THE INTERNATIONAL JOURNAL OF BLOCKCHAIN LAW

Volume 1

November 2021

GBBC
Global Blockchain
Business Council

GLOBAL BLOCKCHAIN BUSINESS COUNCIL

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

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.

Over the past years, blockchain technology has been recognized as a multi-faceted technology which may be beneficial in a variety of use cases. Its greatest potential lies in the creation of value for individuals and groups where trust is either expensive or non-existent. However, blockchain technology does not always fit neatly within existing legal norms and regulatory principles. Among the innovative and disruptive artifacts of blockchain technology are decentralization, pseudonymity/anonymity, immutability/finality and, particularly in the context of smart contracts, automation, that is the lack of a third-party intermediary to assume control and responsibility. These characteristics are often the root cause of difficult legal questions.

Blockchain technology will have a significant impact on the field of law. We are only at the very beginning of understanding how this nascent technology intersects with longstanding jurisprudence in the global community. Will current law bend to new use cases inspired and enabled by blockchain technology or will we see new laws enacted, especially in such areas as contract, intellectual property, regulatory, and antitrust law? We aim to explore these issues and much more here.

The International Journal of Blockchain Law (IJBL) is presented in an accessible language and format; written by lawyers for lawyers and professionals dealing with blockchain technology. The IJBL is published online and available to GBBC members and non-members. It aims to cover thrilling legal topics related to blockchain, and across various jurisdictions. We hope the IJBL educates and, most importantly, offers food for thought.

The IJBL's editors have rich and diverse blockchain-related experience, and each brings a unique perspective to the publication. I encourage you to review their backgrounds here. As for me, I will draw from my experience as co-editor of the Handbook of Blockchain Law (published by Wolters Kluwer in 2020) to bring high quality articles on far reaching blockchain-related topics that inform and challenge our current thinking.

I want to thank Sandra Ro and the GBBC for taking the IJBL under its umbrella. Without her dedication and support the IJBL would never have left the design and concept phase.

In our inaugural issue, we have collated a great collection of articles on topics ranging from decentralized finance (DeFi) (from both SEC Commissioner's and practitioner's perspectives), the viability of crypto securities in the U.S., the novel legal issues arising from disputes involving Decentralized Autonomous Organizations (or DAOs), the use of NFTs by celebrities, and smart derivative contracts. I look forward to continuing to present cutting-edge blockchain-related articles from around the globe to assist and support your legal blockchain journey.

ABOUT THE CO-EDITORS

You can find the editor's 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. WEINGARTEN

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

DEFI RISKS, REGULATIONS, AND OPPORTUNITIES

CAROLINE CRENSHAW[1]
COMMISSIONER
UNITED STATES SECURITIES AND EXCHANGE COMMISSION (SEC)

Whether in the news, social media, popular entertainment, and increasingly in people's portfolios, crypto is now part of the vernacular.[2] But what that term actually encompasses is broad and amorphous and includes everything from tokens, to non-fungible tokens, to Dexes to Decentralized Finance or DeFI. For those readers not already familiar with DeFi, unsurprisingly, definitions also vary. In general, though, it is an effort to replicate functions of our traditional finance systems through the use of blockchain-based smart contracts that are composable, interoperable, and open source.[3] Much of DeFi activity takes place on the Ethereum blockchain, but any blockchain that supports certain types of scripting or coding can be used to develop DeFi applications and platforms.

DeFi presents a panoply of opportunities. However, it also poses important risks and challenges for regulators, investors, and the financial markets. While the potential for profits attracts attention, sometimes overwhelming attention, there is also confusion, often significant, regarding important aspects of this emerging market. Social media questions like "who in the U.S. regulates the DeFi market?" and "Why are regulators involved at all?" abound. These are crucial questions, and the answers are important to lawyers and non-lawyers alike. This article attempts to provide a short background on the current regulatory landscape for DeFi, the role of the United States Securities and Exchange Commission ("SEC"), and highlights two important hurdles that the community should address.[4]

1. Commissioner, United States Securities and Exchange Commission. I am deeply grateful to my colleagues Robert Cobbs, Kathleen Gallagher, Micah Hauptman, Claire O'Sullivan, and Gosia Spangenberg, whose hard work made this submission possible. I also would particularly like to thank my colleague David Hirsch, who has been instrumental not only to this submission, but also provides valuable support to my office's overall approach to digital assets. We are also grateful to a variety of industry experts and attorneys who generously shared their time and ideas, and helped deepen my understanding of these questions. Any errors are solely my own.

2. The views I express herein are my own and do not reflect the views of the Commission, my fellow Commissioners, or the SEC Staff.

3. Composable refers to the ability to link smart contracts and build on existing modular code, which leads some to refer to DeFi applications as money Legos. Quantstamp Labs, "DeFi's Composability: More Possibility, More Risk;" Jul. 15, 2021. The term interoperable describes the ability to use DeFi protocols and applications across platforms and smart contracts. Fabian Schär, "Decentralized Finance: On Blockchain and Smart Contract-Based Financial Markets," Federal Reserve Bank of St. Louis Review, Second Quarter 2021, pp. 153-74. https://doi.org/10.20955/r.103.153-74

4. In addition to the securities law issues addressed in this article, regulators have also raised concerns about DeFi projects' failures to comply with rules relating to anti-money laundering, combating the financing of terrorism, tax compliance, the Commodity Exchange Act, and other issues. While not the primary focus of this article, I share some of those same concerns.

I. MANY INVESTMENTS SHARE IMPORTANT ATTRIBUTES

Many DeFi offerings and products closely resemble products and functions in the traditional financial marketplace.[5] There are decentralized applications, or dApps, running on blockchains, that enable people to obtain an asset or loan upon posting of collateral, much like traditional collateralized loans.[6] Others offer the ability to deposit a digital asset and receive a return. Both types of products offer returns, some directly, and some indirectly by enabling the use of borrowed assets for other DeFi investing opportunities. In addition, there are web-based tools that help users identify, or invest in, the highest-yielding DeFi instruments and venues.[7] Other applications let users earn fees in exchange for supplying liquidity or market making.[8] There are also tokens coded to track the prices of securities trading on registered U.S. national securities exchanges, and then can be traded and used in a variety of other DeFi applications. So while the underlying technology is sometimes unfamiliar, these digital products and activities have close analogs within the SEC's jurisdiction.

These similarities should come as a surprise to no one, considering finance is in the name. It should also come as a surprise to no one that investing is often at the core of DeFi activity. This movement is not about merely developing new digital asset tokens. Developers have also constructed smart contracts that offer individuals the ability to invest, to lever those investments, to take a variety of derivative positions, and to move assets quickly and easily between various platforms and protocols. And there are projects that show a potential for scalable increased efficiencies in transactions speed, cost, and customization.

These projects are evolving incredibly fast with new and interesting potential. Considering the relative infancy of blockchains that support the scripting needed for sophisticated smart contracts, DeFi development is particularly impressive. But these offerings are not just products, and their users are not merely consumers. DeFi, again, is fundamentally about investing. This investing includes speculative risks taken in pursuit of passive profits from hoped-for token price appreciation, or investments seeking a return in exchange for placing capital at risk or locking it up for another's benefit.

II. UNREGULATED MARKETS SUFFER FROM STRUCTURAL LIMITATIONS

Market participants who raise capital from investors, or provide regulated services or functions to investors, generally take on legal obligations. In what may be an attempt to disclaim those legal obligations, many DeFi promoters disclose broadly that DeFi is risky and investments may result in losses, without providing the details investors need to assess risk

5. The DeFi market overall has grown dramatically. DeFi today has more than $101 billion in total value locked, representing rapid expansion since September 2020 when that figure stood at $19.5 billion. https://dmarketforces.com/defi-market-size-soared-335-to-85-billion/

6. Schar at 164.

7. *Id.* at 165.

8. *Id.* at 162.

likelihood and severity.[9] Others could accurately be characterized as simply advocating a "buyer beware" approach; by participating, investors assume the risk of any and all losses. Given this, many current DeFi participants recommend that new investors exercise caution, and many experts and academics agree there are significant risks.[10]

While DeFi has produced impressive alternative methods of composing, recording, and processing transactions, it has not rewritten all of economics or human nature.

Certain truths apply with as much force in DeFi as they do in traditional finance:

- Unless required, there will be projects that do not invest in compliance or adequate internal controls;
- when the potential financial rewards are great enough, some individuals will victimize others, and the likelihood of this occurring tends to increase as the likelihood of getting caught and severity of potential sanctions decrease; and
- absent mandatory disclosure requirements,[11] information asymmetries will likely advantage rich investors and insiders at the expense of the smallest investors and those with the least access to information.

Accordingly, DeFi participants' current "buyer beware" approach is not an adequate foundation on which to build reimagined financial markets. Without a common set of conduct expectations, and a functional system to enforce those principles, markets tend toward corruption, marked by fraud, self-dealing, cartel-like activity, and information asymmetries. Over time that reduces investor confidence and investor participation.[12]

Conversely, well-regulated markets tend to flourish, and I think our U.S. capital markets are prime examples. Because of their reliability and shared adherence to minimum standards of disclosure and conduct, our markets are the destination of choice for investors and entities seeking to raise capital. Our securities laws do not merely serve to impose obligations or burdens, they provide a critical market good. They help address the problems noted above, among others, and our markets function better as a result. But, in the brave new DeFi world, to date there has not been broad adoption of regulatory frameworks that deliver important protections in other markets.

III. WHO REGULATES DEFI?

In the United States, multiple federal authorities likely have jurisdiction over aspects of DeFi, including the Department of Justice, the Financial Criminal Enforcement Network, the Internal Revenue Service, the Commodity Futures Trading

9. I listened to a recent podcast in which a young developer acknowledged that humans as a species are attracted to high returns, but are also bad at considering risk in choosing where to invest and at what price. He also said that people were mortgaging their homes to free up funds with which to invest in DeFi, and that he was concerned the outcome could be scary. Without reference to this specific person, it seems like common knowledge that some retail investors are taking on huge exposure in DeFi without understanding the risk or having the ability to price for it. Developers should build systems that are compliant with important regulatory and policy frameworks so that investors have all material information, including about the potential risks, and are protected from misconduct that puts them at a disadvantage.

10. Nic Carter and Linda Jeng, "DeFi Protocol Risks: The Paradox of DeFi."

11. For activity within the SEC's jurisdiction, compliance with the investor protections of the Securities Act of 1933 and the Securities and Exchange Act of 1934 requires important disclosures.

12. There is a great deal of academic research into network effects and how network adoption and engagement benefits the value of networks. I would be interested in research that studies how fraud and other violations of trust within a network impact that network's value by reducing adoption and engagement, and the potential for this impact to extend to competing networks.

Commission, and the SEC.[13] State authorities likely have jurisdiction over aspects as well.[14] In spite of the number of authorities having some jurisdictional interest, DeFi investors generally will not get the same level of compliance and robust disclosure that are the norm in other regulated markets in the U.S. For example, a variety of DeFi participants, activities, and assets fall within the SEC's jurisdiction as they involve securities and securities-related conduct.[15] But no DeFi participants within the SEC's jurisdiction have registered with us, though we continue to encourage participants in DeFi to engage with the staff. If investment opportunities are offered completely outside of regulatory oversight, investors and other market participants must understand that these markets are riskier than traditional markets where participants generally play by the same set of rules.

13. The U.S. government has dedicated significant resources to providing feedback, supporting innovation, and developing in-house expertise to ensure regulatory approaches are based on an accurate understanding of the technology. For example, the SEC has a FinHub, and a number of other authorities have innovation initiatives that engage with market participants and study the technology.

14. https://www.thinkadvisor.com/2021/10/01/state-securities-regulators-report-tripling-of-digital-asset-enforcement-actions/

15. At the SEC we have existing laws and rules that guide our approach and are shaped by court interpretations. Rather than proactively labeling every investment vehicle as a security or not a security, we look at specific facts and circumstances and apply the law based on that analysis. We do not have a measuring box like at airports, where if a bag fits inside it can be carried on, and otherwise must be checked. That type of mechanical jurisdictional test might be easier to apply and yield a faster conclusion, but ultimately would require us to revise the test and adapt the rules every time a new type of investment is introduced or changes in form. Considering that we regulate capital markets exceeding $110 trillion, made up of tens of thousands of entities, that type of proactive "define everything" approach is too rigid, and markets are too large, for it to be workable. Our statutes recognize that and provide for a flexible, principles-based approach, but one that also inherently requires a more detailed analysis to determine whether specific conduct or assets are within the SEC's jurisdiction.

IV. THE ROLE OF THE SEC

As an SEC Commissioner I have a duty to help ensure that market activity, whether new or old, operates fairly, and offers all investors a level playing field.[16] I would expect this goal to be one DeFi market participants also support.

To do this, the SEC has a variety of tools at its disposal ranging from rulemaking authority, to various exemptive or no action relief, to enforcement actions. Importantly, if DeFi development teams are not sure whether their project is within the SEC's jurisdiction, they should reach out to our Strategic Hub for Innovation and Financial Technology ("FinHub"), or our other Offices and Divisions, all of which have experts well-versed in issues relating to digital assets.[17] It is my understanding that FinHub has never refused a meeting, and their engagement is meaningful.[18] If a series of meetings is needed, they spend the necessary time. If a project does not fit neatly within our existing framework, before proceeding to market, that project team should come and talk

16. My responsibility extends to conduct within the SEC's jurisdiction, and my able colleagues at sibling agencies are responsible for other types of conduct.

17. See www.sec.gov/finhub

18. FinHub comprises representatives across the SEC's Divisions, and so those meetings includes access to a broad range of experts. FinHub is also an important resource to the Commission as it considers policy choices.

to us.[19] The more the project team can lead that discussion with possible solutions, the better outcomes they can expect. Our staff cannot offer legal advice, but they stand ready to listen to ideas and provide feedback, as developers know their projects better than we ever could. If the project is seemingly constrained by our rules, it is critical for us to get specific ideas about how these new technologies can be integrated into our regulatory regime to ensure the market and investor protections afforded by the federal securities laws, while allowing innovations to flourish.

That being said, for non-compliant projects within our jurisdiction, we do have an effective enforcement mechanism. For example, the SEC recently settled an enforcement action with a purported DeFi platform and its individual promoters. The SEC alleged they failed to register their offering, which raised $30 million, and misled their investors while improperly spending investor money on themselves.[20] To the extent other offerings, projects, or platforms are operating in violation of securities laws, I expect we will continue to bring enforcement actions. But my preferred path is not through enforcement, and I do not consider enforcement inevitable. Broad non-compliance that necessitates numerous enforcement actions is not an efficient way to achieve what I believe are shared goals for DeFi. The more projects that voluntarily comply with regulations, the less frequently the SEC will have to pursue investigations and litigation.

V. STRUCTURAL HURDLES

I recognize it is not the SEC's role to prevent all investment losses. It is also not my goal to restrict investor access to fair and appropriate opportunities. But it is my job to demand that investors have equal access to critical information so they can make informed decisions whether to invest and at what price. I am similarly committed to ensuring markets are fair and free from manipulation. Given this, it seems that there are two specific structural problems that the DeFi community needs to address.

A. LACK OF TRANSPARENCY

First, although transactions often are recorded on a public blockchain, in important ways, DeFi investing is not transparent. I am concerned that this lack of transparency contributes to a two tier market in which professional investors and insiders reap outsized returns while retail investors take more risks, get worse pricing, and are less likely to succeed over time.[21] Much of DeFi is funded by venture capital and other professional investors. It is unclear to me how well known this is in the DeFi retail investor community, but the underlying funding deals often grant professional investors equity, options, advisory roles, access to project team management, formal

19. Coming in to speak with SEC staff does not provide amnesty for violative conduct. It is, however, an important path to help projects identify potential SEC regulatory compliance issues, discuss possible solutions, and develop a plan to operate legally. To the extent a project team has already been operating outside of compliance, working with staff to prevent future violations may also position it to more quickly and inexpensively resolve any potential enforcement action for related past violations. Our Division of Enforcement considers cooperation when determining what remedies to recommend for violative conduct and we have agreed to settle multiple cases with reduced or no penalties in response to self-reporting violations, including in the digital assets space. See, e.g., In the Matter of Gladius Networks, Order Instituting Cease and Desist Proceedings, Securities Act Release No. 10608, (Feb. 20, 2019).

20. In the Matter of Blockchain Credit Partners d/b/a DeFi Money Market, Gregory Keough, and Derek Acree, Order Instituting Cease and Desist Proceedings, Securities Act Release No. 10961 (Aug. 6, 2021).

21. I recognize that DeFi has experienced significant asset price appreciation, and that is part of what motivated me to write this. The impacts of the information disparities or market conduct on retail investors may not be easy to see until the next DeFi market downturn or crisis.

or informal say on governance and operations, anti-dilution rights, and the ability to distribute controlling interests to allies, among other benefits. Rarely are these arrangements disclosed, but they can have a significant impact on investment values and outcomes. Retail investors are already operating at a significant disadvantage to professional investors in DeFi,[22] and this information imbalance exacerbates the problem.

Some contend that DeFi is, in fact, more egalitarian and transparent because much of the activity is based on code that is publicly available.[23] However, only a relatively small group of people can actually read and understand that code, and even highly-qualified experts miss flaws or hazards. Currently the quality of that code can vary drastically, and has a significant impact on investment outcomes and security. If DeFi has ambitions of reaching a broad investing pool, it should not assume a significant portion of that population can or wants to run their own testnet to understand the risks associated with the code on which their investment prospects rely. It is not reasonable to build a financial system that demands investors also be sophisticated interpreters of complex code.

Put simply, if a retail investor has $2,000 to invest in a risky programmable asset, it is not cost effective for that investor to hire experts to audit the code to ensure it will behave as advertised. Instead, retail investors must rely on information available through marketing, advertising, word of mouth, and social media. Professional investors, on the other hand, can afford to hire technical experts, engineers, economists, and others, before making an investment decision. While this professional advantage exists historically in our financial markets, DeFi exacerbates it. DeFi removes intermediaries that perform important gatekeeping functions and operates outside the existing investor and market protection regime. That can leave retail investors without access to professional financial advisors or other intermediaries who help screen potential investments for quality and legitimacy. These provide meaningful fraud reduction and risk assessment assistance in traditional finance, but there are limited substitutes in DeFi.

B. PSEUDONYMITY

A second foundational challenge for DeFi is that these markets are vulnerable to difficult to detect manipulation. DeFi transactions occur on a blockchain, and each transaction is recorded, immutable, and available for all to see. But that visibility extends only down to a certain identifier. Because of pseudonymity, the blockchain displays the blockchain address that sent or received assets, but not the identity of the person who controls it.

Without an efficient method for determining the actual identity of traders, or owners of smart contracts, it is very difficult to know if asset prices and trading volumes reflect organic interest or are the product of manipulative trading by, for example, one person using bots to operate multiple wallets, or a group of people trading collusively. There are specific U.S. securities laws prohibiting trading for the purpose of giving the false appearance of market activity or to

22. Joel Khalil, "Investing in DeFi is Seriously Risky But Maybe It Doesn't Have to Be" Techradar.com, Jan. 31, 2021 (describing "[h]igh transaction fees, market volatility and security incidents linked with vulnerabilities in smart contracts" as risks that are more pronounced for retail investors).

23. Kevin Werbach, "Finance 3.0: DeFi, Dapps, and the Promise of Decentralized Disruption," The Reboot, July 15, 2021.

manipulate the price of a security,[24] because successful investing depends on reliable information and market integrity. Pseudonymity makes it much easier to conceal manipulative activity and almost impossible for an investor to distinguish an individual engaging in manipulative trading from normal organic trading activity. In DeFi, because markets often turn on asset price, trading volumes, and momentum, investors are vulnerable to losses due to manipulative trading that makes those signals unreliable. To the extent transactions occur off public blockchains, it is even more difficult to assess whether trading is legitimate.

I recognize that in some ways DeFi is synonymous with pseudonymous. The use of alphanumeric strings that obscure real world identity was a core feature of Bitcoin and has been present in essentially all blockchains that have followed. But in the U.S., investors have long been comfortable with a compromise in which they give up some limited degree of privacy by sharing their identity with the entity through which they trade securities. In return, they benefit from regulated markets that are more fair, orderly, and efficient, with less manipulation and fraud.

In moving to DeFi, I suspect most retail investors are not doing so because they seek greater privacy; they are seeking better returns than they believe they can find from other investments. While some in DeFi believe in absolute financial privacy, I expect that projects that solve for pseudonymity are more likely to succeed, because investors can then be comfortable that asset prices reflect actual interest from real investors, not prices pumped by hidden manipulators. Projects that address this problem are also more likely to be able to comply with SEC regulations and other legal obligations, including requirements around anti-money laundering and countering the financing of terrorism imposed by the Bank Secrecy Act.

VI. CONCLUSION

My respect for innovation does not lessen my commitment to help ensure all our financial markets are sustainable and offer average investors a fair chance of success. DeFi is a shared opportunity and challenge. Some DeFi projects fit neatly within our jurisdiction, and others may struggle to comply with the rules as currently applied. It is not enough to just say it is too hard to regulate or to say it is too hard to comply with regulations.

It is a positive sign that many projects say they want to operate within DeFi in a compliant way. I credit their sincerity on this point, and hope they commit resources to collaborating with the SEC staff in the same spirit. For DeFi's problems, finding compliant solutions is something best accomplished together. Reimagining our markets without appropriate investor protections and mechanisms to support market integrity would be a missed opportunity, at best, and could result in significant harm, at worst. In conceiving a new financial system, I believe developers have an obligation to optimize for more than profitability, speed of deployment, and innovation. Whatever comes next, it should be a system in which all investors have access to actionable, material data, and it should be a system that reduces the potential for manipulative conduct. Such a system should lead capital to flow efficiently to the most promising projects, rather than being diverted by mere hype or false claims. It should also be designed to advance markets that are interconnected, but with sufficient safeguards to withstand significant shocks, including the

24. Section 9(a) of the Securities and Exchange Act of 1934.

potential for rapid deleveraging.

"In decentralized networks with diffuse control and disparate interests, regulations serve to create shared incentives aligned to benefit the entire system and ensure fair opportunities for its least powerful participants."

My staff and I have been actively engaged in helpful discussions with DeFi experts and my door remains open.[25] I can't promise an easy or quick process, unfortunately, but I can assure you of good faith consideration and a true desire to help promote responsible innovation.

25. In a recent speech I requested input from digital assets market participants. See "Digital Asset Securities – Common Goals and a Bridge to Better Outcomes," SEC Speaks, Oct. 12, 2021. Unfortunately, that has not yet yielded much of a response from a community that often says it lacks necessary guidance from the SEC, among others. My door remains open, and I welcome your ideas. I've created a dedicated mailbox for this purpose: Crenshaw-defi@sec.gov.

ARTICLE II

DEFI: A PATHWAY FORWARD

ALEXANDER LIPTON
CO-FOUNDER & CHIEF INFORMATION OFFICER
SILA

LEWIS COHEN
CO-FOUNDER
DLX LAW

This article is courtesy of the International Financial Law Review (IFLR.) You may find the original article here.

Decentralised finance (DeFi) has seen remarkable growth over the last eighteen months and has quickly established itself as one of the first true "killer apps" for smart contract networks like Ethereum, Cardano, Polkadot, and Solana. DeFi allows parties to create precisely tailored and highly complex economic arrangements that execute automatically without the need to rely on a central intermediary or other trusted party. Even in its current early stages, DeFi raises the promise of a more decentralised and resilient financial system capable of embracing both established players and nascent market entrants.

The value of assets deployed in DeFi, barely $1 billion in June 2020, grew to over $80 billion at the end of August 2021. DeFi takes many forms, including secured lending, asset trading, and a wide variety of derivative transactions, all occurring almost instantaneously, and all recorded on the ledger of a public blockchain network. Not surprisingly, most, if not all, of the activity in DeFi to date has concentrated on the use of natively digital assets, represented by a plethora of blockchain-based tokens and "stablecoins" – digital assets pegged with various degrees of reliability to a fiat currency (almost always the US dollar); however, proponents are increasingly looking at incorporating real world assets, such as real estate, intellectual property rights, traditional equity, and other fiat currencies, thus dramatically expanding DeFi's importance.

The absence of traditional intermediaries also means that anyone with the know-how and a wallet full of digital assets can directly access DeFi protocols without undergoing any prior know-your-customer (KYC) or anti-money laundering (AML) checks, or sanctions compliance. While this open access approach supports a vastly more inclusive type of financial innovation, it has raised concerns among policymakers that it could at some point give rise to an alternative financial system, one that allows illicit actors and those who run afoul of governments in developed nations to transact without the scrutiny and oversight provided by the current system of regulated financial intermediaries.

The Financial Action Task Force (FATF) Draft Guidance, issued in March of this year, suggested that parties directing the creation, development and/or deployment of DeFi protocol software — but who do not act as intermediaries controlling customer funds — should nevertheless be considered "virtual asset service providers" (VASPs), and should be held responsible for complying with relevant AML/KYC obligations. If this approach was widely adopted, DeFi protocol developers would be treated like banks, money transmitters, and other financial institutions that do control customer

funds. Even though there is much more room for automation in the KYC/AML process, enforcing these obligations invariably comes down to numerous human judgment calls, something which banks, with their large compliance departments, have learned to manage. Attempting to impose such an across-the-board KYC/AML requirement at the DeFi protocol layer or on entities with no control over customer funds and no means to comply as a practical matter simply would not work and would swiftly drive this activity into a gray market with even less visibility for regulators than they have today.

We believe that a vibrant and diverse DeFi ecosystem is essential to the promise of "Web 3.0" – a more decentralised and democratised internet and the foundation of a more open and inclusive society. At the same time, we also acknowledge that the concerns raised by FATF in the Draft Guidance need to be taken seriously. Whether these concerns can be addressed without stifling the remarkable level of innovation occurring in the DeFi space is far from certain, though.

A potential solution begins by looking at decentralised exchanges (DEXes), those protocols (that is, software-based platforms running on blockchain-based networks) that utilise various permutations of automated market making (AMM) by freely participating third-party liquidity providers in order to facilitate efficient and trustless exchanges of digital assets by users. DEXes effectively underlie all other DeFi activity. Recently, the company that developed Uniswap, one of the world's most popular DEXes, announced that it would remove certain tokens from its company-controlled web-based user interface (UI) to the protocol. (These tokens may still be accessed and traded using the Uniswap protocol through third-party UIs or by directly accessing the protocol software.)

The Uniswap announcement generated intense introspection in the DeFi community about the nuanced relationship between the traditional corporate entities that control popular DEX and other DeFi UIs and the underlying permissionless protocol software itself. But the debate the announcement engendered also points toward a way forward.

INCENTIVISE PERMISSIONED AUTOMATED FINANCE

Rather than attempting to impose regulatory obligations on either the protocol software (impossible) or on all UI providers (impractical, as alternative UIs can be created cheaply and anonymously).

"We believe that the focus of regulators should instead turn toward finding ways, both formal, through rule-making, and informal, through the regular flow of supervisory dialogue, of incentivising the development and operation of permissioned access points (UIs) to the many protocols developed for use in DeFi."

These alternative platforms, which might more properly be known as Automated Finance, rather than Decentralised Finance, could be

operated by both traditional financial services businesses and new market entrants. They would provide the benefits of access to the same innovative DeFi protocol software on the same public blockchain networks, but would have UIs operated by identifiable entities willing to take on some or all of the responsibilities of being a VASP and of evaluating the underlying protocol software being accessed by users.

This Automated Finance approach would allow commercial users of the digital asset ecosystem desiring or required to transact only with others who are known to have also met industry-standard KYC/AML and sanctions compliance checks in a relevant jurisdiction to do so. Of course, others preferring to exchange digital assets in a permissioned environment using DEX protocol software could also use these access points and their associated pools of underlying assets. How the permissioning is accomplished would be open to the market and could feature the use of "zero knowledge proofs" and separate layers of activity, among other techniques, to enhance privacy and reduce vulnerable data "honeypots". Work would also need to be done to facilitate integration of these Automated Finance platforms with "DEX aggregators" – separate front-end UIs that originate most digital asset trading volume at this point and allow those interested in trading digital assets to quickly identify the best DEX to which to route a trade, depending on the user's priorities (e.g., lowest spread, least price slippage, etc.).

BENEFITS OF A COMPROMISE POSITION

Such an approach would require compromise on the part of both regulators and industry. We understand that simply accepting the idea of permissioned access to DEX protocol software is contrary to the core tenets of many developers, entrepreneurs, and users in the DeFi sector and inevitably means that, at least in the early days of Automated Finance, there will be far fewer liquidity providers who support the exchange of pairs of digital assets in that environment as well as an overall smaller number of pairs of assets to trade there. Even over the long term, permissioned actors will inevitably also be more selective as to the asset pairs for which they provide AMM liquidity. The remarkable network effects that have quickly developed around existing fully open DEXes through innovations like liquidity mining would need to be rebuilt as liquidity is rebalanced between permissioned access and non-permissioned access asset pairs. Business models would also need to develop for arbitrageurs who can operate in both permissioned and non-permissioned pools to keep asset prices broadly uniform across marketplaces.

We also understand that a significant part of the current appeal of DeFi is its composability – complex arrangements that can be quickly constructed by combining the use of distinct lending, exchange, and other DeFi protocols into a single transaction (these arrangements are sometimes referred to as building with money Legos). At best, it will take Automated Finance time to be established across the full range of protocols used in DeFi, initially limiting composability; at worst, corresponding permissioned environments for some DeFi protocols may never be developed, excluding these tools from use in composing transactions for users of Automated Finance.

In fact, some may question why public infrastructure (such as the Ethereum network) would even be used for Automated Finance, when plenty of consensus protocols

designed for permissioned networks (like Hyperledger's Fabric) already exist. Herein lies a key observation: while the levels of interest in DeFi in the legacy financial system is unprecedented, after more than five years of trials by many disparate groups (and outside of some important specialised exceptions), the demand to participate in the day-to-day operation of permissioned "layer 1" blockchain protocols ranges from tepid to non-existent. Moving the economic burdens and benefits of participating in the core tasks required to maintain and secure the blockchain network itself to a group of open and self-selecting "validators", allows the public good of the network to exist, without any single participant required to take responsibility for the network or the other validators who from time to time are securing in it.

At the same time, by encouraging the development of Automated Finance, regulators would need to fundamentally re-think their approach as well, signaling to commercial users, investment funds, financial institutions, and other regulated entities that, with other appropriate precautions, they may begin to utilise AMM protocols and other of the underlying innovative tools developed through the growth of DeFi on public blockchain infrastructure without potentially violating AML/KYC or sanctions regulations applicable to them. As a result, the utilisation of these platforms (and their associated liquidity) should increase significantly and similarly permissioned access to lending and other protocols developed by the DeFi community may expand, thus spurring further growth and innovation in the DeFi sector while substantially enhancing transparency and regulatory visibility into the activity, relative to traditional markets.

Because all activity on these protocols (whether or not through permissioned access) occurs and is recorded on public blockchain networks, the level and detail of real-time monitoring to which regulators will have access will provide a huge improvement over the current system that consists solely of aggregated and delayed reporting by centralised financial intermediaries. In addition, with much activity occurring in permissioned environments, regulators will be able to work more efficiently with blockchain analytics providers to detect the true bad actors operating on non-permissioned networks. Consumer protection advocates should also be pleased, as the presence of an active Automated Finance sector running in parallel with peer-to-peer use of DeFi protocols by non-regulated entities will put a meaningful check on the power currently exercised by a handful of giant centralised financial institutions and should dramatically reduce costs to consumers and increase product choice, much as the switch to VoIP (voice over internet protocol) infrastructure 20 or so years ago did for telephone service. In addition, where user access to Automated Finance platforms is provided by regulated financial market participants, there will exist opportunities to integrate traditional services, such as insured fiat currency deposit accounts, with new uses for customer digital asset portfolios (such as lending against a basket of non-fungible tokens (NFTs) owned by a customer).

Moreover, by abandoning the idea of an outright prohibition on the use of DEXes and other true DeFi protocols that provide permissionless access to all users, regulators would be acknowledging the reality that, once written, the protocol software for virtually all DeFi applications will be available from public repositories, and that access points (and associated liquidity pools) for these protocols can be created by anonymous developers

and maintained on decentralised storage platforms like Arweave, Swarm and IPFS.

Nor is this a new phenomenon for regulators, who have managed the dual system of account relationships with banks and other regulated entities that are subject to KYC/AML and the fluid and non-transparent use of physical cash. Further, attempting to do otherwise would give privacy tech a huge shot in the arm, igniting an arms race of cryptography and, likely, further obfuscating most if not all DeFi activity. Despite the sound-bite appeal of mandating across-the-board KYC for all DeFi, as with the handling of physical cash, attempting to prevent both illicit actors as well as those many other users with perfectly appropriate and legally supportable reasons to prefer true privacy in their financial dealings in digital assets from interacting with the smart contracts developed for use in DeFi needs to be recognised as an undesirable, functionally impossible, and ultimately counterproductive, mission.

WHAT THE FUTURE MAY HOLD

It is critical that regulation in Web 3.0 should be applied functionally to users of DeFi services, not to the protocol software or its developers, or to those operating access points. An intermediary-based compliance mindset served us well for the 70-plus years since World War II but will be an abject failure if applied to DeFi. DeFi presents a once in a lifetime opportunity to rethink our financial infrastructure from the ground up.

A two-tier system of open access through non-permissioned portals (or direct access to the underlying smart contracts for users who are not subject to mandatory KYC/AML obligations and who are comfortable using decentralised peer-to-peer systems), on the one hand, and, on the other, permissioned portals for institutions, enterprises, and others required to comply with KYC/AML obligations due to their existing regulatory status or otherwise seeking to conduct significant transactions in a managed environment, could create a viable pathway forward. This side-by-side development of Automated Finance and Decentralised Finance would support the growth of DeFi as we know it today while allowing many more to benefit from its innovations. At the same time, such an approach would still give regulators the opportunity to protect the next generation of financial infrastructure from those seeking to exploit these developments for unlawful or illicit ends.

ARTICLE III

ARE CRYPTO SECURITIES VIABLE IN THE U.S.?

ERIC W. HESS
FOUNDER
HESS LEGAL COUNSEL

Publicly marked with his speech to the American Bar Association in July, Gary Gensler, Chair of the United States Securities and Exchange Commission (SEC), has become increasingly vocal about the need for most digital assets traded within the U.S. to be registered as securities and for digital asset "exchanges" to register with the SEC as exchanges. Digital asset enthusiasts who bemoaned the lack of regulatory clarity from Washington DC may now wish for a return to less clarity. For many projects the choices are disentangling themselves from the U.S. market entirely, reaching for the Excalibur of "sufficient decentralization," or securities registration, fitting into an exemption or a yet unrealized token safe harbor. If projects issuing native tokens are sufficiently decentralized, those tokens would be commodities regulated under the Commodities Exchange Act and not subject to the more company-centric requirements of the Securities Act of 1933. This is significant, because the additional burdens of securities registration include quarterly and annual accounting, legal, regulatory and shareholder reporting and disclosure obligations which effectively require centralized administration.

Due to the globalized nature of digital asset trading, many existing projects may simply opt to remain offshore and, at worst, block sales to all U.S. residents. But what about projects that want to comply with U.S. securities regulation and tap into the U.S. capital markets? Is there a viable pathway? Moreover, to the extent that such projects go through a restructuring to accommodate compliance with registration or exemption requirements, is there even a viable market structure for their issuance?

> "For decentralized projects, securities regulation not only threatens to reverse the efficiencies of disintermediation but may also threaten their own viability."

Notably, if the utility and monetary aspects of a token cannot be separated (e.g. services paid for with ETH or USD versus a native token) registering as a security would likely require licensed securities professionals or registered platforms to effect its transfer...and thus limit its utility and competitiveness versus other projects not so restricted.

Moreover, the regulation of markets for digital asset issuers is still evolving. Despite this, Chair Gensler has suggested that digital asset

"exchanges" should register as security exchanges. Having served as General Counsel for both SEC registered exchanges and Alternative Trading Systems (ATSs), both throughout their registration process and thereafter, I don't believe that registering as an exchange for digital assets is either a realistic or viable path for most trading platforms based on the current state of regulation. As a result, digital asset issuers are likely to avoid such regulated markets, which creates a chicken and egg problem. Further, even if the chicken decides to cross that road, the SEC and FINRA have not established a clear path for platforms to receive approvals to facilitate such markets. ATSs, on the other hand, are exempt from exchange registration and thus, not subject to the same burdens notably, not being required to maintain their own exchange specific rule sets subject to SEC review (as well notice and comment requirements to amend), which is particularly important for a marketplace still in a nascent state. While ATSs provide a better alternative, the bar is quite low.

Lastly, even if securities registration and regulated marketplace issues are resolved, market intermediaries are struggling with interpreting the basic custody questions under the Customer Protection Rule such as how they can promptly obtain and maintain possession or control of a digital asset carried on the account of a customer or the "good control test". In short, in the event of a broker dealer insolvency, assets must be identified, isolated, protected and potentially transferred in a speed and efficient manner. With this issue unresolved for broker dealers for years, they are effectively blocked from offering custody of digital asset securities.

There is regulatory uncertainty and viability concerns at each stage of capital formation: what the instrument is, how it is traded and whom can trade it.

SECURITIES REGISTRATION & EXEMPTIONS

Most projects in the early stages seeking to raise capital in the U.S. will take advantage of securities registration exemptions available under Regulation D to raise from a limited number of accredited investors through venture capital or angel investor funding. Whether or not the round will be from VCs and angels, the path for project viability typically involves both the launch of the platform and creating market demand for its native tokens This is where the U.S. capital markets and the burdens of registration become more challenging. Thus, projects at this stage will often opt for offerings outside of the U.S. to non U.S. persons. Digital asset projects wishing to continue to proceed in the U.S. market are likely to need to restructure to accommodate securities registration, thus an exemption potentially provides more flexibility.

Amendments made to the exemptive relief provided by Regulation CF or Regulation A (also known as Reg A+) in March of this year might appear promising, at least for smaller U.S. based issuers. Under Reg CF, issuers can raise up to $5mm in an offering on a crowdfunding or ATS platform (e.g. Republic, StartEngine, etc) and under Regulation A issuers can raise up to $75mm. Both Reg CF and A+ offerings have been growing more rapidly than domestic venture capital financings over the last two years.

Much of these benefits may be subsequently lost if an issuer is subsequently forced to register as a public reporting company under

Section 12g. If triggered, it basically imposes much of the disclosure and reporting regime of registered securities on the issuer. Assuming an issuer has graduated from Reg CF to Reg A, the public reporting requirements would be triggered when the issuers public float crosses $75mm. This is a good news, bad news scenario that drastically limits the exemptive relief's benefits for digital asset issuers.

REGULATED DIGITAL ASSET MARKETPLACES

The statements of both the SEC and Chair Gensler suggest that if a digital asset marketplace meets the functional test of an exchange under Rule 3b-16, it must register as an exchange. Why? How could such an exchange be economical to operate in the current environment? Its not as if a regulated U.S. exchange can facilitate trades in unregistered securities on its platform...in fact, registration may ultimately force the platform to only trade digital asset securities. In addition, pursuant to Regulation National Market System (Reg NMS), exchanges are required to use central clearing parties to clear trades. Whether that would be extended to a registered digital asset exchange (either as a condition for approval or subsequently imposed by regulation) or how a central clearing party would even be implemented in the U.S. remains unclear. Exchange registration is a time consuming and expensive undertaking...for a novel digital asset exchange a two-year approval process is likely best case. What if you build it and the digital asset security issuers don't list? Moreover, what is the incentivization to list?

ATSs could be explored as an alternative to exchange listings for digital asset platforms, particularly for Regulation A+ and even Regulation CF issues. ATSs need to register as a broker dealer with the Financial Institution Regulatory Authority (FINRA) and file with the SEC, but their compliance burdens are significantly less than those for an exchange. SEC has provided some no-action relief guidance in connection digital asset security trading on ATSs and token-based ATSs like Rialto Markets and Securitize are already operating in the U.S. While they cannot technically "list" securities for cross market trading like an exchange can, they can facilitate primary offerings and secondary trading in new issues on their platforms and provide similar issuer services to exchanges. ATSs can structure their markets to rely transfer agents instead of central clearing parties to record changes of ownership, maintain security holder records, cancel and issue certificates, and distribute dividends. A number of transfer agents, such as Securitize and tZero, are registered with the SEC as transfer agents for securitized tokens. For clarity, registering as a broker dealer and an ATS requires FINRA licensed professionals and investor protection rules govern their operation such as their being subject to examinations, inspections, and investigations; recordkeeping and reporting; maintenance of written procedures for supervision as well as cybersecurity; specific fair access and capacity, integrity and security requirements.

REGULATION OF INTERMEDIARIES

The uncertainty surrounding the Customer Protection Rule and custody led the SEC to put a proposal out for comment in March 2021 to create "special purpose broker dealer" for digital asset securities. The purpose of the special designation was to isolate associated digital asset risks, suggesting the difficulties in coming to a consensus. Part of the challenge is the broader implications for new

clearance and settlement paradigms impacting traditional equities. While workable solutions will no doubt emerge, in the interim there will be more uncertainty. At least investment advisers can rely on various state trust structures and qualified custodians for similar needs.

"There is little reason to anticipate that the Customer Protection Rule and custody will be the only unique regulatory challenge that securities intermediaries will face. Those contemplating acting in these roles should anticipate new rulemaking and guidance...as well as intervening uncertainty."

Such current and prospective issues will discourage securities intermediaries from the trading of digital asset securities, particularly for the U.S. retail investor.

CONCLUSION

The SEC is pressing crypto issuers and investors to an irreconcilable chicken and egg dilemma. If the formation of a digital asset marketplace is being actively restrained and even discouraged by regulators at all stages of the capital formation process, how is a viable market supposed to emerge? At the very least, effectively integrating digital asset securities into the National Market System is still a few years away and even then, will likely be limited to a small number of projects. Perhaps this forces some projects to become more centralized, drop their native token and operate more like U.S. exchange listed companies. In the interim, exemptive relief from securities registration and, for secondary markets, trading on ATSs may provide the best option for digital asset security issuers within the U.S. regulatory framework...provided that they are prepared to withdraw or are prepared to comply if they trigger public company reporting status under 12g. While experimentation is likely and will ultimately facilitate progress, participants in the ecosystem should think twice about being too early pursuing either the registration of digital asset securities or registration as an SEC regulated exchange. There's no shame in playing chicken!

ARTICLE IV

LEGAL DISPUTES INVOLVING DAOS CREATE NOVEL ISSUES FOR LAWYERS

ANDREW HINKES
PARTNER
K&L GATES

This article is distilled from a transcript of a conversation between Eric Hess, host of The Encrypted Economy podcast, and Andrew Hinkes, partner at K&L Gates. The weekly podcast features discussions exploring the business, laws, regulation, security, and technologies relating to digital assets and data. You may find the original podcast here.

INTRODUCTION

Decentralized technology continues to gain in popularity and enables parties to reimagine how to transact business. But what happens when parties that are trying in a good-faith way to conduct their affairs, using code-driven projects and code-driven structures, have a bona fide dispute. Because of the way that law imposes its will over systems, if we are going to use technology to coordinate the actions of several parties and to allow those parties to control property, we will need to consider the myriad issues that might arise from disputes involving these types of decentralized transactions. We begin with smart contracts.

A smart contract is a direction given to a computer. It's a piece of code that tells the software how to execute. So smart contracts are not necessarily legal contracts, they're best understood as instructions to computers.

There has been some very creative and intriguing messaging around smart contracts as a technology. Some people believe that smart contracts are going to change commercial relationships, perhaps even eliminate the need for transactional lawyers. And while that's interesting to think about, it is best to consider smart contracts as code that can automate certain transactions. Those transactions and the execution of the code can be part of a series of representations and agreements that could amount to a legally enforceable agreement or legal contract.

DISPUTES ARISING FROM SMART CONTRACTS

Disputes arising from smart contracts aren't that different from traditional disputes. They occur because some sort of expectation has not been met. You expected the code to do something and it didn't, which caused you harm. But with smart contracts there is additional complexity because smart contracts are generally designed to operate in certain ways. Once the

terms of the smart contract (code) are put into motion, they're difficult to change, and that limits what courts can do. Courts can't tell the code to rewrite itself in the middle of the transaction.

There are structural differences in the way that assets controlled by smart contracts are to be handled versus digital assets controlled by legally addressable entities. So, if the code takes control over a digital asset and will only give up control over the digital asset under a certain set of circumstances, and a court orders that the asset be turned over, there isn't really a legal person that can effectuate that. Nor can a court order a smart contact to have the code rewritten. Contrast that, for instance to a bank that holds specific assets. The court can send an order to the bank and require the banks to turn over specific assets to a receiver or trustee.

Banks are legally addressable. They understand that they're subject to court orders and will generally either respond in some meaningful way to the legal order or comply. In contrast, based on the structure of smart contracts, certain types of orders simply cannot be complied with.

The result is that certain court remedies may or may not be available to be implemented against digital assets controlled by smart contracts. You might only be able to have ex-post or ex ante remedies as opposed to remedies that affect digital assets while they're in the process of being transacted with.

Further, a plaintiff seeking relief for a loss stemming from a transaction involving a smart contract may face challenges related to even initiating a lawsuit. Pleading claims for relief in a legal complaint comes with its own set of challenges. You will need to consider whether to base your claims on the way that the smart contract code operates and, if so, you need to consider with what level of specificity to allege the breach. Also, you need to consider whether to make certain claims against the person (people) who wrote the code and, if so, how? How will you know who they are? All of these are thorny and, in some cases, impossible questions.

If your claim is based on something along the lines of: there was a series of nine smart contracts that were supposed to execute in a certain way in order for this transaction to occur, and there was a problem in the way that the fifth one acted, which resulted in the subsequent ones not acting properly, which then deprived me of some assets, eventually, you will need to back that up with sufficient detail to make your case.

It could be that you simply plead that you expected these code segments to work in a certain way and they didn't and, as a result, you were deprived of some property. But what is the right level of detail to be made in the allegation? Certainly, it would be simpler if the thing in dispute were milk, rather than digital assets, and you could claim that the defendant promised to drop off a gallon of milk, but he failed to do it. Here, you need to allege there was an intricate machine that was supposed to result in a gallon of milk being dropped off at my house, and this one particular segment of the code failed to execute and the milk never arrived.

The next consideration is to what extent the court's analysis is informed by code transparency. That is, to what extent does the fact that code is open for all to see inform the court's judgment on whether the plaintiff has been aggrieved. Does transparency absolve the defendant of responsibility? Will a court invoke principles of tort law and consider what

would a reasonable person have done under the similar circumstances? That is, would a reasonable person have reviewed the code before entering into such an agreement?

"It seems unreasonable or unlikely in the case of a commercial (or other) dispute involving digital assets that a court would state as part of its holding that the user of a smart contract platform should have audited the code before transacting business."

It's more likely that the court will consider the overall agreement or representations that were made as part of the agreement and make its decision based on that, rather than a code audit.

WHEN THE DEFENDANT IS A DAO

Moving to the question of jurisdiction, how does a plaintiff obtain personal jurisdiction over putative defendants when a dispute involves smart contracts. This may seem like an easy question, but it can be complicated when the party is a Decentralized Automated Organization, generally referred to as a "DAO."

"When you think about DAOs, the first question that comes to mind is whether the defendant is a legally addressable entity."

The DAO could be a business entity whose governance is conducted by people who use smart contracts. Or, it could be a loose association of individuals who use digital assets (often referred to as governance tokens) to participate in the governance of the organization. Still yet, the DAO could simply be a bunch of people who are using a smart contract platform to signal what they want to have happen to some asset that's also controlled by the technology.

In the case of a DAO that isn't incorporated, a court might look at the facts and decide that they will apply gap fillers or default rules in order to assign the group legal significance. The court could find that the group of people looks like a general partnership or a joint venture which could have some very bad consequences for the people involved because that would mean no limitation on liability, each of the individuals would be equally liable for any damages resulting from the dispute.

There are also some states that have created default rules for groups that don't act under legally addressable entities. Surprisingly, a lot of groups that we think about as traditional organizations, such as churches, religious organizations, generally are not formed as legally addressable entities. Sometimes labor unions don't even incorporate, but are simply loose affiliations of individuals acting together. Some states, like Georgia in particular, have civil procedure rules that address these types of unincorporated entities, enabling them to be sued and to designate a representative.

And then there is the question of exactly who represents the party in the case of an unincorporated DAO, where there may not be a legal entity. There are several different theories, none of which have actually been tested in a

court case that has been appealed. For now, we assume that under current law, if a bunch of people are acting together without a legal entity (to control property or for some other reason) they would be considered either a joint venture or a general partnership.

This conclusion has important implications. The first of which is that everybody in the DAO is the entity. That means if you want to sue DAO ABC, and it is not incorporated, all you need to do is find a single participant in the DAO, and serve that person. You can claim that they stand for their compatriots in the DAO and should be permitted to serve as the representative of the DAO.

After that, the burden would shift to that person to try to assert otherwise. They could claim, for example, that they are not a full participant of the DAO, that they only hold tokens, that they have never voted, that they don't control anything, etc. Maybe those arguments would carry the day, but, then again, maybe not.

The question of who can be held to be a representative of a DAO raises interesting questions. Imagine that a DAO requires a token for their governance. Could anybody who holds a token be an agent that could be sued? Hypothetically, could a plaintiff serve a crypto exchange and allege that, because the exchange owns tokens or holds tokens for third parties, it is acting on behalf of a decentralized organization? That could lead to an absurd outcome.

Most of these decentralized ventures don't require participants to give names, addresses, phone numbers, social security numbers, etc. to participate. And they generally don't geoblock participants. So, you might have a difficult time finding someone to serve. And if you can even figure out who they are, locating them and serving them will be difficult to do.

But if you successfully serve a defendant, if you can get that one person, then that person is on the hook to respond. And that means, even if they have great arguments, they probably will have to spend some money to get out of that position. It's not entirely clear how a court would respond to a defense where the defendant claims that they just bought the tokens, didn't know anything about anything and never participated in the governance of the DAO. The court will likely want to know that if there's an aggrieved party, that somebody is liable (at least in the eyes of law). So, when it comes to DAOs, the bear theory applies. You don't have to be able to outrun a bear. You just have to be able to outrun the slowest person in the group.

ARTICLE V

NON-FUNGIBLE TOKENS (NFTS): ARE THEY A WAY FOR CELEBRITIES TO 'RECLAIM' THEIR IMAGE?

CIARA CULLEN
PARTNER
RPC

ALESSANDRO CERRI
SENIOR ASSOCIATE
RPC

SOPHIE PARKINSON
TRAINEE SOLICITOR
RPC

Non fungible tokens, unique blockchain-backed certificates of authentication, can monetise digital assets, or in some instances help to 'reclaim' one's image – but it's not one NFT- fits-all for IP rights.

WHAT IS AN NFT?

By now, most people in the art world, at least, have heard of non-fungible tokens (NFTs). NFTs are a certificate of title of a digital asset, minted (certified) by blockchain. Blockchain, a digital ledger, provides a transparent trail of activity. The digital asset is tied to a blockchain location (the token). This uniquely identifies the digital asset and provides it with a non-fungible authenticity certificate (here, non-fungible means unique).

A copy of the original NFT would not have the same blockchain details (or certificate) so would be recognisable as a fake. Blockchain technology provides a way to authenticate assets, reducing the risk of counterfeit sales and ensuring that IP rights are effectively transferred (where appropriate), as well as facilitating the automatic payment of any royalties. Digital art and other items can be backed by an NFT, ranging from animations, songs and videos to virtual handbags (Gucci) and racehorses (Zed Run, beer brand Stella Artois' virtual horseracing collaboration). Insightful actors, artists and creators are using NFTs to protect their digital property, with creatives like Emily Ratajkowski taking it to the next level – using NFTs to protect and monetise their own image.

WHAT HAPPENS TO THE IP RIGHTS IN NFTS?

IP rights is an umbrella term for intangible assets that flow from "creations of the mind", for example IP rights can offer protections over artistic works such as photographs, graphic images and drawings. IP rights usually give the creator exclusive rights to use and exploit the asset. The main IP rights that might be present in an NFT (at

least, under English law, which is the focus of this article) are copyright and trade marks.

Under English law, copyright arises automatically where an original work, such as a photograph or illustration, is created. It prevents others from using the creator's work without permission. Designs, drawings, photographs and images used as NFTs will likely be subject to copyright protection (as illustrated below).

Trade marks can be registered or unregistered and when it comes to NFTs they can apply to, for example, words, logos and colours. Essentially trade marks operate as a badge of origin and protect brands and the goodwill in the brand from exploitation and reputational damage. An NFT may infringe on a trade mark if, for example, a logo is used in the NFT without prior authorisation from the trade mark owner.

"Digital assets only have value in their IP as there is no tangible property; assets can be infinitely copied, replicated and forwarded (e.g. by downloading and saving an image with a new name). NFTs and the underlying agreements can protect the IP rights in digital assets – preventing NFT buyers from monetising and licensing the digital asset without permission."

Unless ownership rights or use-permissions are granted, the copyright in the NFT-backed asset is not transferred to the buyer, and the agreement merely provides a licence to display the digital asset or artwork.

There can be multiple levels to copyright protections afforded in a single digital artwork. Emily Ratajkowski recently sold, for $140,000, an NFT of a photograph of herself standing next to a re-claimed Instagram photograph of herself from a Sports Illustrated shoot in 2014. Potential copyright protections may have been afforded to the original owners/authors of the first (and second) photograph, including Sports Illustrated and/or its photographer, and Richard Prince (who used the original photo and Instagram screenshot in his own "New Portraits" series). The story of how Ratajkowski had previously purchased the "New Portraits" canvas from Prince was detailed in her first published essay in The Cut in 2020.

Ultimately, it will be important for NFT creators to ensure that they obtain the necessary rights from the underlying work's creator – for example by obtaining a licence or assignment from the photographer (in the case of a photo NFT) or artist to use the photo/artwork for the purposes of the NFT, as without this they will likely be infringing the creator's copyright.

Photographers with rights to license their photos have regularly challenged their muses over copyright infringement for re-posting on Instagram. Ratajkowski is one of many public facing individuals to have been challenged for re-posting pictures of themselves online. Ariana Grande, Gigi Hadid, Khloé Kardashian and Jennifer Lopez have all faced copyright infringement actions when re-posting pictures of themselves on Instagram. NFTs have provided an opportunity for such celebrities to 're-claim' their images.

Whereas some argue that the use of one's own images ought to fall within the fair dealing exception (fair use in the USA), which may protect a user from an infringement of copyright claim, this exception only applies in the UK in a small number of specific (and largely non-commercial) uses, such as research, private study, criticism or review, or parody or pastiche. However, the safest course is always to obtain an assignment or licence from the copyright owner.

On the other hand, if the image in an NFT features a person's name or likeness (such as the photograph of a celebrity) the person in question may have recourse under the package of rights loosely referred to in English law as "image rights". These are rooted in a number of legal regimes, including the law of privacy and data protection, and some jurisdictions such as the US even recognise a specific "right of publicity". Again, where an individual is featured in an NFT photograph, it would be prudent to seek that individual's consent, as well as the photographer's (or copyright owner's, if different).

HOW CAN BLOCKCHAIN TECHNOLOGY MAINTAIN AUTHENTICITY AND REDUCE THE RISK OF UNAUTHORISED COPYING?

"The transparent trail of activity listed on the blockchain can be used to verify an asset's authenticity. Where an asset is tied to the blockchain and certified by an NFT, any later changes to the blockchain code relating to that NFT will be recorded on the transaction ledger, leaving an audit trail for future buyers to inspect."

This ensures the authenticity of the asset, as the wallet identifier of its creator will be visible on the blockchain, as will any changes made to the NFT after its creation.

Further, the purchaser of an NFT can review the provisions of the accompanying smart contract (which are written in code and embedded within the token itself, on the blockchain), to verify the wallet address of the seller, and any linked metadata, on the public blockchain records, in order to check that they are buying the intended NFT from the intended person or company.

Unfortunately, the use of blockchain technology cannot act as a complete safety net for authenticating an underlying asset. This is because digital assets may not be directly attached to the blockchain, which is often an expensive and cumbersome process. Instead, the blockchain token may only contain a link to the file that is hosted on a third-party website. Although any changes to the link itself will show up on the blockchain, if an artist (or hacker) alters the page being linked to or the host server, the NFT may no longer direct the viewer to the original asset.

The crypto artist Neitherconfirm, for example, swapped underlying JPGs of his NFT artwork to JPGs of rugs in a widely publicised Twitter stunt that highlighted the ease of modifying an underlying asset ("pulling the rug"). As the blockchain ledger itself was unaffected, there was no evidence that the creator had modified the asset(s) underlying the NFT(s). Blockchain

technology cannot, on its own, protect against copying an underlying asset tied to a link. A linked asset could be copied where someone gains access to the embedded link, however, assets that are directly placed on the blockchain and certified by NFTs are better protected.

PROTECTING AND PURCHASING (IP) RIGHTS

To protect the creator or rights-holder of the underlying work in an NFT, the purchase agreement should clearly outline the rights which it is intended that the buyer should obtain (e.g. whether the buyer should be permitted to copy, edit, adapt or distribute that work). The terms governing an NFT are often set out in digital "smart contracts" which are written in code and embedded within the token itself. IP rights embedded in this way are afforded blockchain protection. A new buyer would be able to review any previous iterations of the smart contract on the ledger to determine whether any rights have been altered.

Further, the smart contracts themselves provide an additional means of redress should something go wrong; an opportunity to claim for breach of contract. Provisions that are embedded within the token can operate automatically, based on certain pre-defined triggers (for example, making any royalty payments automatically upon an onward sale of the NFT). Royalty clauses can ensure the creator or rights-holder receives payment for any licensed activities, sub-licensing or onward transfers.

As well as setting out royalty provisions, NFT smart contracts will likely set out:

- What rights, if any, are being transferred with the sale. NFTs will typically include a licence allowing the buyer to display any artwork (for example as a profile picture), but they may also include certain other commercial rights, such as the ability to create merchandise incorporating the underlying artwork;

- Details of the NFT collection (if applicable) such as the total amount created, the number (and identity) of owners and details of each transaction; and/or

- Details of the link to any underlying artwork, if it is hosted on a third-party server.

Some NFT marketplaces have standard terms of sale, whereas others allow sellers to determine the terms in the relevant smart contract. It is worth noting however that the legal status of smart contracts is yet to be tested by the English courts!

For onward sales, would-be sellers should ensure they have all the rights necessary to transfer ownership. If a digital asset-creator has entered a robust agreement with no reserved rights and all the image rights cleared and moral rights waived, there should be little issue with selling the rights to an artwork-based NFT. For a video-form or music-based NFT, a seller will need to ensure that all underlying rights were cleared when the NFT was created, including composition/recording rights in music, the chain of title in films, as well as permissions from any actors/performers involved to use their likeness or performance. It is worth noting that film marketing and ancillary content rights often remain with the distributor.

Caution must be taken to avoid misleading advertising regarding the sale of the digital asset or artwork. Potential buyers should be notified where the digital authentication

certificate alone is being sold – as opposed to the rights in and to use the underlying work. Increasing advertising, financial and tax regulation is likely and must be carefully navigated alongside consumer protection law (NFTs can be bought by the public!).

COMMENTS

Having been faced with a copyright infringement lawsuit for posting an image of herself on Instagram, it is no surprise that Emily Ratajkowski was one of the celebrities who harnessed the power of NFTs to reclaim her image.

When we spoke to Ellie Heisler (partner and Entertainment group lead at Nixon Peabody, a fellow TerraLex member) who advised Emily Ratajkowski on the legal aspects of her NFT, she remarked: "this digital marketplace allows creators to participate in the exploitation of their name, image and likeness on a perpetual basis, giving them proper credit and consideration".

Unsurprisingly, other actors, artists and creatives have followed suit. Lindsey Lohan has also sold an NFT portrait containing the word Lightning, and "Lullaby" an NFT music single. Snoop Dogg, Damien Hirst, Kings of Leon, Grimes and John Cleese have also taken advantage of NFTs to protect their digital property. We will likely see more involvement from innovative companies like AB InBev (the owners of various brands including Stella Artois), looking to keep up with ever increasing digitalisation and the movement towards a virtual economy.

ARTICLE VI

EVENTS WITHIN SMART DERIVATIVES CONTRACTS

CIARÁN MCGONAGLE
ASSISTANT GENERAL COUNSEL
INTERNATIONAL SWAPS AND DERIVATIVES ASSOCIATION (ISDA)

CHRISTOPHER D. CLACK
PROFESSOR
UNIVERSITY COLLEGE LONDON (UCL)

INTRODUCTION

When asked by a journalist what was most likely to blow governments off course, Harold McMillan is alleged to have responded "Events, dear boy, events."[1] The occurrence of unexpected events is similarly problematic for the operation of Smart Derivatives Contracts, specifically the automation of payment and delivery obligations. In this article, we explain how certain events contemplated within the ISDA Master Agreement (see below) may impact the automation of payments and deliveries under a Smart Derivatives Contract. We provide a framework for understanding how derivatives contracts are structured at different levels and we discuss the extent to which these are amenable to automation.[2]

ISDA DOCUMENTATION

High-value derivatives transactions establish a financial relationship between counterparties that may last for a very long period of time and may involve very substantial notional sums. This relationship requires extensive legal protection. In practice many derivatives transactions utilise standardised legal documentation provided by the International Swaps and Derivatives Association, Inc. (ISDA). Central to the ISDA documentation architecture is the ISDA Master Agreement. The ISDA Master Agreement is the standard contract used to govern all over-the-counter (OTC) derivatives transactions entered into between the parties. The ISDA Master Agreement sets out provisions which govern the parties' overall trading relationship, including how payments and deliveries are made and how certain events might impact upon the parties' obligations.[3]

WHAT ARE SMART DERIVATIVES CONTRACTS?

Smart Derivatives Contracts are smart contracts[4] for automating derivatives contracts.

"Automating the performance of derivatives contracts may allow for a

1. P. Kellner (Nov. 1 1985) Why Neil Kinnock has a new spring in his step. New Statesman, London, England, page 9.

2. A more detailed discussion can be found in our previous paper: C.D. Clack and C. McGonagle (2019) Smart Derivatives Contracts: the ISDA Master Agreement and the automation of payments and deliveries. arXiv:1904.01461. https://arxiv.org/pdf/1904.01461.pdf

3. A more detailed explanation of the ISDA documentation architecture can be found in ISDA (2019) ISDA Legal Guidelines for Smart Derivatives Contracts: Introduction. https://www.isda.org/a/MhgME/Legal-Guidelines-for-Smart-Derivatives-Contracts-Introduction.pdf

4. C.D. Clack, V.A. Bakshi, and L. Braine (2016, Revised March 15 2017) Smart Contract Templates: foundations, design landscape and research directions. arXiv:1608.00771. https://arxiv.org/pdf/1608.00771.pdf

substantial reduction in costs for large financial institutions through greater efficiencies and reduced human error.[5]"

Derivatives are generally considered to be fertile territory for the application of smart contracts because their main payment and delivery obligations are heavily dependent on conditional logic.[6][7] Much of the operational detail of payments and deliveries can be found in the economic terms and payment mechanics of the particular derivatives product i.e., within the transaction confirmation and associated product definitions. However, it is not sufficient only to automate these operational aspects of the contract. The broader contractual relationship must also be considered.

UNDERSTANDING EVENTS

The processing of payments and deliveries throughout the lifetime of a derivatives transaction can be affected by different kinds of events. ISDA documentation establishes rights, obligations and mechanisms reflecting the occurrence of these events that can affect both the timing and quantum of payments and deliveries for a potentially very large number of transactions. In the context of ISDA documentation, an "Event" is an event or circumstance that may (either immediately or with the passage of time) impact upon the parties' respective ability to perform their obligations, including payment and delivery obligations, under the transactions entered into between them. It is important that parties are able to react to events which may be indicative of either a deterioration in creditworthiness of their counterparty or some fundamental change in their counterparty's legal, regulatory, or operating framework such that their ability to continue making payments and/or deliveries could be impeded. The Master Agreement therefore contemplates the occurrence of a broad range of such events and provides each party with a mechanism to terminate derivatives transactions in order to eliminate or mitigate its financial exposure to its counterparty.[8]

The ISDA Master Agreement contemplates two distinct categories of Events. Events of Default generally relate to events where one of the parties is (in a general sense) considered to be at fault, whereas Termination Events relate to events where neither party is strictly at fault. The ISDA Master Agreement contains a number of standard Events, in both categories, all of which are capable of customisation.

Additional Events can also be defined by the parties. While the ultimate consequence of the occurrence of either type of Event is the same i.e., the potential termination of derivatives transactions entered into between the parties, they are necessarily distinct. For example, while the occurrence of either type of

5. See ISDA (2016) The Future of Derivatives Processing and Market Infrastructure. https://www.isda.org/a/UEKDE/infrastructure-white-paper.pdf

6. See ISDA and Linklaters (2017) Smart Contracts and Distributed Ledger – A Legal Perspective. https://www.isda.org/a/6EKDE/smart-contracts-and-distributed-ledger-a-legal-perspective.pdf

7. Certain aspects of derivatives contract have implemented on blockchain using smart contracts. For example, see: https://www.deutsche-boerse.com/dbg-en/media/press-releases/DZ-BANK-BayernLB-and-Deutsche-B-rse-prove-functionality-of-digital-smart-derivative-contracts-2637128

8. A more detailed discussion of different types of events under the ISDA Master Agreement can be found in ISDA (2019) ISDA Legal Guidelines for Smart Derivatives Contracts: The ISDA Master Agreement. https://www.isda.org/a/23iME/Legal-Guidelines-for-Smart-Derivatives-Contracts-ISDA-Master-Agreement.pdf

Event gives a party the potential right to terminate derivatives transactions entered into under the Master Agreement, the manner in which these derivatives transactions terminate may differ depending on whether an Event of Default or Termination Event has occurred. The different outcomes and potential for customisation makes it important for smart contract developers to understand and correctly categorise the relevant Event in order to reflect accurately the contractual consequences that flow from the occurrence of an Event and the precise manner in which the Event may impact upon the parties' respective payment and delivery obligations.[9] Any technology solution that intends to automate payments and deliveries within a derivatives transaction will need to take account of the various events that might occur and be capable of i) observing the occurrence of a circumstance that might give rise to an event; ii) determining that an event has occurred; and iii) taking action to manage the consequences that might arise from the occurrence of the event (which may entail notifying the parties where further assessment is required).

LEVELS OF EVENTS

The "contract" relating to derivatives transactions between two parties is often represented by a combination of documents. These documents are highly interdependent. It is not possible to fully understand a single derivatives transaction or the overarching contractual relationship between the parties simply by looking at the terms of an individual transaction or even by reference to the Master Agreement. To fully understand the terms of a particular transaction and how external events may impact upon it, it is important to look at each of the various levels of obligation that exist within the ISDA documentation architecture, the key documents involved, and how they interrelate.[10] Within this contractual architecture, it is possible to distinguish four different levels (described below) at which circumstances or events might be observed and which may ultimately give rise to the occurrence of an Event. A single event might be observed at more than one level, and there will typically be a hierarchy of events within the contract, allowing one to determine how best to treat an event which may be observed within two or more levels.

Events may occur at the Transaction Level. Events occurring at the Transaction Level are typically related to the specific product lifecycle, with expected behaviour being set out in the Confirmation and product definitions. Observing the occurrence of an event at this level would seem to present the fewest challenges for smart contract code. For example, it should be relatively straightforward for the code to determine whether a party has failed to make a required payment of the required amount at the required time as the parties will have immediate access to the relevant transaction data.

Events may occur at the Relationship Level. Events occurring at this level are related to the agreement negotiated between the counterparties and may involve more than one transaction. Events of Default and Termination Events are examples of Events that might be triggered through the observation of information relating to the parties themselves. For example, the smart contract code might be able to observe the bankruptcy of

9. The unnecessary customisation of clauses within the Master Agreement is being addressed through initiatives such as the ISDA Clause Library. https://www.isda.org/2020/04/20/what-is-the-isda-clause-library/

10. A more detailed overview of the ISDA documentation architecture can be found in ISDA (2019) ISDA Legal Guidelines for Smart Derivatives Contracts – Introduction. https://www.isda.org/a/MhgME/Legal-Guidelines-for-Smart-Derivatives-Contracts-Introduction.pdf

a party by monitoring information sources that might publish information relating to the insolvency of that party (e.g., a regulatory authority or similar administrative, regulatory, or judicial body).

Events may occur at the Third-Party Level. Observing the occurrence of potential Events at the Third-Party Level is likely to be more challenging. Here, the smart contract code may be unable to establish the potential occurrence of an Event by reference to either the derivatives transaction data or to information relating solely to the counterparties. Instead, the code will need to observe information relating to a third party i.e., a party who is not a contracting party to the Master Agreement . Without continuing access to information or data relating to third party arrangements, deciding whether the relevant circumstances have arisen may prove very challenging to automate.

Finally, Events may occur at the Exterior Level (i.e. not related to either party, nor to a specific third party). Much of the complexity at this level arises due to the large number of external events that may arise and the difficulty of assessing whether those external events could be relevant in determining when an Event has occurred under the Master Agreement.[11] Some Events (e.g., a Force Majeure) are necessarily broad in scope. This is necessary due to the existence of a very wide range of circumstances that may, for example, make it impossible for parties to fulfil their obligations. Ongoing observation and interpretation of information relating to each of the legal and regulatory frameworks applicable to all parties is likely to prove both challenging and inefficient to automate.. Despite the inherent difficulties, we believe it may be possible to automate some aspects of the monitoring of events at this level, perhaps with the smart contract code monitoring some readily available external information and providing alerts that will then be followed by human interpretation. In other situations, human observation of an external event may require the ability to pause or stop the smart contract code (e.g., in the case of an Illegality).[12]

MANAGING EVENTS

Effective processing of Events within a smart derivatives contract will require the following steps:

Observation: The first step in processing events is the ability to observe. Observation breaks down into two aspects: what to observe, and how to observe. These are linked: for example, some events may arise within the technology platform and are relatively straightforward for smart contract code to observe, whereas events arising externally may be more difficult to observe. For example, with a distributed ledger platform, an “oracle” must be established in advance to make the external observation and route it through to multiple instantiations of the smart contract code so that they all receive identical information.

Determination: Once an event or circumstance has been observed, the smart contract code must be

11. For example, certain events of default and termination events may be extended in scope to capture certain designated ‘specified entities.’ A specified entity would typically be an affiliate or entity within the same corporate group, the circumstances of which are likely to have some impact upon a party’s creditworthiness or its ability to continue meeting its obligations under the Master Agreement. Such an entity would typically not be a party to the Master Agreement.

12. If the smart contract code were to run on a distributed ledger, both incoming and outgoing interaction with the parties might occur via the use of “oracle” services as for example described in M. Hearn and R.G. Brown (2016) Corda: A distributed ledger. Corda Technical White Paper.

able to determine whether or not the criteria for triggering an Event of Default or a Termination Event might be fulfilled. This requires the smart contract code to obtain and monitor information and understand the implication of that information as it relates to the precise circumstances that may ultimately constitute or give rise to the occurrence of a particular Event. Of course, for computer code "understanding the implication" of a set of observed events means that the mechanism and thresholds for such determination must be analysed in advance and incorporated into the smart contract code.

"While in most cases objective criteria are used in determining whether or not a relevant Event has occurred, the determination of some Events may include subjective elements. In these instances, a party seeking to trigger the Event must therefore rely upon their own subjective interpretation of the relevant criteria and convey this information to the smart contract code. An appropriate dispute resolution mechanism (which may or may not be automated) should be triggered where the parties disagree on the subjective interpretation."

Action: When the circumstances giving rise to a potential Event have occurred and are continuing, the parties may be entitled to exercise certain contractual rights under the Master Agreement. A party may wish to terminate their contractual relationship with their counterparty. Alternatively, they may decide that the Event is relatively immaterial or inconsequential and that they do not wish to take any action. Therefore, there will often be uncertainty as to what the exact consequences of an Event will be due to the levels of human intervention and discretion required. It is unlikely that all counterparties will have identical appetites for risk, and therefore unlikely that they will all wish the consequences of an Event to be managed in the same way. Thus, it would seem that the default action for smart contract code to take once an Event has been determined should be to inform the relevant parties and await further authorisation (though for greater efficiency this should be structured, so that for each Event a human can authorise one of a selection of pre-programmed further actions).

Looking ahead, it might be possible for smart contract code to have pre-programmed actions that are different for each party. For example, one party may have a lower tolerance for risk and may wish to terminate the contract upon the occurrence of minor, technical breaches, whereas their counterparty may have a higher risk tolerance and may be prepared to waive certain breaches that are not indicative of serious deterioration in the creditworthiness of the other party. Since the smart contract code must be authorised by all parties, these pre-programmed responses will of course be known to all parties in advance, so some care will be required to ensure that these known responses cannot be exploited to the advantage of defaulting party. More subtle schemes might be imagined — for example, the smart contract code

could be instructed to observe a rising level of smaller events and thereby infer a rising level of risk, so that as the risk grows the automated response to each subsequent Event becomes less lenient (or perhaps triggers an alert to the party at growing risk).

HOW MUCH TO AUTOMATE?

Assessing the impact of events on contractual provisions is a complex exercise. In many cases, it will require a user to observe data that is not immediately available or accessible and/or exercise subjective judgement as to the impact of the relevant event. Given these challenges, it is unlikely that the entirety of a legal contract will ever be converted into smart contract code.[13] It is important therefore to choose which provisions should be automated. In making this assessment, it is important to consider both (i) what can be automated, and (ii) what should be automated. This of course is not a static consideration: the former will increase for example as we gain a better understanding of contract semantics and as technology improves, and the latter will vary for example according to jurisdiction and legal certainty and the risk appetites of the parties.

WHAT CAN BE AUTOMATED?

As noted above, derivatives contracts are considered good candidates for automation as many of their obligations are highly operational in nature. However, it is not always possible to identify whether a part of a contract is operational or non-operational in nature simply by inspecting the text to determine whether it uses conditional logic. Some operational phrases do not use conditional logic, and some phrases that use conditional logic are non-operational. Furthermore, it is not always the case that an "operational" aspect of contractual language is easier to automate than a "non-operational" aspect. Many operational clauses could require very complex code to automate, particularly where multiple conditional statements are used in combination.

In the context of derivatives contracts specifically, the documentation framework provides many different sources of both operational and non-operational aspects, many of which interact with others. Studies of the semantics of the Master Agreement have revealed not only a large operational aspect, but also an unexpected entangling of deontic, temporal, and operational aspects.[14] This is referred to as the "separability problem."[15]

WHAT SHOULD BE AUTOMATED?

If automation were limited to the basic economic conditions outlined in the Confirmation and product definitions, the accruing benefit would be modest in comparison to what could be achieved by also automating the provisions of the Master Agreement. A truly autonomous Smart Derivatives Contract should for example be capable of observing a range of events. This does not mean that the entirety of the Master Agreement must necessarily be automated, and it is important to reason about which parts should be automated — e.g., because they are

13. See C. McGonagle (2021) Translations: creating legally effected smart derivatives contracts. Journal of International Banking and Financial Law 8(540).

14. C.D. Clack (2018) Smart Contract Templates: legal semantics and code validation. Journal of Digital Banking 2(4),338–352. Author's preprint: http://www0.cs.ucl.ac.uk/staff/C.Clack/research/JDigitalBanking-Clack-AuthorPreprint.pdf

15. C.D. Clack and G. Vanca (2018) Temporal aspects of smart contracts for financial derivatives. Lecture Notes in Computer Science 11247:339–355. http://arxiv.org/abs/1805.11677/

easy to automate, or because their automation although difficult would bring great benefit.

ISDA has proposed some guidelines to support the selection of parts of the contract which are likely to be amenable to automation:[16]

- Focus on automating common, standardised, aspects of derivatives contracts, so that the automation is widely applicable across a large number of different contracts.
- Avoid automating complex legal provisions, since these might be more difficult to establish, operate and maintain. We have observed that complex legal text can sometimes be captured with quite simple logic (and therefore simple code). The reverse is also true, that seemingly simple legal text may require quite complex logic (and therefore complex code).
- Consider how external factors such as observable events or discretion (including by a third party) will be efficiently incorporated into the smart contract code.
- When designing functions aimed at automating derivatives contracts, these should be common across multiple products.[17]
- Only automate those aspects of a derivatives contract where a lawyer can confirm that their legal effect will not be changed when automated.

CONCLUSION

Smart Derivatives Contracts aim to automate high-value derivatives contracts, including automation of aspects of the Master Agreement as well as automation of lifecycle events stated in the economic terms of the specific derivatives product. This vision raises many issues to be solved, such as (i) how the smart contract code can be faithful to the legal agreement, and (ii) to what extent the provisions of the legal agreement can be automated. This requires an inter-disciplinary approach that brings together computer scientists, lawyers, and banking practitioners to consider how much of a derivatives contract can be automated so that the greatest possible efficiency gains are realised. Central to this assessment will be the consideration of how events might impact the expected operation of a smart derivatives contract. We hope this article will prove useful in providing a framework to understand how the occurrence of different types of Events might impact upon derivatives contracts and how these Events might be considered within the operation of autonomous, self-executing Smart Derivatives Contracts.

16. See ISDA and King & Wood Mallesons (2018) Smart Derivatives Contracts: From Concept to Construction. https://www.isda.org/a/cHvEE/Smart-Derivatives-Contracts-From-Concept-to-Construction-Oct-2018.pdf

17. The ISDA Common Domain Model, for example, creates a single, common digital representation of derivatives trade events and actions to enhance consistency and facilitate interoperability across firms and platforms: https://www.isda.org/a/z8AEE/ISDA-CDM-Factsheet.pdf

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 **law@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