JOURNAL OF EMERGING ISSUES IN LITIGATION

Tom Hagy
Editor-in-Chief

Volume 2, Number 4
Fall 2022

Editor's Note: New Money, New Expectations, New Technologies: Litigation and Regulations Responding to Rapid Change
Tom Hagy

Insurance Coverage for Digital Assets: Mitigating Losses in Cryptocurrency and Non-Fungible Token Markets
Scott DeVries, Jessica Cohen-Nowak, and Adriana Perez

The Environmental, Social, and Governance Police Have Arrived: Is Your Insurance Ready?
Robert D. Chesler and Dennis J. Artese

Litigating a Claim to Recover Liquidated Damages: Enforceability Depends on Evidence of Good Faith Expectations
Laura Fraher

Government Involvement in Personal Medical Care Decisions During Outbreaks of Disease: How Far Is Too Far?
Bryce McColskey and Sandra M. Cianflone

EMR Audit Trail—What Is It? Why Do They Matter? What Should You Look For?
Haley K. Grieco and Brooke E. Reddin

Flying Cameras: Gaps in Drone Regulation and How Courts Can Fill Them . . . For Now
Kathryn M. Rattigan and Blair Robinson

Employers Be WARNed: Workforce Reduction Rules Meet New Workplace Definitions as Employees Go Remote
Juan Enjamio and Steven DiBeneditto

fastcase FULL COURT PRESS

Journal of Emerging Issues in Litigation

Volume 2, No. 4 Fall 2022

249 **Editor's Note: New Money, New Expectations, New Technologies: Litigation and Regulations Responding to Rapid Change**
Tom Hagy

255 **Insurance Coverage for Digital Assets: Mitigating Losses in Cryptocurrency and Non-Fungible Token Markets**
Scott DeVries, Jessica Cohen-Nowak, and Adriana Perez

277 **The Environmental, Social, and Governance Police Have Arrived: Is Your Insurance Ready?**
Robert D. Chesler and Dennis J. Artese

285 **Litigating a Claim to Recover Liquidated Damages: Enforceability Depends on Evidence of Good Faith Expectations**
Laura Fraher

293 **Government Involvement in Personal Medical Care Decisions During Outbreaks of Disease: How Far Is Too Far?**
Bryce McColskey and Sandra M. Cianflone

301 **EMR Audit Trail—What Is It? Why Do They Matter? What Should You Look For?**
Haley K. Grieco and Brooke E. Reddin

309 **Flying Cameras: Gaps in Drone Regulation and How Courts Can Fill Them . . . For Now**
Kathryn M. Rattigan and Blair Robinson

317 **Employers Be WARNed: Workforce Reduction Rules Meet New Workplace Definitions as Employees Go Remote**
Juan Enjamio and Steven DiBeneditto

EDITOR-IN-CHIEF

Tom Hagy

EDITORIAL ADVISORY BOARD

Dennis J. Artese
Anderson Kill P.C.
General and climate change insurance

Hilary Bricken
Harris Bricken
Cannabis

Robert D. Chesler
Anderson Kill P.C.
General and climate change insurance

Sandra M. Cianflone
Hall Booth Smith P.C.
Health care and medical

Joshua Davis
Center for Law and Ethics
University of San Francisco
School of Law
Class actions and ethics

Scott P. DeVries
Hunton Andrews Kurth LLP
Insurance and complex litigation

Laura A. Foggan
Crowell & Moring LLP
Insurance and reinsurance

Scott M. Godes
Barnes & Thornburg LLP
General insurance and cyber insurance

Katherine V. Hatfield
Hatfield Schwartz LLC
Labor

Charlie Kingdollar
Insurance Industry Emerging
Issues Officer (ret.)
Insurance coverage and emerging claims

Judah Lifschitz
Shapiro, Lifschitz & Schram, P.C.
Construction

Dan Mogin
MoginRubin LLP
Antitrust and class actions

Jennifer M. Oliver
MoginRubin LLP
Antitrust, data security, and class actions

Edward L. Queen, Ph.D., J.D.
Center for Ethics, Emory University
Ethics

Kathryn M. Rattigan
Robinson & Cole LLP
Drone technology

Jonathan Rubin
MoginRubin LLP
Antitrust and class actions

Dowse Bradwell "Brad" Rustin IV
Nelson Mullins Riley &
Scarborough LLP
Fintech

Stefani C Schwartz
Hatfield Schwartz LLC
Employment

Judith A. Selby
Kennedys Law LLP
Insurance and emerging technologies

Jeff Trueman
JeffTrueman.com
Mediation and Arbitration

Newman Jackson Smith
Nelson Mullins Riley & Scarborough
LLP
Energy, climate, and environmental

Vincent J. Vitkowsky
Gfeller Laurie LLP
Insurance, security, and cybersecurity

John Yanchunis
Morgan & Morgan
Class actions

JOURNAL OF EMERGING ISSUES IN LITIGATION at $395.00 annually is published four times per year by Full Court Press, a Fastcase, Inc., imprint. Copyright 2022 Fastcase, Inc. No part of this journal may be reproduced in any form—by microfilm, xerography, or otherwise—or incorporated into any information retrieval system without the written permission of the copyright owner. For customer support, please contact Fastcase, Inc., 711 D St. NW, Suite 200, Washington, D.C. 20004, 202.999.4777 (phone), 202.521.3462 (fax), or email customer service at support@fastcase.com.

Publishing Staff
Publisher: Morgan Morrissette Wright
Production Editor: Sharon D. Ray
Cover Art Design: Morgan Morrissette Wright and Sharon D. Ray

Cite this publication as:

Journal of Emerging Issues in Litigation (Fastcase)

This publication is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

Copyright © 2022 Full Court Press, an imprint of Fastcase, Inc.

All Rights Reserved.

A Full Court Press, Fastcase, Inc., Publication

Editorial Office

711 D St. NW, Suite 200, Washington, D.C. 20004
https://www.fastcase.com/

POSTMASTER: Send address changes to JOURNAL OF EMERGING ISSUES IN LITIGATION, 711 D St. NW, Suite 200, Washington, D.C. 20004.

Articles and Submissions

Direct editorial inquiries and send material for publication to:

Tom Hagy, Editor-in-Chief, tom.hagy@litigationconferences.com

Material for publication is welcomed—articles, decisions, or other items of interest to attorneys and law firms, in-house counsel, corporate compliance officers, government agencies and their counsel, senior business executives, scientists, engineers, and anyone interested in the law governing artificial intelligence and robotics. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the Editorial Content appearing in these volumes or reprint permission, please contact:

Morgan Morrissette Wright, Publisher, Full Court Press at mwright@fastcase.com or at 202.999.4878

For questions or Sales and Customer Service:

Customer Service
Available 8am–8pm Eastern Time
866.773.2782 (phone)
support@fastcase.com (email)

Sales
202.999.4777 (phone)
sales@fastcase.com (email)

Insurance Coverage for Digital Assets: Mitigating Losses in Cryptocurrency and Non-Fungible Token Markets

Scott DeVries, Jessica Cohen-Nowak, and Adriana Perez*

Abstract: *Companies and individuals are riding the ups and downs of cryptocurrency and NFTs—with losses and swings in the billions of dollars—but digital assets are not going away. The risk of loss in certain categories may be mitigated by insurance, whether provided by tailored policies and/or under policies designed specifically for digital asset owners. Those with exposure to the digital asset sector should be attuned to the emerging marketplace for such insurance products. While it is early days for NFT-specific coverage, the rise of cryptocurrency has created a substantial marketplace for crypto coverage. Insurers are becoming increasingly able to model and assess risk, so more products are coming to market. That said, digital asset holders need to be able to select coverage that best suits their needs. In this article, the authors discuss the history and status of coverage for digital assets to assist readers in exploring how they might use insurance to mitigate risk in this emerging and rocky sector of global finance.*

Crypto markets are experiencing the greatest crash in their history to date. The value of a Bitcoin has plummeted 70% from its peak and Ethereum has fallen 77%. Since last November, the value of cryptocurrency tokens has lost $2 billion in value.[1] As noted financial publication *Barron's* put it: "Crypto is having a 'Lehman moment,' a shattering of confidence triggered by plunging asset prices, liquidity freezing up, and billions of dollars wiped out in a few scary weeks."[2] Cryptocurrency companies are halting

Journal of Emerging Issues in Litigation / Fall 2022, Vol. 2, No. 4, pp. 255–276.
© 2022 Full Court Press. All rights reserved.

withdrawals and transfers, platforms are seizing up, and regulators are circling.[3]

The devastation has not been limited to the coins themselves. Non-fungible token (NFT) sales have reduced by 90% since September 2021.[4] The *New York Times* reported that Opensea.io (OpenSea), an NFT marketplace that receives 2.5% share of the proceeds for each NFT sale, has been plagued by "a surge of plagiarism, as sellers convert traditional artwork into NFTs and then list the images for sale without compensating the original creator."[5] For example, DeviantArt, an artist collective that scans OpenSea for copyright infringement of the work of its artists, found 290,000 instances of unauthorized NFTs copying its artists' works.[6] While infringing listings can be deleted in response to takedown requests filed by the artist, buyers of counterfeit NFTs are rarely given a refund.

Against this backdrop, the issue of whether there may be claims associated with cryptocurrency and NFTs is far from a theoretical or esoteric thought exercise. It is very real. And when there are claims, businesses and investors doubtless will look to their insurers.

A business or home is devastated by a wildfire. Property insurance is available up to limits. A home is broken into, and art and jewelry are stolen. Crime/specie insurance is available.

But what about new age assets? What about cryptocurrency? What about NFTs? These obviously are not immune from theft by hackers. In 2021, hackers stole at least $3.2 billion in cryptocurrency with schemes short of outright theft accounting for another $7.8 billion.[7] In the first four months of 2022, NFT hacks accounted for $52 million in losses, an almost eight-fold increase from 2021.[8]

There typically is a significant time lag between the development of a product and the availability of product-specific insurance. This general proposition applies with equal force here. Over the course of a decade, the marketplace for cryptocurrency has increased from zero to an estimated $250 billion. However, only $6 billion in insurance coverage is currently available. It would be a gross understatement to say that there is a truly remarkable imbalance between market value and insurance capacity.

Although NFTs have been around for the better part of a decade, it was only during the past two years that the marketplace has grown to upward of $41 billion.[9] In addition to its newness,

NFTs pose additional risks for insurers, including questions of ownership, authenticity, and the valuation of a truly "unique" asset. Consequently, availability of insurance coverage for NFTs is even further behind.

Given the rapid rate at which the digital asset field is developing, and claims are emerging, and the insurance industry's attempts to specifically address coverage for these losses and claims, anything written on this topic will, at least in part, be outdated by the time it is published. The objective of this article is to educate the reader on the history and status of the field, enabling them to ask the questions they need to ask, and to procure the coverage they need if available now or in coming months.

Key Cryptocurrency/NFT Terminology

Like many areas, the field of digital assets has its own jargon. A brief refresher follows.

- *What is blockchain?* A blockchain is a decentralized, publicly distributed, digital ledger consisting of records called "blocks" that are used to record transactions.
- *What is cryptocurrency?* A cryptocurrency is a digital form of money. Unlike physical money, cryptocurrencies are not created, regulated, or issued by governments or other financial institutions (i.e., The Federal Reserve). Instead, they are created and secured online through "cryptographic" algorithms with a decentralized network of computers validating and maintaining the transactions. Bitcoin is the biggest and most well known while others have emerged like Ethereum.
- *What is a cryptocurrency exchange?* An exchange is a digital marketplace where cryptocurrencies can be traded. Different exchanges have different options and features.
- *What is an NFT?* An NFT, or non-fungible token, is a non-interchangeable or unique and authenticated unit of data stored on a blockchain. Types of NFT data units may be associated with digital files such as images of art, photos, music, film, and games.

- *What is a wallet?* Digital assets may be secured offline or online. Storage offline on a piece of hardware akin to a USB drive is referred to as a "cold wallet." In contrast, a "hot wallet" is maintained in a digital form online. Like a PIN number at a bank account, a hot wallet is accessed through a private digital key.

Who Can Incur Losses Associated With Digital Assets?

Who can incur losses associated with cryptocurrency or digital assets? The real question is who uses them.

Among the most obvious users would be exchanges in which cryptocurrency is traded. It has been reported that the largest insurance market in the cryptocurrency industry consists of exchanges that insure against thefts from cryptocurrency hackers. Among the more prominent exchanges are Coinbase, Crypto.com, and Gemini. Similarly obvious are the third-party custodians that store cryptocurrency and other forms of digital assets on consumers behalf such as BNY Mellon Crypto Currency or Fidelity Digital Assets. They provide safekeeping of digital assets, including keys, and ensure accessibility.

However, usage is far more expansive with the penetration of cryptocurrency and digital assets into the economy expanding in an almost parabolic manner since its inception. A 2020 survey released by HSB reports that "[a]t least one-third of U.S. small and medium-sized businesses accept cryptocurrency as payment for goods and services…with newer companies up to twice as likely to trade in digital credits."[10] The survey adds that 59% of the companies that accept cryptocurrency also purchased it for their own use.[11] Deloitte reported by late 2020, more than 2,300 businesses in the United States accepted bitcoin.[12]

And market penetration is not limited to businesses. While a 2015 Pew Research Center survey reflected that 1% of the population "collected, traded or used" cryptocurrency, a survey conducted six years later in September 2021 found the percentage had increased to 16%.[13] Given the demographic tilt of users with higher usage among younger adults (e.g., 31% of all adults between 18 and

29) reported in the survey, adult usage can be expected to continue to increase over time. This is all the more so given the increasing levels of mainstream and web-based advertising featuring personalities like Matt Damon (crypto.com) and Stephen Curry (FTX).

Potential Risks of Loss and Liability Related to Digital Assets

The risk of loss or liability associated with digital assets presents in many ways.

Like stock trading, crypto-based asset investments risk a loss due to price fluctuation and market crashes. Loss due to price fluctuation will affect any individual or company that buys, sells, accepts, or relies on cryptocurrency in any form. It also affects the value of NFTs that were previously sold at a significantly higher exchange rate.

However, the digital asset context also presents some very different forms of loss and liability. Loss on both small and large scales occurs frequently through hacking thefts. Relatedly, cryptocurrency exchange or wallet-security software companies are beginning to face liability for their failure to protect users from (or quickly react to) hackers. Unsurprisingly, it has been reported that the largest insurance market in the cryptocurrency industry consists of exchanges that insure against hackers. However, the type of hack may affect whether the hacking victim has any recourse against the exchange or access to insurance.

Particularly as respects NFTs, a large portion of the recent litigation (and liability) in this industry concerns claims of intellectual property infringement.

These and other claims associated with digital assets may be covered under traditional and/or new insurance products—subjects addressed in the following sections.

Traditional Insurance Products and Issues

In the early years of cryptocurrency, there were no crypto-specific insurance coverages. Instead, policyholders sustaining

losses were left to try to access coverage under traditional insurance policies such as:

- Directors and officers (D&O) policies (breach of duty, securities violation, regulatory investigation).
- Commercial crime policies: "[T]ypically provides several different types of crime coverage, such as: employee dishonesty coverage; forgery or alteration coverage; computer fraud coverage; funds transfer fraud coverage; kidnap, ransom, or extortion coverage; money and securities coverage; and money orders and counterfeit money coverage."[14]
- Specie policies (endorsement to a crime policy covering specifically scheduled high-value assets like fine art and jewelry).
- Cyber policies: While there is much variance among these policies, they typically cover ancillary costs, notification of breach, resolution of identity theft issues, recovery of lost or compromised data, network interruption, responding to cyber-extortion, repair of computer systems, and sometimes business loss. They generally do not compensate for stolen assets.[15]
- Errors and omissions policies: Typically "protects the insured against liability for committing an error or omission in performance of professional duties. Generally, such policies are designed to cover financial losses rather than liability for bodily injury (BI) and property damage (PD)."[16]
- First-party policies: Insurance applying to the policyholder's own property (e.g., home insurance).
- Third-party (otherwise referred to as commercial general liability) policies: Insurance applying to claims made against the insured by third parties. This coverage often contains a duty to defend the policyholder from third-party claims as well as a duty to indemnify the policyholder for the costs of settlement or judgment.
- Kidnap and ransom coverage: Often available for purchase through crime policies (though policy provisions often prevent the policyholder from disclosing their existence).[17]

Because these policies were not designed for the unique features of cryptocurrency and digital assets such as NFTs, early commentators discussed the existence of various potential obstacles to coverage.[18]

Frequently discussed is whether the loss involved "covered property." Many crime policies define this to include "money, security, or other property" with "money" defined as currency, coins and bank notes in current use and having a face value, or traveler's checks. Insurers maintain that cryptocurrency does not reasonably come within the definition of "money." Securities typically are held to be negotiable or non-negotiable instruments or contacts, a class of assets that cryptocurrency likewise may not satisfy. And insurers often maintain, on the basis of older cases, that tangible property does not include data (though, given current knowledge concerning computer data, it is difficult to envision any court reaching a similar outcome).[19] As a counterpoint, the IRS treats cryptocurrency as property and taxable.[20,21] Insurers also may assert other issues such as whether there was a physical loss, coverage for contract exposures or regulatory seizure as a cause of loss, and proof of ownership. And while not an exclusion, fluctuation of cryptocurrency prices may result in substantial issues regarding valuation.

This is not to say that these defenses are viable or should be successful, but rather that they are reflective of types of arguments insurers may make in an attempt to avoid coverage under traditional policies.

On the other hand, insurers should readily acknowledge that some of these traditional insurance policies, such as errors and omissions or third party, cover litigation and liability costs for defending certain claims, such as copyright infringement, trademark infringement, and false advertising.

History of Insurance Coverage Specifically Designed for Cryptocurrency

In the eighteenth century, underwriting desks at what came to be known as Lloyd's of London were developed to share or transfer risks associated with shipping.[22] Availability of risk sharing, or insurance, provided protection for maritime investors and

facilitated increased levels of investment and thus increased levels of maritime activity. Risk transfer has become an essential part of the development of a marketplace for many products.

In the early years of cryptocurrency, there were no insurance products specifically designed to cover cryptocurrency-related losses. Much like the presence of insurance fosters development of a marketplace, the absence of insurance hinders it.

This started to change in June 2014, when Great American Insurance Company began insuring bitcoin losses, issuing bitcoin-specific endorsements covering criminal acts of employees.[23] The underwriting process required, among other things, satisfactory responses to questions concerning audits of internal control processes.[24]

While early crime policy forms were silent concerning virtual currency, this changed in 2015 when the Insurance Services Office (an entity charged with drafting policy language for the insurance industry) developed a Commercial Crime Policy form that broadly excluded any form of "virtual currency." Contemporaneously, it created a "Virtual Currency as Money" endorsement that revised the definition of money to include virtual currency but required the policyholder to provide a schedule listing the cryptocurrency to be covered and subject to sublimit.[25]

Also in 2015, The Bitcoin Financial Group LLC created The Bitcoin Insurance Agency, which it touted as the first insurance and financial services company specifically created to handle the insurance needs, from the routine to the unique, of companies in the bitcoin industry.[26] It offered a "Bitcoin Theft Insurance" policy covering any act, error, or omission of the insured that resulted in theft of insured bitcoins or their related private keys. This coverage extended to hot and cold storage.

The following year, Elliptic Enterprise Ltd. created Elliptic Vault, which stores bitcoin in cold storage. Keys needed to access the bitcoin are encrypted and stored offline where they were protected with layers of cryptographic and physical security, and only accessible to a quorum of Elliptic's directors. It was insured for loss or theft of bitcoin holdings by Lloyds companies.[27]

Products were not limited to the US and UK markets. Later in 2016, Mitsui Sumitomo codeveloped an insurance product, bitFlyer,

with the Japanese Bitcoin exchange.[28] It covered damages and losses caused by hacking incidents, unauthorized access, other cyber-attacks, human error, and impropriety by employees. The product was available for the domestic Japanese bitcoin market and also covered costs incurred while dealing with international lawsuits.

Coverage was not limited to the traditional vehicle of insurance policies. There has even been a kind of crowdfunding "insurance" issued through Nexus Mutual Decentralized.[29]

It bears note that it is commonplace in the insurance industry for new insurance companies to be created when product prices peak; reliance on these sorts of new companies, however, may present its own risks.

Since then, the marketplace has continued to expand both in terms of available insurance companies and products as discussed in the next section.

How Companies and Consumers With Cryptocurrency Risk Approach Insurance

The prior discussion focused on the evolution of the insurance marketplace for digital assets. This section focuses on the market-place as it now exists, providing examples of products being bought by companies and consumers facing cryptocurrency risks.

Cryptocurrency theft is no abstract concept. As *Bloomberg* reported in January of 2022, "Crypto.com said customer accounts that held about $34 million in cryptocurrencies and cash were hit by unauthorized withdrawals. Hackers seized more than $80 million of digital assets from a blockchain extension by Qubit Finance last week."[30] And unlike bank accounts that are insured by the FDIC for amounts up to $250,000 per account, this insurance currently is limited to monies (*viz.*, legal tender) in checking, savings, and money market accounts at banks and does not extend to crypto-currency holdings.[31]

As in any marketplace, some companies are fully self-insured (or bare), some are partially self-insured, and some have consider-able amounts of insurance although the nature, scope, and amount vary widely.

Some of the major exchanges and custody providers reportedly have policies with $100+ million limits.

For example, Coinbase reportedly has a $255 million crime policy available for losses sustained due to platform wide breaches,[32] warning investors in boldface type that its crime policy "does not cover any losses resulting from unauthorized access to your personal Coinbase account due to a breach or loss of your credentials."[33]

Bitstamp insures assets held in the BitGo and Copper wallets it uses (95% of its stored digital assets are in cold storage).[34] This is supplemented by a $300 million crime policy issued through London and other companies which "applies to digital assets held at Bitstamp either offline or online and covers an array of crime-related cases. These include employee theft, loss while the assets are stored at any premises, loss in transit, loss caused by computer fraud or funds transfer fraud, as well as loss related to legal fees and expenses."[35]

Meanwhile, Blockfi has theft insurance through its custodial wallet Gemini.[36]

In addition to insurance policies providing crime coverage, the larger exchanges also may seek to transfer or mitigate their risk through other options. Some, like Gatehub, make insurance available through wallets, with customers having the ability to insure all or some of the contents.[37] Others reportedly divert 10% of all trading fees into a self-managed fund. For example, earlier this year, Binance Holdings Ltd. reported that it has been earmarking monies since 2018 and has accumulated a $1 billion "insurance" fund for its users.[38]

The decision to obtain insurance or determine the appropriate coverage may vary with how coins and wallets are stored. Some companies cover only "cold storage" because the coins are kept offline and are at lower risk of hacking. Other companies offer insurance for "warm" or "hot" storage (recognizing that online storage creates increasing levels of exposure and threat of potential hacks).

Historically, most cryptocurrency insurance products were not targeted to consumers (*i.e.*, individual traders). In early 2022, however, Breach Insurance Company announced the launch of a "Crypto Shield" product that reportedly is the first insurance

product for crypto investors.[39] This theft insurance, available in selected states, covers hacks of over 20 types of cryptocurrencies for customers using Binance US, Coinbase, CoinList, and Gemini.

Coincover provides security services and limited coverage for individuals holding assets in nearly 20 wallets and exchanges including Crypto.com, FTX, and Coinbase.[40] Among other things, it covers theft of digital currency resulting from a security breach or hack, employee theft, or fraudulent transfer, with an insurance guarantee from Lloyds for loss of access or stolen funds. Coincover policies can provide a "dynamic limit" that increases/decreases in line with price fluctuations of cryptocurrency. "Standard" plans ($159/year) provide up to $10,000 in coverage for lost or hacked funds from multiple wallets, a higher-priced "Pro" Plan providing $100,000 in coverage ($749/year) for more wallets with higher levels of protection is available upon request.

BitGo likewise provides detail on its website.[41] It has secured a $250 million policy through London and other European companies covering digital assets "where the private keys are held 100% by BitGo Trust Company or BitGo, Inc. in the event of: Copying and theft of private keys, Insider theft or dishonest acts by BitGo employees or executives, [and] Loss of keys."[42] This insurance is provided at no cost to BitGo clients who may purchase additional insurance as needed.

In deciding whether to write a new line of insurance, and settling on the terms of coverage, insurers look for as much certainty as possible, considering analogous risks to assist in modeling and the availability of a robust set of regulations/rules. In the latter regard, future guidance and clarity from the SEC and the Office of Comptroller and Currency may be helpful in the underwriting process.

As is apparent, insurance products have been and continue to be developed to cover cryptocurrency assets. There are several reasons to consider purchasing this insurance. It can serve the traditional purpose of reducing exposure through risk transfer. Insurer experience may assist in risk assessment/mitigation (though this may require audits and background checks). And it may assist the company in marketing the availability of insurance increasing the customer's comfort level.

Cost of Insuring Cryptocurrency

It is a truism in insurance underwriting that the threat or risk level materially and directly influences the cost; as one increases, so too does the other.

Applying this concept here, premiums associated with cryptocurrency coverage are higher than for non-cryptocurrency-related coverages. For example, an early article reported that $10 million in cryptocurrency theft coverage could cost 2% of limits as contrasted to 1% or less for traditional claims.[43] More recently, FIT Small Business reported in December 2019 that while a standard crime insurance policy costs less than 0.5% of assets covered, cold storage premiums may be in the range of 0.8%–1.2% and hot storage premiums in the range of 3–5%.

Role of Brokers in Obtaining Cryptocurrency Insurance

Several of the largest brokers have developed a considerable bench. For example, Marsh has a Digital Asset Risk Team (DART)[44]; Lockton has its Lockton Emerging Asset Protection Team (LEAP)[45]; and Aon and others have their own teams.[46]

There are multiple advantages to procuring cryptocurrency insurance through brokers that have deep experience in this particular area of insurance. These may include:

- Access to markets—especially overseas ones like London.
- Assistance in the design of cryptocurrency insurance programs. For example, there are public reports of Marsh working with Arch in covering $150 million in digital assets secured by the Ledger Vault Security Firm,[47] as well as its work with Munich Re for Curv.[48]
- Assistance sorting through the array of insurance companies offering products. Much like businesses have their own risk profile, so do insurers, and insurance is only as good as the insurer; brokers can provide valuable assistance in sorting through the array of potential insurers and helping policyholders to select those with

appropriate experience, balance sheets, ratings, and other factors to maximize the fit.

Insurance for NFTs

As discussed above, the insurance industry has developed an array of policies specifically tailored to cover cryptocurrency claims, and some of these policies may also cover certain NFT claims. Separate and apart from these tailored policies, policyholders with NFT claims also may look to traditional forms of insurance.

NFTs are collectible and one of a kind, yet digital. The most common NFT is a type of visual art image like a digital painting, a photograph, or generative designs (created by artificial intelligence). However, this high-level definition doesn't do justice to just how pervasive these have become. In addition to traditional artwork, there are:

- Sports, movie, or other collectible NFTs are tokenized collectibles. Sports collectibles include trading cards, jerseys, and photos containing digitized images/videos of players. As an example, LeBron James NFTs have sold for $230,000.[49] Movie collectibles include digitized versions of scripts and movie posters, such as when DC recently released a Batman collection of NFTs with images drawing on the 83-year history of Batman comics.[50]
- Music NFTs are tokenized albums, songs, and/or music videos. Music NFTs may provide simple streaming access (and a higher royalty opportunity for the artist than typical streaming) or even concert access. Artist 3LAU, auctioned 33 NFT collectible versions of his album *Ultraviolet*, for a total of $11.7 million.[51]
- Gamified NFTs are assets that can be collected to use within a game experience or to gain access to a particular video game. For example, ZED RUN is a digital horse racing game with NFTs available in a variety of unique breeds and themed skins.[52]

There are even digitized images of tweets, such as the highly publicized first tweet from Twitter President Jack Dorsey.[53]

Before the most recent market crash, the media feverishly reported on the rise of the NFT economy over the past two years. In particular, they have focused on high-value art auction sales (even though most sales occur through peer-to-peer marketplaces like OpenSea). For example, artist Mike Winkelman's (aka "Beeple") compilation of 5,000 images into a singular NFT was sold for $69.3 million at a Christie's auction in March 2021. The entrance of Christie's, Sotheby's, and other auction powerhouses has, for some, legitimized NFT transactions as equivalent to other art sales.

Like non-digitized art, NFTs are subject to theft. Hackers are targeting the logins of digital wallets or marketplace user accounts to move NFTs and sell them as their own. Some of these hacks have caused NFT investors to lose millions in assets. For example, one account reports that thieves stole $2.2 million worth of NFTs from an individual's wallet. In another reported hack, $1.7 million in NFTs was stolen from various OpenSea users. In some instances, the marketplace, such as OpenSea, reacts by delisting the second sale (by the hacker) but typically does not reverse sales or retrieve the stolen assets for the original owner.

The most pervasive issue among NFTs is the prevalence of unauthorized copyright-protected works. For example, artist Aja Trier's viral "Vincent Van Gogh-style paintings" were turned into 86,000 different NFTs by an unauthorized third party.[54] Importantly, artists report that filing takedown requests to remove infringements on NFT marketplaces has been, for the most part, inefficient. As a result, most artists will be required to turn to litigation to enforce their rights.

Unlike traditional high-value art, where the provenance can typically be authenticated back to the original artist, an NFT creator often has anonymity, which complicates confirming that the NFT is the product of an original creation or an unauthorized replica of someone else's work. Thus, the ledger-based code that authenticates sale transactions in a transparent way may not assist in ensuring authenticity of the art itself. This poses a risk that the NFT may be essentially worthless after a purchase (as it cannot be resold if it is a counterfeit).[55]

In a traditional context of non-digitized art, these assets would be covered by various types of insurance (art, for example, would be scheduled and covered by specie insurance under a crime policy). Infringement-related claims asserted against an NFT creator and/or the NFT marketplace may be covered by traditional coverages such as errors and omission or third-party insurance as well as others.

However, the insurance industry has been slow to develop and issue policies specifically tailored to encompass digitized products. In fact, as of the date this article is published, only one insurance product has generally been made available, through CoinCover.[56] While YAS Digital Limited announced a micro insurance product specifically covering NFTs in the fine arts field in April 2021, and followed this during the next month with announcements that it would issue coverage for additional NFTs, its website is silent on the subject, there has been no subsequent media attention concerning its participation in NFT coverage, and further monitoring is warranted.[57]

There are several reasons why the insurance market has been so tepid to enter the NFT space. First, as mentioned above, non-digitized artwork can be readily authenticated and blockchain ledgers by design can be established. While there may be ways to authenticate the NFT, insurers have yet to be satisfied with these solutions because there may be challenges to authenticating the NFT creator's ownership of the underlying rights to the name or image of the NFT.

Second, there may be considerable uncertainty when valuing digital property, especially where there are few if any comparable sales. This is perhaps best illustrated by the Jack Dorsey tweet referenced above that initially sold for $2.9 million in 2021 and, in an auction one year later on April 22, 2022, sold for only $6,800.[58]

Given the expanding value of the NFT marketplace, the insurance industry doubtless is considering ways to provide a tailored insurance product. Until they do, NFT holders are left with arguments that their NFTs are covered under existing crime, specie, professional liability, errors and omissions, third party, directors and officers, and other coverages and would be well advised to provide their insurer with a schedule at least as detailed as that which is provided for non-digitized artwork.

Conclusion

Companies and individuals that have sustained (and are sustaining) losses associated with cryptocurrency and NFTs may have access to insurance, whether under tailored policies and/or under digital asset–specific policies. They would be well advised to assess all available products and discuss with their brokers and lawyers specializing in the field.

On a forward going basis, those with exposure to the digital asset sector should be attuned to the emerging marketplace for insurance products. While the field of insurance specific to NFTs is in the nascent stage, the increasing prevalence of cryptocurrency has created a substantial marketplace for crypto-specific insurance. As insurers become increasingly able to model and assess risk, they are making more insurance products available. The coverages are far from unique, and it is important for digital asset holders to understand the types of products available and determine which ones fit its particular needs. Doing so will better enable the digital asset holder to respond to the insurer if and when a claim arises.

Notes

* Scott DeVries (sdevries@huntonak.com) is Special Counsel at Hunton Andrews Kurth and long-time insurance coverage attorney for policyholders in a range of complex disputes as well as mass torts, class action, product liability, and complex business litigation. Jessica Cohen-Nowak (jcohen-nowak@huntonak.com) is an associate in Hunton Andrew Kurth LLP's Intellectual Property group in the firm's New York office. Jessica focuses her counseling and litigation practice on intellectual property matters in the fashion, fitness, entertainment, hospitality, and gaming industries as well as in technology and digital assets. Adriana Perez (pereza@huntonak.com) is an associate in the firm's Miami office where she focuses on insurance, reinsurance, and other business litigation.

1. Joe Light, *Crypto Winter Could Become Crypto Hell*, Barron's (June 20, 2022).

2. *Id.*

3. The White House, Executive Order on Ensuring Responsible Development of Digital Assets (Mar. 9, 2022), https://www.whitehouse.gov/briefing-room/presidential-actions/2022/03/09/executive-order-on-ensuring-responsible-development-of-digital-assets/.

4. David Yaffe-Bellany, *Thefts, Fraud and Lawsuits at the World's Biggest NFT Marketplace*, New York Times (June 6, 2022).

5. *Id.*

6. *Id.*

7. Aaron M. Lane, *Crypto theft is on the rise. Here's how the crimes are committed, and how you can protect yourself*, The Conversation (Feb. 3, 2022, 12:59 AM EST), https://theconversation.com/crypto-theft-is-on-the-rise-heres-how-the-crimes-are-committed-and-how-you-can-protect-yourself-176027.

8. *Losses from NFT crimes up 667% in 2022 compared to whole of 2021: Report*, Mint (May 9, 2022, 06:01 PM IST), https://www.livemint.com/market/cryptocurrency/losses-from-nft-crimes-up-667-in-2022-compared-to-whole-of-2021-report-11652099260806.html.

9. *NFT Insurance Is Coming, but Is There an Industry to Support It?*, PYMNTS.com (Mar. 3, 2022), https://www.pymnts.com/nfts/2022/nft-insurance-is-coming-but-is-there-an-industry-to-support-it.

10. *One-Third of Small Businesses Accept Cryptocurrency. Do They Understand the Cyber and Financial Risks?*, HSB (Jan. 15, 2020), https://www.munichre.com/hsb/en/press-and-publications/press-releases/2020/2020-01-15-one-third-of-small-businesses-accept-cryptocurrency.html.

11. *Id.*

12. *The rise of using cryptocurrency in business*, Deloitte, https://www2.deloitte.com/us/en/pages/audit/articles/corporates-using-crypto.html (last visited July 12, 2022). *See also* Judy Greenwald, *Some insurers accept premium payments in cryptocurrency*, Business Insurance (Apr. 1, 2022), https://www.businessinsurance.com/article/20220401/STORY/912348700/Some-insurers-accept-premium-payments-in-cryptocurrency?ticks=637836230060262412&ticks=637836230060262412, reporting that the companies include insurance companies such as Universal Fire & Casualty Insurance Co. and Axa S.A.'s Swiss unit.

13. Andrew Perrin, *16% of Americans say they have ever invested in, traded or used cryptocurrency*, Pew Research Center (Nov. 11, 2021),

https://www.pewresearch.org/fact-tank/2021/11/11/16-of-americans-say-they-have-ever-invested-in-traded-or-used-cryptocurrency/.

14. *Commercial Crime Policy, Definition*, International Risk Management Institute, Inc. (IRMI), https://www.irmi.com/term/insurance-definitions/commercial-crime-policy#:~:text=A%20commercial%20crime%20policy%20typically,and%20money%20orders%20and%20counterfeit (last visited July 11, 2022).

15. *Cyber and Privacy Insurance, Definition*, IRMI, https://www.irmi.com/term/insurance-definitions/cyber-and-privacy-insurance (last visited July 11, 2022).

16. *Errors and Omissions (E&O) Insurance, Definition*, IRMI, https://www.irmi.com/term/insurance-definitions/errors-and-omissions-insurance#:~:text=Errors%20and%20Omissions%20(E%26O)%20Insurance%20%E2%80%94%20an%20insurance%20form%20that,and%20property%20damage%20(PD) (last visited July 11, 2022).

17. *Kidnap and Ransom Insurance, Definition*, IRMI, https://www.irmi.com/term/insurance-definitions/kidnap-and-ransom-insurance (last visited July 11, 2022).

18. *See, e.g.*, Abramowicz, Michael B., Blockchain-Based Insurance (2019). Blockchain-Based Insurance, in Blockchain and the Constitution of a New Financial Order: Legal and Political Challenges.

19. *See, e.g.*, *Ward Gen. Ins. Servs., Inc. v. Employers Fire Ins. Co.*, 114 Cal. App. 4th 548 (2003); *Am. Online, Inc. v. St. Paul Mercury Ins. Co.*, 347 F.3d 89, 96 (4th Cir. 2003).

20. *See, e.g.*, *Kimmelman v. Wayne Insurance Group*, No. 18 CV 1041, 2018 WL 11417314, at *2 (Ohio Com. Pl. Sept. 25, 2018) (Court relied on IRS federal tax valuation to hold that virtual currency is treated as property.).

21. Similarly, the current version of the ISO form for third-party liability coverage, CG 00 01 04 13, contains a provision to the effect that "electronic data is not tangible property" and also contains an exclusion for electronic data, https://www.google.com/search?q=insurance+services+office+form+CG+00+01+04+13&rlz=1C1GCEB_enUS900US900&oq=insurance+services+office+form+CG+00+01+04+13&aqs=chrome..69i57j0i546l3.16062j0j4&sourceid=chrome&ie=UTF-8.

22. *Corporate history*, Lloyd's, https://www.lloyds.com/about-lloyds/history/corporate-history (last visited July 11, 2022).

23. Daniel Cawrey, *$5 Billion Insurance Company Offers Bitcoin Coverage to Businesses*, CoinDesk (June 2, 2014, 4:20 PM EDT), https://www.coindesk.com/markets/2014/06/02/5-billion-insurance-company-offers-bitcoin-coverage-to-businesses/.

24. *Internal Control Questionnaire for Bitcoin Coverage*, Great American Insurance Group, https://www.greatamericaninsurance group.com/docs/default-source/fidelity-crime/bitcoin-coverage-questionnaire.pdf?sfvrsn=dc1e70b1_2.

25. Insurance Services Office form CR 2545.

26. Mellisa Tolentino, *Five ways to secure and insure your Bitcoin startup*, SiliconANGLE (Jan. 18, 2016, 15:47 EDT), https://siliconangle.com/2016/01/18/five-ways-to-secure-and-insure-your-bitcoin-startup/.

27. *Id.*; *see also* https://www.reddit.com/r/Bitcoin/comments/1usgil/elliptic_vault_insured_storage_for_bitcoins/ (last visited July 11, 2022).

28. Gautham, *Japan's Mitsui Sumitomo Introduces New Bitcoin Insurance*, NEWSBTC, https://www.newsbtc.com/news/mitsui-sumitomo-bitcoin-insurance/ (last visited July 11, 2022).

29. *Get covered against smart contract failure & exchange hacks*, Nexus Mutual, https://nexusmutual.io/ (last visited July 11, 2022).

30. Ben Bartenstein, *Binance Builds Up $1 Billion Insurance Fund Amid Crypto Hacks*, Bloomberg (Jan. 31, 2022, 5:58 AM EST), https://www.bloomberg.com/news/articles/2022-01-31/binance-builds-up-1-billion-insurance-fund-amid-crypto-hacks.

31. *How is Coinbase insured?*, Coinbase, https://help.coinbase.com/en-in/coinbase/other-topics/legal-policies/how-is-coinbase-insured (last visited July 11, 2022).

32. Marcos Cabello, *Can You Insure Bitcoin? Here's What You Need to Know*, CNET (Feb. 23, 2022, 5:00 AM PT), https://www.cnet.com/personal-finance/crypto/can-you-insure-bitcoin/.

33. *How is Coinbase insured?*, Coinbase, https://help.coinbase.com/en-in/coinbase/other-topics/legal-policies/how-is-coinbase-insured (last visited July 11, 2022).

34. Marcos Cabello, *Can You Insure Bitcoin? Here's What You Need to Know*, CNET (Feb. 23, 2022, 5:00 AM PT), https://www.cnet.com/personal-finance/crypto/can-you-insure-bitcoin/; *We're extending our crime insurance policy*, Bitstamp (July 8, 2021), https://blog.bitstamp.net/post/were-extending-our-crime-insurance-policy/.

35. Alastair Walker, *Bitstamp Increases Crypto Insurance Limits With Paragon*, Insurance Edge (July 10, 2021), https://insurance-edge.net/2021/07/10/bitstamp-increases-crypto-insurance-limits-with-paragon/.

36. Dean Fankhauser, *BlockFi Review Pros and Cons. Is BlockFi safe?*, Bitcompare (June 1, 2022), https://bitcompare.net/reviews/blockfi.

37. Brian O'Connell, *Guide to Insurance on Cryptocurrency*, Insurance Thought Leadership (Mar. 3, 2021), https://www.insurancethoughtleadership.com/emerging-technologies/guide-insurance-cryptocurrency.

38. Ben Bartenstein, *Binance Builds Up $1 Billion Insurance Fund Amid Crypto Hacks*, Bloomberg (Jan. 31, 2022, 5:58 AM EST), https://www.bloomberg.com/news/articles/2022-01-31/binance-builds-up-1-billion-insurance-fund-amid-crypto-hacks.

39. *Breach Launches Crypto Shield, the Industry's First Regulated Insurance Product for Retail Crypto Investors*, GlobeNewswire (Feb. 15, 2022, 08:15 ET), https://www.globenewswire.com/news-release/2022/02/15/2385260/0/en/Breach-Launches-Crypto-Shield-the-Industry-s-First-Regulated-Insurance-Product-for-Retail-Crypto-Investors.html.

40. *A unique approach to securing your crypto business*, Coincover, https://www.coincover.com/products/personal-crypto-protection (last visited July 11, 2022).

41. *Digital Asset Insurance*, BitGo, https://www.bitgo.com/resources/digital-asset-insurance/ (last visited July 11, 2022).

42. *Id.*

43. Suzanne Barlyn, *Insurers Begin to Offer Cryptocurrency Theft Cover, Tackling Risks of Growing Sector*, Insurance Journal (Feb. 1, 2018), https://www.insurancejournal.com/news/international/2018/02/01/479202.htm#:~:text=Annual%20premiums%20for%20%2410%20million,loss%20history%20and%20other%20factors.

44. *Blockchain and Digital Asset Risk Transfer Insurance Solutions*, Marsh, https://www.marsh.com/us/services/financial-professional-liability/products/digital-risk-management.html (last visited July 11, 2022).

45. Ryan Smith, *Lockton launches emerging asset protection team*, Insurance Business (Oct. 14, 2021), https://www.insurancebusiness

mag.com/us/news/breaking-news/lockton-launches-emerging-asset-protection-team-313165.aspx.

46. *Financial Institutions Practice Cryptocurrencies, Other Digital Assets & Blockchain*, Aon, https://www.aon.com/industry-expertise/financial-institution-risk-management/digital-assets-and-blockchain.jsp (last visited July 11, 2022).

47. Miranda Wood, *Marsh, Arch insures $150m of digital assets for Ledger Vault*, Ledger Insights (Nov. 14, 2019), https://www.ledgerinsights.com/ledger-insures-digital-assets-150m-marsh-arch/.

48. *Blockchain and Digital Asset Risk Transfer Insurance Solutions*, Marsh, https://www.marsh.com/us/services/financial-professional-liability/products/digital-risk-management.html (last visited July 11, 2022).

49. Sports NFT Marketplace, https://www.airnfts.com/nft/sports-nft-marketplace (last visited July 11, 2022); NBA Top Shot, https://nbatopshot.com (last visited July 11, 2022).

50. Todd Spangler, *DC to Sell 200,000 Batman Cowl NFT Digital Collectibles, Eyeing $60 Million Haul*, Yahoo!Finance (Mar. 29, 2022), https://finance.yahoo.com/news/dc-sell-200-000-batman-210013750.html.

51. OpenSea, https://opensea.io/category/music (last visited July 11, 2022); Rania Aniftos, *Billboard Explains: NFTs & The Music Industry*, Billboard (Mar. 23, 2022), https://www.billboard.com/music/music-news/billboard-explains-nfts-music-industry-1235047955/.

52. Cathy Hackl, *Stella Artois Gallops into the Metaverse With Horse Racing NFTs*, Forbes (June 18, 2021, 02:25 PM EDT), https://www.forbes.com/sites/cathyhackl/2021/06/18/stella-artois-gallops-into-the-metaverse-with-horse-racing-nfts/?sh=26cfdb357b8b.

53. Taylor Locke, *Jack Dorsey sells his first tweet ever as an NFT for over $2.9 million*, CNBC.com (Mar. 22, 2021, 3:07 PM EDT), https://www.cnbc.com/2021/03/22/jack-dorsey-sells-his-first-tweet-ever-as-an-nft-for-over-2point9-million.html.

54. Harrison Jacobs, *The Counterfeit NFT Problem Is Only Getting Worse; So Artists Are Joining Together to Fight Back*, The Verge (Feb. 8, 2022, 8:00 AM EST), https://www.theverge.com/22905295/counterfeit-nft-artist-ripoffs-opensea-deviantart.

55. There is also a potential for other ruses. In one widely reported event, an NFT identified as "The Big Daddy Ape Club" was created to

take advantage of a popular NFT named "Bored Ape Yacht Club." Tokens for the fabricated entity were never minted and investors were scammed out of $1.13 million. Lawrence Carrel, *As NFT Scams Grow in Number, NFT Insurance Hits the Market*, FORBES (Jan. 28, 2022, 09:30 PM EST), https://www.forbes.com/sites/lcarrel/2022/01/28/as-nft-scams-grow-in-number-nft-insurance-hits-the-market/?sh=4a7def5c7bcb.

56. Michael Giusti, *NFTs Are Hot; Where Is the Insurance?*, INSURANCE THOUGHT LEADERSHIP (Feb. 8, 2022), https://www.insurancethoughtleadership.com/emerging-technologies/nfts-are-hot-where-insurance.

57. *YAS Launches the World's First Microinsurance "NFTY" Covering NFT*, CISION PR NEWSWIRE (Apr. 15, 2021, 06:37 ET), https://www.prnewswire.com/news-releases/yas-launches-the-worlds-first-microinsurance-nfty-covering-nft-301269677.html; *YAS' NFTY extends its coverage to fine arts showcased at Art Central Hong Kong*, NEWS HUB ASIA (May 22, 2021), https://www.newshubasia.com/living/57239/; YAS Micro Insurance, https://yas.io/en/ (last visited July 11, 2022).

58. *The NFT for Jack Dorsey's first tweet ever is worth only $6800 now*, BUSINESS INSIDER INDIA (Apr. 18, 2022, 11:14 IST), https://www.businessinsider.in/cryptocurrency/news/the-nft-for-jack-dorseys-first-tweet-ever-is-worth-only-6800-now/articleshow/90847052.cms.