spot markets in which this growing class of assets trades to the nation's commodities regulator - the Commodities Futures Trading Commission ("CFTC").

Further, to address the information asymmetries that can arise between members of the public considering whether to invest in a given digital asset, and the founding team that created the digital asset, the Act mandates that the digital assets' founding team provide comprehensive periodic disclosures. These disclosures generally focus on information about the assets themselves and the developers and the technology underpinning the project, among many other things.

Notably, to avoid overburdening founding teams whose digital assets have relatively little impact on the wider markets, the Act requires a minimum level of secondary market trading before the disclosure requirements kick in. In this way, the Act addresses the leading concern about the secondary trading of digital assets – the absence of a meaningful disclosure regime – without imposing a "legal fiction" that somehow commodity digital assets embody the investment contract under which they were originally sold.

But that is only half the story.

The other half relates to the Act's expansion of the CFTC's jurisdiction to include regulatory authority over digital assets.

Traditionally, the CFTC has had exclusive jurisdiction over any transaction "for the contract of sale of a commodity for future delivery." The Act expands that jurisdiction to include any agreement, contract, or transaction involving (among many others) involving digital assets, except for the specific periodic reporting requirements (discussed above) which is the exclusive purview of the SEC.

This makes a lot of sense.

Digital assets share common characteristics with commodities. Some of which, such as Ether and BTC, have already been recognized by both the CFTC and the SEC as commodities. **The CFTC is well positioned to take on this mantle of enforcer against fraud and manipulation in the markets for commodity digital assets**. To wit, the agency recently settled charges against Glencore for fraud and manipulation with a payout of $1.186 billion, the highest civil monetary penalty in any CFTC case.

As to the SEC, under the Act, the agency will have the critical role of monitoring compliance with the periodic disclosures, whenever they are required – something that falls squarely within its mandate and core competencies.

Moreover, **the Act does nothing to change the SEC's primary jurisdiction over the offers and sales of "investment contracts" under the *Howey* test, whether it is oranges, digital assets, or anything else**. If something is sold in a transaction in which there is a common enterprise between buyer and seller, and the buyer is primarily expecting to make a profit from the transaction through the efforts of the seller, that will still be a "securities" transaction under the Act and will still require registration with the SEC if offered to the general public without some exemption.

BOTTOM LINE

Lummis-Gillibrand is a big, ambitious piece of legislation, comprehensive in nature, and does what we were hoping it would do, namely fix the rough spots, fill the gaps and address open issues in existing legislation.

And, in the process, it amends:

- The Internal Revenue Code of 1986 to preclude taxation on gains by reason of changes in exchange rates from the disposition of digital assets in a personal transaction where the transaction is $200 or less.
- The Infrastructure Investment and Jobs Act to exclude form the definition of "broker" persons who are engaged in the business of validating distributed ledger transactions, selling hardware or software whose function is to permit a person to control private keys which are used for accessing digital assets on a distributed ledger, as well as those who develop digital assets or their corresponding protocols or applications, namely, coders.

Significantly, the Act also includes a lexicon of concepts related to digital assets, including some new ones, like, "digital asset intermediary," "payment stable coin," "ancillary asset," and "decentralized autonomous organization." The Act also requires that final guidance be adopted by the Secretary of the Treasury on a range of issues, including:

- The classification of forks, airdrops and other similar value
- Merchant acceptance of digital assets, and the tax treatment of payment and receipts
- Treatment of digital asset mining and staking as a production activity in which income is not realized until disposition of the asset produced.

These are turbulent times for the crypto industry. It is heartening to see bi-partisan cooperation that offers smart and reasonable crypto legislation that Republicans and Democrats can support.

Note: A version of this article was first published by Forbes.com. It is reprinted here with permission.

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

Legal Disclaimer

While we endeavor to publish information that is up to date and correct, IJBL makes no representations or warranties of any kind, express or implied, about the completeness, accuracy, reliability, suitability, or availability, with respect to the Journal or the information or related graphics contained in this publication for any purpose.

IJBL shall not be responsible for any false, inaccurate, inappropriate or incomplete information. Certain links in this Journal will lead to websites which are not under the control of IJBL.

To the extent not prohibited by law, IJBL shall not be liable to you or anyone else for any loss or damage (including, without limitation, damage for loss of business or loss of profits) arising directly or indirectly from your use of or inability to use, the Journal or any of the material contained in it.