THE INTERNATIONAL JOURNAL OF BLOCKCHAIN LAW

Volume 2

March 2022

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.

Welcome to the 2nd issue of the IJBL!

I am proud to present a great set of new articles covering various legal topics surrounding blockchain technology from around the globe and from different perspectives.

First things first: For this issue the editor's board has decided to add a new feature to the Journal: a written round table. My fellow editors, Andrea Tinianow and Stephen Palley, took the initiative to reach out to top US attorneys in the blockchain space to ask them about the most pressing legal issues pertaining to DeFi. The result is a comprehensive and insightful discussion on currently unresolved legal topics around this issue from an American legal perspective. This piece is deservedly the leading article of this issue. A special shout out to Andrea and Stephen for making this happen.

DeFi is touted by many in the crypto space as having potential to significantly disrupt the traditional financial industry over the next decade. With that in mind, this issue continues with two more appealing articles covering DeFi from different perspectives: Norton Rose Fulbright lawyers Robert A. Schwinger, Harriet Jones-Fenleigh and Jonathan Hawkins look at some of the disputes that may arise in the DeFi space and set out the steps to be taken by users of DeFi- or smart contract protocols to manage these potential risks.

Following the DeFi pieces, Samir Patel explores the issue of fractionalization of NFTs.

It is a matter of fact that blockchain/DLT based solutions continue to be prone to hacks, frauds and scams. Barry Sookman (Mc Carthy/Tetrault Toronto) presents a case study and the pertaining remedies as well as challenges in recovering digital assets.

Michael Jünemann and Udo Milkau from Bird & Bird Frankfurt explore the practical challenges of using smart contracts, in comparison to traditional written contracts. This will be the first "episode" of a broader discussion around smart contracts, as my fellow co-editor Jake van der Laan is drafting an article on the same topic for the 3rd issue of the IJBL focusing on the more technical aspects of how smart contracts currently function and the limitations this creates in their utility in the "contractual life cycle".

Further, Raoul Renard, Carmen María Ramírez Ortiz, Oswald Kuyler and Steven Beck provide an overview of the state of play on the adoption of the Model Law on Electronic Transferable Records (MLETR) in conjunction with blockchain-based trade deals in the APAC region.

Finally, Prof. Tran Viet Dung and Le Tran Quoc Cong present an interesting perspective of the legal and regulatory aspects of DeFi Lending in Vietnam.

Happy reading!

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. WEINGARDEN

ASSISTANT VICE PRESIDENT, DATA PROTECTION OFFICER
NOTARIZE, INC

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

ARTICLE I

A ROUND TABLE DISCUSSION (IN FOUR PARTS): PRESSING LEGAL ISSUES IN DECENTRALIZED FINANCE

DAVID ADLERSTEIN
COUNSEL
WACHTELL, LIPTON

OLTA ANDONI
DEPUTY GENERAL COUNSEL
AVA LABS

COLLINS BELTON
MANAGING PARTNER
BROOKWOOD P.C.

LEWIS COHEN
CO-FOUNDER
DLX LAW

JASON GOTTLIEB
PARTNER, CHAIR
MORRISON COHEN LLP

CHRISTINE PARKER
VICE PRESIDENT,
DEPUTY GENERAL COUNSEL
COINBASE

LEE SCHNEIDER
GENERAL COUNSEL
AVA LABS

ANDREA TINIANOW
CHIEF LEGAL OFFICER
IOV LABS

STEPHEN D. PALLEY
PARTNER
ANDERSON KILL

This roundtable discussion was curated and edited by Andrea Tinianow and Stephen Palley, Editors of the IJBL. See their bios and headshots on page 4.

INTRODUCTION

With more than $USD 92 billion locked in decentralized finance (DeFi) protocols, DeFi is hot and it's not showing any signs of cooling down soon. We reached out to top attorneys in the blockchain space to ask them about the most pressing legal issues pertaining to DeFi. Here is what they had to say.

A special shout out to attorney Gabe Shapiro for helping us to craft these questions and to the attorneys who provided commentary. We appreciate their excellent contributions to this article as well as the crypto/blockchain ecosystem overall. The roundtable discussion assumes that the reader has some basic information about crypto and DeFi.

PART ONE

Certain on-chain protocols allow transactions (trades, borrowing, etc.) relating to tokens, and it is likely that some of these tokens are securities or, some of the transactions are securities transactions under U.S. law.

CHRISTINE PARKER: The focus on securities is important, **but in the future, the vast amount of value will be transacted in the derivatives market, based on the non-security tokens, bitcoin and ether ("BTC and ETH").** There will be an increase in the relative notional value of tokens that are commodity-based, as opposed to security-based. In the future, there will be large derivative exchanges for retail investors. And, once there is robust trading in the derivatives markets in the U.S., **it will be much greater than the securities markets, with massive leverage on long term contracts.**

Do such on-chain protocols constitute "exchanges" as that term is defined under the Securities Exchange Act of 1934 ("1934 Act")?

LEE SCHNEIDER: The answer to this question depends on a variety of factors, including how the protocol is involved in effecting transactions. The 1934 Act definition would seem to exclude from "exchange" a smart contract that has no single point of failure, no single source of truth and no single authority capable of, or responsible for, effecting transactions and recording or altering data. In other words, if there is no operator (or group constituting an operator), then something is not an exchange. Therefore, each protocol needs to be scrutinized to determine applicability of the definition.

JASON GOTTLIEB: I agree with Lee. Definitionally, **if the protocol is allowing the trading of securities tokens, it is more likely to be deemed an exchange; but if it allows trading of only non-security tokens, it cannot be** (at least, under the 1934 Act).

COLLINS BELTON: While I philosophically agree with Lee and Jason, there is at least some cause to believe that historical precedent may bias the Securities Exchange Commission ("SEC") towards a different finding. In particular, some of the earlier literature and procedural history discussing the creation and categorization of electronic communication networks, which did ultimately largely fall into the category of an alternative trading system ("ATS"), seems to be at least in part applicable to protocols allowing for certain exchanges. Like Lee suggests, specific factors will weigh heavily in the Exchange Act's "functional" test, but I'm not sure if the lack of a single point of

failure alone will be dispositive (even though it largely should be).

LEWIS COHEN: I tend to agree with Collins on this. The question to me is less whether technically the network of computers running the relevant protocol code are operating an "exchange" (assuming that the protocol facilitates the bids/offers of "securities"). If that was the function of the protocol code, a judge would likely conclude that the network was an exchange. But it does raise difficult questions around enforcement, though. For example, which participants would a regulator be able to go after? An Ethereum node operator whose node passively validates whatever code has been deployed? The developer who actually deployed the relevant code? And what if multiple people contributed to the creation of the code, and the person who physically deployed the code was just an unknowing agent? What about transient holders of governance tokens for the protocol, or the person that runs a front end for accessing the protocol (even if it is just one of many such front ends)?

Does a website that offers access to these types of on-chain protocols constitute an "exchange," as that term is defined under the Securities Exchange Act of 1934?

LEE SCHNEIDER: It depends on what "access" means. If it just means that you can see what's going on, look at pricing information, etc., then probably not. If the website is the execution facility and is operated by a single authority, then probably yes. If the website allows users to effect/execute trades on the protocol but does not operate the protocol, then it is probably a broker. All of this assumes the tokens are securities.

CHRISTINE PARKER: Same outcome for commodity-based tokens EXCEPT that the exchange and broker are not regulated under the Commodity Exchange Act, unless the tokens are offered with some form of financing/leverage (e.g, a commodity derivative).

Does the combination of such an on-chain protocol and such a website constitute such an exchange and, if so, does that depend on the website being operated by the same person or group of persons which developed or deployed the protocol?

LEE SCHNEIDER: Yes, it depends on who is operating both.

COLLINS BELTON: I tend to agree that the combination of providing the service functionality and access likely increases the risk of a site being deemed an exchange, although the protocol may still retain colorable arguments against that classification. That said, if the developer-operator is one of many interfaces, and further, that single site is not the sole or primary means by which persons interact with the protocol or engage in activity, then the argument for treating that particular combination as an exchange is weaker (unless *all* other combinations are similarly treated as such).

LEWIS COHEN: if you are an identifiable person over whom a relevant regulator or member of law enforcement can get jurisdiction that derives an economic benefit from providing services (even indirectly) that are not in compliance with relevant law/regs, you are at risk for an enforcement action. Another reason why we need better laws. Soon.

Are there ways for non-banks (again, in the U.S.) to structure so-called decentralized finance (DeFi) or centralized finance ("CeFi") "yield" protocols that do not run afoul of the securities laws (including the registration requirements

of the Securities Act of 1933 (the "1933 Act"), the Investment Company Act of 1940 and the Investment Advisers Act of 1940)?

LEE SCHNEIDER: These are very broad questions. Let's focus on the question of whether such arrangements are investment contracts or otherwise securities. Let's also consider similar arrangements and ask why they have not been treated as securities: payment for order flow; maker-taker arrangements; credit card rebates. If the answer relies on "pooling" of funds and returns, that seems a little thin because these 3 examples rely on pooling as well.

CHRISTINE PARKER: There is likely a role that a futures commission merchant ("FCM") can have in offering DeFi or CeFi yield protocols for BTC/ETH products. This would be outside of the scope of their regulated activity but comports with the financing/lending FCMs provide based on warehouse receipts.[1]

COLLINS BELTON: I agree with Christine that the most likely non-bank entity to embody a hybrid CeFi/DeFi model that doesn't run afoul of securities laws like the one described above is a commodities entity. We are already beginning to see some examples of this model being experimented with in DeFi and established commodities players. That said, to the extent that assets are treated as security-based swaps, I'm not sure it would be accurate to refer to these as being outside of the securities law requirements, but the offerings wouldn't necessarily run afoul of them either.

1 To learn more, we refer you to the advisory from The Division of Swap Dealer and Intermediary Oversight (DSIO) of the Commodity Futures Trading Commission which provides guidance to FCMs on how to hold and report certain deposited virtual currency from customers in connection with physically-delivered futures contracts or swaps.

LEWIS COHEN: I agree with Lee that the central question here is whether the "facts and circumstances" around the yield product implicates the formation of an "investment contract." I would say that in many cases, the answer will be "yes," but it depends on the details of how the program is being run.

DAVID ADLERSTEIN: I would add that in addition to securities laws, these products involve bank-like functions, so depending on the circumstances, other areas of law may also be implicated. The ability for retail to place money with a counterparty in exchange for a yield and to withdraw the money on demand resembles a bank deposit. The legal considerations around these products need to be considered case-by-case.

PART TWO

Automated Market Makers ("AMMs") are the underlying protocol that enable users to trade crypto on a decentralized basis. Where do AMMs fit into the current structure of U.S. securities laws, if at all? How does MGM Studios Inc. v Grokster, Ltd. impact your conclusion?

JASON GOTTLIEB: Ultimately, most AMMs are just software, and software that can be used for a host of completely legal purposes. **The software developers cannot be held responsible for misuse of the platform, any more than Bill Gates could be held responsible if a drug gang used Microsoft Excel to keep track of their drug deal profits.**

Some lawyers look to the file-sharing cases for the Supreme Court's ultimate opinion in Grokster. I have a different, more pragmatic view. Ultimately, the courts could shut down Grokster (or Napster, or Limewire, or or or...), but ultimately, during the several years it took to shut down a file-sharing service in the courts, several others sprung up. DeFi

protocols are easier: a team can "fork" an open-source protocol in a half-hour, host it on a distributed website like IPFS, and walk away from it. Maybe they're liable under Groskster, maybe not, but good luck suing a bunch of people who may be foreign, may be anonymous, and may be unwilling to comply with any US court orders.

Ultimately, what killed the Groksters wasn't the courts. It was Apple, and iTunes. Apple figured out a way to make music file sharing easy, cheap, and 100% legal. The protocols that do that will win, and settle the argument.

COLLINS BELTON: I strongly agree with Jason that a "truly decentralized" AMM, even with an unrelated treasury or something else, should not and is not properly viewed as an exchange or function that is covered under the 1933 Act or 1934 is Act. However, the term "truly decentralized" does much lifting here, and ironically, I would say the **SEC's action against something like EtherDelta, which was ostensibly a DeFi exchange that could be likened to an early AMM, was the correct outcome.** Similarly, for several AMM models where critical components core to the protocol's ongoing or future functionality are not decentralized (e.g. backend servers or unilateral control of a governance token allowing material operational changes by a single group or group of affiliates), the risks attendant with other entities and platforms that we regulate under the securities laws often are resurgent, and in those cases, they fit squarely within the existing framework of securities laws.

Grokster can be distinguished on the grounds that there, the court focused much attention on the fact that the arguable core functionality and practical reality of the platform was illicit activity, and that the operators knew about such activity and took no action to prevent it. Further, given their control of certain access points, software distribution mechanisms required to maintain the service and other areas of central control, ascribing illicit activity to them was more practical and reasonable. In contrast, here, AMMs have largely shown that they are totally neutral and, in many jurisdictions, allow completely permissible transactions. **The fact that the U.S. and certain jurisdictions have nebulous rules that have yet to make broad determinations about assets should not be analogized to enabling the illegal sharing of copyrighted materials (which was already a well-known prohibition prior to the development of basic file sharing).**

AMM liquidity pools enable users to buy and sell crypto without the need for centralized market makers. Liquidity is provided by "liquidity providers" ("LPs") and pooled, with each LP receiving a pro rata share of the pool's assets (including accumulated trading fees) represented by an "LP token". In addition to receiving a pro rata share of trading fees paid by people who trade assets through the AMM pool, LPs can often stake their LP tokens in third-party smart contract systems to receive governance tokens relating to those systems–a process known as "liquidity mining." AMM systems sometimes also reward LPs with governance tokens relating to that AMM system itself. Thus, LPs are potentially triple-incentivized to provide liquidity to AMM pools–by trading fees from the pool, by third-party governance tokens and by the AMM's own governance tokens. Is liquidity-providing to an AMM pool an investment contract under Howey?

LEE SCHNEIDER: No, it is an order type that results in trades, with the share of trading fees being equivalent to maker-taker fees or payment for order flow.

LEWIS COHEN: I agree - not investment contracts. However, **if a court were to take the position**

(wrongly!) that the specific tokens were "securities," identifiable U.S. persons in a liquidity pool would run a risk of being unregistered broker-dealers.

Are LP tokens representing positions in AMM pools investment contracts under Howey?

LEE SCHNEIDER: No, they are claim-checks for the assets placed in the pool.

LEWIS COHEN: I agree with Lee, inasmuch as an "investment contract" necessarily involves a legal relationship between two or more persons and an LP token does not create such a relationship. This said, someone could create an investment contract by marketing LP tokens as the object of the scheme (similar to ML's marketing of certificates of deposit in Gary Plastic).

Is there a credible argument that liquidity pools are investment companies under the Investment Company Act of 1940?

LEE SCHNEIDER: No, because there is insufficient pooling of assets (my assets get traded when an order matches with them) and because there is no investment adviser.

LEWIS COHEN: Not sure I agree here. If a court found that the digital assets in a Liquidity Pool were "securities" then that pool could well be considered an "investment company" in the same way that a segregated account could be an "investment company".

Is there a credible argument that LPs are securities market-makers, brokers, dealers or underwriters under the securities laws?

LEE SCHNEIDER: It depends on whether there is a single point of failure, single source of truth and single authority capable of, or responsible for, effecting transactions and recording or altering data.

PART THREE

Should the developer of a website that does no more than serve as a non-exclusive interface to a blockchain DeFi protocol require anti-money laundering/ know your customer ("AML/KYC") compliance? What if the website cannot interface with the protocol without being paired on the user side with a third-party wallet software under the user's control?

OLTA ANDONI: Although we tend to lump AML/KYC together for DeFi protocols, I would emphasize AML for DeFi protocols. **If the developer does no more than serve as a non-exclusive interface to a blockchain, I would not impose AML/KYC requirements.** But a different scenario may be applicable when a protocol operates via third-party wallet software under the user's control.

LEE SCHNEIDER: T**here are several problems here, most prominently the problem that many different asset types trade in DeFi protocols, and AML laws are bleeding into general commerce rather than their traditional purview of financial instruments.** This is no small issue and reflects a major policy shift that has not been justified or gained broad support other than at the Financial Action Task Force ("FATF"). On the question of "should" the developer require AML/KYC compliance, that is up to the developer. If the question is whether there is an existing requirement that they do so, that depends on the activities that can be accomplished through the website and the compensation, if any, the developer receives.

COLLINS BELTON: Absent additional activity, **merely providing a non-exclusive interface to an existing protocol should not require KYC under a consumer due diligence** ("CDD"), as such activity should not be

treated as being engaged in a money service business or otherwise trigger the provisions of a Bank Secrecy Act ("BSA") by making such provider a financial institution. On the side of sanctions/AML, imposing such requirements is not aligned with the intent or text of existing law, but unlike the KYC/CDD arguments under the BSA, I believe that Lee's perspective is right, and that t**he reach of AML/ sanctions is now well beyond its original intent or text.** As such, while I have a normative position on AML/ sanctions, I believe many policymakers in the U.S. and outside of the U.S. believe existing law does require such checks, and regulators operate under this guise many times.

LEWIS COHEN: The answer may change if you are hosting a website front-end to the protocol and profiting economically by doing so.

DAVID ADLERSTEIN: L**et's just come out and state the fundamental policy issue at the root of this question – specifically, currently operational DeFi protocols are enabling large transactions between pseudonymous counterparties, which may include bad actors** such as Office of Foreign Assets Control ("OFAC")-sanctioned persons and criminal organizations. More sophisticated bad actors can be expected to circumvent the guarded routes of regulated finance where they can (although studies indicate that the prevalence of criminal activity involving cryptoassets is significantly less than is generally believed).

Fundamentally, then, the issue is whether AML/KYC compliance—acknowledging the prior points that there are distinctions between AML and KYC and policy questions about when frameworks should appropriately apply—should be achieved by imposing requirements on website developers. As others have pointed out (including Gabe Shapiro, if I recall correctly), it is difficult to envision imposing affirmative content requirements on software developers, especially in the case of open-source software which could be replicated and deployed from anywhere in the world.

Nonetheless, for the policy reasons noted, it stands to reason that an AML/KYC touchpoint be required somewhere along the line, a**nd a logical starting point might be to impose obligations on DeFi users at scale, requiring that they have their identity validated by a qualified third party in order to participate in DeFi transactions involving value transfers exceeding a particular threshold of value,** and to prohibit users of scale from transacting through protocols, or pools within protocols, involving participation of non-validated participants. This need not entail fully "permissioned" DeFi but rather could entail portable proof of digital identity (not unlike a digital vaccination card associated with a wallet, perhaps even in the form of a non-fungible token ("NFT")) or integration with wallet software featuring a mandatory KYC integration, and could lead to a situation where most users "vote with their feet" and transact through protocols that make allowance for this type of functionality. Practically, this would not prevent bad actors from transferring or receiving large amounts of value using decentralized software, but could facilitate enforcement by driving them into more concentrated, darker corners.

PART FOUR

What are your predictions for legal/ regulatory developments for DeFi in 2022 (and beyond)?

LEE SCHNEIDER: For the U.S., no developments from a rulemaking perspective in 2022. Perhaps some enforcement actions against low-

hanging fruit (clear situations where a single authority has control and profits, which isn't really DeFi).

JASON GOTTLIEB: I agree that **we're unlikely to see significant rulemaking from the SEC, but the Commodity Futures Trading Commission ("CFTC") may consider some new guidance on certain issues** (the 28-day rule, DAO control). I agree that we're likely to see more enforcement actions and, like Lee, I think most of those will be against either low-hanging fruit, or settlements with companies/developers who are happy to pay a relatively modest settlement and walk away if they are allowed to continue their business. The regulators are going to have great difficulty figuring out how to enforce settlements (or even court orders) against truly decentralized platforms.

CHRISTINE PARKER: Agreed. **The bipartisan, bicameral letter from the leaders of the Agriculture Committee to the newly confirmed Chair of the CFTC, which focused on digital assets, suggests there will be a renewed focus on the CFTC's role in regulating digital assets.** The letter focused on a number of topics, including DeFi, indicating that this will be an area of focus for the CFTC in 2022. We should expect to see some proposed guidance or advanced notice of proposed rulemaking addressing certain DeFi principals.

Are U.S. securities laws suited to address the risks that DeFi platforms create for users or is a new/different regulatory regime an inevitability?

OLTA ANDONI: T**he current regulatory bodies are not ready to address and regulate DeFi.** But at the same time, the creators of DeFi protocols should address real regulatory risks. We cannot regulate technology, but we can minimize our appetite for risk. There are big regulatory issues with DeFi protocols. At the end of the day, DeFi protocols function in a centralized system which will not let go of transparency requirements for its players.

LEE SCHNEIDER: This question presumes that securities laws are the only relevant ones. T**he focus on securities laws is too narrow because all different asset types trade on DeFi platforms,** and since the nature of the asset typically determines the applicable regulation (in the U.S.), focus on securities laws is too narrow.

Given the mix of asset types trading in DeFi and the fact that that mix will only become wider and more diverse, **the focus should be on market integrity principles,** both for DeFi and CeFi. Such principles will be easier to dictate for CeFi and pretend DeFi (i.e., DeFi in name only) but **true defi (no single authority) will involve lots of experimentation in market integrity,** which is overall beneficial. And yield farming (liquidity mining under the above definition) will add to the market integrity discussion and experimentation because it stitches together many platforms.

JASON GOTTLIEB: No, the securities laws are woefully inadequate to address crypto. To begin with, there are vast pockets of crypto that do not implicate securities law at all. The CFTC is relatively much smaller than the SEC, and has jurisdiction only in matters involving futures, derivatives, etc. (except for fraud in spot trading of commodities that have futures or derivatives). So the CFTC's jurisdiction is limited as well. Financial Crimes Enforcement Network ("FinCEN"), the Department of Justice ("DOJ"), states, even consumer protection agencies - they all might have jurisdiction, in certain circumstances, but their laws/regulations tend not to be designed for crypto either (except FinCEN, which

has issued more specific guidance than most of the other agencies). And even within the securities laws, there are a host of "square peg, round hole" problems that the current laws and regulations do not address.

CHRISTINE PARKER: This question seems oddly narrow in scope. It should be whether U.S. financial statutes and regulations are currently suited to address the risks posed by DeFi platforms and even if they are suited, does it make sense to update the regulatory regime to accommodate these new types of financial markets/ products?

DAVID ADLERSTEIN: Today at least, your elderly relatives probably aren't using metamask to buy wrapped ETH through a decentralized exchange in order to liquidity mine and yield farm. The technical UX (user experience) hurdles could help explain why regulators haven't acted here with as much alacrity as in the case of some retail-oriented initial coin offerings (ICOs). But returning to first principles, U.S. securities laws and other investment-related laws are predicated on the idea of individual freedom to participate in markets, but with the ability to obtain information about the merits and risks of an investment in order to make an informed investment decision. That policy imperative applies here too, and as Jason alludes, **the key macro challenge is to protect investors without fitting disclosure and other regulatory requirements into a paradigm geared towards traditional equity and debt investments offered by unitary, centralized issuers. There is work to do here.**

Are there jurisdictions that strike the right (regulatory) balance and could serve as a model for the U.S.?

OLTA ANDONI: No, I do not think there are jurisdictions that strike a perfect regulatory balance, especially for DeFi protocols.

COLLINS BELTON: No, but there are elements of other jurisdictions that the U.S. could adopt to dramatically improve our balance. For instance, **a limited sandbox program with responsive participants such as Singapore's could be helpful.** But, more importantly, fostering deeper engagement like what we've seen with FINMA (Swiss Financial Market Supervisory Authority) or MAS (Monetary Authority of Singapore) at various levels could drastically cut down on misunderstandings of technology and help them narrow their focus, as the current scattershot approach is not only ineffectual, but it is failing to capture real risks while largely preventing only good faith actors from moving forward.

Do DAO governance tokens in and of themselves fall outside of SEC regulations where token holders are required to participate? Is more needed?

COLLINS BELTON: More is needed, and the circumstances of the tokens' distribution and tokenomics is also material. For instance, **to the extent a DAO is dominated by one party or a group of affiliated parties, the perfunctory participation of many other members is unlikely to abate regulators' concerns that the risks of conflicts of interest or information asymmetries in favor of the majority will dominate.** Similarly, if the participation of the minority holders is relegated to immaterial decisions, with the decision-making authority for decisions that materially impact future profit expectations being relegated to a subgroup, the general participation of the group might not suffice to make such an arrangement fail to appear similar to a traditional GP-LP relationship, which would have securities law implications. So, as a general matter, mere participation by

a broad number of people alone won't suffice to determine the applicability of securities laws in most cases.

LEWIS COHEN: As I have noted elsewhere, **I agree that large groups of people can act in a coordinated way without being security holders.** The presence (or absence) of the Williamson v. Tucker factors is critical in determining whether "securities" have been created.

JASON GOTTLIEB: The classic lawyer's answer: it depends. First, I'm not sure there are protocols where holders are required to participate. But I'm not sure participation is the key difference-maker. After all, most retail holders of Apple stock don't vote their stock either, but there's no doubt Apple common stock is a security. We go back to Howey: did people invest money in a common enterprise with the expectation of profits from the efforts of others? If all you can do with your governance token is vote, and if the "others" that would take action are just everyone else in the DAO, it's hard to see how governance tokens fit the Howey test. (Nor do I think they fit the Reves test, but that's a separate issue.) So, I don't think DAO governance tokens would automatically fall outside SEC regulations, but in my view, the governance tokens of the major decentralized protocols very clearly are not securities, and are outside the securities law.

ARTICLE II

SPOTTING AND MANAGING LITIGATION RISK IN DEFI

ROBERT SCHWINGER
PARTNER
NORTON ROSE FULBRIGHT

HARRIET JONES-FENLEIGH
PARTNER
NORTON ROSE FULBRIGHT

JONATHAN HAWKINS
DISPUTES ASSOCIATE
NORTON ROSE FULBRIGHT

By the end of 2021, USD 88 billion of crypto assets alone were held in DeFi protocols. This figure is startling given the real uncertainty regarding the legal rights and obligations of those using DeFi and smart contract protocols and the ability to enforce them when disputes arise. The resolution by courts and tribunals of disputes in the context of DeFi and smart contract protocols is still largely uncharted territory. In this article, we look at some of the issues that may give rise to disputes in the DeFi context and the importance for developers and users of DeFi protocols of incorporating mechanisms for the orderly resolution of any disputes that do arise.

THE CAUSES OF UNCERTAINTY

DeFi protocols and applications are designed to provide certainty, and in many respects the decentralised and autonomous nature of DeFi products can offer significantly more robust systems. They create indelible records and remove certain single points of failure that can exist in classical centralised financial transactions.

However, the very characteristics that allow DeFi protocols to solve certain problems – decentralised networks, automaticity, and pseudonymous participation – also create significant legal uncertainty.

WHAT UNCERTAINTIES DO THESE CHARACTERISTICS CREATE?

The major disputes risks arising from DeFi and related technologies stem from the following issues:

1. What is the nature of the legal relationship between participants in DeFi transactions?
2. Will agreements entered into via DeFi protocols satisfy the necessary formalities to be considered binding legal contracts?
3. When disputes arise as to the terms of an agreement entered into via DeFi protocols, how will a court interpret the agreement?
4. What remedies will be available to the

parties to enforce their legal rights?
5. How will the successful party/ies enforce a court's decision

RELATIONSHIP BETWEEN PARTICIPANTS

Most of the time courts and arbitral tribunals resolve commercial disputes arising out of relationships that have been around for hundreds of years, such as purchaser and seller, lender and borrower, or landlord and tenant. The law has had a long time to adapt to the nature and nuances of those relationships. However, DeFi and related technologies are still relatively novel. Our legal systems have had very limited time to get to grips with them and often there is no legal consensus yet as to who owes what duties to whom, and in what situations.

Partnerships

One legal risk that may arise, particularly in the context of sophisticated DeFi protocols, is whether all of the participants involved might be found to have formed a partnership. Under New York law, this might be an actual or de facto partnership, while under English law it might be a general partnership. In either case participants might be held to have unlimited liability for the acts of other participants. The law has not begun to grapple with the application of partnership law to DeFi transactions, and it is conceivable that various classes of users, such as investors, tokenholders, promoters, miners and node operators, may be found to either comprise a single partnership, or for each class to form separate partnerships.

Do these relationships create legal duties?

We have highlighted the specific relationship risk that the participants are found to be in partnership because of the potential for unlimited liability, but there are many more potential areas of uncertainty arising from the relationships between the participants themselves. Will they be deemed to owe duties to one another that could give rise to tort claims if those duties were deemed to be breached? There is a web of potential tort-like duties between such participants as the platform, the developers, the cloud service providers, individual users, and perhaps an outside oracle. While the law provides certain tests and guidance regarding when and where it is appropriate to infer such tort-like duties among participants in a situation where their relationship is not governed by a contract, there is still considerable scope for argument as to the application of those tests, especially in the novel landscape of DeFi protocols.

User agreements

User agreements, which define contractual relationships upon entry into the relevant DeFi system, help significantly to minimise the risk that a court imposes a relationship that the participants did not foresee.

However, they do not prevent claims from those who are not themselves parties to the user agreements. In the US, third parties have based claims on grounds as varied as negligence, fraud, conversion, trespass to chattels, unfair trade practices, and racketeering. As legal systems grapple with DeFi, we expect to see creative claims being issued, as parties test the limits of the law and platforms' user agreements.

FORMALITIES

Each jurisdiction has its own formalities for entering into a contract. However, agreements struck across DeFi platforms have certain fundamental differences when compared to classical contracts. These differences will only become starker with the rise of smart legal contracts. It is not yet clear how the law will apply these formalities in the context of DeFi protocols or whether they will recognise all such agreements as being akin to classical contracts.

Execution formalities

The requirements for the formal recognition of a contract in each jurisdiction are idiosyncratic. While the requirements of some jurisdictions raise obvious issues – such as the requirement for 'wet ink' signatures by certain Middle Eastern jurisdictions – even more flexible jurisdictions such as New York and England have their own areas of uncertainty.

For example, the UK Law Commission has recently concluded its investigation into how the current law of contract is able to apply to smart legal contracts, and flagged the requirement that certain contracts, such as guarantees, must be made in writing. Whether a smart legal contract, written only in code (i.e., no natural language such as English) can satisfy this requirement is uncertain.

Legal capacity

A contract entered with a party who lacks the capacity to contract is unenforceable. In order to determine the capacity of a party, it is necessary to know the identity of the party. For example, a mortgage lender may require a passport, to allow it to determine that a borrower has reached 18 years old (or whatever the age of capacity their jurisdiction requires). Under New York and English law, a contract with a minor is voidable at the minor's discretion. However, DeFi protocols are often pseudonymous, meaning that participants do not automatically know their counterparties' real-world identities and consequently whether or not they have capacity to contract.

Multiple participants

Further uncertainties as to legal relationships arise when there are multiple participants involved in a transaction on a DeFi platform. Are there two transactional parties in a single contract with each other? Or is each of them in an independent contract with the platform, which is essentially operating as a middleman? Or is there one three-party relationship, for example if the platform is taking a commission of some kind on a sale transaction between the other two?

INTERPRETATION

The DeFi market is still in its nascent stages, and participants do not typically use the long formal contractual documents like those that govern many traditional finance transactions. When people talk informally about their affairs, they often speak in broad generalizations and overstatements and sometimes use imperfect metaphors or analogies. This can lead to unwelcome surprises when they are found to owe legal obligations that do not reflect their understanding of arrangements. The interpretation of smart legal contracts is particularly complex, and there are different schools of thought as to how disputes over interpretation should be resolved.

Code is law

One school of thought argues that "code is law", i.e. the contract is whatever the system is programmed

to do, so that if the outcome of the programming does not reflect what participants expected, they have to live with it. "Code is law" may sound appealing to some technologists or others who want to be able to operate without the risk of interference from the courts. However, businesspeople want predictable and commercially reasonable results when they enter into commercial transactions. The majority will not be willing to execute and perform commercial transactions involving the transfer of millions of dollars' worth of value via DeFi protocols if that in practice necessitates a side bet on whether the programmer got everything right.

Interpreting code

Assuming that the market or our legal systems are unwilling to adopt code as law, then our courts will soon be faced with the challenge of interpreting the parties' intentions. Not only may these parties never have met, but they may never have engaged even in a single natural language communication. Just as transactional lawyers today may exchange mark-ups of contracts with little or no commentary as to the changes, or two businesses may engage in a battle of the forms, code-only contracts and amendments may be exchanged between participants in a DeFi platform. Just how the court will interpret the intentions of each party as against the effect of their code is uncertain. One approach that has been suggested is for the court to adopt the interpretation that a 'reasonable coder' would give to the relevant code, but this comes with its own complications and uncertainties.

Market standards

As the DeFi market develops we expect that industry-standard terms and supporting commentary will emerge just as parties in the derivatives and loan markets have adopted ISDA, LSTA and LMA standard documentation. Those standard terms are likely to be built on early smart legal contracts which have been subjected to the crucible of litigation and judicial consideration.

REMEDIES

Courts historically have been willing to intervene where enforcement of a contract would produce commercially unreasonable or outrageous results, such as where there has been a fraud, a commercial misunderstanding, or a misrepresentation. It seems reasonable to expect that courts may look to intervene in smart legal contracts in similar circumstances. What is uncertain is how courts will use their traditional remedies in a DeFi context.

Immutability of the distributed ledger

A fundamental characteristic of a distributed ledger is that transactions cannot be erased. If a court determines that a smart legal contract does not represent what the parties agreed and should be rectified, or that it is void for frustration or illegality, the record of that initial transaction is going to remain on the ledger. A likely solution is an offsetting transaction (often referred to as an 'equal and opposition transaction') cancelling out the initial transaction. However, it remains uncertain how aspects of this process will work in the real world. What happens if only part of the transaction is voided or rectified? What happens if assets involved in the transaction have already been transferred to an innocent third party? How will a party subsequently prove ownership for the period in between the two transactions? The latter may be especially complicated in the context of

tax liabilities.

ENFORCEMENT

Even if the uncertainties highlighted above regarding parties' rights and obligations are resolved, they are not worth much unless there is a practical mechanism by which to enforce a judgment or award. A recent bug in Compound's code (a money market run on Ethereum) involved a single character error that led to the mistaken disbursement of an estimated USD 80 million of funds to incorrect parties. The self-executing nature of the protocol meant that there was no one person in charge, and therefore no administrator controls to disable at mistaken distribution.

Parties should foresee that they may need to amend their transactions. Even 'fire and forget' contracts or decentralised autonomous organisations (DAOs) will need a method by which to receive instructions from the outside world. DeFi transactions that do not provide a mechanism for resolving disputes generate a significant amount of uncertainty that is likely to slow the adoption of such technology by sophisticated parties.

Jurisdiction and governing law

Identifying which court has jurisdiction to decide a dispute arising out of a DeFi transaction and what law should be applied to do so are fundamental issues for smart legal contracts. Traditional tests used to answer these questions, such as the physical location where the contract was entered into, will often be unworkable in the context of a decentralised system. It will take time for a body of case law to evolve, and different jurisdictions may take opposing views, creating unforeseen complications. It is therefore especially important that parties specify the governing law and jurisdiction in their smart legal contracts.

How will the counterparty know there's a dispute?

Even if a court in New York or London, or an arbitral tribunal, is willing to hear a dispute, how will a claimant make a potential defendant aware of the proceedings? The pseudonymous nature of certain protocols further complicates the process of identifying the defendant.

Dispute resolution mechanisms

We expect that the DeFi market will coalesce around standard dispute resolution clauses and mechanisms as it matures. Until then, parties entering into DeFi transactions should ensure that their arrangements include a dispute resolution mechanism making clear who is to resolve any dispute, under what law, and how the dispute will be run and the decision implemented.

KEY TAKEAWAYS

As the DeFi market grows and increasingly complicated and high-value transactions are entered into and performed via DeFi protocols, it is inevitable that disputes will sometimes arise, especially given the uncertainties caused by unsettled issues of law in this area. Parties entering into DeFi transactions should approach smart legal contracts with the same critical eye as they would a classical contract and take legal advice to ensure that their transactions are documented in a way that clearly defines the legal relationships between the parties and provides a mechanism for resolving disputes and implementing the decision.

ARTICLE III

IF NFTS RULED THE WORLD: A NEW WAVE OF OWNERSHIP

SAMIR PATEL
ASSOCIATE
HOLLAND & KNIGHT LLP

In 1997, avant-garde artist David Bowie, with incredible accuracy, prophesized how the internet will disrupt music distribution systems, erode copyright laws and revolutionize fandom consumption. He hedged his bets by selling Bowie Bonds that securitized the royalty rights to his songs for $55 million. It was the first ever securitization of music recordings, publishing rights and privately held intellectual property rights.[1]

Fast forward 25 years later, legendary hip-hop artist Nas sold a non-fungible token ("NFT") entitling the holder of the NFT to a percentage of a song's streaming royalties. In a matter of minutes, Nas sold 1,870 NFTs grossing over $560,000 in revenue. Unlike the Bowie Bond, no publishing nor intellectual property rights were transferred with Nas' NFT. Consistent with blockchains' disruptive and rebellious hubris, the NFT was sold not as an investment contract, but as a collectible or music memorabilia, whereas the Bowie Bond was sold pursuant to US securities laws. Just as how the internet and securitization provided a new revenue model for artists, blockchain technology and NFTs may have forged a new way for artists to disrupt the music industry.

WHAT IS AN NFT?

An NFT is a unique digital asset that utilizes blockchain technology to record ownership of an asset and evidence authenticity. Fungible tokens can be substituted without losing value and have properties that make them exactly the same in type. Unlike fungible tokens such as Bitcoin or Ether, NFTs cannot be traded for another identical token. An NFT is not a content file—it does not contain digital art or a video clip, only a uniform record locator to the content, which itself has intrinsic value. Rather, the NFT is a unique cryptographic key contained within a digital token that verifies the corresponding content file as genuine and establishes a record of ownership as it is transferred on a blockchain, which allows it to be transferred without risk of fraud. While others may have copies of the same content, only one person can own the specific token authenticating ownership of the content.

Collectors of many items (antiques, baseball cards, art) purchase NFTs as a way to support their favorite artists, actors, musicians, and athletes. Certainly, there are others that purchase NFTs as speculative assets hoping they will increase in value and be a good investment.

1 Bowie Ch-Ch-Changes the Market, CFO: the Magazine for Senior Financial Executives, Apr. 1, 1997, 1997 WL 8300101.

The legal and regulatory analysis of an NFT will be heavily influenced by how it is intended to be used and how it is marketed.

MUSIC NFTS

The single-edition NFT is the most commonly used form of NFT in the music industry. One NFT is associated with one song. Much like its digital image kin, music NFTs do not convey economic nor intellectual property rights to the NFT holder, unless specified. Under U.S. copyright law, the artist, by default, owns the copyright to their work. All the NFT does is simply point to a file's, video's or image's web location. Catalog is the primary market-place for single edition music NFTs. Artists using Catalog earn seven times more from NFT sales than one year's worth of streams on Spotify.[2] One artist made $226,800 using Catalog compared to $178 on Spotify.[3] On the Catalog FAQ page, under "What do I receive when I buy a record?" it reads "[b]esides being a priceless piece of art, buying a record on Catalog is the biggest cosign another artist can give, the most immediate patronage a fan can offer, and a key to anything the creator (or anyone else) might provide for its holder. No rights are included with Catalog records unless otherwise specified."[4]

In contrast, Opulous is a marketplace that sells music NFTs that are securities and sold pursuant to Regulation Crowdfunding ("Reg CF") of the Securities Act of 1933 ("Securities Act"). Unlike NFTs on Catalog, Opulous sold NFTs entitling holders to receive royalties every time the song is streamed across streaming platforms or played on the radio, TV, movie, or video game ("Mona Lisa NFTs"). Opulous partnered with investment platform Republic, a Securities Exchange Commission ("SEC") registered crowdfunding portal, to sell these securities to main street investors. A Delaware LLC was created and given 50% of the master and publishing rights to the song.[5] The LLC then conducted a Reg CF offering, which provides an exemption from the registration requirements for securities-based crowdfunding, allowing companies to offer and sell up to $5 million of their securities without having to register the offering with the SEC.

BOWIE BONDS

Applying the basic securitization structure to Bowie Bonds, David Bowie's assets are a twenty-five-album catalogue—roughly 300 songs—of Bowie's recordings and song copyrights. The two main sources of revenue were recording royalties and publishing revenues. Since David Bowie actually owns his own record masters, all record royalties go to him. As for publishing revenues, there are mechanical royalties, synchronic usage (e.g. films, commercials), sheet music, air play, Muzak, voice mail, live performances and tours by Bowie. EMI Music entered into a 15-year licensing deal for Bowie's songs. The licensing deal was the collateral put up for the investor, Prudential Insurance.

NAS NFT

Royal.io, is a platform that allows music fans to purchase the right to earn royalties from their favorite songs. In November 2021, Royal announced

2 https://twitter.com/Cooopahtroopa/status/1489327698430234625

3 Id

4 https://www.notion.so/Catalog-FAQ-98ee85092bad441daa1ee9426daa4be8

5 Mona Lisa LLC – cite to EDGAR https://musically.com/2021/11/05/lil-pump-soulja-boy-music-nft-populous/

Tier	Royalty Amount	Purchase Price
Diamond	1.5789%	$9,999
Platinum	0.0658%	$499
Gold	0.0113%	$99

a $55M Series A round that included Nas as an investor. In January of 2022, using NFTs, Nas sold 50% of his royalty rights to Rare ("Rares") — a single song from his 2022 Grammy Award-nominated album, King's Disease II. The royalty rights were limited to only streaming royalties derived from digital service providers, as such term is commonly used in the music industry (ex. Spotify, Apple, Music, Youtube Music). The royalties are divided into three tiers with each tier having a different royalty amount and purchase price.

Unlike NFTs on Opulous, Rares convey no publishing rights nor royalties when the song is played on the radio, TV, movie, or video game.

UNDERSTANDING MUSIC ROYALTIES

A master recording is the official original recording of a song, sound or performance. Also referred to as "masters", it is the source from which all the later copies are made. As an artist, owning the master recording gives them the legal rights to freely appropriate and maximize their money-making opportunities. If the master recording belongs to a record label, then they have the right to license out the recording (and collect the royalties).

Mechanical royalties compensate the masters owner for the reproduction of the composition, paid by third-parties that want to record, manufacture, and distribute the musical work. With digital service providers, mechanicals are primarily generated whenever the user chooses to play a specific song on a streaming service, thus reproducing (or rebroadcasting) the composition. Public performance royalties compensate masters owners when the song is performed or displayed publicly. Every time a composition is publicly performed, the rights owners get paid — whether it's a radio broadcast, performed live at a concert or a digital stream. Synchronization license fees are generated when a derivative work based on the composition is created. In essence, every time someone wants to use the composition as a part of any other type of content, whether it's a TV show, a movie, an ad or a radio show, masters owners are financially compensated. That process is generally known as sync licensing and is more a bespoke contractual arrangement than the first two royalty streams.

MUSIC NFTS ARE SECURITIES?

The Howey Test is the standard to determine whether a financial instrument is an investment contract, and is therefore subject to SEC regulation. This is a three-part test in which the Supreme Court determined that an investment contract exists when there is (1) an investment of money; (2) in a common enterprise; (3) with a reasonable expectation of profit derived from the entrepreneurial or managerial efforts of others. If an asset does not meet all three prongs, it is not an investment contract, and not a security. Importantly, the SEC has stated that neither bitcoin nor ether are securities under the Howey test, but also specified that whether a digital asset is an investment

contract at a particular time is unique to both the asset and the facts and circumstances at the it is being sold or resold. If the Howey Test is satisfied, then the issuance of the asset must be registered with the SEC, or be eligible for an SEC exemption.

When rights to master recordings and publishing are securitized and sold as investments, the offering needs to abide by the relevant securities laws.

In a now famous interview in 2002, Bowie, again with incredible accuracy, predicted that the amount of income generated by an artist will radically shift from mechanical to performance royalties. Bowie said "I don't even know why I would want to be on a label in a few years, because I don't think it's going to work by labels and by distribution systems in the same way . . . You'd better be prepared for doing a lot of touring because that's really the only unique situation that's going to be left."[6] The basket of revenue rights conveyed through Bowie Bonds not only included mechanical royalties, but any revenue generated from the master recording, solely owned by Bowie himself and not a record label. The income from the royalty stream from the copyrights, licenses, and sales of Bowie's music was also predictable enough to warrant securitization. Accordingly, Bowie Bonds were sold pursuant to the Securities Act via a private offering to a single qualified institution investor, Prudential Insurance.[7]

Similarly, Mona Lisa NFTs on Opulous were also sold pursuant to the Securities Act. Like Bowie Bonds, Mona Lisa NFTs include revenue rights generated by the master recording. The NFT entitles holders to 50% of the revenue generated from the master recording and publishing royalties. Specifically, NFT holders not only receive revenue from the songs streams on digital service providers, but from downloads, TV broadcasts, radio broadcasts, use in video games and films, and public performances.

As such, NFT holders may very well see the NFTs as investments, and are expecting to make a profit off the artist's efforts in promoting and performing the song.

This certainly is consistent with Bowie's prediction that touring and live performances will become the artist's most significant means of generating revenue. The more the artist performs the song, the more money will be made by investors. Opulous chose to use Reg CF to sell these securities. Unlike the exempted securities offered via the Bowie Bond, Reg CF allows main street investors to buy the securities without a minimum investment

6 https://www.nytimes.com/2002/06/09/arts/david-bowie-21st-century-entrepreneur.html?pagewanted=all

7 The Bowie bonds qualified for the section 4(2) exemption of a private offering. Thus both Regulation D and Rule 144A apply. The Qualified Institutional Buyer ("QIB") in this transaction is Prudential Insurance. A QIB is a large institutional investor that owns at least $100 million worth of securities, not counting securities issued by its affiliates. For registered broker-dealers, the threshold is lower, just $10 million. A bank must also have a net worth of at least $25 million in order to be considered a QIB.

Digital Service Provider	Royalty Rate Per Steam to Artist[9]	Royalty Rate Per Stream to NFT Holder	Number of streams to break even
Apple Music	$0.008	Diamond – 0.00012631 Platinum – 0.000005264 Gold – 0.0000009	Diamond – 79,162,378 Platinum – 94,794,832 Gold – 110,000,000
Spotify	$0.00318	Diamond – 0.00005021 Platinum – 0.00000209 Gold – 0.00000036	Diamond – 199,132,597 Platinum – 238,755,981 Gold – 275,000,000
YouTube Music	$0.002	Diamond – 0.00003158 Platinum – 0.00000132 Gold – 0.00000023	Diamond – 316,624,446 Platinum – 378,030,303 Gold – 430,434,783

threshold.[8]

Conversely, Rares only entitles holders to the royalties from digital service providers. The Assignment of Streaming Royalties Agreement for Rares states "this Agreement does not convey any rights in the underlying musical composition embodied in the Recording, (the so called "Publishing Rights") or any other rights, interests, revenues or royalties earned form the commercial exploitation of the Recording (specifically including, but not limited to, mechanical royalties or monies earned from synchronizations, as such terms are commonly used in the music industry) other than the Streaming Royalty Share of the Streaming Royalties[.]" The song was released four months prior to the sale of Rares, so purchasers were not entitled to back-dated royalties retrospectively. Furthermore, Rares come with other benefits such as exclusive community access, merchandise and concert tickets.

Above is a chart that illustrates how much a Rare holder gets per stream and how many times the song would need to be played to break even

As of this writing, Rare was played on Spotify 11,800,000 times. The possibility that a Rare purchaser would make their money back is very small and the probability of making any kind of significant return on their "investment" is even smaller. Because 100% of the master recordings rights are still held with Nas, there is no potential to make money off the song's other uses for example, public performances or synchronization licenses.

A sound argument for Rare not being a security is that the royalty is a novelty, and the scarcity of the NFT makes it a valuable collectible, especially to die-hard fans.

Conversely, the Mona Lisa NFT included 50% of the master recording, so the potential to make a profit

8 Regulation D private placements are securities offerings that are exempt from the normal SEC registration process and in many cases are sold only to "accredited investors" or limit the involvement of investors who are not accredited. Accredited investors are investors whose financial status or investment knowledge may give them a greater ability to handle the risks inherent in a private placement.

9 https://producerhive.com/music-marketing-tips/streaming-royalties-breakdown/

significantly increases because the holder receives 50% of all revenue generated by the song. Additionally, Opulous partnered with a regulated crowdfunding platform and sold the Mona Lisa NFTs pursuant to the Securities Act indicating a strong conviction that their NFTs are securities and holders may expect a profit. At the time of the Bowie Bond, Bowie consistently sold one million compact disks, cassettes, albums, and singles per year around the world.[10] Bowie Bonds were sold pursuant to an exempted securities offering because the qualified institutional buyer was expecting a significant return on their $55 million investment.

CONCLUSION

Determining whether music NFTs are considered securities requires a judgment based on the totality of the facts and circumstances. There are certainly correlations between the bundle of rights given to NFT holders and whether or not the NFTs are sold pursuant to securities laws. Clearly outlined mechanical royalty rights can be constricted to the point where the NFT holders cannot expect to make a profit, but the inclusion of master recording rights open up the possibility for the song to generate much more revenue through the its different uses. If Young Americans buy NFTs of their favorite musical Heroes, Changes in popularity can make holders have Moonage Daydreams as revenue increases from Station to Station. But depending on your State of Mind, the NFT can Represent a stroll down Memory Lane and It Ain't Hard to Tell that it's not about the money, but The Message.

10 Jay Mathews, Securities Oddity: The Bowie Bond, Washington Post, Feb. 6, 1997, at C1.

ARTICLE IV

BLOCKCHAIN VULNERABILITIES AND CIVIL REMEDIES TO RECOVER STOLEN ASSETS

BARRY SOOKMAN[1]
SENIOR COUNSEL
MCCARTHY TÉTRAULT LLP

It is often assumed that blockchain based digital currencies and applications are safe and secure. In fact, blockchain ecosystems including cryptocurrencies such as bitcoin and Ether, smart contracts that power a plethora of transactions, and blockchain exchanges have many vulnerabilities. Like many other financial systems, blockchain based systems are subject to all manner of hacks, frauds, scams, errors, and vulnerabilities. They often happen at the speed and anonymity of the Internet. There are, understandably, numerous legal challenges when it comes to obtaining civil remedies for these Internet based crimes. This is as true, and perhaps even more so, for blockchain hacks, scams, and frauds as it is for a whole host of other Internet crimes and wrongs.

This article provides a brief overview of blockchain vulnerabilities, hacks, frauds and scams and then provides an overview of civil remedies, and in particular interim and interlocutory remedies, that may be available to trace, freeze or recover stolen assets.

BLOCKCHAIN VULNERABILITIES, HACKS, FRAUDS, AND SCAMS

There are trillions of dollars invested in blockchain based digital currencies. Bloomberg recently estimated that the cryptocurrency market is now worth more than U.S. $3 trillion.[2] There are well recognized financial risks associated with cryptocurrencies volatility. But, this does not seem to have dampened the market for these items.

The technical vulnerabilities associated with blockchain are not as widely recognized. Blockchain is often touted as being secure, immutable and "unhackable".

1 Barry Sookman is a technology, intellectual property, and privacy lawyer with the Canadian law firm McCarthy Tetrault in the Toronto office. This article is adapted from Barry Sookman's blog post Blockchain vulnerabilities – crypto hacks, blockchain forensics and legal challenges, online: Blockchain vulnerabilities – crypto hacks, blockchain forensics and legal challenges

2 Crypto World Hits $3 Trillion Market Cap as Ether, Bitcoin Gain, November 8, 2021 online: Bitcoin ($BTC USD), Ether ($ETH) Lead Crypto to $3 Trillion Market Cap - Bloomberg

There are, however, many vulnerabilities associated with cryptocurrencies and their ecosystems, some human and some technical.

This should not be surprising. We can learn a lot from history. As Jesse James showed in the wild west, Charles Ponzi showed us in 1920, and as hackers show us day in and day out, no matter how secure a financial institution, financial application, or financial asset is, someone will try to find a way to steal it, defraud or trick people out of it, or hack it. Sadly, the same is true with digital currencies.

While losses from hacks and vulnerabilities are hard to estimate, by one account hackers have stolen nearly $2 billion worth of cryptocurrencies in the two-year period between 2017-2019.[3] Some hacks are by lone hackers, but many are by sophisticated cybercrime organizations. According to a recent article In the MIT Security review, the hype that these assets are unhackable is "dead wrong":

... while blockchain technology has been long touted for its security, under certain conditions it can be quite vulnerable. Sometimes shoddy execution can be blamed, or unintentional software bugs. Other times it's more of a gray area—the complicated result of interactions between the code, the economics of the blockchain, and human greed. That's been known in theory since the technology's beginning. Now that so many blockchains are out in the world, we are learning what it actually means—often the hard way.[4]

A comprehensive article on the subject confirmed the many vulnerabilities associated with blockchain technology:

Blockchains are relatively new and there are countless news stories of people losing money through compromises in the components of blockchain ecosystems. Blockchain technologies are not invulnerable and have actually many known vulnerabilities, just as with any software....[5]

Another recent article came to the same conclusion:

Until recently, blockchains were seen as an "unhackable" technology powering and securing cryptocurrencies — but that's no longer the case...

In other words, forget what you heard from Bitcoin boosters — just because information or currency is on a blockchain doesn't necessarily mean that it's more secure than any other form of storage...

In fact, the same qualities that make blockchain technology so secure may also be the source of several unique vulnerabilities — a stark reminder that despite the hype, cryptocurrencies can't entirely sidestep the vulnerabilities of any other banking systems.[6]

One group of researchers recently concluded, as "distributed ledger software by nature, blockchain

3 Mike Orcutt, "Once hailed as unhackable, blockchains are now getting hacked" (19 February 2019), online: MIT Technology Review <https://www.technologyreview.com/2019/02/19/239592/once-hailed-as-unhackable-blockchains-are-now-getting-hacked/> ("Orcutt"),

4 Orcutt,

5 Nils Amiet, "Blockchain Vulnerabilities in Practice" (26 March 2021) 2:2 Digital Threats Research and Practice, online: <https://doi.org/10.1145/3407230> ("Amiet")

6 Victor Tangermann, "Blockchains Were Supposed to Be "Unhackable." Now They're Getting Hacked" (17 May 2021), online: Futurism <https://www.futurism.com/blockchains-unhackable-getting-hacked> ("Tangermann")

inevitably has software issues." They found, among other things, by studying the bitcoin, Ethereum, Monero, and Stellar blockchains that some blockchain modules related to consensus, wallet, and networking were "highly susceptible to vulnerabilities".[7]

As with every other financial system, there are opportunities for fraud. One vector is fraud associated with online marketplaces. An Ontario example involved the downfall of crypto asset trading platform QuadrigaCX (Quadriga). It resulted from fraud committed by Quadriga's co-founder and CEO Gerald Cotten. Clients entrusted their assets to Quadriga, which provided false assurances that those assets would be safeguarded. In reality, Cotten spent, traded and used those assets at will. Operating without any proper system of oversight or internal controls, Cotten was able to misuse client assets for years, unchecked and undetected, ultimately bringing down the entire platform and losses to customers of $169 million. Approximately $115 million of the losses arose from Cotten's fraudulent trading on the Quadriga platform. He opened Quadriga accounts under aliases and credited himself with fictitious currency and crypto asset balances which he traded with unsuspecting Quadriga clients. He sustained losses when the price of crypto assets changed causing a shortfall in assets to satisfy client withdrawals. He covered this shortfall with other clients' deposits, in effect, operating a Ponzi scheme. Cotten also lost an additional $28 million while trading client assets on three external crypto asset trading platforms without authorization from, or disclosure to, clients. He also misappropriated millions in client assets to fund his lifestyle.[8]

There are other types of fraud cases as well. For example, in the U.K. case, *Ion Sciences vs Persons Unknown and Others,*[9] Ion and its Director were induced by persons unknown to transfer bitcoin in the belief that they were investing in a legitimate initial coin offering (ICO), but later discovered that the recipient was a scammer.

There is a plethora of other examples. Private key security attacks are another known means by which malicious actors steal cryptocurrencies.[10] A recent hack involved the cryptocurrency exchange Cryptopia described in the New Zealand case, *Ruscoe v Cryptopia Limited* (in liquidation).[11] The hack occurred in January 2019 leading to an estimated NZD 30 million worth of cryptocurrency stolen from the exchange by the unauthorized use of private keys for the currencies in question. Another example is described in the U.K. case, *Fetch.AI Lrd & Anor v Persons Unknown Category A*

7 V Xiao Yi, et al, "Diving Into Blockchain's Weaknesses: An Empirical Study of Blockchain System Vulnerabilities" (23 October 2021) [unpublished, archived at Cornell University arXiv.org, online: <https://arxiv.org/abs/2110.12162>]

8 Ontario Securities Commission, "QuadrigaCX: A Review by Staff of the Ontario Securities Commission" (14 April 2020), online: <https://www.osc.ca/quadrigacxreport/>

9 (unreported) 21 December 2020 (Eng. Commercial Court) ("Ion Sciences")

10 Saurabh Singh, A.S.M. Sanwar Hosen, and Byungun Yoon, "Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network" (26 January 2021) 9 IEEE Access 13938-13959, online:<https://doi.org/10.1109/ACCESS.2021.3051602> ("Singh et al"). A "private key security attack" is described as follows: "A private key allows individuals to access funds and verify transactions; it is only created once and cannot be recovered if lost. Malicious actors perform a variety of actions to steal cryptocurrency by targeting key custodial services because cryptographic keys are particularly attractive targets. An attacker who has discovered vulnerability in an elliptic curve digital signature algorithm can recover a user's private key, and if a private key is stolen, it is difficult to track any related criminal activity and recover the relevant blockchain information."

11 [2020] NZHC 728 (8 April 2020), online: http://www.nzlii.org/nz/cases/NZHC/2020/728.html.

& Ors.[12] This case involved fraudulent trading using a person's trading account with the cryptocurrency exchange Binance. It was perpetrated by unauthorized access to the plaintiff's private key. The hackers obtained access to the accounts maintained by the plaintiff and were able to trade the crypto assets in the account by adopting massive undervalues for the products traded with the result that, in the aggregate, losses totaling in excess of US$2.6 million were sustained over a very short period. Hackers have also been known to steal the keys to cryptocurrency wallets.[13]

Marketplaces have also been subject to all manner of hacks with Mt.Gox, being a well known example.[14] In 2011 hackers used stolen credentials to transfer bitcoins from accounts. Deficiencies in network protocols also resulted in several thousand bitcoins being "lost".

Phishing attacks[15] and SIM swap attacks[16] are also not uncommon. Hackers have also been known to exploit technical weaknesses in blockchain systems, the Poly network hack [17] and the DAO, are two examples. [18] Hackers can also engage in routing attacks[19] including BGP hijacking attacks.[20] They can also exploit cryptographic flaws such as in the cryptocurrency Zcash case.[21] Another well known, but very difficult, attack vector is the 51% vulnerability attack.[22] Research shows that there are also many other security vulnerabilities

12 [2021] EWHC 2254 (Comm) (15 July 2021), online @ https://www.bailii.org/ew/cases/EWHC/Comm/2021/2254.html

13 Tangermann (supra)

14 Jake Frankenfield, "Mt. Gox" (25 March 2021), online: Investopedia <https://www.investopedia.com/terms/m/mt-gox.asp>; Cameron Keng, "Bitcoin's Mt. Gox Goes Offline, Loses $409M — Recovery Steps and Taking Your Tax Losses" (25 February 2014), online: Forbes <https://www.forbes.com/sites/cameronkeng/2014/02/25/bitcoins-mt-gox-shuts-down-loses-409200000-dollars-recovery-steps-and-taking-your-tax-losses/?sh=5e5c7b6d5c16>

15 Estevao Costa, "The Benefits and Vulnerabilities of Blockchain Security" (19 October 2021), online: CENGN <https://www.cengn.ca/information-centre/innovation/the-benefits-and-vulnerabilities-of-blockchain-security/> ("Costa")

16 BlockFi, "Incident Report" (14 May 2020), online: <https://blockfi-s3-static-prod.s3.amazonaws.com/pdf/Incident+Post+Mortem%2C+May+14%2C+2020.pdf>; These articles discuss the steps BlockFi took following the breach: Paddy Baker, "BlockFi Says Hacker SIM-Swapped Employee's Phone, No Funds Were Lost" (19 May 2020), online: CoinDesk <https://www.coindesk.com/markets/2020/05/19/blockfi-says-hacker-sim-swapped-employees-phone-no-funds-were-lost/>; Robert Anzalone, "BlockFi Hires New Chief Security Officer After Last Month's Hack" (16 June 2020), online: Forbes <https://www.forbes.com/sites/robertanzalone/2020/06/16/blockfi-hires-new-chief-security-officer-after-last-months-hack/?sh=242bc5354c57>

17 For more detail about the Poly Network hack and a technical analysis of how exactly the hack occurred and the inherent vulnerability of the cross-chain protocol, see: Mudit Gupta, "Poly Network Hack Analysis – Largest Crypto Hack"(11 August 2021), online (blog): Mudit Gupta's Blog <https://mudit.blog/poly-network-largest-crypto-hack/>; Mudit Gupta and Laura Shin, "Why did the Poly Network Attacker Return Half the Money They Stole" (13 August 2021), online (podcast): Unchained Podcast <https://unchainedpodcast.com/why-did-the-poly-network-attacker-return-half-the-money-they-stole/>; Harry Robertson, Poly Network says all $610 million stolen by a hacker has been returned after Tether released the final $33 million", (27 August 2021), online: Markets Insider, <https://markets.businessinsider.com/news/currencies/poly-network-hack-610-million-tether-mr-white-hat-defi-2021-8>; Sumejja Muratagić-Tadić, "Tether Frozen in Poly Hack Return to Owners, Fueling Centralization Debate" (26 August 2021), online: Cryptonews.com <https://cryptonews.com/news/tether-frozen-in-poly-hack-returned-to-owners-fuelling-centr-11569.htm

18 US, Securities and Exchange Commission, Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO, Release No. 81207 (25 July 2017), online: <https://www.sec.gov/litigation/investreport/34-81207.pdf>

19 Costa (supra)

20 Singh et al (supra)

21 Orcutt (supra)

22 Singh et al (supra); Orcutt (supra); Amiet (supra)

associated with smart contracts, the DOA being an example of this.[23] Other types of attacks include the "Balance Attack" and "Sybil Attacks".[24]

Future developments in technologies will also undoubtedly present new security challenges that blockchain systems will need to address. For example, quantum computing has the theoretical capability of breaking the encryption deployed in blockchains and cryptographic codes, upending basic security assumptions. It is expected that quantum computers will one day be able to break some of the blockchain's cryptographic algorithms currently being used. To stay ahead, there will be a need to transition to quantum-resistant schemes to mitigate potential security risks.[25]

CIVIL REMEDIES

Obtaining remedies and especially interim or interlocutory remedies to freeze, trace, or recover assets for Internet based wrongs are a continuing exercise of "whac-a-mole". Obtaining effective civil remedies against blockchain hackers is, without doubt, challenging. They act at the speed of the internet, anonymously, almost always reside and act from foreign jurisdictions, and are notorious for covering their tracks including by peeling their stolen crypto assets[26] to obfuscate recoveries. While it is possible to investigate and trace transfers of cryptocurrencies from public blockchains, recovering those assets or tracing those assets once converted into fiat currency can be difficult.

There are however several cases that show that if the attacked party acts quickly there are pre-trial legal remedies that can be used to freeze, trace, and even recover stolen or transferred crypto assets.

It is likely that these remedies will increasingly be used not just in blockchain hacks, but also by companies and their insurers who have made payments following ransomware attacks.[27]

An example is the U.K. case *AA v Persons Unknown & Ors, Re Bitcoin.*[28] In this case a Canadian insurance company (the "Insured") was subject to

23 Singh et al (supra); Orcutt (supra); Amiet (supra)

24 These are described in Singh et al (supra); see also: Orcutt (supra) and Amiet (supra). See also, "A Survey on the Security of Blockchain Systems", Xiaoqi Li et al, Future Generation Computer Systems, Volume 107, June 2020, Pages 841-853, online: <https://www.sciencedirect.com/science/article/abs/pii/S0167739X17318332>

25 Nicole Smith, "Quantum's Potential Impact on Blockchain Computing" (August 2020) ISSA Journal 12-16, online:<https://cdn.ymaws.com/www.members.issa.org/resource/resmgr/journalpdfs/feature0820.pdf>; Joseph J. Kearney, Carlos A. Perez-Delgado, "Vulnerability of blockchain technologies to quantum attacks" (July 2021) 10 Array 100065, online: <https://doi.org/10.1016/j.array.2021.100065>

26 Peeling is described as follows: "This characteristic pattern, where a stash of bitcoins is moved between addresses, with a small proportion sent to a destination at each step, is known as a "peeling chain". The use of peeling chains, as well as "layering" by sending the funds through numerous new addresses and different chains of transactions, can make it very time-consuming to trace proceeds of crime in crypto manually." "Elliptic Follows the $7 Billion in Bitcoin stolen from Bitfinex in 2016" May 21, 2021 online @ https://www.elliptic.co/blog/elliptic-analysis-bitcoin-bitfinex-theft

27 See, "Subrogation Actions Following Ransomware Claims: What Policyholders Should Expect in the Ever-Changing Cyber Insurance Market", Lynda Bennett et al, February 3, 2022, online: https://www.lowenstein.com/news-insights/publications/client-alerts/subrogation-actions-following-ransomware-claims-what-policyholders-should-expect-in-the-ever-changing-cyber-insurance-market-insurance

28 [2019] EWHC 3556 (Comm) (13 December 2019) online @ https://www.bailii.org/ew/cases/EWHC/Comm/2019/3556.html

a ransomware attack that encrypted and locked up its computer systems. It had cyber insurance from an English insurer (the "Insurer"). The Insurer hired an incident response company which negotiated the decryption software for a ransom of US $950,000 which was paid with 109.25 bitcoins to an address that was provided.

The Insurer then hired Chainalysis Inc., a blockchain investigations company, which was able to track 96 of the bitcoins paid as ransom, to an exchange known as Bitfinex (the remaining ransom paid had been converted into a fiat currency).

The Insurer then commenced legal proceedings in the UK (based on its subrogated rights) against the unknown hacker that made the ransom demand (the first defendant), the unknown person who held/controlled the 96 bitcoins (the second defendant), and two entities trading as the Bitfinex exchange.

The relief claimed and the court's order are described below.

An order that the hearing be conducted in private and for an anonymity order

The Insured asked for an order that the hearing be conducted in private and for an anonymity order. This order was granted. The publicity would have defeated the object of the hearing. The overarching purpose of the application was to assist the applicant in its efforts to recover the 109.25 bitcoins that were unlawfully extorted. If the hearing were to be held in public there was a strong likelihood that the object of the application would be defeated because it would potentially tip off the persons controlling the bitcoin and enable them to dissipate the bitcoins. There would also be the risk of further cyber or revenge attacks on both the Insurer and the Insured by persons unknown. There could also be a risk of copycat attacks on the Insurer and/or the Insured.

Norwich Order, Bankers Trust and Freezing Order Application

Norwich orders can be used to compel non-parties to disclose information or documents in their possession required by a plaintiff.[29] Norwich orders have increasingly been used in the online context by plaintiffs who allege that they are being anonymously defamed or defrauded, in order to obtain orders against Internet service providers to disclose the identity of the perpetrator. Norwich disclosure may be ordered against non-parties who are not themselves guilty of wrongdoing, but who are so involved in the wrongful acts of others that they facilitate the harm. Norwich orders also supplies a principled rationale for granting injunctions against non-parties who facilitate wrongdoing.[30]

In the AA v Persons Unknown case, the Insurer asked for Norwich disclosure orders requiring the operators of the exchange to provide specified information in relation to the crypto currency account owned or controlled by the second defendant.

The Insurer also asked for disclosure orders requiring the operators of the exchange to provide information based on the Bankers Trust jurisprudence. These types of orders can be made against financial institutions to disclose confidential documents to support a proprietary claim in fraud or to trace assets or their proceeds that are the subject

29 The remedy is recognized in the leading case, *Norwich Pharmacal Co. v. Customs and Excise Commissioners*, [1974] A.C. 133.

30 *Google Inc. v. Equustek Solutions Inc.*, 2017 SCC 34 at para. 31 Note, Canadian cases are all available online @ canlii.org.

of a proprietary injunction.[31] These orders are also available in Canada and elsewhere in the Commonwealth.[32]

The insurer also asked for a worldwide Mareva injunction order to freeze all the assets of the hackers. Mareva injunctions are also available in Commonwealth countries including Canada They are used to freeze assets to prevent their dissipation pending the conclusion of a trial or action. A Mareva injunction often requires the assistance of a non-party such as a financial intermediary which can be ordered to assist if it is just and equitable to do so. Banks and other financial institutions have, as a result, been bound by Mareva injunctions even when they are not a party to an underlying action.[33]

All of the above relief was adjourned at the request of the Insurer because of uncertainty whether the Bankers Trust and Norwich orders could be made and served against institutions outside of the UK. (In the UK there must be a jurisdictional gateway before service of a claim outside the UK can be ordered). This illustrates, in part, some of the cross jurisdictional challenges of getting civil remedies against foreign parties.

In subsequent U.K. cases, Bankers Trust interlocutory orders were made in *Ion Sciences vs Persons Unknown and Others*[34] and Fetch.AI Lrd & Anor v Persons Unknown Category A & Ors.

31 *Bankers Trust Co. v. Shapira*, [1980] W.L.R.1274 (C.A.)

32 *Alberta Treasury Branches v. Leahy*, 2000 ABQB 575

33 Equustek at para 33 citing Aetna Financial Services Ltd. v. Feigelman, [1985] 1 SCR 2, 1985 CanLII 55 (SCC)

34 (unreported) 21 December 2020 (Commercial Court)

Proprietary Injunction

The Insurer also sought a proprietary injunction against all four defendants, with respect to the bitcoin held in the exchange's accounts, on the basis of restitution and/or constructive trust. The Insurer additionally claimed that the paid-out sum of $950,000 also belonged to the Insurer. That money was used to purchase bitcoin and the proceeds of that money could be traced into the accounts with Bitfinex. The Insurer argued that Bitfinex was a constructive trustee of those funds on behalf of the Insurer.

This claim raised a number of issues.

A central issue was whether bitcoin is "property", as proprietary remedies can only be granted with respect to property. There are some cases that held that to be property a thing had to be a "chose in possession" or "chose in action". While the issue was not free from doubt, the court concluded that for the purpose of granting an interim injunction, crypto currencies are a form of property capable of being the subject of a proprietary injunction. In coming to this conclusion, the court relied on Lord Wilberforce's classic definition of property in *National Provincial Bank v Ainsworth*[35] as being definable, identifiable by third parties, capable in their nature of assumption by third parties, and having some degree of permanence. The Court also relied on a decision of a Singapore court in B2C2 Limited v Quoine PTC Limited.[36] The Court further relied on a legal statement on *Crypto assets and Smart contracts* published by the UK Jurisdictional Task Force ("UKJT"). The court also referenced two prior English authorities where crypto currencies

35 [1965] 1 AC 1175

36 [2019] SGHC (I) 03. See also the decision of the Singapore Court of Appeal, Quoine Pte Ltd v B2C2 Ltd. [2020] SGCA(I).

were treated as property, First, Vorotyntseva v Money -4 Limited t/a as Nebeus.com,[37] where a worldwide freezing order was made in respect of a substantial quantity of bitcoin and Ether, and secondly, the case of *Liam David Robertson*[38] where an asset preservation order over crypto currencies was made.

The court concluded that it was a proper case to make the proprietary injunction.

Although as noted above, the court adjourned the request for the Norwich and Bankers Trust order, some of the relief asked for was granted as ancillary relief to the proprietary injunction. Specifically, the Court ordered the exchange to provide information of the identity and address of the exchange operators and the hackers. The court was satisfied that that information was necessary to police the proprietary injunction and would also be appropriate to be provided by way of pre-action disclosure in the action.

There was no reported follow up decision, so it is not clear whether the crypto assets or any of the fiat currencies were actually recovered.

Other Commonwealth cases have reached similar results on whether crypto currencies are property. For example, the New Zealand case of *Ruscoe v Cryptopia Limited (in liquidation),* concluded that cryptocurrencies were "property" within the definition of section 2 of the New Zealand Companies Act "and also probably more generally" . The Court also held that these digital assets, being property, are capable of forming the subject matter of a trust.

This conclusion was echoed in the more recent U.K. case of Ion Sciences vs Persons Unknown. There Ion Sciences and its sole director, Duncan Johns, were victims of alleged initial coin offering (ICO) fraud. The court stated it was "satisfied that there is at least a serious issue to be tried that crypto assets such as bitcoin are property within the common law definition of that term." The court granted a proprietary injunction and a worldwide freezing order against persons unknown to preserve the transferred bitcoin or their traceable proceeds and an ancillary disclosure order to identify the alleged fraudsters. The court also made a Bankers Trust order against two cryptocurrency exchanges operating outside of the U.K. and an order to trace the transferred bitcoin or their proceeds that were the subject of the proprietary injunction.[39]

Another recent U.K. case *Fetch.ai Ltd and another v Persons Unknown Category A* and others reached the same conclusion and made orders similar to those made in the Ion Sciences case. In Fetch, the plaintiff's private key was somehow accessed in breach of confidence and used to fraudulently trade cryptocurrencies at a value well below market using the plaintiff's trading account. The court, relying on a breach of confidence legal claim, granted a proprietary injunction including against non-UK residents, a worldwide freezing order, and a Bankers Trust disclosure order. The injunction was based on the "simple

37 [2018] EWHC 2598 (Ch)

38 (unreported 15th July 2019)

39 For a summary of the case, see Scott Nodder, "Proprietary Injunction and Bankers Trust Order made in fraud case involving crypto currency" (3 April 2021), online (blog): Womble Bond Dickinson <https://financialinstitutionsnews.com/2021/03/04/proprietary-injunction-and-bankers-trust-order-made-in-fraud-case-involving-cryptocurrency>; Ben Packer, Michael Munk and Rose Lynch, "In Ion Sciences, the English courts take a traditional approach to determining governing law and jurisdiction in a dispute relating to crypto assets" (19 March 2021), online (blog): Linklaters <https://www.linklaters.com/en/insights/blogs/fintechlinks/2021/march/the-english-courts-take-a-traditional-approach-to-determining-governing-law-and-jurisdiction>

proposition that, when property is obtained by fraud, equity imposes a constructive trust on the fraudulent recipient, with the result that the fraudulent recipient holds the legal title on constructive trust for the loser".

Further the court held, given the nuances of the U.K. jurisdictional gateways, it had the jurisdiction to make the order against the defendants even though they resided outside of the UK.

REMEDIES AVAILABLE IN CANADA

Many of the legal remedies discussed in the U.K. *AA v Persons Unknown* and other U.K. cases and possibly even other equitable remedies may be available in Canada.

The Canadian Supreme Court recently confirmed in *Google Inc. v. Equustek Solutions Inc.*,[40] that Canadian courts have broad jurisdiction to grant orders "where just and equitable" to do so. In Equustek, the Court granted a world-wide de-indexing order against Google. The order required Google to delist links to websites that made products, created using trade secrets of the plaintiff, available for purchase.

In the Gold TV case, the Canadian Federal Court of Appeal also made a blocking order against ISPs requiring them to block copyright infringing websites, a remedy also widely available in the U.K. and in the European Union.[41]

Some causes of action such as the torts of conversion and detinue, and remedies like tracing orders and constructive trusts depend on digital currencies being "property". It is likely that they will be recognized as such in Canada as they are in the U.K., New Zealand, Singapore, and elsewhere. The issue arose in the B.C. case *Copytrack Pte Ltd v Wall*,[42] where the plaintiff had mistakenly transferred 530 Ether tokens to the defendant, valued at the time at $495,000, rather than the intended transfer of 530 CPY tokens, valued at $780. When the defendant failed to return the Ether tokens Copytrack sued the defendant alleging the torts of conversion and detinue and asked for "... [a]n order that Copytrack be entitled to trace and recover the 529.8273791 Ether tokens received by Wall from Copytrack on 15 February 2018 in whatsoever hands those Ether tokens may currently be held." The Court noted the difficulty in characterizing the tokens as property, but nevertheless concluded that "regardless of the characterization of the Ether tokens, it is undisputed that they were the property of Copytrack, they were sent to Wall in error, they were not returned when demand was made and Wall has no proprietary claim to them. While the evidence of what has happened to the Ether tokens since is somewhat murky, this does not detract from the point that they should rightfully be returned to Copytrack".

Copytrack adds to the developing jurisprudence throughout the Commonwealth which has recognized digital currencies as being a form of property and in which proprietary remedies have been ordered.

LIMITATIONS IN REMEDIES

There are, however, significant practical and evidentiary challenges with the remedies described above.

There is often the problem of being able to determine the cause of a loss, as well as challenges in being able to

40 2017 SCC 34

41 *Teksavvy Solutions Inc. v. Bell Media Inc.*, 2021 FCA 100

42 [2018] BCSC 1709

trace the transactions to particular sources where crypto assets could be frozen. Action must be quick enough, to avoid digital currencies being traded or converted to fiat currencies and dissipated without a trace.

Tracing assets also gets more complicated when the asset is transferred from one crypto currency to another one…

…especially when the fraudsters engage in "peeling" to obscure or hide digital currencies obtained illicitly.

Tracing the transfers of cryptocurrency assets is something that, in some cases, experts have been able to do. In the Colonial Pipeline case,[43] the FBI was able to track multiple transfers of bitcoins and identify that approximately 63.7 bitcoins, representing the proceeds of a victim's ransom payment, had been transferred to a specific address. Approximately, $3.6 billion in bitcoin was also traced and seized by United States authorities arising from the 2016 hack of the Bitfinex exchange in Hong Kong.[44] Similar tracing was also done by experts in the *AA v persons Unknown, Ion sciences* and *Fetch* cases. An expert in tracing transfers of cryptocurrencies from CipherTrace also gave evidence in a 2019 Canadian case involving $1.4 million bitcoins confiscated in a crypto seizure by Canadian police. Recently in a Canadian case involving ransomware attacks using malware referred to as NetWalker, a defendant who received over USD $15 million in ransom payments involving over 2,000 Bitcoins was convicted of extortion, mischief in relation to data, and participation in the activities of a criminal organization contrary to the Criminal Code of Canada. The RCMP, with the assistance of the FBI, were able to trace and seize slightly less than 720 Bitcoins from the Defendant's e-wallets and accounts worth over $30 million when seized.[45]

Worldwide freezing orders are also not particularly helpful where the fraudsters are anonymous and operate in foreign (and non-friendly) countries, particularly once stolen crypto currency has been dissipated.

A significant issue in all these cases is whether relief can effectively be obtained where the unknown defendants or innocent intermediaries such as cryptocurrency exchanges have no connections to Canada or the jurisdiction in which the plaintiff is resident or carries on business.

Under Canadian law for a court to assume jurisdiction, there must be "personal jurisdiction" (also known as "territorial competence") over the defendant. In Canada, the Supreme Court held in *Club Resorts Ltd. v. Van Breda*,[46] that various presumptive connecting factors are applied to determine if there is personal jurisdiction over a person. The connecting factors are whether the defendant is domiciled or resident in the province; the defendant carries on business in the province; the tort was committed in the province; and a contract connected with the dispute was made in the province. There is also a framework for identifying new factors.

43 See, Wikipedia, "Colonial Pipeline ransomware attack", online: https://en.wikipedia.org/wiki/Colonial_Pipeline_ransomware_attack, (accessed February 13, 2022)

44 See, "New York couple arrested in alleged scheme to launder billions in stolen bitcoin", USA Today, February 8, 2022, online: https://www.usatoday.com/story/news/politics/2022/02/08/couple-arrested-alleged-scheme-launder-cryptocurrency/6705021001/.

45 See, R. v. Vachon-Desjardins, 2022 ONCJ 43

46 2012 SCC 17

For blockchain-based cryptocurrencies there is a question as to where the situs of the asset or tort is.

This has not yet been resolved in Canada. Two U.K. decisions have suggested that the lex situs of a crypto asset is the place where the person or company who owns it is domiciled.[47] Where a claim is based on fraud a Canadian court would likely be able to assume personal jurisdiction over the perpetrator, as fraud would likely be regarded as a tort committed within a province. However, in a complicated case the courts might struggle as did the U.K. courts in the AA v Persons Unknown, Ion Sciences, and Fetch cases.

The more challenging issue is when a Canadian court will grant a remedy against a foreign based defendant or innocent third party such as a cryptocurrency exchange. As the Equustek case confirmed, common law courts can make worldwide orders against defendants (depending on the cause of action). Orders can also be made against innocent intermediaries who get "mixed up" in the tortious or other wrongful acts of others. However, Canadian courts are often reluctant to exercise their enforcement jurisdiction outside of Canada.[48] There will likely, therefore, be cases where the courts will have to decide how far they can go in making extra-territorial orders. There will also be cases where even if orders are made, or are made on terms that protect foreign entities (such as the "Babanaft" Mareva injunction orders),[49] the orders will not be immediately enforceable or be enforced by foreign courts.

The upshot of all of this is that if one of your clients is subject to a loss of crypto assets stored on a public blockchain, or paid out as a ransom in a ransomware attack, there are things they can do to try and recover them, but they must act quickly and with the right team. They will need a good forensic blockchain investigator – some of the leaders in this area are being used repeatedly in these cases. They will need to move very quickly to obtain a proprietary tracing and constructive trust injunction, Norwich and Bankers Trust disclosure orders, a worldwide Mareva injunction, and an anonymity and evidence sealing order. They will also need to reach out to crypto currency exchanges or other entities that are holding transferred assets to get their cooperation. They will also need foreign counsel ready to help get a local order enforced in foreign jurisdictions. They will also need to be lucky.

47 Ion Sciences (supra); Fetch.ai Ltd and another v Persons Unknown Category A and others, [2021] EWHC 2254 (Comm)

48 R. v. Hape, 2007 SCC 26

49 Babanaft International v. Bassantne, [1990] Ch. 13 (C.A.)

ARTICLE V

CAN CODE BE LAW? A REVIEW OF CURRENT DEVELOPMENTS

DR. MICHAEL JÜNEMANN
PARTNER
BIRD & BIRD LLP

UDO MILKAU
DIGITAL COUNSELOR

INTRODUCTION

Although the idea of a smart contract was developed in the 1990s[1], a broader discussion did not take place until the development of the blockchain[2] and the implementation of smart contracts (i.e. computer scripts) on the Ethereum platform in 2015. Now, with the current hype about decentralised finance (DeFi), claiming that traditional finance could be replaced with technologies like smart contracts (without intermediaries and human interaction), discussions around the efficacy and utility of smart contracts towards that purpose are increasingly taking place.

Some scholars have discussed the opportunities of such smart contracts compared to traditional contract law such as Raskin[3] - primarily by increasing automation:

> "[...] agreements wherein execution is automated, usually by computers. Such contracts are designed to ensure performance without recourse to the courts. Automation ensures performance, for better or worse, by excising human discretion from contract execution."

The achievability of such a future is at odds with aspects of our current reality. Among other issues, no (non-trivial) software is free of errors and, furthermore, the interdependency of software layers in actual runtime environments, with many different interacting programs and unsynchronized release changes,

1 Szabo N. Formalizing and Securing Relationships on Public Networks. FirstMonday 1997 Vol. 2/9; Szabo N. Smart Contracts: Building Blocks for Digital Markets. Extropy: Journal of Transhumanist Thought 1996;18:18.

2 There is not the "one" blockchain, but many variants with different technological properties, which are especially based on the mechanism to synchronise the dis-tributed databases in a network without (or even with) central intermediaries. The rather sophisticated debate about "open" blockchains based on game theoretical assumptions about rational agents without any coordination, but strong generic inefficiency versus "consortium-like" blockchains with a pure technical redundancy would be beyond the scope of this paper. Milkau U, Bott J. Towards a Framework for the Evaluation and Design of Distributed Ledger Technologies in Banking and Payments. Journal of Payments Strategy & Systems 2016 Vol 10/2;153:153.

3 Raskin M. The Law and Legality of Smart C0ntracts. 1 Georgetown Law Technology Review 2017;305:306.

undoubtedly result in "software aging"[4], i.e. unavoidable errors over time.

To discuss the question of whether Code can be Law? or, more specifically, whether smart contracts could replace the nexus of contracts, contract law, and the factual context within which the contract is negotiated and applied, we outline three different perspectives (illustrated in Fig. 1.):

Normative perspective

A smart contract is a software script, which is (i) stored and compiled for execution on blockchain based infrastructure (typically the Ethereum Virtual Machine), (ii) published to everyone (but in bytecode which is not easily readable by anyone not familiar with software development principles and the language used, and thus may contain hidden errors or complex interdependencies), (iii) immutable due to the cryptographical linked blockchain entries, but not immune to changes of the blockchain itself (so-called hard forks), and (iv) said to be self-executing, although this is a rather trivial feature of any contemporary computer program after a program was started (and fees are paid for cloud computing resources or "gas"[5] is paid for using the Ethereum platform). Some blockchain enthusiasts even postulate that a set of self-executing smart contracts could establish a DAO (Distributed Autonomous Organization), which would have a legal identity in its own right without any human interference.

Positive perspective

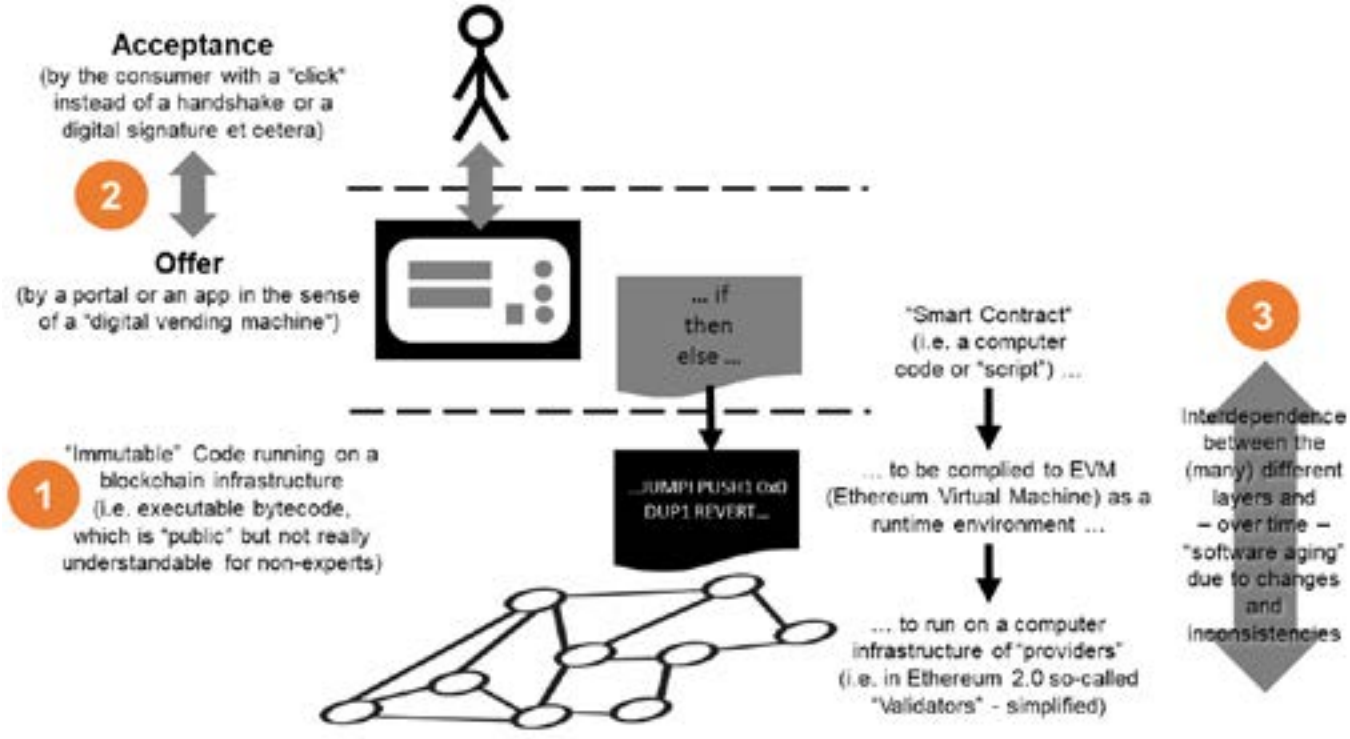
Smart contracts are technological protocols, which document the meeting of minds between the Seller (with an offer) and the Buyer (with an acceptance), while the legal agreements are exchanged by a front-end, e.g. by a vending machine (for a coke at a railway station), a digital portal or an app.[6]

Economic situation

4 Parnas D L. Software aging. ICSE '94 proceedings 2014;279:279.

5 Frankenfield. Gas (Ethereum), https://www.investopedia.com/terms/g/gas-ethereum.asp.

6 BGH judgement dated 16.10.2012 – file no. X ZR 37/12.



Current blockchain platforms in reality are a highly complex environment of many technical layers. In parallel, the approach of DeFi morphed from peer-to-peer to a layer-on-layer-on-layer-structure, where many entities looking for their individual business case. Looking on the technical part only, it starts with the smart contract code, which has to be compiled by a compiler, which runs on a virtual machine and requires some external data feed (depending on the trustworthiness of the so-called oracle). This runtime environment sits on a blockchain infrastructure such as Ethereum 2.0, which applies a certain consensus mechanism (changed between Ethereum 1.0 and 2.0 including changing commercial incentives), which is running on different computers with different operating systems and different hardware, which are operated in a data center or in the cloud. And all such services or resources have to be paid for, or vice versa are linked to some commercial purpose - just ask cui bono.

For simplification, this paper will skip the change from the former concept of Ethereum 1.0 (with a proof of work consensus mechanism to synchronise all transactions based on a game theoretical approach) to Ethereum 2.0 (with a proof of stake consensus mechanism with a primarily commercial incentive structure) and focus on the legal issues of "Code is Law". In Figure 1, the actual situation is summarized: 1 represents smart contract self-execution based on implemented software in a back-end black box whereas 3 questions every vision of technical immutability in the long run, while the relationship between offer and acceptance 2 will be - still - the basis for any contractual agreement.

In the current debate, blockchain enthusiasts proposed that smart contracts could replace every aspect of a legal contract agreement including all legal context and automate contract law to the extreme of "code is law".

However, (non-trivial) contracts are always incomplete, because human beings have limited insight into the future and will never be able to codify each and every future development in some contract or code ex-ante (as expressed in the concept of "bounded rationality"[7]). Consequently, ex-post governance will be required to deal with misunderstandings, dispute, or inconsistencies, whether they result from a misunderstanding of the agreement or from technical problem of the implementation.

Contracts can be made in very different forms (from a handshake via a signed piece of paper to an electronic message with a digital signature based on the freedom of contract except special situation with formal requirements) - this includes portals, apps or even pure exchange of messages. However, it will be the meeting of the minds, which makes a contract, while technical protocols can support this communication (from handshake via written text to e-mails and electronic messages with digital signature), but also have severe limitation due to unforeseeable technological interdependencies in the long run. It should be added as a remark that smart contracts (computer scripts) are literally chained to a blockchain, and any connection to the physical world e.g. for a delivery confirmation must made by so-called 'oracles'. Besides being a point-of-failure, these 'oracles' illustrate that the world of blockchain and the physical world are different things.

Last but not least, we need

7 Simon H A. Bounded rationality and organizational learning. Organization Science 1991;125:125.

contract, contract law and contractual governance not primarily to document agreed obligations (i.e. a protocol for executing the defined transactions), but for the case of dispute. In other words, contracts are required for the situation beyond our bounded rationality, i.e. for rights and duties in situation which cannot be programmed in computer code such as smart contract ex-ante, as we do not know what the future will bring (and how assumptions have to be interpreted in a future contexts).

SET-UP OF A SMART CONTRACT

Fundamental Aspects

The legal part of a smart contract comprises the transfer of a written contract document into a coded (smart) contract and its potential legal enforcement. The technical part includes the coding process, the deployment into a runtime environment, and potentially a trigger to external (technical) systems. This excludes all parts of a contract, which results from the legal context but not the written in code.

Technically, the exchange of offer and acceptance ("meeting of minds") could be performed by using a portal and entering the parameters. The given parameters are displayed and sent to the recipient for confirmation. After the confirmation process, a computer script is activated by the two-sided acceptance and the smart contract "lives" on the blockchain including the data stored within the script.

Besides the way of setting up a basic structure, the applicable law, jurisdiction, format and language would need to be agreed upon and must be programmed. While in traditional contracts e.g. jurisdiction is a simple definition of the applicable place of jurisdiction and, consequently, a link to a legal context, a smart contract must trigger such functions that are in line with the chosen jurisdiction, but not include any external context. Therefore, everything - and that means really every piece of legal context applicable to the respective smart contract. The various legislations differ not only in terms of certain nuances in the different types of law (e.g. commercial law) but also on fundamental definitions and aspects (e.g. definition of working days). Hence, besides the type of function, also such aspects must be programmed into the smart contract that are regulating when a function is triggered. One might say that in this way, the smart contract receives its rulebook of each determining how something should be performed by each party to the contract.

However, a properly recorded smart contract may in fact be (legally) void without the parties being aware of it, as they perceive a functional computer program. Under Common Law principles, a contract is voidable for mistakes, and it therefore can be considered ineffective from the moment it was made. This clashes with the principle of the blockchain (i.e. being immutable and self-executable).[8] Questions particularly arise whether it is possible to write a legal contract only in code as its contractual language. According to the principle of the so-called freedom of contract and freedom of choice, this is possible unless a specific form requirement is stipulated by statutory law.[9] However, a smart contract is a naked piece of computer language, which can perform a protocol (i.e. documentation

8 Martin Heckelmann, Zulässigkleit und Handhabung von Smart Contracts, NJW 2018 504, 507 (2018).

9 Jünemann M, Kast A. Rechtsfragen beim Einsatz der Blockchain. ZfgK 2017;531:534.

of agreement and exchange of messages), but not perform the complexity of a contractual agreement in a legal context.[10]

For example, smart contracts written in code raise concerns regarding consumer protection: An average consumer cannot be expected to be able to read the terms and conditions written in code. Therefore, a translation of the code into common languages could be necessary.

The legal concept of pacta sunt servanda means that agreements which are legally binding must be performed. At first sight, this seems comparable to the principle of code is law, stipulating that the agreed or programmed aspects may not be changed afterwards (ex-post). Having said this, the legal concept of pacta sunt servanda can be limited by the right of revocation of one party, which will contradict the principle of code is law by changing the contract ex-post.[11] Moreover, part of the principle of freedom of contract is that contracts can be renegotiated and also modified by the parties through a further contract.[12] Hence, the principles of pacta sunt servanda and freedom of contract are to be understood as what the parties finally agreed or are agreeing on that must be performed. This differs from the principle of code is law, meaning the agreed is unchangeable and must be performed.

Interpretation and Renegotiation of Smart Contracts

It is questionable whether smart contracts can and need to be renegotiable. In case of ambiguities, contracts are interpreted, and the will of both parties is carved out. Only what the parties really wanted to agree on shall be agreed and shall apply regarding their contractual relationship.

By contrast, interpretations of code performed by machines are based on so-called Boolean logic, meaning something is either true or false. Therefore, the principle embedded in German law falsa demonstratio non nocet, meaning wrong designation does not harm, does not apply.

In 2012, the German Federal Court of Justice (Bundesgerichtshof - BGH) ruled that the way an automated system is expected to understand and process a declaration of intent, which was made using electronic means of communication, does not determine the content of the declaration. What matters is how the human addressee is allowed to understand the respective declaration in good faith and custom.[13] This means the displayed and confirmed content is binding but not the bits and bytes within a computer system (such as a blockchain).

(Smart) dispute resolutions and risk management

If a smart contract is set up and a dispute arises the (local) courts will probably need specialists or expert witnesses to evaluate technical details (e.g., actual effect of instructions programmed in a special computer language, software errors or attack vectors for hacking attacks). Some companies started developing arbitration proceeding based on blockchain technology.[14] One way of designing a blockchain-based arbitration implementation might function as follows: In case of a (detected) legal breach or a bug in

10 Jünemann/Kast, ZfgK 2017, p. 531,p. 534.

11 Palandt, 2017, . section 145 footnote 4 lit. a

12 BeckOGK/Herresthal, 1.5.2018, BGB section 311 footnote 128.

13 BGH judgement dated 16.10.2012 – file no. X ZR 37/12.

14 For example: “CodeLegit White Paper on Blockchain Arbitration” available here: h

the smart contract, the respective party triggers the arbitration process. A grace period pausing the execution of the smart contract will commence. The arbitration service will then be performed.[15] Afterwards, the smart contract will be continued, modified by the appointed authority as foreseen in the arbitration library, or ended.[16] Depending on the settlement or award, the appointing authority continuous, modifies or ends the smart contract.[17]

By the choice of arbitration, the parties restrict their access to the state courts by contract; the parties can determine the scope of the dispute and whether to proceed to court at all (Dispositionsgrundsatz).

The advantage of such blockchain arbitration rules over traditional arbitration rules is that all parties involved have access to the documents which are made available by a blockchain that serves as a verification tool.[18] Several tech enthusiasts claim that blockchain arbitration will replace traditional arbitration.[19]

15 https://docs.google.com/document/d/1v_AdWbMuc2Ei70ghITC1mYX4_5VQsF_28O4PsLckNM4/edit

16 A complex scheme is given in the Appendix – Arbitral Proceeding using CodeLegit Arbitration Library and Blockchain Arbitration Rules, https://docs.google.com/document/d/1v_AdWbMuc2Ei70ghITC1mYX4_5VQsF_28O4PsLckNM4/edit.

17 Appendix – Arbitral Proceeding using CodeLegit Arbitra-tion Library and Blockchain Arbitration Rules, https://docs.google.com/document/d/1v_AdWbMuc2Ei70ghITC1mYX4_5VQsF_28O4PsLckNM4/edit

18 CodeLegit White Paper on Blockchain Arbitration, https://docs.google.com/document/d/1v_AdWbMuc2Ei70ghITC1mYX4_5VQsF_28O4PsLckNM4/edit#

19 Marike R. P. Paulsson, The Eve of the New York Con-vention 60th Anniversary and the Birthday Party: How to Prepare with too Many Guests at the Table. "Il ne faut pas melangér les tables., Kluwer Arbitration Blog (Aug. 8, 2019, 2:22 PM), http://arbitrationblog.kluwerarbitration.com/2018/06/21/eve-new-york-conventions-60th-anniversary-b irthday-party-prepare-many-guests-table-il-ne-faut-pas-melanger-les-tables/.

Freezing and Exit Scenarios

Unfortunately, smart contracts deployed on a blockchain cannot be modified, since they are permanently written on the blockchain.[20] But given the fact that smart contracts cannot be changed, unless the possibility to freeze the execution of the smart contract is encoded, how could a government agency react if the review of the smart contract has shown that the aged smart contract is vulnerable to hacking and could lead to unwanted results?

If an emergency exit was coded into the respective smart contract, then the smart contract could be stopped (frozen) or ended (killed). The essential key data of the contract (e.g., contractual parties, object of purchase, purchase price) could be extracted from the aged contract and a new smart contract with the same content could be coded.[21] This would be very similar to an update. Such a mechanism (automatic data readout) could, in principle, be written into the code of a legal model smart contract. The address of the aged smart contract would have to be updated, and the users would see the address of the new smart contract.

CONCLUSION

Due to the immutability of smart contracts, as long as there is no hard fork, the parties are only able to rescind or unravel the smart contract if such rights are programmed in the smart contract from the outset. It is, however, debatable whether other emergency exits, other than rights of rescission, can be written into the

20 https://medium.com/@merunasgrincalaitis/can-a-smart-contract-be-upgraded-modified-1393e9b507a.

21 https://medium.com/@merunasgrincalaitis/can-a-smart-contract-be-upgraded-modified-1393e9b507a.

code of a smart contract.[22] Even if the coder of a smart contract was both a lawyer and an IT expert, the question would arise as to how the coder could foresee every possible scenario in an uncertain future. However, it would be necessary (but not feasible) to include all possible situations and solutions into the smart contract, or to abandon the fairness aspect of a contract as provided under traditional legal principles.

22 Martin Heckelmann, Zulässigkleit und Handhabung von Smart Contracts, NJW 2018 504, 507 (2018).

ARTICLE VI

DIGITALIZING TRADE IN ASIA NEEDS LEGISLATIVE REFORM[1]

RAOUL RENARD
LEGAL REFORM LEAD
INTERNATIONAL CHAMBER OF COMMERCE

CARMEN MARÍA RAMÍREZ ORTIZ
CONSULTANT
TRADE AND SUPPLY CHAIN FINANCE
ASIAN DEVELOPMENT BANK

OSWALD KUYLER
MANAGING DIRECTOR
ICC DIGITAL STANDARDS INITIATIVE

STEVEN BECK
HEAD OF TRADE AND SUPPLY CHAIN FINANCE
ASIAN DEVELOPMENT BANK

The novel coronavirus (COVID-19) pandemic was a huge stress test for international commerce. In addition to impacting the balance sheets of businesses large and small, COVID-19 also tested the resilience of supply chain processes. The ability of traders to import and export goods, operating within the traditional paper-based paradigm, was hindered by lockdowns, health and safety procedures, and teleworking measures. The pandemic revealed that our continued reliance on physical documents is not only an antiquated way of working—holding us back from unlocking new forms of productivity, traceability, products, and services—but is a source of significant risk to supply chains.

Even before COVID-19, paper-based transferable records remained a stubborn form of inefficiency and risk in international trade. Goods sometimes arrived at their port of destination before documents were fully processed, leaving parties to bear additional costs to either hold the cargo or secure a letter indemnifying the carrier for delivering the goods without the relevant transferable record (e.g., a bill of lading). Paper documents also gave rise to risks of fraud, as forgery of transferable records was and remains possible. Verifying document authenticity consumed significant resources.[2]

Technology exists to upgrade trade into the modern digital world. Distributed ledger technologies such as blockchain are now being used in some trade transactions but currently only a small number of deals on a relatively tiny scale. With a blockchain-based platform, the participants in a trade deal and the financial entities supporting it confirm proper documentation within minutes or hours. All participants can be informed simultaneously of the deal's approval; a sharp contrast to the way multiple documents get signed and handed from party to party in a traditional transaction that can take days to finish.

Given the current environment, with the pandemic highlighting

1 A version of this paper was originally published by the Asian Development Bank

2 These issues have been mentioned as reasons for the adoption of the MLETR in Singapore: S. Iswaran. 2021. Opening Speech at the Second Reading of the Electronic Transactions (Amendment) Bill. 1 February.

the shortcomings of face-to-face processes, many would have expected to see a groundswell in the adoption of technology platforms offering paperless trade services. Yet while COVID-19 accelerated digital transformation in some sectors (U.S. e-commerce experienced a decade worth of growth in Q1 of 2020),[3] anecdotal evidence suggests that uptake in the existing providers has been lackluster, with percentage use increasing in the single digits. Despite the pandemic, according to the Digital Container Shipping Association, only 0.1% of bills of lading were issued electronically in 2020.[4]

A considerable roadblock to greater uptake of existing solutions is the lack of legal recognition of electronic transferable records. Most jurisdictions require negotiable instruments to be in paper form. Because of this, importers and exporters seeking to use digital means have relied on platforms that enable the transfer of title using rulebooks grounded in the private contract law of the United Kingdom and the United States. These solutions thus present a potential drawback for companies operating in the ASEAN[5], CAREC[6] and SASEC[7] regions.

The single greatest driver of electronic record adoption in the post-COVID-19 era in Asia will be their recognition within the domestic legal systems of trading nations. Adoption of the Model Law on Electronic Transferable Records (MLETR), developed by the United Nations Commission on International Trade Law (UNCITRAL), holds the greatest promise to increase efficiency, consistency, and coherence in the modernization and harmonization of legislation bearing on electronic documentation.

THE MODEL LAW ON ELECTRONIC TRANSFERABLE RECORDS

MLETR was drafted in a globally inclusive process, in a manner designed to be compatible with all legal traditions and economic systems. It enables the legal recognition and use of electronic transferable records both domestically and across borders. Paper-based transferable documents or instruments entitle the holder to claim the performance of the obligation indicated therein and allow a transfer of title through the transfer of possession of the document or instrument.

Transferable documents or instruments typically include, among others, bills of lading, bills of exchange, promissory notes, and warehouse receipts. They are essential commercial tools. Their availability in electronic form will cause a paradigm shift in international trade by democratizing accessibility to reliable, high quality, and trusted data. Digitalizing transferable documents or instruments will spark a revolutionary step in how companies engage with each other and local communities and governments, bringing manifold benefits across the transaction cycle.

Today, only large multinationals can deal with the complexity of paper-heavy processes and data quality

3 McKinsey & Company. 2021. COVID-19: Implications for business, Briefing note #68. 18 August.

4 Eleanor Wragg, Global Trade Review. 2020. DCSA standardises electronic bill of lading. 9 December.

5 ASEAN is a regional grouping comprised of Brunei Darussalam, Cambodia, Indonesia, the Lao People's Democratic Republic, Malaysia, Myanmar, the Philippines, Singapore, Thailand, and Viet Nam.

6 CAREC is a regional grouping comprised of Afghanistan, Azerbaijan, the People's Republic of China, Georgia, Kazakhstan, Kyrgyz Republic, Mongolia, Pakistan, Tajikistan, Turkmenistan and Uzbekistan.

7 SASEC is a regional grouping comprised of Bangladesh, Bhutan, India, the Maldives, Nepal, and Sri Lanka.

challenges. The transformation toward electronic records will lead to many benefits, including:

1. access to new forms of metadata throughout supply chains, further enabling industries to measure and course-correct their progress toward the UN's Sustainable Development Goals;
2. improved quality of the data that companies use for their reporting and analytics needs, increasing analytic accuracy and enabling all companies—from the smallest operators to multinationals—to better anticipate market movements; and
3. through the liberation of quality data throughout supply chains and international trade processes, financial institutions will be able to find new mechanisms to measure risk, offering up new asset classes that can help minimize the trade finance gap.

MLETR ensures the singularity of claim throughout a transaction cycle (whether domestic or cross-border) and is informed by three fundamental principles that underly existing UNCITRAL texts on e-commerce: (i) non-discrimination, (ii) functional equivalence, and (iii) technology neutrality:

The principle of technology neutrality accommodates all technologies and models – whether based on registry, token, distributed ledger technology (DLT), or indeed technologies not currently developed – entailing the adoption of a system-neutral approach. The UNCITRAL explanatory note for MLETR provide some guidance on the application of distributed ledgers in implementing the MLETR by clarifying that electronic transferable records management systems do not imply the existence of a system administrator or other form of centralized control. Therefore, blockchain solutions seem a natural fit under the scope of MLETR.

The principle of functional equivalence also lends itself to the use of DLT. With respect to signatures, for instance, MLETR Article 9 provides that "[w]here the law requires or permits a signature of a person, that requirement is met by an electronic transferable record if a reliable method is used to identify that person and to indicate that person's intention in respect of the information contained in the electronic transferable record". One can therefore imagine the expression of an intention coupled with the use of, for instance, a decentralized identifier, stored on the blockchain, to meet the signature requirement contained in a given legal framework.

Use of these principles—together with the general reliability standard—is what makes MLETR both deceptively simple yet forward-thinking in its design: simple in that it preserves the key features of substantive law applicable to paper-based transferable records across jurisdictions, and forward-thinking in that it ensures the law is able to accommodate unforeseen technological advances and the incorporation of standards, including standards developed by industry.[8]

Hence, an electronic bill of lading issued under MLETR is subject to the same law that applies to a paper-based bill of lading irrespective of the method so long as the general reliability standards for verifying signatures, integrity and other aspects of electronic records are satisfied. This avoids creating a special legal regime for electronic transferable records, with complications to business practices and additional costs. These features can be readily appreciated

8 See MLETR Article 12(a)(vii).

through analysis of the experience of Singapore, a pioneer in the field of e-commerce and a recent adoptee of the MLETR.

INTERNATIONAL PUSH FOR DOMESTIC ADOPTION OF MLETR: SINGAPORE'S APPROACH

Seamless digitalized trade would lead to a radical transformation cross-border merchandise trade as we know it. Digitalization of trade is key to closing the finance gap, boosting transparency and efficiencies and strengthening global supply chains while cutting trade-related costs. There are multiple benefits linked to digitalization of electronic transferable records: traceability and real-time tracking, fraud prevention, faster clearance of shipments, etc. Many of these benefits are paradigmatic use cases for distributed ledger technology,- but they cannot be achieved unless a clear framework for the legal recognition of electronic transferable records is established.

Despite its clear, multiple benefits, adoption of MLETR has been relatively slow to date. The COVID-19 pandemic and subsequent disruptions to the processing of trade transactions have, however, accelerated progress. With the rise in trade costs across the Asia-Pacific, especially shipping costs, countries increasingly acknowledge the importance of enabling the use of digital solutions to mitigate COVID-19-related burdens.

Singapore has a longstanding history of leadership on matters relating to electronic commerce. It enacted its Electronic Transactions Act (ETA) in 1998,[9] becoming the first country to adopt the 1996 UNCITRAL Model Law on Electronic Commerce (MLEC).

On 1 February 2021, Singapore passed an amendment to the ETA, the Electronic Transactions (Amendment) Bill, which introduces a new Part IIA to the act to adopt MLETR with modifications. In doing so, Singapore became the second trading nation to adopt MLETR, following the 2019 adoption by Bahrain.[10]

The benefits of the functional equivalence approach are readily apparent. Owing to the careful design of MLETR, there is no need to amend the substantive underlying legislation already applicable to paper-based transferable records.

An interesting feature of Singapore's approach is the inclusion of a provision that enables the Government of Singapore to introduce, if necessary, an accreditation framework for providers of a management system for electronic transferable records.[11] Though not a requisite feature of text adopting MLETR, a declaration of an accrediting body is one of the potential methods of assuring reliability that is enumerated in the MLETR general reliability standard found.[12]

On its efforts to stablish an interoperability framework for the exchange of digital trade documentation, Singapore's Infocomm Media Development Authority developed TradeTrust in collaboration with the International Chamber of Commerce and other key stakeholders.

Using distributed ledger

9 The ETA was repealed and re-enacted in 2010 to adopt the United Nations Convention on the Use of Electronic Communications in International Contracts in 2010.

10 M.-O. Al-Suhaimi. 2019. Bahrain First Country to Enact MLETR. Asharq Al-Awsat. 16 January.

11 Electronic Transactions (Amendment) Act 2021 Division 6.

12 See MLETR Article 12(a)(vi).

technology, the TradeTrust framework ensures authenticity and origin of documents, enabling parties to perform title transfer on trade documents electronically. TradeTrust is an open-source licensing tool which is blockchain-based, designed to achieve three key functionalities: (i) assure authenticity of documents; (ii) assure provenance of documents; and (iii) provide legally valid performance obligation transfers between implementers of the framework.

As of October 2021, five jurisdictions have adopted MLETR, and there is clear evidence of the strong global push for MLETR. Legislative change is underway in several jurisdictions, with the Group of Seven countries committing support for legal reform efforts aligned with MLETR and the Law Commission of England and Wales announcing proposed reforms that would give legal recognition to electronic versions of trade documents.

FRAMEWORK AGREEMENT ON PAPERLESS TRADE IN ASIA AND THE PACIFIC

The Framework Agreement on Facilitation of Cross-border Paperless Trade in Asia and the Pacific (CPTA) is a welcome development in the advancement of paperless trade in the region. The CPTA aims to accelerate the implementation of digital trade facilitation measures for trade and development and entered into force on 20 February 2021. Azerbaijan, Bangladesh, Iran, the People's Republic of China, and the Philippines have ratified the agreement. Armenia and Cambodia have signed but not yet ratified.[13]

The CPTA's current draft road map calls for the establishment of a national policy framework for paperless tradeincluding by identifying and selecting relevant international legal frameworks and best practices within 9 months of entry into force.[14]

Notably, the agreement will be guided by the principles of non-discrimination, functional equivalence, technology neutrality, and the promotion of interoperability. These are the same general principles underpinning UNCITRAL texts, including the MLETR. Further, Article 10 of the CPTA states that the parties "may, where appropriate, adopt relevant international legal instruments concluded by United Nations bodies and other international organizations." The CPTA thus may serve as a powerful driver of MLETR adoption in Asia and the Pacific in 2021 and beyond.

CONCLUSION

COVID-19 has accelerated pre-existing trends toward digitalization of economies. Huge benefits can accrue to those countries that provide an enabling domestic legal environment for electronic transferable records by adopting MLETR. Many states in Asia have adopted one or more UNCITRAL texts on e-commerce in the past, and/or are parties to the CPTA, suggesting a willingness to adopt. The straightforward revision of the Electronic Transactions Act by Singapore may serve as inspiration for countries in Asia and beyond.

13 A list of Member State signatures and ratifications can be found in UN Treaty Collection. Status of Treaties.

14 UNESCAP. 2018. Draft Road Map for the Implementation of the Substantive Provisions in the Framework Agreement on Facilitation of Cross-Border Paperless Trade in Asia and the Pacific. Fourth Meeting of the Interim Intergovernmental Steering Group on Cross-border Paperless Trade Facilitation. Bangkok, Thailand. 22–23 March.

ARTICLE VII

THE EMERGING LEGAL AND REGULATORY FRAMEWORK FOR DEFI LENDING PLATFORMS IN VIETNAM

TRAN VIET DUNG
ASSOCIATE PROFESSOR
DEAN OF INTERNATIONAL LAW
HO CHI MINH CITY UNIVERSITY OF LAW

LE TRAN QUOC CONG
LECTURER OF INTERNATIONAL LAW
HO CHI MINH CITY UNIVERSITY OF LAW

Many NFT and GamFi[1] projects have recently launched in Vietnam, including projects such as Kyber Network, Tomochain, Coin98 or Axie Infinity. So called "decentralized finance" (DeFi), is also a fast-growing sector of the blockchain ecosystem both in Vietnam and abroad. According to a report by analytics firm Chainalysis, Vietnam is ranked second in the overall index ranking on Global Defi Adoption, after the United States.[2]

While growth has been rapid, it is hampered by the fact that Vietnam has yet to adopt a clear legal framework for blockchain sector. As a result, Vietnamese startups engaging in blockchain activities, especially in sensitive service fields such as finance, face various obstacles and regulatory risks, as their legal status is currently not recognized by the government. Many companies seek to mitigate their risks by registering overseas. However, cross-border governance issues may create other legal obstacles.[3]

Thanks to the COVID-19 pandemic, the government has realized the need to promote legal infrastructure for e-finance. At the end of 2020, the Prime Minister issued a Decision No. 2117/QD-TTg to announce that blockchain is one of the priority technologies for research, development and application, in order for Vietnam to actively participate in the Fourth Industrial Revolution.[4] The Government has also assigned the State Bank of Vietnam (SBV) to thoroughly research and build a cryptocurrency development and management mechanism based on blockchain technology. It is expected that government efforts will create

1 GamFi is a combination of decentralized finance (Defi), non fungible token (NFT) and blockchain based online games. This term was first used by Andre Cronje, founder of Yearn in September 2020. Since then, "GameFi" has been used more and more often to describe games with financial elements enabled by blockchain technology.

2 Chainalysis, Introducing the Chainalysis Global DeFi Adoption Index, https://blog.chainalysis.com/reports/2021-global-defi-adoption-index/

3 Vietnamese Government electronic news, Blockchain technology: Opportunities for Vietnamese startups https://baochinhphu.vn/cong-nghe-blockchain-co-hoi-cho-cac-start-up-viet-102301627.htm

4 Decision No 2117/QD-TTg of the Prime Minister promulgating a list of priority technology sectors, including blockchain, for research, development, and application to enhance digitally-led services in the Fourth Industrial Revolution.

avenues for further development of DeFi services in Vietnam.

In the current context of Vietnam, the government has acknowledged that certain blockchain technologies are inevitable. The SBV has gradually accepted a limited number of fintech applications operated by banks. SBV is currently considering allowing non-banking organizations with new technology applications to provide financial services, including payment services, money transfer, peer-to-peer lending. It is worth noting that under the draft Decree on Fintech by the SBV, the term non-banking financial services is defined rather broadly to include: Payment services, money transfer, peer-to-peer lending or new technology financial services. This broad language leads to an assumption that DeFi lending in Vietnam can now be regulated under this new regulatory framework should DeFi lending developers and their products meet certain conditions.

This paper provides an overview of the legal and financial regulatory landscape for DeFi lending in Vietnam, highlighting particularly, the risks and challenges for regulators and investors.

THE LEGAL CHALLENGE OF DEFI LENDING IN VIETNAM

DeFi is a broad term for financial services built on top of the decentralized blockchain technology. The space has evolved since the launch of the Ethereum network in 2015, which laid the groundwork by implementing blockchain-based smart contracts.[5] DeFi transactions are executed and recorded according to the explicit logic of a DeFi protocol's predetermined rules, on a permissionless basis.

DeFi lending functionality is quite similar to traditional P2P services, but with one core difference. In DeFi, loans are issued on decentralized platforms that lock cryptocurrencies through smart contracts on public blockchains. It allows users to lend cryptocurrency in exchange for interest. Smart contracts are used in DeFi lending. Due to their availability through a decentralized settlement layer, DeFi lending transactions do not require involvement of a third-party intermediary. Tech firms in Vietnam show great interest in DeFi and are willing to invest into this business platform. However, there is, as yet, no specific legal framework on DeFi in Vietnam. Like most fintech companies operating P2P lending, companies engaging in DeFi lending are still obliged to comply with the regulations of general laws such as the Civil Code,[6] Law on Investment[7] and Law on Enterprises.[8] Overall, the regulations under these laws are suitable for traditional business only.

In the current context of Vietnam, there are two issues which need to be resolved for DeFi in order to operate effectively:

1. The legal status of cryptocurrency in Vietnam as the nature of DeFi has always been closely related to a cryptocurrency. (Defi needs to be operated on smart contracts backed by cryptocurrencies, such as, e.g., Ethereum, Solana, Polkadot); and
2. The issue of how to regulated and risk manage related to new financial models like DeFi lending in context the government is still vague about

5 World Economic Forum, Decentralized Finance (DeFi) Policy-Maker Toolkit, (2021) https://www3.weforum.org/docs/WEF_DeFi_Policy_Maker_Toolkit_2021.pdf (last visited 20 January 2022).

6 Civil Code (Law No. 91/2015/QH13) of the National Assembly, dated 24 November 2015.

7 Law on Investment No. 61/2020/QH14 of the National Assembly, dated June 17, 2020

8 Law on Enterprises No. 59/2020/QH14 of the National Assembly, date 17 June 2020.

these concept and the legislation of Vietnam is not ready yet.

Vietnam does not currently have any regulations prohibiting the use of cryptocurrency as a store of value.[9] The State Bank of Vietnam (SBV) while addressing the blockchain financial platforms often uses the term "virtual currency" (tiền ảo) to address cryptocurrency. However, the SBV does not accept virtual currencies/cryptocurrency as currency.[10] This means that individuals and organizations are not allowed to issue or use it for payment since use of cryptocurrency a payment unit is prohibited. Therefore, in the case of DeFi, lending, borrowing, exchanging and paying through cryptocurrencies may be inconsistent with Vietnamese law. Even stablecoins such as USDT, USDC, BUSD commonly used in DeFi transactions may not be legal in Vietnam.

There are two potential reasons why Vietnam has not yet recognized cryptocurrency like other countries.

First, there may be a concern by the government that cryptocurrencies will weaken state control over currency issuance, directly impacting monetary policy. In addition, the Vietnamese government is also concerned that this decentralization is a risk to national financial safety when the price of cryptocurrency on the free market is unstable.[11]

Secondly, the government has expressed concern that anonymous cryptocurrency transactions can also facilitate the risk of money laundering, financing of terrorism, fraud and tax evasion.[12]

Recently, however, the government has presented a less conservative and relatively flexible approach in the space of digital currencies or cryptocurrencies. In June 2021, the Prime Minister issued Decision No. 942/QD-TTg (Decision 942) which requires the SBV to research, develop and test cryptocurrency in the 2021-2023.[13] Although Decision 942 does not describe exactly how this cryptocurrency works, it does create an important legal basis for the SBV to issue a stablecoin specifically for blockchain applications, including DeFi in Vietnam in the near future. It is expected that DeFi lending platforms in Vietnam will be able to use stablecoins issued by the SBV. Such stablecoins can serve as a payment instrument in Vietnam, while other tokens, digital coins can only act as a store of value in DeFi transactions. Consequently, the lingering concern of the government about loss of sovereignty in currency issuance and the financial instability due to free fluctuation of cryptocurrencies could be mitigated throught the use of a sovereign stablecoin.

Second, there may be policy concerns about the stability and robustness of the underlying technology. One of the most significant drawbacks in DeFi Lending is smart contract risk. Instead of centralized custody and/or servers,

9 Until now, Vietnam's civil law does not recognize cryptocurrency as a type of property or property right. (Article 105 of the 2015 Civil Code).

10 In addition: the issuance, supply and use of Bitcoin and other similar virtual currencies as a means of payment may be administratively sanctioned with a fine of between VND 150 million and VND 200 million according to the provisions of Clause 6. Article 27 of Decree 96/2014/ND-CP on administrative sanctions in the field of currency and banking activities.

11 Press release dated February 27, 2014 of State Bank of Vietnam on bitcoin and other similar virtual currencies.

12 Directive No. 10/CT-TTg dated April 11, 2018 of the Prime Minister on strengthening the management of activities related to bitcoin and other similar virtual currencies.

13 Decision No. 942/QD-TTg dated June 15, 2021 of the Government approving the e-Government development strategy towards the digital Government in the 2021 – 2025 period, with a vision to 2030.

participants in DeFi have to trust that smart contracts do not have any vulnerabilities that put assets at risk. In a way, DeFi lending replaces custodial risk with smart contract risk, which has allowed attackers to steal funds escrowed in smart contracts. The most prominent attacks involve the exploitation of bugs in code and the manipulation of external price feeds for assets within DeFi protocols.[14] Therefore, the security of DeFi largely on the developer's ability to predict technical flaws that can be subject to hacker's attacks. The relevant programming codes of smart contracts must be carefully tested to ensure that the Defi protocols can be used by parties in the transaction. Technically, once these DeFi protocols are operational, any changes or modifications to the relevant smart contract would need to be agreed upon by the entire blockchain system.

Regulators in Vietnam are addressing this technology risk concern through the creation of regulatory sandboxes.

The goal is to assess the impact of business models that adopt new technologies. The pilot implementation of the Sandbox Program will help the Government identify both positive and negative aspects in DeFi lending, while developing a more advanced management mechanism. This mechanism will provide regulators an opportunity to learn more about the technology and will help to limit the abuse of DeFi activities for fraud and illegal activities. The Sandbox program is described below in greater detail.

14 Cointelegraph: 169 blockchain hacking incidents in 2021, $7 billion in funds lost. https://cointelegraph.com/news/cointelegraph-consulting-recounting-2021-s-biggest-defi-hacking-incidents

SANDBOX PROGRAM – A CHANGE TO TESTING DEFI LENDING

In early June 2020, the SBV released a Draft Decree on the regulatory sandbox for FinTech activities in Vietnam ("the Draft Decree"). This Draft Decree proposes a framework for a sandbox program for Fintech Services (Sandbox Program) by detailing, among other things, the eligibility criteria and procedural requirements for participation. This Sandbox Program will allow startup companies to promote innovation under the regulator's supervision. Companies that are allowed to join the Sandbox Program can operate with special exemptions. While Fintech and Defi are different concepts, the definitions and conditions for participating in the Sandbox allow individuals and organizations in the DeFi field to take part in it.

According to the Draft Decree, entities with innovative technology application solutions such as blockchain, and other services supporting banking activities (e.g. savings, capital mobilization, etc.) are welcome to participate in the pilot implementation. The Draft Decree expressly requires that only business entities established and operating in Vietnam are eligible to apply for the Sandbox Program. Currently, the Government allows the SBV to continue to receive comments and contributions from Government members on the Draft Decree.[15]

To obtain a Sandbox Certificate for DeFi services, the solutions offered by participating companies must meet all the requirements of the draft decree, including but not limited to the

15 Government Resolution No. 100/NQ-CP dated September 6, 2021 approving the proposal to develop a decree on a controlled pilot implementation for financial technology (fintech) activities in the banking sector.

following key points:[16]

- "The solution is fully or partially unregulated by Vietnamese laws;
- The solution must be a creative solution, applied for the first time in Vietnam [...];
- The solution must be equipped with a good risk management system, without or with little possibility of having adverse impact on financial institutions and the financial sector of Vietnam, and capable of tackling and reducing risks during the Sandbox Program; and
- The solution does not pose any risks possibly resulting in financial and economic disorder."

When making its assessment, the SBV and each subject entity will engage in discussions as to the scope of operation of such solution/service in terms of (i) applied geographic areas; (ii) transaction limitation; and (iii) number of customers using the service.

The duration of the Sandbox Program in Vietnam, including that of DeFi lending, is up to two years from the date of issuance of approval from the Prime Minister. The duration will vary depending on the solution and relevant area and is subject to the Prime Minister's discretion. Extensions of periods of less than one year are possible subject to the Prime Minister's approval.[17] Upon completion of the Sandbox Program, the SBV at its discretion can make a request to the Prime Minister for the issuance of a certificate of completion of the Sandbox Program, which will serve as the basis for the entity to legally provide the relevant services to the Vietnam.[18]

CONCLUSION

Although the Vietnamese market has actively embraced DeFi, lawmakers and regulators have lagged in providing clear regulations. DeFi lending can develop in a more certain way when the regulations are ready.

Vietnam's Sandbox Program provides a useful space for collaboration between innovators and regulators and will hopefully lead to responsible innovation and, ultimately, the development and promulgation of clearer regulation.

16 Article 9, Draft Decree.

17 Article 12, Draft Decree.

18 Article 13, Draft Decree.

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